

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS Y COMPUTACIÓN

"DISEÑO DE UN MODELO DE SEGURIDAD DE INFORMACION EN REDES LAN"

AUTOR:

ANA CRISTINA TUFIÑO GALÁN

DIRECTOR:

Mtr. DAMIÁN ANÍBAL NICOLALDE RODRÍGUEZ

QUITO, JULIO 2018.

DEDICATORIA

"Siembra un acto y cosecharas un hábito.

Siembra un hábito y cosecharás un carácter.

Siembra un carácter y cosecharas un destino"

Charles Reade.

El presente trabajo de disertación se lo dedico en primer lugar a Dios, quien siempre ha sido mi luz, protector y guía para tomar el camino correcto y avanzar pese a las adversidades en el camino. A mis padres: Jorge Marcelo y Nehi, que son un ejemplo a seguir, brindándome todo su amor, comprensión y apoyo incondicional para que siga siempre mis sueños. A ellos que nunca dejaron de creer en mí y por enseñarme que con esfuerzo y sacrificio se consigue el éxito.

A mis hermanas Gabriela Fernanda, que es mi ejemplo a seguir, por su constancia y perseverancia, a Andrea Alejandra, que vea en mi un referente para que culmine su carrera, siempre persiga sus sueños y no se deje vencer por las adversidades, a mi primo Fausto Harry, para que siga el ejemplo de mis hermanas y el mío, para que culmine sus estudios y se realice profesionalmente.

A mi mejor amigo Juan Carlos que siempre estuvo presente, alentándome y apoyándome incondicionalmente, a mi amiga Pamela Belén por brindarme calidez, risas, consejos y estar presente cuando más lo necesité, finalmente y no menos importante a todos mis amigos, por hacer de esta carrera momentos increíbles e inolvidables.

AGRADECIMIENTO

La disertación de mi tesis, la dedico con todo mi corazón y amor a Dios, a quien agradezco por haberme permitido culminar con éxitos y bendiciones mis objetivos. Gracias por ser mi apoyo espiritual incondicional porque ha sabido guiar mi camino para culminar la etapa más importante de mi formación profesional.

A mis padres y hermanos, porque me brindaron su amor, su apoyo moral y el más importante el apoyo económico, para estudiar en tan prestigiosa Universidad, haciendo posible que mi sueño se haga realidad.

De manera especial a mi Director de tesis Msc. Damián Nicolalde, por haberme guiado en la presente titulación y brindarme el apoyo desinteresado para desarrollarme como una verdadera Ingeniera de Sistemas.

Gracias a mi profesora preferida Suyana Arcos, quien con sus sabios consejos y su alegría contagiosa me ayudo a llegar a uno de mis anhelados sueños. Al Ing. Charles Escobar, que ha compartido sus conocimientos para formarme como profesional gracias a sus consejos y recomendaciones.

Mis más sinceros agradecimientos a mi querida Universidad la Pontificia Universidad Católica, del Ecuador, a todos los que forman parte de la Facultad de Ingeniería de Sistemas, a mis queridos profesores, amigos y compañeros gracias y que Dios los bendiga, por su paciencia, apoyo incondicional y amistad

RESUMEN

El presente trabajo de disertación tiene como finalidad Diseñar un Modelo de Seguridad de Información para Redes LAN, basadas en ataques y vulnerabilidades que pueda tener una red al momento de intercambiar información entre sí.

Se desarrolló a través de un método científico los cuales aplican conceptos puntuales sobre redes, sistemas operativos, hacking ético incluida sus aplicaciones, análisis de tráfico, escaneo de puertos, entre otros.

Las herramientas que se han utilizado son: Oracle VM Virtual Box, Máquina Virtual Kali Linux, Máquina Virtual Metaexploitable 2, Máquina Virtual Windows 7, Máquina Virtual Windows XP, Wireshark, Ettercap, Yersinia, John de Ripper, Zenmap Linux, Nmap, Consola de comandos de cada uno de los sistemas operativos, Simuladores de red GNS3 y Cisco Packet Tracer, Firewall Untangle siendo utilizados con el objetivo de simular posibles ataques y mitigaciones hacia la red.

Como resultado de todo este análisis se obtiene las mejores medidas preventivas para ser una posible guía en el diseño y construcción de redes para cualquier tipo de empresa basadas en la familia de la ISO 27000[1]. Por otro lado, el uso de la máquina virtual Kali Linux permitió realizar este análisis gracias a sus herramientas incluidas ya que se ha creado con el objetivo de auditar y asegurar cualquier red, además Wireshark fue la aplicación más utilizada para analizar el trafico antes y después de cada uno de los ataques desarrollados.

[1] **ISO 27000:** Define estándares para lograr un sistema de gestión de seguridad de la información, garantizando que la información se trasmita de manera segura, confiable e integra.

Este trabajo de disertación puede ser utilizado como un manual para realizar simulaciones de los ataques desarrollados más adelante; se detalla y explica con ejemplos sencillos cómo funcionan los ataques en la red. Considerar que no se puede responsabilizar por el mal uso de la misma.

INDICE

1. CAPITULO I 23

1.1 INTRODUCCION 23

1.2 ANTECENDENTES 24

1.3 OBJETIVOS 25

1.3.1 General 25

1.3.2 Específicos 25

2. CAPÍTULO II: FUNDAMENTOS TEORICOS 26

2.1 SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN 26

2.2 IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA 27

2.3 TIPOS DE SEGURIDAD INFORMÁTICA 27

2.3.1 Seguridad Física 27

2.3.1.1 Entorno Físico 28

2.3.1.2 Entorno Humano 28

2.3.2 Seguridad Lógica 28

2.4 VULNERABILIDAD 28

2.5 AGUJEROS DE SEGURIDAD 29

2.6 ATAQUES 29

2.6.1 Intencionados 29

2.6.2 No Intencionados 29

2.7 FASES DE UN ATAQUE 30

2.7.1 Reconocimiento 30

2.7.2 Escaneo 31

2.7.3 Obtener Acceso 31

2.7.4 Mantener Acceso 31
2.7.5 Borrar Huellas 31
2.8 TIPOS DE ATACANTES 32
2.8.1 Hacker 32
2.8.2 Cracker 32
2.8.3 White Hats 32
2.8.4 Grey Hats 33
2.8.5 Black Hats 33
2.8.6 Newbie 33
2.8.7 Scriptkiddie 33
2.8.8 Lammers 34
2.8.9 Gurú 34
2.9 HACKING ÉTICO 34
2.10 AMENAZAS 35
2.11 RIESGOS 35
2.12 IMPACTO 36
2.13 PROTOCOLO 36
2.14 ESTÁNDARES 37
2.15 CAPA O NIVEL 37
2.16 ARQUITECTURA DE RED 37
2.16.1 Tolerancia a Fallos 37
2.16.2 Escalabilidad 37
2.16.3 Calidad de Servicio 38
2.16.4 Seguridad 38
2.17 SERVICIOS 38

2.17.1 Orientado a la Conexión 38
2.17.2 No Orientado a la Conexión 38
2.18 UNIDADES DE INFORMACIÓN 39
2.18.1 Unidad de Datos de Protocolo (PDU) 39
2.18.2 Unidad de Datos de Servicio (SDU) 39
2.18.3 Información de Control de Protocolo (PCI) 39
2.19 DIRECCIÓN IP 40
2.19.1 Clase A 40
2.19.2 Clase B 40
2.19.3 Clase C 41
2.19.4 Clase D 41
2.19.5 Clase E 41
2.20 DIRECCIÓN MAC 42
2.21 MODO PROMISCUO DE UNA TARJETA DE RED 42
2.22 SUBRED 42
2.23 INGENIERÍA SOCIAL 42
1.23.1 Tipos de Ingeniería Social 42
1.23.1.1 Ataque Telefónico 43
1.23.1.2 Ataque vía Internet 43
1.23.1.3 Ataque Dumpster Diving 43
1.23.1.4 Ataque Vía SMS 43
1.23.1.5 Ataque Cara a Cara 44
2.24 FIREWALL 44
3. CAPÍTULO II: CARACTERIZACION DE LA SEGURIDAD DE LA INFORMACION 46
3.1 PRINCIPIOS FUNDAMENTALES DE LA SEGURIDAD DE LA INFORMACIÓN A LA RED 46

3.1.1 Confidencialidad 47
3.1.2 Integridad 47
3.1.3 Disponibilidad 48
3.2 PRESENTACIÓN DEL MODELO DE INTERCONEXIÓN DE SISTEMAS ABIERTOS (OSI) ... 49
3.3 FUNCIONAMIENTO DE LOS 7 NIVELES DEL MODELO DE INTERCONEXIÓN DE SISTEMAS ABIERTOS (OSI) 51
3.3.1 Capa Física 52
3.3.1.1 Entorno Físico 52
3.3.1.1.1 Software como Servicio (SaaS) 53
3.3.1.1.2 Plataforma como Servicio (PaaS) 54
3.3.1.1.3 Infraestructura como Servicio (IaaS) 54
3.3.1.2 Autenticación y Control de Acceso 55
3.3.1.3 Medios Empleados para Transmitir Información 55
3.3.1.3.1 Medios Guiados 55
a) Medios Magnéticos 55
b) Par Trenzado 56
c) Cable Coaxial 56
d) Fibra Óptica 57
3.3.1.3.2 Medios No Guiados 57
a) Ondas de Radio 57
b) Microondas 58
c) Infrarrojo 58
3.3.1.4 Medios Físicos de Almacenamiento y Procesamiento de Información 58
3.3.1.4.1 Nube Pública 59
3.3.1.4.2 Nube Privada 59

3.3.1.4.3 Nube Híbrida 60
3.3.2 Capa Enlace de Datos 60
2.3.2.1 Protocolos 61
a) Control de Enlace de Alto Nivel (HDLC) 61
b) Punto a Punto (PPP) 61
c) Ethernet y CSMA/CD 62
d) Redes Inalámbricas LAN 63
e) Árbol de Extensión (STP) 65
f) Virtual LAN (VLAN) 65
g) Resolución de Direcciones (ARP) 65
3.3.3 Capa de Red 66
3.3.4.1 Protocolos 67
a) Internet Versión 4 (IPv4) 67
b) Internet Versión 6 (IPv6) 68
c) Seguridad de Internet (IPSec) 69
d) Mensajes de Control de Internet (ICMP) 70
3.3.4 Capa de Transporte 71
3.3.4.1 Protocolos 71
a) Datagrama de Usuario (UDP) 71
b) Control de Transmisión (TCP) 72
c) Capa de Puertos Seguros (SSL) 73
d) Capa de Seguridad en la Capa de Transporte (TLS) 73
3.3.5 Capa de Sesión 74
3.3.5.1 Protocolos 74
a) NetBIOS 74

b) Llamada de Procedimiento Remoto (RPC) 75
3.3.6 Capa de Presentación 75
3.3.7.1 Protocolos 76
a) Notación Sintáctica Abstracta 1 (ANSI.1) 76
b) Representación de Datos Externos (XDR) Sintáctica Abstracta 1 (ANSI.1) 76
c) Extensiones de Multipropósito de Correo Internet (MIME) 76
3.3.7 Capa de Aplicación 77
3.3.7.2 Protocolos 77
a) Sistema de Nombres de Dominio (DNS) 77
b) Red de Telecomunicaciones (TELNET) 78
c) Trasferencia de Archivos (FTP) 78
d) Secure Shell (SSH) 79
e) Protocolo Simple de Trasferencia de Correo Electrónico (SMTP. 80
f) Protocolos de Oficina de Correos (POP) 80
g) Protocolo Simple de Administración de Red (SNMP) 80
h) Protocolo de Trasferencia de Hipertexto (HTTP) 81
i) Protocolo de Configuración Dinámica de Host (DHCP) 81
j) Protocolo de Acceso a Mensajes de Internet (IMAP) 82
3.4 Ataques Comunes en los 7 Niveles en el Modelo de Interconexión de Sistemas Abiertos (OSI) 83
3.4.1 Capa Física 83
3.4.2 Capa Enlace de Datos 84
3.4.2.1 ARP Spoofing 84
3.4.2.2 ARP Poisoning 85

3.4.2.3 ARP Hijacking o Proxying 85
3.4.2.4 Hombre en el Medio (MitM) 85
3.4.2.5 Denegación de Servicio ARP 86
3.4.2.6 ARP Sniffing 86
3.4.2.7 MAC Flooding 87
3.4.2.8 VLAN Hopping 87
3.4.2.9 Doble Etiquetado 88
3.4.2.10 Denegación de Servicio basado en STP 88
3.4.2.11 Inundaciones DHCP 88
3.4.3 Capa Enlace de Red 89
3.4.3.1 Recopilación de Información (Networking Footprinting) 89
3.4.3.2 IP Spoofing 89
3.4.3.3 Nuke 90
3.4.3.4 Ping de la Muerte 90
3.4.3.5 Land 90
3.4.3.6 Supernuke o Winnuke 90
3.4.3.7 Teardrop 91
3.4.3.8 ICMP Flood 91
3.4.3.9 Smurf o Pitufo 91
3.4.4 Capa Enlace de Transporte 92
3.4.4.1 Fingerprinting 92
3.4.4.2 TCP Connect Scanning 92
3.4.4.3 TCP SYN Scanning 92
3.4.4.4 TCP FIN Scanning 93
3.4.4.5 TCP NULL Scanning 93

3.4.4.6 TCP ACK Scanning 93
3.4.4.7 TCP Fragmention Scanning 93
3.4.4.8 TCP Windows Scanning 94
3.4.4.9 Inundación UDP 94
3.4.4.10 SYN Flood 94
3.4.4.11 Connection Flood 95
3.4.5 Capa Enlace de Sesión 95
3.4.5.1 NetBIOS 95
3.4.5.2 Llamada de Procedimiento Remoto 95
3.4.6 Capa Enlace de Presentación 96
3.4.6.1 Fuerza Bruta 96
3.4.6.2 Diccionario 96
3.4.6.3 Textos Cifrados 96
3.4.6.4 Textos Claros Conocidos 96
3.4.7 Capa Enlace de Aplicación 97
3.4.7.1 Sniffing 97
3.4.7.2 Denegaciones de Servicios (DoS) 97
3.4.7.3 Denegaciones Distribuidas de Servicios (DDoS) 97
3.4.7.4 SMPT Flood 98
3.4.7.5 DNS Spoofing 98
3.4.7.6 Telnet 98
3.4.7.7 Ataque al protocolo SSH 98
3.4.7.8 Ataque por Inyección 99
3.4.7.9 Ataque HTTP y HTTPS 99

3.5 APLICACIÓN DE LOS ATAQUES MÁS COMUNES EN LOS 7 NIVELES EN EL MODELO DE INTERCONEXIÓN DE SISTEMAS ABIERTOS (OSI) 99
3.5.1 ARP Poisoning – Hombre en el Medio 99
3.5.1.1 Medios de Prevención 101
3.5.1.2 Resultados 104
3.5.2 CDP –Denegación de Servicio 105
3.5.2.1 Medios de Prevención 107
3.5.2.2 Resultados 109
3.5.3 DHCP – Hombre en el Medio 110
3.5.3.1 Medios de Prevención 111
3.5.3.2 Resultados 113
3.5.4 Syn Flood 114
3.5.4.1 Medios de Prevención 115
3.5.4.2 Resultados 117
3.5.5 Sesiones, contraseñas y aplicaciones 117
3.5.5.1 Medios de Prevención 118
3.5.4.3 Resultados 120
4. CAPÍTULO IV: DESCRIPCIÓN DEL MODELO OSI Y TCP 121
4.1 DEFINICIÓN DE LAS CAPAS DE LOS MODELOS DE REFERENCIA 121
4.1.1 Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI) 121
4.1.2 Modelo de Referencia de Control y Transmisión / Protocolo de Internet (TCP/IP) 122
4.2 DEFINICIÓN DE LOS NIVELES DE LOS MODELOS DE REFERENCIA 123
4.3 DEFINICIÓN DE LOS PROTOCOLOS DE LOS MODELOS DE REFERENCIA 124
4.4 PRINCIPALES VENTAJAS DEL MODELO OSI Y TCP/IP 126

4.5 PRINCIPALES DESVENTAJAS DEL MODELO OSI Y TCP/IP 127

5. CAPITULO V: MODELO DE SEGUIRDAD APLICADA AL MODELO OSI 128

5.1 SEGURIDADES EN LOS NIVELES DEL MODELO DE REFERENCIA DE INTERCONEXIÓN DE SISTEMAS ABIERTOS 128

5.1.1 Capa Física 128

5.1.2 Capa de Enlace de Datos 131

5.1.3 Capa de Red 134

5.1.4 Capa de Transporte 136

5.1.5 Capa de Sesión 136

5.1.6 Capa de Presentación 137

5.1.7 Capa de Aplicación 138

6. CONCLUSIONES Y RECOMENDACIONES 140

6.1 CONCLUSIONES 140

6.2 RECOMENDACIONES 142

7. BIBLIOGRAFÍA 146

8. ANEXOS 151

8.1 Desarrollo del Ataque y Mitigación de ARP Poisoning – MitM 151

8.2 Desarrollo del Ataque y Mitigación de CDP –Denegación de Servicio 161

8.3 Desarrollo del Ataque y Mitigación de DHCP – Hombre en el Medio 169

8.4 Desarrollo del Ataque y Mitigación de Syn Flood 175

8.5 Desarrollo del Ataque y Mitigación de Sesiones, contraseñas y aplicaciones 184

ÍNDICE DE ILUSTRACIONES

Ilustración 2-1: Fases de un Ataque Informático

Ilustración 2-2: Niveles de riesgo que se puedan materializar

Ilustración 2-3: Cabeceras asociadas a cada nivel OSI

Ilustración 2-4: Numero de redes y su tamaño para cada dirección IP

Ilustración 2-5: Ubicación de un Firewall en una red LAN

Ilustración 3-1: Seguridad de la información según la norma ISO/IEC 17799

Ilustración 3-2: Niveles del Modelo OSI

Ilustración 3-3: División principal de SaaS, PaaS, IaaS

Ilustración 3-4: Migración de IPv4 a Ipv6

Ilustración 3-5: Migración de IPv4 a Ipv6 en el Ecuador

Ilustración 3-6: Visualización del ataque MitM y ARP Spoofing en Wireshark

Ilustración 3-7: Visualización de la Mitigación MitM y ARP Spoofing a través de rutas estáticas.

Ilustración 3-8: Diseño de Red CDP

Ilustración 3-9: Ataque CDP y Denegación de Servicios

Ilustración 3-10: Log Ataque con Yersinia

Ilustración 3-11: Visualización de la mitigación del Ataque CDP – Denegación de Servicios

Ilustración 3-12: Diseño de Red DHCP – Denegación de Servicio

Ilustración 3-13: Ataque con Yersinia DHCP – Denegación de Servicio”

Ilustración 3-14: Visualización de la Mitigación del Ataque DHCP – Denegación de Servicio

Ilustración 3-15: Visualización del Ataque Syn Flood en Wireshark

Ilustración 3-16: Visualización de la Mitigación del Ataque Syn Flood

Ilustración 3-17: Ataque Robo de Sesiones, Contraseñas y Aplicaciones

Ilustración 3-18: Ataque Robo de Sesiones, Contraseñas y Aplicaciones

Ilustración 4-1: Modelo OSI y Modelo TCP/IP

Ilustración 4-2: Proceso del Modelo TCP/IP

Ilustración 8-1: Dirección IP y MAC del atacante ARP Poisoning – Hombre en el Medio

Ilustración 8-2: Herramienta Grafica Ettercap

Ilustración 8-3: Despliegue Gráfico de Ettercap

Ilustración 8-4: Búsqueda de interfaz de red a trabajar

Ilustración 8-5: Selección de interfaz de red

Ilustración 8-6: Información actual de la Máquina Atacante

Ilustración 8-7: Escaneo de Equipos Disponibles en la Red

Ilustración 8-8: Búsqueda de equipos victimas en la red

Ilustración 8-9: Registro de Posibles Máquinas Victimas

Ilustración 8-10: Dirección IP de Metasploitable

Ilustración 8-11: Dirección IP de Windows

Ilustración 8-12: Selección maquinas victimas

Ilustración 8-13: Selección ataque ARP Poisoning mediante MitM

Ilustración 8-14: Sniff remote conections

Ilustración 8-15: Asociación de direcciones MAC e IP

Ilustración 8-16: Selección de Plugin remote_browser

Ilustración 8-17: Log de Ettercap

Ilustración 8-18: Ataque direcciones MAC

Ilustración 8-19: Asignación de Direcciones Estáticas

Ilustración 8-20: Asignación de Rutas Estáticas

Ilustración 8-21: Mitigación después del Ataque

Ilustración 8-22: Diseño de Red para Ataque de red CDP – Denegación de Servicios

Ilustración 8-23: Llamar Modo Gráfico de Yersinia

Ilustración 8-24: Interfaz de la herramienta Yersinia de Kali Linux

Ilustración 8-25: Cargar tipo de ataque CDP

Ilustración 8-26: Cargar ataque de Inundación de tabla CDP

Ilustración 8-27: Incremento notable de paquetes CDP

Ilustración 8-28: Log Yersinia

Ilustración 8-29: Filtrado de dirección IP en Wireshark

Ilustración 8-30: Captura de paquetes CDP en Wireshark

Ilustración 8-31: Log de Yersinia

Ilustración 8-32: Log de Yersinia

Ilustración 8-33: Configuración Router 1

Ilustración 8-34: Configuración enlace Router 1 a Router 2

Ilustración 8-35: Configuración Router 2

Ilustración 8-36: Configuración Router 2

Ilustración 8-37: Captura de Mitigación del Ataque CDP- Denegación de Servicio

Ilustración 8-38: Diseño de red para realizar ataque DHCP - Denegación de Servicio

Ilustración 8-39: Desplegar el modo grafico de la herramienta Yersinia

Ilustración 8-40: Modo grafico de la herramienta Yersinia

Ilustración 8-41: DHCP en Yersinia

Ilustración 8-42: Cargar Ataque en DHCP Yersinia

Ilustración 8-43: Seleccionar tipo de Ataque DHCP

Ilustración 8-44: Inundación de direcciones MAC

Ilustración 8-45: Crecimiento de paquetes DHCP

Ilustración 8-46: Maquinas a configurar su IP

Ilustración 8-47: Configuración IP

Ilustración 8-48: Establecer Dirección IP mediante DHCP

Ilustración 8-49: Configuración switch en modo DHCP Snooping

Ilustración 8-50: Visualización de la Mitigación del DHCP-Denegación de Servicios

Ilustración 8-51: Escaneo de puerto Zenmap

Ilustración 8-52: Terminal Metasploit de Kali Linux

Ilustración 8-53: Buscar Tipo de Vulnerabilidades Telnet

Ilustración 8-54: Buscar Tipo de Vulnerabilidades Telnet

Ilustración 8-55: Dirección Victima Vacío

Ilustración 8-56: Dirección Victima Establecida

Ilustración 8-57: Inicio del Ataque Syn Flood – Denegación de Servicios

Ilustración 8-58: Inicio del Ataque Syn Flood – Denegación de Servicios

Ilustración 8-59: Descarga de Untangle

Ilustración 8-60: Finalización de la Instalación de Untangle

Ilustración 8-61: Creación de Cuenta Untangle

Ilustración 8-62: Verificación de Tarjeta de Red

Ilustración 8-63: Bloqueo del Puerto 80

Ilustración 8-64: Bloqueo del Puerto 80

Ilustración 8-65: Verificación del Puerto 80 con Zenmap

Ilustración 8-66: Configuración para permitir el tráfico de una determinada dirección IP

Ilustración 8-67: Configuración para permitir el tráfico de una determinada dirección IP

Ilustración 8-68: Levantamiento de servicios PostgreSQL

Ilustración 8-69: Levantamiento de servicios Apache

Ilustración 8-70: Verificación Actual de Apache

Ilustración 8-71: Descargar John The Ripper

Ilustración 8-72: Creación de Carpeta para guardar aplicativo John the Ripper

Ilustración 8-73: Guardar aplicativo John the Ripper

Ilustración 8-74: Verificación de Aplicativo John the Ripper en Apache

Ilustración 8-75: Ingreso a la dirección 192.168.100.166

Ilustración 8-76: Descomprimir archivos Jon de Ripper

Ilustración 8-77: Abrir consola de Metasploit

Ilustración 8-78: Búsqueda de Vulnerabilidades al puerto 21

Ilustración 8-79: Selección de vulnerabilidad al puerto 21

Ilustración 8-80: Configuración de dirección victima

Ilustración 8-81: Control de Sesión Abierta

Ilustración 8-82: Control total del equipo victima

Ilustración 8-83: Comando para averiguar contraseñas

Ilustración 8-84: Comando para averiguar usuarios

Ilustración 8-85: Abrir directorio de la aplicación John de Ripper

Ilustración 8-86: Descomprimir John the Ripper

Ilustración 8-87: Visualización de recursos - John the Ripper

Ilustración 8-88: Uso del comando make generic para ordenar usuarios y contraseñas

Ilustración 8-89: Llamar archivo donde se encuentra la información requerida

Ilustración 8-90: Archivo de claves y contraseñas

Ilustración 8-91: Configuración de reglas para reenvío de puertos

Ilustración 8-92: Reenvío de puertos a una dirección segura

ÍNDICE DE TABLAS

Tabla 3-1: Variantes del Estándar 8020.11

Tabla 3-2: Direcciones IP y MAC antes del Ataque MitM y ARP Spoofing

Tabla 3-3: Direcciones IP y MAC después del Ataque MitM y ARP Spoofing

Tabla 3-4: Direcciones IP y MAC después de la mitigación del Ataque MitM y ARP Spoofing

Tabla 4-1: Modelo OSI vs Modelo TCP/IP

Tabla 4-2: Protocolos del Modelo OSI vs Modelo TCP/IP

Tabla 4-3: Protocolos del Modelo OSI vs Modelo TCP/IP

Tabla 4-4: Principales Ventajas del Modelo OSI y TCP/IP

1. CAPITULO I

1.1 INTRODUCCION

En la actualidad las computadoras se encuentran presentes en todas las actividades cotidianas del ser humano (Arnedo Moreno, 2013), para esto el intercambio de comunicación también es un aspecto relevante, la importancia de tener una excelente red permitirá que su desempeño sea lo más óptimo posible.

Según datos del INEC, hasta el año 2016 todas las empresas, organizaciones incluso hogares tienen el 36% de acceso a internet (INEC, 2016); tomando en cuenta que desde su creación como medio de interconexión global se ha tenido problemas de inseguridad que se ha ido incrementando de una manera alarmante.

A medida que las instituciones, empresas y otras organizaciones ampliaban su número de trabajadores, esta también se incrementaba en número de computadoras, incluyendo la configuración de redes que permitan transmitir todo tipo de información y recursos que se puedan compartir dentro o fuera de la organización u empresa, ahorrando tiempo y dinero.

Cuando se habla de intercambiar información, se aplica un término muy importante y especifico, que es la seguridad de información, por este motivo a lo largo del tiempo se consideró herramientas y técnicas que se usan para fortalecer los tres principios fundamentales de un sistema informático, todo depende del sistema, su función y todos los factores de riesgo que puedan amenazarlo.

La seguridad de información puede estudiarse como un proceso que se puede implementarse en 7 niveles, estudiados desde abajo hacia arriba: Nivel 1: Físico, Nivel 2: Enlace, Nivel 3: Red, Nivel 4: Transporte, Nivel 5: Sesión, Nivel 6: Presentación y Nivel 7: Aplicación.

El caso particular de TCP/IP es un derivado de 4 capas que se referencia en el modelo OSI, que simplifica la arquitectura en 4 capas (Stallings, 2004) sobre las cuales, conceptualmente se pueden identificar los 7 niveles, e identificar las vulnerabilidades y seguridades a aplicarse por capas.

1.2 ANTECENDENTES

El 12 enero del año 2010 nace "Operación Aurora". ¿De qué se trata esto? Es el nombre que recibe un ataque masivo contra varias corporaciones internacionales entre las cuales se menciona a Google, Adobe Systems, Yahoo, Rackspace incluidas 30 más que hasta el día de hoy no se han dado a conocer. Básicamente, el ataque fue originado en China con el objetivo de exhibir las vulnerabilidades del navegador Internet Explorer en sus versiones 6,7 y 8, la cual contenía una gran falla, el control remoto total de una maquina victima hacia personas que tenían privilegios de acceso especiales.

El ataque se basó en la propagación de exploits[2] mediante correo electrónicos los cuales supuestamente eran de confianza, entonces a través de un link los invitaban a acceder a una página de Internet y después surgió lo que hoy en día se llama "Ciberataques" siendo uno de los más sofisticados hasta ahora registrados.

Las consecuencias de este ataque fueron devastadoras, debido a que los daños oscilaron entre 6,3 millones de dólares y tomando en cuenta que muchas compañías multinacionales fueron afectadas directamente, actualmente se cuestiona el hecho de que aun el 20% de la población utilice esta herramienta de navegación.

[2] **Exploits:** Agujeros de Seguridad

Ante este antecedente deja en evidencia que ninguna empresa incluso multinacionales cuentan con una seguridad del 100% ya que no se encuentran exentos de vulnerabilidades, ataques y riesgos. Sin embargo, diseñar un modelo de seguridad permitirá que la empresa tome medidas de prevención que deben ser consideramos como una estrategia global.

1.3 OBJETIVOS

1.3.1 General

1.3.1.1 Diseñar un modelo de seguridad para la Interconexión de Sistemas Abiertos (OSI), que permita establecer mecanismos de protección en las 7 capas.

1.3.2 Específicos

1.3.2.1 Determinar los principios fundamentales de la seguridad de información aplicada a la red.

1.3.2.2 Analizar el funcionamiento y las vulnerabilidades de los 7 niveles del modelo OSI.

1.3.2.3 Identificar los tipos de ataques y medios de prevención en cada nivel que se presentan en el modelo OSI.

1.3.2.4 Estudiar comparativamente las herramientas que permitan proteger las comunicaciones a través de las 7 capas del modelo OSI

1.3.2.5 Establecer los mecanismos de protección en cada nivel OSI

2. CAPÍTULO II: FUNDAMENTOS TEORICOS

2.1 Seguridad Informática y Seguridad de la Información

En la actualidad la informática y las redes se han convertido en un recurso indispensable, desde el punto de vista de seguridad tenemos dos conceptos relevantes:

La Seguridad de la Información: *"Es el conjunto de medidas y procedimientos, tanto humanos como técnicos que permiten proteger la integridad, confiabilidad y disponibilidad de la información"* (Escrivá Gascó, Romero Serrano, & Ramada, 2013).

La Seguridad Informática: *"Es una rama de la seguridad de la información que trata de proteger la información usando infraestructura informática y de telecomunicaciones para ser almacenada o trasmitida"* (Escrivá Gascó, Romero Serrano, & Ramada, 2013).

Sin olvidar al autor (Gómez Vieites, 2011) que tiene un concepto más concreto debido a que explica a la "Seguridad Informática" como un proceso y no como un producto que se puede comprar o instalar, consta de ciclos repetitivos para la prevención, detección, respuesta y riesgos ante accidentes.

Se debe considerar que los conceptos expuestos con anterioridad son diferentes, pero asemejándose en la búsqueda de un objetivo en común, la protección de datos e información ante cualquier ataque que perjudique gravemente a la empresa.

2.2 Importancia de la Seguridad Informática

Muchas empresas se encuentran vulnerables a ciertos tipos de ataques, amenazas o riesgos ya sea por personas ajenas, intrusos o programas maliciosos que su principal objetivo es lograr el fracaso de una entidad.

Por tal motivo, la protección y seguridad de la información es esencial para evitar ataques informáticos, entre los cuales consta robo y/o pérdida de información, suplantación de identidades, denegaciones de servicios, entre otros. Todas las empresas ya sean pequeñas o grandes deben resguardar los recursos que consideren valiosos como datos, software o hardware, cabe recalcar que los usuarios también deben tener conocimientos básicos sobre cómo mantener la seguridad informática de su computadora y tener todos sus datos seguros.

En síntesis, la seguridad informática no es un juego y se debe dar la importancia suficiente por medio de medidas necesarias como el contratar personal con experiencia o entidades que se dediquen a realizar auditorías para evitar futuras pérdidas.

2.3 Tipos de Seguridad Informática

2.3.1 Seguridad Física

"Medidas de prevención y detección destinadas a evitar daños físicos a los sistemas informáticos y proteger los datos almacenados en ellos". (Escrivá Gascó, Romero Serrano, & Ramada, 2013).

Para evitar cualquier tipo de daños físicos se debe tener en cuenta los siguientes aspectos:

2.3.1.1 Entorno Físico

De tipo inundaciones, terremotos, tornados, incendios entre otros.

2.3.1.2 Entorno Humano

De tipo robos, sabotajes, actos voluntarios e involuntarios.

2.3.2 Seguridad Lógica

"Conjunto de medidas destinadas a la protección de los datos y aplicaciones informáticas, así como a garantizar el acceso a la información únicamente por las personas autorizadas" (Escrivá Gascó, Romero Serrano, & Ramada, 2013).

2.4 Vulnerabilidad

El autor (Escrivá Gascó, Romero Serrano, & Ramada, 2013) considera a una vulnerabilidad como: "*Debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento de un sistema informático*".

Las vulnerabilidades pueden aparecer en elementos básicos de una computadora como en sistemas operativos, aplicaciones, inclusive en cableados de red, medios de almacenamientos, entre otros.

Estas debilidades permiten a un atacante quebrantar los 3 pilares fundamentales de la seguridad informática (integridad, confidencialidad y disponibilidad), asumiendo el control total y acceso a los datos, información inclusive aplicaciones.

2.5 Agujeros de Seguridad

"Errores o fallos que se asocian al mal funcionamiento o implementación de un sistema, es importante y necesario corregir estas vulnerabilidades cuando se las detecte ya que puede causar una inestabilidad de seguridad del sistema en general" (Escrivá Gascó, Romero Serrano, & Ramada, 2013).

2.6 Ataques

(Baca Urbina, 2016) considera que existen 2 tipos de ataques definidos que hace a la empresa u organización más vulnerable a ataques, motivo por el cual no se podrá prevenir todas las amenazas que puedan existir en el entorno.

2.6.1 Intencionados

"Accesos no autorizados al sistema, donde el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, con el objetivo principal de robar información o alterar registros, además puede emplearlos con fines inapropiados aun cuando tiene autorización para usarlos, por ejemplo, vandalismo, terrorismo, entre otros" (Baca Urbina, 2016).

2.6.2 No Intencionados

"Son hechos que perjudican a la información, a la tecnología informática (TI) o a la empresa sin que ocurra por las acciones intencionales de alguien. Por ejemplo: incendios, inundaciones, fallas de suministro de energía eléctrica, errores o equivocaciones de usuarios, entre otros" (Baca Urbina, 2016).

2.7 Fases de un Ataque

Se consideran todos los puntos vulnerables que pueda existir dentro de un sistema informático, siendo de tipo software, hardware incluyendo factores humanos con el principal objetivo de obtener beneficios generalmente económicos; derivando en gran impacto negativo en una empresa.

Un ataque informático básicamente desestabiliza, daña o toma el control total de un sistema informático, por tal motivo se busca procedimientos y las mejores prácticas que reduzcan en un gran porcentaje cualquier tipo de ataque a la que se encuentre expuesto.

Entonces, el estudio de la seguridad informática nos ayuda a comprender cuales son las debilidades más comunes y los riesgos asociados a esta; por tal motivo se han desarrollado cinco fases que facilitará esta identificación con el propósito de desplegar de manera inteligente ciertas estrategias de seguridad que logren ser efectivas.

Por otro lado, (Mamani Quisbert, 2013) expresa que una atacante debe tomar con suma importancia y cuidado cada una de las cinco fases debido a que cada una de ellas llevaran al éxito de su objetivo, caso contrario un pequeño descuido podría provocar consecuencias graves como: multas, prisión, entre otros.

2.7.1 Reconocimiento

Es un estudio previo que hace un atacante hacia su víctima u objetivo, es extrae toda la información como sea posible.

2.7.2 Escaneo

Es organizar toda la información de la fase de “Reconocimiento”, toma lo más importante para realizar un análisis profundo y de esta manera identificar las características más relevantes para encontrar vulnerabilidades.

2.7.3 Obtener Acceso

Es aplicar una estrategia planteada después de haber pasado por la fase de “Escaneo”, sin embargo, es la más crítica de todas las fases ya que debe utilizar conjuntamente todas las habilidades y herramientas adquiridas para realizar cualquier tipo de ataque. Es un paso decisivo ya que se podrá visualizar el alcance del ataque.

2.7.4 Mantener Acceso

Consiste en conservar el acceso que se ganó en la fase de “Obtener Acceso” en el sistema. Se usa herramientas de Sniffer con el objetivo de capturar todo el tráfico que pasa por la red, con el objetivo de conocer con qué dispositivos de red se encuentra trabajando la víctima y efectuar cualquier tipo de ataque.

2.7.5 Borrar Huellas

En esta fase se debe usar todas las herramientas posibles para evitar que existan registros de las acciones del victimario debido a que si la victima encuentra o sospecha de algún rastro extraño podría ser detectado.

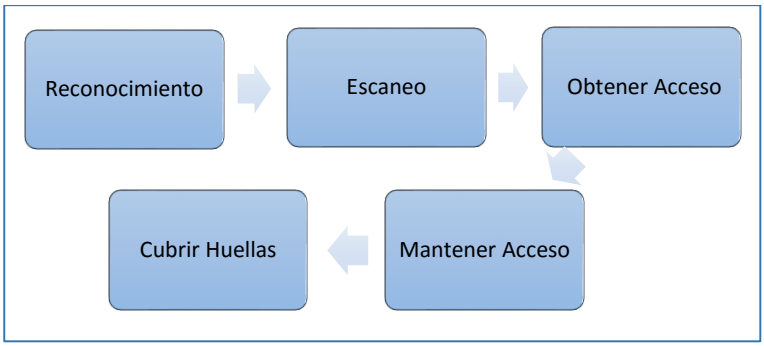


Ilustración 2-1: *"Fases de un Ataque Informático"*

2.8 Tipos de Atacantes

En este apartado se mencionará los tipos de atacantes que puedan existir para los sistemas informáticos, según (Conecta Software, 2017) los más comunes son:

2.8.1 Hacker

Son aquellos que se destacan por su excelencia y habilidad en la rama de la programación y electrónica, poseen altos conocimientos en ordenadores y redes informáticas. Su principal objetivo es buscar y detectar vulnerabilidades de una computadora o red informática.

2.8.2 Cracker

Son atacantes que tienen avanzados conocimientos en programación y electrónica, el cual les permite "romper" las protecciones de sistemas y software. Todas estas acciones las realizan por el valor económico que puedan obtener.

2.8.3 White Hats

Se los conoce como "Hackers Éticos", son expertos en informática debido a que usan sus conocimientos para buscar vulnerabilidades. Además, realizan test

de penetración para estudiar y corregir fallos de seguridad logrando mejorar los sistemas en materia de seguridad.

2.8.4 Grey Hats

Son aquellos que usan las mismas técnicas de los “White Hats”, buscan vulnerabilidades para luego venderlas a quien esté dispuesto a pagar por ellas. Entre su público se encuentra gobiernos, servicios militares y otros hackers.

Adicionalmente, se pueden presentar como expertos en seguridad para resolver fallos encontrados. Básicamente se enfoca en las ganancias económicas que perjudicar a empresas.

2.8.5 Black Hats

Usan conocimientos para realizar actividades ilegales, suelen ser creadores de tipo de malware y además de beneficiarse económicamente buscan aumentar su reputación.

2.8.6 Newbie

Son atacantes novatos que busca comenzar en el mundo del hacking; no sabe absolutamente nada de reglas o el peligro que conlleva realizar un ataque (OWASP, 2017).

2.8.7 Scriptkiddie

Son aquellos que usan programas y scripts desarrollados por otros para atacar sistemas de computadoras y redes. No poseen ninguna habilidad para programar sus propios exploits, por lo que buscan impresionar o ganar reputación (OWASP, 2017).

2.8.8 Lammers

Son atacantes que presumen de ser piratas informáticos, cracker o hacker. Intentan usar programas de fácil manejo los cuales son realizados por auténticos hackers. No poseen habilidades para manejar software básico o conocidos.- (OWASP, 2017).

2.8.9 Gurú

Son atacantes maestros que enseñan a los hackers, se tratan de personas adultas porque ya poseen la experiencia necesaria sobre sistemas informáticos y están allí para ayudar a jóvenes que recién se están iniciando en el mundo del hackeo (OWASP, 2017).

Para terminar, la información que atraviesa por medio de una red se encuentran vulnerables a la acción de todo tipo de hackers, crakers y entre otros; los cuales realizan fallos en los sistemas informáticos incluyendo a servidores web que permiten tener un acceso privilegiado para administrar y realizar cualquier tipo de acción ya sea beneficiosa o no para la empresa.

2.9 Hacking Ético

Es un proceso que analiza los sistemas informáticos asumiendo el rol principal de un ciberdelincuente de tal manera que simule ataques con el objetivo de evaluar el estado real de la seguridad de la información de una empresa. (Socialetic, 2018), expresa que para realizar un hacking ético es necesario contar con previas autorizaciones de dicha empresa el cual se encuentre plasmado en un documento donde se indique las obligaciones que debe cumplir un auditor como la confidencialidad, integridad, secreto

profesional, entre otros. El resultado de este proceso es indicar cuales son los puntos débiles y los pasos a seguir para eliminar o mitigar sus vulnerabilidades.

2.10 Amenazas

Es considerada como: *"Cualquier entidad o circunstancia que atente contra en buen funcionamiento de un sistema informático"* (Escrivá Gascó, Romero Serrano, & Ramada, 2013).

También cuenta como la posibilidad que pueda provocar daños permanentes sobre la información ya sea de tipo económico y/o material; lo fundamental es buscar la manera que no se quebrante los 3 pilares de la seguridad de la información.

2.11 Riesgos

Es considerada como: *"Probabilidad de que una amenaza se materialice"* (Escrivá Gascó, Romero Serrano, & Ramada, 2013).

En términos generales, una empresa u organización siempre tiende a estar amenazada de sufrir algún daño en su sistema informático, desembocando en graves pérdidas de diversos tipos debido a sus vulnerabilidades

Los niveles de riesgo a los que se pueda estar expuesto un activo, dependerá de la probabilidad de que se materialice una amenaza y en el grado de impacto, tomando en cuenta que no existe un riesgo cero ya que no es posible prever y evitar todas las situaciones a los que se puedan estar expuesto nuestros sistemas. A continuación, se muestra en la Ilustración 1-2 los tipos de niveles y con sus respectivos tipos de riesgo:

Nivel	Tipo de riesgo
Alto	Robo de información Robo de hardware
Medio	Accesos no autorizados
Muy bajo	Inundaciones

Ilustración 2-2: *"Niveles de riesgo que se puedan materializar", (Escrivá Gascó, Romero Serrano, & Ramada, 2013)*

2.12 Impacto

Se considera como: *"Medición y valoración del daño que podría ocasionar un incidente de seguridad hacia la empresa"* (Gómez Vieites, 2011)

Es muy importante valorar el impacto por lo que se debe clasificar tanto los daños tangibles como la estimación de daños intangibles, por este motivo es de gran ayuda realizar entrevistas en profundidad con los responsables de cada área con el objetivo de determinar cuál sería el impacto real de la pérdida, robo y alteración de la información.

2.13 Protocolo

"Conjunto de normas y procedimientos que los diseñadores de una red eligen o establecen para que utilicen los componentes de dicha red" (Castaño Ribes & López Fernández, 2013).

2.14 Estándares

"Es un modelo o patrón que se propone para que distintos fabricantes lo sigan y elaboren componentes que sean compatibles entre sí. Pueden proceder de una iniciativa propia de las empresas, estándares de facto, organismo oficial, entre otros" (Castaño Ribes & López Fernández, 2013).

2.15 Capa o Nivel

"Estructura de diferentes funciones y servicios que tiene como objetivo normalizar o estandarizar las técnicas de comunicación, favorece la conectividad entre equipos de diferentes fabricantes que comparten un mismo estándar" (Abad Domingo, 2013).

2.16 Arquitectura de Red

"Conjunto organizado de capas y protocolos que la red usa para comunicarse entre sí a través de nodos" (Abad Domingo, 2013).

Para que una arquitectura de red sea encuentre bien estructurada, debe cumplir con las siguientes características básicas:

2.16.1 Tolerancia a Fallos

Ayudar a limitar el impacto de error de software o hardware y recuperarse de dicho error rápidamente.

2.16.2 Escalabilidad

Permitir el crecimiento de las redes sin involucrarse en su funcionamiento.

2.16.3 Calidad de Servicio

Establecer como prioridad el suministrar una calidad de servicio para los usuarios.

2.16.4 Seguridad

Establecer mecanismos de seguridad para que la información llegue correctamente desde su origen hasta su destino.

2.17 Servicios

Es el proceso de comunicación entre capas definiendo cada uno de sus límites; es decir, emplea una división modular de interfaces entre capas más sencillas. Gracias a la organización jerárquica propuesta por el modelo OSI[3], cada nivel atenderá "peticiones" del nivel inmediatamente superior, ocultando detalles irrelevantes para dicho nivel.

2.17.1 Orientado a la Conexión

Son servicios que requieren el establecimiento de una conexión antes de empezar a trasmitir cualquier dato, durante este proceso los equipos de red que van a comunicarse pueden decidir ciertos parámetros para su comunicación.

2.17.2 No Orientado a la Conexión

Son servicios que no requieren del establecimiento de una conexión para poder comunicarse.

[3] **OSI:** Open System Interconnection (Interconexion de Sistemas Abiertos)

2.18 Unidades de Información

De acuerdo a la definición del autor (Romero Ternero, y otros, 2014), las entidades que pertenecen al mismo nivel, tienden a intercambiar información, los cuales siguen un formato predeterminado de acuerdo a un protocolo.

2.18.1 Unidad de Datos de Protocolo (PDU)

Es la unidad de datos de un protocolo, los mensajes que se coloca como un prefijo el cual indica al nivel que pertenece, es decir (2-PDU, 3-PDU, entre otros).

2.18.2 Unidad de Datos de Servicio (SDU)

Es la unidad de datos de servicio, se los conoce como datos de nivel superior.

2.18.3 Información de Control de Protocolo (PCI)

Es la información de control que posee un protocolo para trabajar en uno de los niveles del modelo OSI.

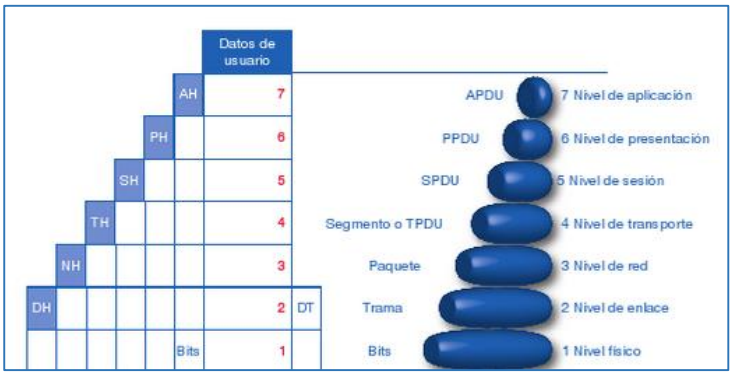


Ilustración 2-3: *"Cabeceras asociadas a cada nivel OSI", (Escrivá Gascó, Romero Serrano, & Ramada, 2013)*

La Ilustración 1-3 explica detalladamente las cabeceras asociadas directamente a cada nivel y su respectiva correspondencia en la jerarquía de los 7 niveles del modelo OSI.

Cuando un usuario necesita transmitir datos hacia un destino, el sistema de red añade información de control para cada uno de los servicios que utilizara la red para ejecutar la orden de transmisión. (Abad Domingo, 2013).

2.19 Dirección IP

Es el número que identifica un equipo dentro de una red que use el protocolo IP. Cada dirección IP es única, ayudando a la comunicación de dos máquinas a través del Internet para lograr identificarse y localizarse entre sí. Sin embargo, se debe tener en cuenta que las direcciones IP difieren de las direcciones MAC, debido a que esta última es un número fijo asignado a la tarjeta de red por un fabricante mientras que las direcciones IP pueden cambiar dinámicamente. (Romero Ternero, y otros, 2014).

Por otro lado, existen tres tipos de redes según su número de bits dedicados a las partes de red y de host, los cuales se detallan a continuación:

2.19.1 Clase A

Empiezan por el bit 0, es decir su primer octeto se encuentra en el rango de 0-127.

2.19.2 Clase B

Empiezan por los 10 bits, es decir su primer octeto está en el rango de 128-191, son ideales para empresas ya que se trata de redes pequeñas.

2.19.3 Clase C

Empiezan por los 110 bits, es decir su primer octeto está en el rango de 192 en adelante, existen muchas de este tipo siendo bastante pequeñas (alrededor de 256 host).

Sin embargo, la autora (Navarro Lacoba, 2014) incluye dos tipos de clases de redes entre las cuales tenemos:

2.19.4 Clase D

Se usa para establecer direcciones de multienvío o multicast[4], su primer bit es 1110, es decir su primer octeto se encuentra entre 224 y 239.

2.19.5 Clase E

Su función es para el futuro, se encuentran reservadas para el uso experimental de proyectos en la red, su primer octeto varía entre 240 y 255.

Clase	Bits de mayor peso	Número de bits para la dirección de red	Número de redes	Número de bits para el host	Número de hosts por red	Valores del primer octeto
A	0	8	126	24	16.777.214	0-127
B	10	16	16.384	16	65.534	128-191
C	110	24	2.097.152	8	254	192-223
D	1110	No aplicable	No aplicable	No aplicable	No aplicable	224-239
E	1111	No aplicable	No aplicable	No aplicable	No aplicable	240-255

Ilustración 2-4: *"Numero de redes y su tamaño para cada dirección IP", (Romero Ternero, y otros, 2014)*

[4] **Multicast:** Los datagramas son entregados a varios hosts dentro de la red.

2.20 Dirección MAC

Es aquella que permite identificar los distintos dispositivos que se encuentran conectados a un mismo medio compartido. Es un numero binario que identifica de forma única un dispositivo en un medio compartido. (Castaño Ribes & López Fernández, 2013).

2.21 Modo Promiscuo de una Tarjeta de Red

Es cuando un adaptador acepta todas las tramas que recibe, vayan o no destinadas a él; esta configuración es especialmente útil si queremos analizar todo el tráfico que pasa por un determinado punto de red. (Castaño Ribes & López Fernández, 2013).

2.22 Subred

(Navarro Lacoba, 2014) explica que cada dirección IP incluye una identificación de la red y la identificación de un host dentro de la red. Estas subredes sirven para una organización a nivel interno de las direcciones IP, por lo cual aplica una técnica enmascaramiento llamada mascara de subred.

2.23 Ingeniería Social

1.23.1 Tipos de Ingeniería Social

Es un conjunto de prácticas que tiene como objetivo obtener información mediante la manipulación de los usuarios que sean legítimos y tengan accesos privilegiados, las victimas se verán confundidas por el atacante para dar información de manera voluntaria o incluso sin darse cuenta de ello.

1.23.1.1 Ataque Telefónico

El atacante realiza una llamada telefónica a la víctima haciéndose pasar por alguien más, es un modo muy efectivo ya que no se conoce físicamente a atacante (Castellanos Sandoval, 2011).

1.23.1.2 Ataque vía Internet

Son ataques que se basa en correos electrónicos, conversaciones en chat, foros, llenando formularios falsos, entre otros. A través de este medio se obtienen información fácilmente sin conocer físicamente al atacante (Castellanos Sandoval, 2011).

1.23.1.3 Ataque Dumpster Diving

Son ataques que se basan en la búsqueda de información relevante en la basura como agendas de trabajo, unidades de almacenamiento, organigramas, entre otros (Castellanos Sandoval, 2011).

1.23.1.4 Ataque Vía SMS

Es un ataque que se aprovecha de las aplicaciones de los celulares, el atacante envía un mensaje SMS a la víctima haciendo creer que el mensaje pertenece a una promoción o servicio (Castellanos Sandoval, 2011).

1.23.1.5 Ataque Cara a Cara

Es el medio más eficiente pero complicado de realizar ya que el atacante debe tener habilidad social y poder manejar cualquier tipo de situación que se le presente (Castellanos Sandoval, 2011).

2.24 Firewall

"Software especializado que se interpone entre las aplicaciones de software de red para realizar un filtrado de paquetes" (Roa Buendía, 2013).

Los cortafuegos tienen como función principal proteger de ataques externos a las computadoras, servidores que se encuentren en la red monitoreando su tráfico entrante y saliente decidiendo si se permiten o bloquean, tomando en cuenta ciertas medidas de seguridad.

El autor (Baca Urbina, 2016) menciona que este software se ubica en la tercera capa del modelo OSI (Capa de Red) de tal manera que funcione como un punto de unión entre dos redes. Por otra parte, el firewall controla el número de conexiones que se encuentran activas en un mismo punto y bloquea aquellas que excedan cierto número de conexiones. Del mismo modo controla que el tipo de aplicaciones que acceden a Internet, entre otras funciones.

Para una empresa u organización, el firewall depende de la política se seguridad, configurando las reglas de operación para permitir o rechazar cualquier solicitud de conexión. Sin embargo, proteger al cien por ciento todas las amenazas de las computadoras o redes es imposible debido a que los cortafuegos poseen ciertas limitantes que solo permiten la protección de aquellos ataques que pasan en forma

directa por la capa de red siendo totalmente vulnerable a los otros tipos de ataques como daño o robo de información proveniente de los empleados.

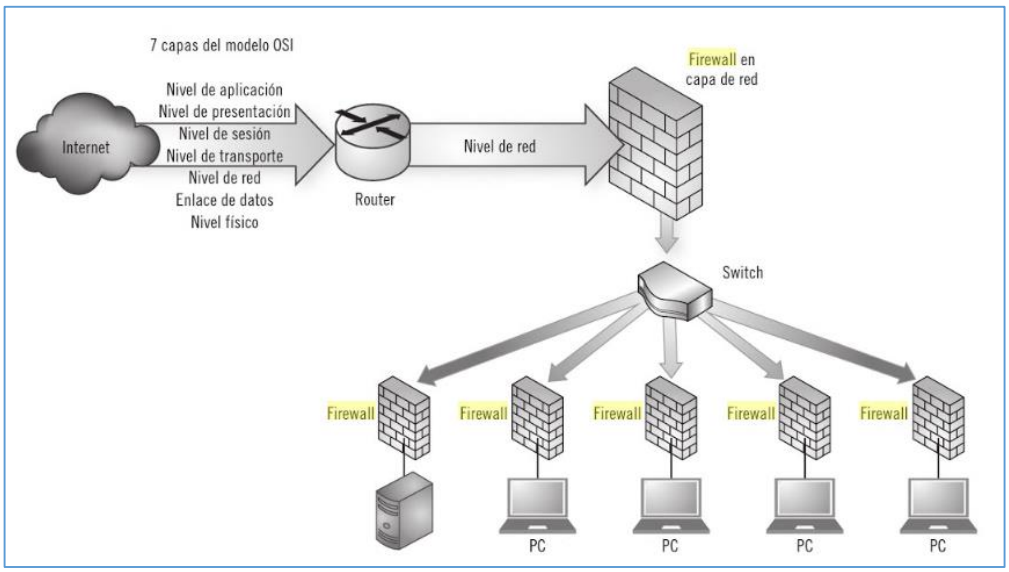


Ilustración 2-5: *"Ubicación de un Firewall en un red LAN", (Baca Urbina, 2016)*

3. CAPÍTULO II: CARACTERIZACION DE LA SEGURIDAD DE LA INFORMACION

3.1 Principios Fundamentales de la Seguridad de la Información a la Red

"Seguridad de la Información" son medidas que impiden la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos pueden conllevar daños sobre la información comprometiendo su confidencialidad, autenticidad o integridad y disminuyendo el rendimiento de usuarios no autorizados al sistema (Gómez Vieites, 2011).

Sin embargo, la Seguridad de la Información asocia un amplio conjunto de definiciones, protocolos, métodos y reglas los cuales tienen como principal objetivo proteger la infraestructura computacional, activos de una empresa y toda la información que circula a través de las redes de computadoras.

(Costas Santos, 2014) expone que los componentes de un sistema informático siempre se encuentran expuestos a un ataque entre los cuales se incluye hardware, software y datos, por lo que es muy importante su protección.

Entonces, si la seguridad de la información también se encarga de la información, esta puede adoptar diversas formas, por lo que para su correcta gestión en su seguridad se basa en 3 principios fundamentales los cuales según la norma ISO/IEC 17799 se debe perseverar la confidencialidad, integridad y disponibilidad (CIA) de sus activos de información.

3.1.1 Confidencialidad

Para los siguientes autores, este principio se define como:

"Garantía que los datos, objetos y recursos que se ha transmitido o almacenado en un sistema informático solo pueden ser leído por su legítimo destinatario." (Álvarez Marañon & Pérez García, 2004).

"Cualidad que debe poseer un documento o archivo para ser entienda de manera comprensible o sea leído por la persona o sistema autorizado." (Costas Santos, 2014).

Entonces, la información puede encontrarse circulando entre dos equipos por medio de una red de comunicaciones o puede estar almacenada en dispositivos físicos (USB, disco duro, memoria, entre otros).

Sin embargo, este principio no se encuentra exento de vulnerabilidades por lo que es expuesto a capturas de tráfico que circulan por la red cuando no existe información cifrada, accesos no autorizados a los recursos, fallos de autenticación.

Un claro ejemplo de este principio es cuando se trasmite un archivo o documento cifrado, si la persona conoce la clave puede acceder a él, caso contrario será imposible.

3.1.2 Integridad

"Garantizar que un mensaje o fichero no ha sido modificado desde su creación o durante su transmisión a través de una red informática" (Gómez Vieites, 2011).

Sin embargo, el autor (Roa Buendía, 2013) expone que el principal objetivo es que los datos queden almacenados tal y como espera el usuario, es decir que no se alteren sin su conocimiento.

Este principio es vulnerable a modificaciones no autorizadas durante su almacenamiento, transporte o procesamiento, fallos humanos involuntarios, mala codificación, borrar o reemplazar información.

Un ejemplo de integridad es la identificación de un usuario, ya que, para realizar acciones de modificación, alteración de una base de datos se requieren ciertos privilegios.

3.1.3 Disponibilidad

"Garantizar que la información sea accesible en el momento adecuado para los usuarios autorizados." (Escrivá Gascó, Romero Serrano, & Ramada, 2013).

Este principio se puede vulnerar cuando los usuarios que tienen acceso a él no pueden utilizarlo, cuando un atacante consigue que un recurso deje de estar disponible para otros usuarios que acceden a él a través de la red, cortes de vías de comunicaciones con el exterior.

Un ejemplo de este principio es la información bancaria, este debe estar disponible para realizar consultas, transacciones, es decir ser utilizada en cualquier momento por el usuario.



Ilustración 3-1: *"Seguridad de la información según la norma ISO/IEC 17799", (Gómez Vieites, 2011)*

Varios autores como (Gómez Vieites, 2011), (Costas Santos, 2014) en sus libros "Enciclopedia de la Seguridad Informática" y "Seguridad Informática" conciertan que no existe un sistema que realmente sea seguro al 100%, por lo que se debe tratar de proteger la información y sus redes de comunicación de manera razonable, considerando que deben cumplir con los pilares fundamentales de la Seguridad de la Información aplicada a la red.

3.2 Presentación del Modelo de Interconexión de Sistemas Abiertos (OSI)

Es un modelo de referencia creado para diseñar una arquitectura de comunicación para computadoras heterogéneas mediante la definición de protocolos y división en niveles para solventar problemas de interconexión en partes que sean completamente manejables.

Fue desarrollado como una arquitectura de red en el año 1.977 por la Organización Internacional de Normalización (ISO) bajo el nombre de "Interconexión de Sistemas

Abiertos (OSI)", cuyo estándar final fue perfeccionado en el año 1.984 denominado ISO 7498.

El modelo OSI surge como una necesidad de compatibilidad e interoperabilidad para que las computadoras puedan comunicarse entre sí a través de una red, gracias a esto varios autores han tomado varias percepciones con respecto a este modelo.

Para (Tanenbaum & Wetherall, 2012) este modelo se encuentra "*Basado en una propuesta desarrollada por la ISO como el primer paso hacia la estandarización internacional de los protocolos utilizados en diversas capas, se ocupa de la conexión de sistemas abiertos, esto es, sistemas que están abiertos a la comunicación con otros sistemas*".

Para (Castaño Ribes & López Fernández, 2013), , "*Surge como un intento de unificar esfuerzos, conocimientos y técnicas para elaborar un modelo de arquitectura basado en capas que sirviera como referencia a los distintos fabricantes de la época para construir redes compatibles entre sí".*

Sin embargo, la Organización Internacional de Normalización añade que este modelo se encuentra formado por una serie de capas con diversos protocolos que cumplen funciones muy bien definidas ofreciendo servicios a la capa inmediatamente superior tomándolos de la capa inferior.

Por este motivo, el modelo OSI además de ser una arquitectura que se basa en niveles permitirá y garantizará la comunicación entre diferentes equipos que se encuentren en red a través de protocolos y estándares que trabajan en cada nivel para cumplir las necesidades básicas para lo que fue creado como compatibilidad entre fabricantes e interoperabilidad.

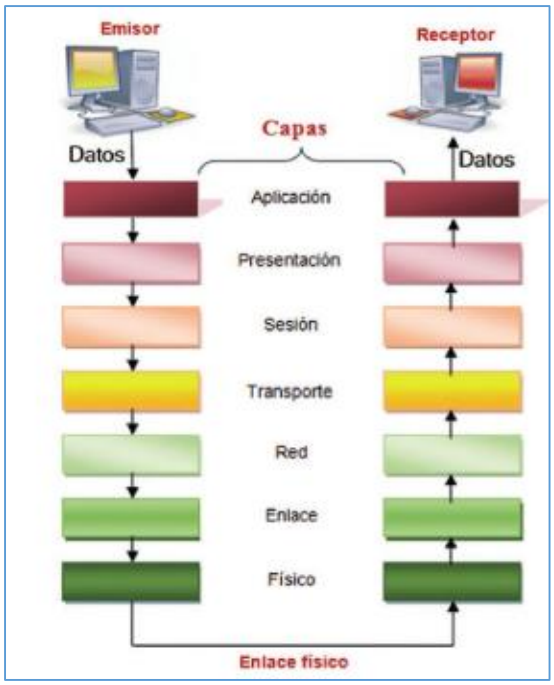


Ilustración 3-2: *"Niveles del Modelo OSI", (Aguilera, 2011)*

3.3 Funcionamiento de los 7 Niveles del Modelo de Interconexión de Sistemas Abiertos (OSI)

El modelo de referencia OSI utiliza una arquitectura basada en niveles o capas, con el objetivo de dividir los problemas de interconexión en partes que sean manejables. Para (Molina Robles, 2014) la aproximación en niveles asegura modularidad y facilita que el software pueda mejorarse sin necesidad de introducir grandes cambios, además de permitir la compatibilidad de equipos diferentes.

Este modelo consta de siete niveles o capas, las cuales realizan funciones bien definidas, permite que las modificaciones de funciones o protocolos que se realicen en una capa no afecten a los niveles contiguos, cada uno de ellos debe interactuar únicamente con los niveles inmediatos (superior o inferior), la función de cada capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente, entre otras funciones.

De acuerdo con (Corletti Estrada, 2011) para tener una idea más clara sobre el porqué de los niveles, a continuación se presenta lo que el modelo OSI plantea para cada uno de ellos, este esquema resalta la división de servicios y funciones en siete niveles, no necesariamente se cumple, ya que es solo una propuesta de estandarización para poder resaltar el diseño de los componentes tanto como Software y Hardware.

Las 7 capas o niveles que conforman este modelo son:

3.3.1 Capa Física

Primera capa del modelo de referencia OSI, responsable de la trasmisión de bits a través de canales de comunicación, su diseño tiene que asegurar que cuando un equipo de red envíe un bit (0, 1), este se reciba de manera correcta en el equipo destino al que va dirigido. (Castaño Ribes & López Fernández, 2013).

Este es el canal principal de comunicación por el cual se va a transmitir la información por lo que utiliza medios de trasmisión como cables o comunicación inalámbrica, definiendo parámetros como la velocidad y distancia máxima que puede alcanzar una señal sin deteriorarse.

Desde la perspectiva de seguridad informática, en esta capa debemos tomar en cuenta los siguientes aspectos:

3.3.1.1 Entorno Físico

Los Data Center tiene como objetivo principal proteger los tres pilares fundamentales de la información citados en el apartado anterior. Como bien afirma (Aguilera, 2011), el entorno físico consiste en la elección

de locales o edificios que albergan dispositivos informáticos, sistemas principales de redes y recursos asociados para el proceso de la información de una empresa u organismo.

Si bien es cierto, el Data Center es un espacio físico construido y no modificable que debe considerar la evaluación de factores físicos y naturales, tales como: ubicación, diseño, espacio, instalaciones eléctricas, inundaciones, incendios, entre otros. De igual manera, éste debe contar con las condiciones adecuadas y altas medidas de seguridad para proteger en su mayor parte los aspectos antes mencionados.

Por otro lado, actualmente existen otras soluciones innovadoras que sustituye a los Data Center como “Cloud Computing” , según (20 COMPUTING?, 2017) es una forma óptima de almacenar, asegurar, garantizar, acceder rápida y eficazmente a la información en tiempo real. El suministro de estos recursos informáticos se basa desde aplicaciones hasta centro de datos mediante el Internet y en un modelo de pago por uso.

Esta nueva tecnología ha ido evolucionando de tal manera que existe diferentes modalidades de servicio entre los cuales (IBM Cloud, 2017) explica los más importantes de la siguiente manera:

3.3.1.1.1 Software como Servicio (SaaS)

Permite a los usuarios conectarse a aplicaciones de software por medio del Internet como correos electrónicos, herramientas ofimáticas, entre otros.

3.3.1.1.2 Plataforma como Servicio (PaaS)

Ofrece un entorno con las funciones y requisitos que son necesarios para dar soporte a la creación y evolución de aplicaciones las cuales se basan en la web sin comprar o gestionar hardware, software.

3.3.1.1.3 Infraestructura como Servicio (IaaS)

Es una infraestructura de servicio que ofrece a las empresas recursos informáticos como servidores, redes, almacenamiento y espacio en centro de pagos en función del uso.

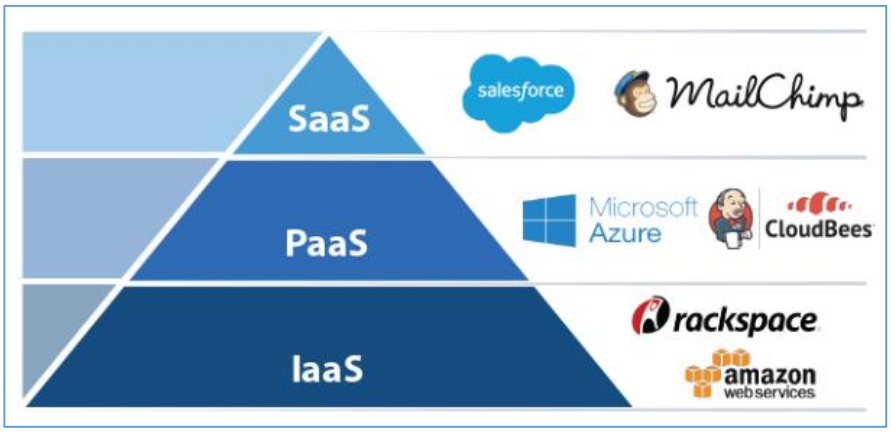


Ilustración 3-3: *"División principal de SaaS, PaaS, IaaS", (Muspratt, 2017)*

Para los usuarios y las empresas esta tecnología es más cómoda que la tradicional tanto desde el punto de vista se seguridad. Hoy en día, existen muchas compañías que promocionan estos tipos de servicios como "Movistar Cloud Computing" y "Google Apps" siendo el usuario quien escoja las funcionalidades de acuerdo a su necesidad.

3.3.1.2 Autenticación y Control de Acceso

La autenticación y control de acceso son aquellos que permitirán el acceso hacia los recursos de la empresa, tanto tangibles como intangibles. Este aspecto es importante porque intervienen factores humanos los cuales tienen contacto directo.

Estas dos condiciones se encuentran estrechamente ligadas ya que son maneras de cumplir las políticas de acceso a la empresa, es decir mientras la autenticación verifica quien dice ser (identidad), el control de acceso decide si un usuario tiene permisos y privilegios para ingresar o procesar activos de información otorgados por su perfil de cargo.

3.3.1.3 Medios Empleados para Transmitir Información

El nivel 1 del modelo OSI posee distintos medios de transmisión para el envío de información a través de distintos dispositivos de red, clasificándolos de la siguiente manera:

3.3.1.3.1 Medios Guiados

Son canales físicos para la transmisión de información de un dispositivo a otro. Los medios guiados pueden ser de distintos tipos destacando los más relevantes:

a) Medios Magnéticos

Es transportar datos de un equipo a otro mediante su almacenamiento en cintas magnéticas o medios removibles

(Tanenbaum & Wetherall, 2012). Estos medios son sensibles a la pérdida de datos cuando son expuestos directamente a campos magnéticos (imanes).

b) Par Trenzado

Para los autores (Castaño Ribes & López Fernández, 2013) son dos alambres entrelazados de forma helicoidal el cual ayuda a reducir interferencias entre dos equipos.

Este medio guiado, consta de 8 hilos los cuales se encuentran trenzados dos a dos e identificados por colores. Dependen del número de trenzas para poder clasificarse y de esta manera obtener mayor velocidad en las transferencias y su costo es mínimo.

c) Cable Coaxial

El autor (Molina Robles, 2014) reconoce a este medio guiado como el cable de mejor blindaje, logrando alcanzar mayores velocidades de transmisión.

Además de transportar las señales eléctricas de altas frecuencias, este cable es muy resistente a interferencias externas y atenuaciones. Estos cables son utilizados en transmisiones datos a largas distancias, ofreciendo soporte confiable y excelente en velocidades de transmisión.

d) Fibra Óptica

(Castaño Ribes & López Fernández, 2013) lo definen como un medio de red el cual es capaz de transmitir pulsos de luz representando los datos a transmitir.

Actualmente muchas empresas, organizaciones se encuentran utilizando este tipo de cable ya que su velocidad de transmisión es muy alta y gracias a esto la propagación de la señal logra mayores distancias sin interferencias electromagnéticas ni radiofrecuencia.

3.3.1.3.2 Medios No Guiados

Son medios inalámbricos que transmiten información a través de ondas electromagnéticas, no usan ningún canal físico de por medio. Los principales tipos en este apartado son:

a) Ondas de Radio

Son ondas son fáciles de generar, pueden recorrer largas distancias, inclusive pueden penetrar edificios viajando en todas las direcciones. (Molina Robles, 2014).

Cuando estas ondas recorren largas distancias, es necesario realizar controles estrictos por parte de las autoridades para que las diferentes transmisiones no interfieran entre sí.

b) Microondas

Este medio no guiado permite transmisiones tanto terrestres como satélite, siendo su principal uso en hornos.

Muchas veces las comunicaciones vía microondas no atraviesan apropiadamente ciertos obstáculos por lo que es necesario situar antenas repetidoras cuando se desea realizar comunicaciones a largas distancias. Mientras que, en el caso de las comunicaciones vía satélite, siempre existe un mínimo retardo en las transmisiones, es decir 0,3 segundos en ir y regresar.

c) Infrarrojo

Son ondas de luz invisibles al ojo humano, viaja por el aire y se caracterizan por un elevado ancho de banda y un reducido alcance. (Pérez Luna, 2014).

Para realizar una trasmisión de información de tipo infrarrojo se deben tener contacto directo y cercano por lo termina siendo una gran desventaja ya que no atraviesan objetos solidos como paredes, puertas, entre otros.

3.3.1.4 Medios Físicos de Almacenamiento y Procesamiento de Información

Son dispositivos informáticos que tienen como objetivo respaldar, transferir o procesar información, siendo los más destacados servidores, torres de discos, cintas, CDs, DVDs, entre otros.

Por otra parte, las maneras de almacenamiento y procesamiento de información también se basan en la famosa “Cloud Computing”, el cual se ejecuta en varios servidores a través de Internet. Claro ejemplos de esta tecnología tenemos a Google Drive, Dropbox, ICloud los cuales facilitan que la información se encuentre disponible en cualquier momento que el usuario requiera. (Microsoft, 2018), considera que una gran variedad de organizaciones tanto pequeñas como multinacionales están adoptando esta tecnología gracias a su costo, velocidad, productividad, rendimiento, confiabilidad, entre otros motivos.

Con el paso del tiempo, este “Modelo de Almacenamiento” dejará obsoletos a los dispositivos informáticos físicos debido a que el principal objetivo de esta tecnología es que los proveedores se ajusten a las necesidades del cliente. De esta manera, los modelos principales que actualmente se encuentra en uso son:

3.3.1.4.1 Nube Pública

Ofrecen recursos informáticos (servidores) y almacenamiento por medio de Internet, todo lo que ofrece esta nube es propiedad y está administrado por el proveedor de la nube.

3.3.1.4.2 Nube Privada

Ofrece recursos de computación en la nube utilizados exclusivamente por una sola empresa u organización. Esta nube puede reemplazar a un Data Center ya que trabaja por medio de una red privada.

3.3.1.4.3 Nube Híbrida

Es una combinación de una nube pública y privada el cual permite compartir datos y aplicaciones entre ellos; gracias a esto puede brindar una mayor flexibilidad y más opciones de implementación.

En fin, Cloud Computing depende mucho de las necesidades de los usuarios el cual debe ajustarse a lo que realmente se va a necesitar para que una empresa funcione adecuadamente, ya que aparte de ser un ahorro de tiempo permite guardar y/o procesar grandes cantidades de información eficazmente.

3.3.2 Capa Enlace de Datos

Es la segunda capa del modelo OSI, responsable de gestionar el proceso de transmisión utilizando enlaces físicos los cuales proporcionan mayor fiabilidad. (Castaño Ribes & López Fernández, 2013).

Este nivel usa los servicios de la capa física para enviar y recibir información a través de sus canales de comunicación; siendo su unidad más básica de datos la trama.

Dentro de las funciones principales que realiza este nivel tenemos entramado, direccionamiento físico, control de acceso al medio, multiplexación, control, detección y corrección de errores.

En efecto, para que la información viaje de manera segura, eficaz y confiable, el nivel 2 del modelo OSI permite que la información fluya libre de errores entre dos equipos que se encuentran conectados directamente, para lograr esto se lo realiza de la siguiente manera: montar bloques de información (tramas), asignar una dirección en la capa de enlace, gestionar la detección o corrección de errores y controlar el flujo entre los equipos.

2.3.2.1 Protocolos

a) Control de Enlace de Alto Nivel (HDLC)

Es el protocolo de comunicación más importante a nivel de enlace, trabaja punto a punto o multipunto; su principal objetivo recuperar paquetes en el caso que se pierdan, fallos de secuencia, detectar y corregir errores, entre otros.

Actualmente, este protocolo es el más utilizado en el nivel de capa 2, siendo la base de muchos protocolos derivados los cuales usan formatos y procedimientos similares (SDLC, LAP-B, PPP).

Además, ofrece una comunicación fiable entre el emisor y el receptor, proporciona servicios orientados y no orientados a conexión y utiliza una técnica llamada “Relleno de Bits y Marcas” para construir y manejar las tramas (establecer inicio y final).

b) Punto a Punto (PPP)

Es un protocolo a nivel de enlace estandarizado para realizar una conexión entre dos puntos, es una versión no propietaria del

protocolo HDLC. Se ha diseñado con el objetivo que sea un protocolo abierto el cual permita trabajar con los protocolos de la capa de red como IP y NetBEUI.

El protocolo PPP permitirte la conexión entre computadoras mediante cables seriales, líneas telefónicas, telefonía celular, enlaces de fibra óptica, entre otros. Adicionando otras funcionalidades como el transporte de datos, autenticación a través de claves de acceso y asignaciones dinámicas.

c) Ethernet y CSMA/CD

Es un estándar conocido como IEEE 802.3 en el área de las redes locales; define características físicas y eléctricas que debe tener una red entre las cuales se destaca los cables de tipo coaxial, par trenzado y fibra óptica.

Sin embargo, (Abad Domingo, 2013) expresa que Ethernet usa el protocolo de acceso al medio conocido como CSMA/CD (“Carrier Sense Multiple Access/ Collision Detection”) en el cual la idea principal es que los equipos antes de transmitir los datos, deben detectar si el canal de transmisión se encuentra en uso, caso contrario provocaría una colisión que hará que se suspenda la transmisión, espere un tiempo y se tramite una trama de aviso e intente nuevamente.

Cualquier equipo que se encuentre en una red Ethernet, debe poseer una tarjeta de red que cumpla con este estándar, componentes y software adecuado para recibir y generar tramas.

d) Redes Inalámbricas LAN

Wireless-Fidelity (Wi-Fi), es un estándar que se define como el más extendido para la creación de redes de área local inalámbricas.

Transmite y recibe datos mediante ondas electromagnéticas a través de puertos, sin necesidad de medios guiados (cables), siendo su principal objetivo crear una marca que permita fomentar la tecnología inalámbrica y asegurar la compatibilidad entre equipos.

Actualmente, las normas de funcionamiento de una WLAN se basan en la IEEE 802.11 y sus variaciones debido a que cada una intenta responder a ciertas necesidades de una empresa. El estándar original se ha modificado para poder optimizar el ancho de banda para garantizar seguridad y compatibilidad por lo cual se encuentra en una continua evolución.

Para desarrollar la IEEE 802.11 existe un grupo de trabajo que tiene como objetivo investigar y desarrollar temas relacionados con este estándar, mencionando y detallando a los más importantes en la siguiente tabla:

ESTÁNDAR	FUNCIONALIDAD
802.11a	Busca crear un estándar de WLAN en la banda 5GHz alcanzando tasas de 5 GHz.
802.11b	Busca crear un estándar de WLAN en la banda 2.4GHz alcanzando tasas de 11 Mbps
802.11c	Define características en los puntos de acceso para que puedan ser usados como puentes.
802.11d	Ofrece definiciones y requisitos para que el estándar 802.11 pueda operar en países que actualmente no se puede implementar este estándar.
802.11e	Trabaja en aspectos relacionados con la calidad de servicio QoS y multimedia
802.11f	Aplica intercomunicación entre puntos de acceso de distintos fabricantes, además funciona bajo el estándar 802.11g
802.11g	Busca una extensión de la 802.11b con el objetivo de mantener compatibilidad entre fabricantes.
802.11h	Evolución de 802.11a, permite asignar canales dinámicos y control automático para evitar interferencias para la capa física.
802.11i	Incorpora mecanismos de seguridad para protocolos de autenticación y codificación; además ofrece soluciones interoperables y un patrón robusto para asegurar datos.
802.11k	Permite a los conmutadores y puntos de acceso inalámbrico calcular y valorar recursos de radiofrecuencia con el objetico de mejorar y gestionar el uso de una WLAN.
802.11x	Mejora los mecanismos de seguridad de la 802.11 con protocolos de seguridad extendida EAP

Tabla 3-1: *"Variantes del Estándar 8020.11"*

e) Árbol de Extensión (STP)

Es un protocolo de capa 2, el cual trabaja con bridges y switches, siendo su principal objetivo mantener una red libre de bucles. STP realiza una exploración constante de la red por lo que cualquier fallo es detectado al instante, es decir, en el momento que reconoce un "bucle" bloquea uno o más enlaces redundantes.

Siempre se encuentra trabajando dentro de la red, por lo que, si existe algún cambio en su topología, este lo reconfigurará para que no exista varias rutas hacia un mismo destino.

f) Virtual LAN (VLAN)

Este protocolo es usado para la creación de LAN's Virtuales, entre sus principales objetivos destacamos a la seguridad, flexibilidad y segmentación.

Dentro de una comunicación entre switches se usa enlaces troncales, los cuales etiquetan a la trama enviada y eliminan dicha etiqueta cuando ingresa al switch de destino; transportando el tráfico de más de una VLAN

g) Resolución de Direcciones (ARP)

Es un protocolo utilizado para obtener direcciones MAC de un equipo a través de su dirección IP, simplemente no se puede asociar directamente con el 2 y 3 del modelo OSI, debido a que usa información de las dos capas para poder funcionar.

Entonces, este protocolo trabaja por medio de la traducción de direcciones IP en direcciones MAC almacenándolas en tablas ARP, de esta manera se pueden relacionar para enviar información al destino correcto; sin embargo, estas tablas son temporales, es decir se crean cada vez que se activa un sistema, realizando de nuevo la asociación correspondiente de direcciones IP y MAC.

3.3.3 Capa de Red

Es la tercera capa del modelo OSI, responsable de controlar una subred y elegir la ruta más conveniente para que los datos lleguen a su destino. (Abad Domingo, 2013).

Sin embargo, (Tanenbaum & Wetherall, 2012) sugiere que en el momento que este nivel escoge la ruta más conveniente para trasmitir los datos se debe tener mucha precaución porque puede sobrecargar líneas de comunicación y enrutadores provocando inactividad.

Este nivel usa los servicios de la capa de enlace y ofrece servicios a la capa de transporte; siendo su unidad más básica de datos los paquetes.

Una de sus principales funciones es dirigir los paquetes enviados del emisor hacia el receptor los cuales pueden estar ubicados a grandes distancias geográficas independientemente del número de dispositivos que tengan que atravesar para poder llegar a su destino.

Además, se encarga de tratar correctamente congestiones en la red; debido a que, si existen muchos paquetes que se encuentran circulando por dicha red, estos obstruyen a otros generando cuellos de botella.

Para lograr todos estos objetivos es necesario conocer la topología de la red, es decir tener conocimiento sobre los enrutadores y enlaces que existen para poder lograr una conexión.

Finalmente, en relación con el proceso que realiza un paquete para llegar a su destino (Cisco Systems, 2012) explica que debe "Direccionar[5], Encapsular[6], Encaminar[7] y Desencapsular[8]" los datos.

3.3.4.1 Protocolos

a) Internet Versión 4 (IPv4)

Es uno de los protocolos principales del Internet, siendo su cuarta versión y obviamente la primera en ser utilizada a gran escala en la mayoría de las redes.

Su principal objetivo es proporcionar direcciones IP, los cuales se puedan identificar dentro de la red, en virtud de (Castaño Ribes & López Fernández, 2013), adiciona ciertas sus características de este protocolo, es decir no establece conexiones antes de enviar paquetes de datos, no usan encabezados para garantizar la entrega de paquetes y operan independiente del medio que lleva los datos.

[5] **Direccionar:** Direcciones únicas que tienen los dispositivos para identificarse dentro de la red.
[6] **Encapsular:** Proceso en el cual los datos son formateados, segmentados e identificados con el direccionamiento lógico y físico para poder ser enviado al medio.
[7] **Encaminar:** Dirige los paquetes al host de destino.
[8] **Desencapsular:** Verifica si el paquete fue direccionado al dispositivo correcto y se prepara para enviar la información a la capa de transporte.

Actualmente, el aumento de los dispositivos que se conectan a internet y el desperdicio de direcciones que existe, este protocolo ya no resulta suficiente por lo que fue necesario crear una mejora.

b) Internet Versión 6 (IPv6)

Es la sexta versión del protocolo IP, resultando ser una mejora de la versión IPv4, debido a que solventa cada uno de sus principales problemas, entre las más importantes la falta de direcciones IP, por lo que está destinado a sustituirlo por completo.

Entre sus mejoras según (Santos Gonzáles, 2014) puntualiza que existe ampliación de espacio de direcciones, direcciones de autoconfiguración, aumento de flexibilidad en el direccionamiento, facilidad de asignación de recursos, capacidad de seguridad, eliminación de control de errores de cabecera, entre otros.

Actualmente, (Google, 2018) siempre se encuentra recopilando información sobre la migración de IPv4 a IPv6 y como se muestran en las siguientes estadísticas, esto llevará tiempo ya que solo hasta el 25 de mayo del 2018 se tiene un 20,74% y en el Ecuador un 20,67%. Esto se debe a que los sitio web y proveedores de servicios de Internet deben realizar el cambio. Hasta que esto suceda, los dos protocolos funcionarán de forma conjunta hasta que IPv4 ya no sea imprescindible.

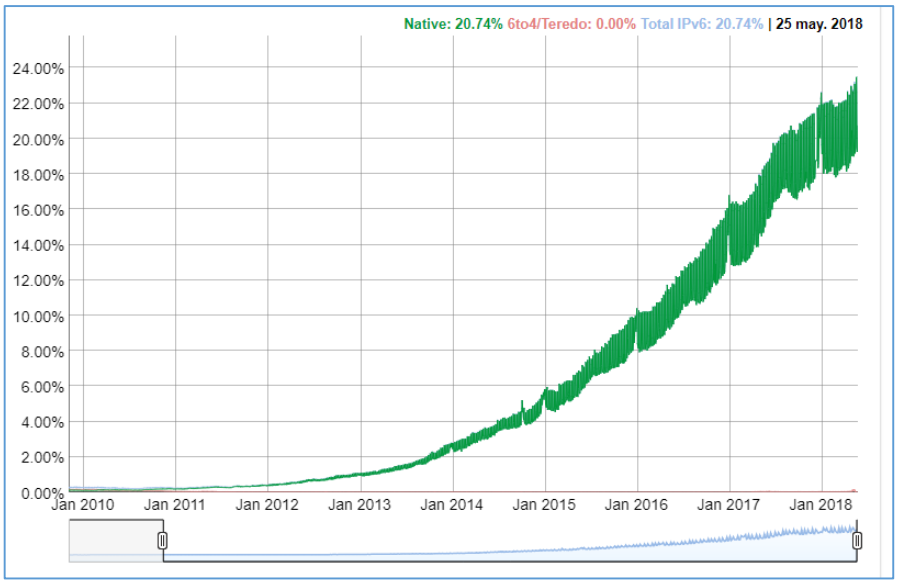


Ilustración 3-4: *"Migración de IPv4 a Ipv6", (Google, 2018)*

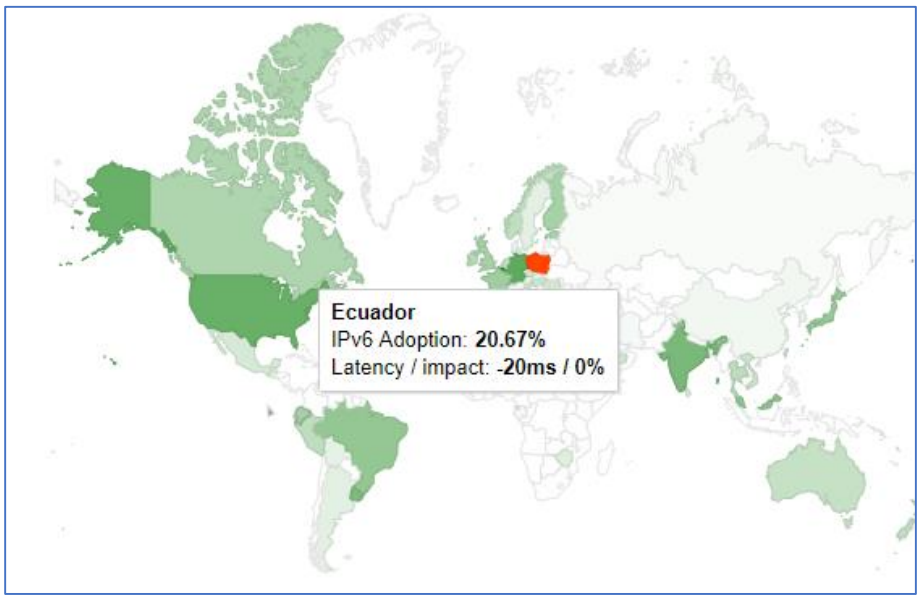


Ilustración 3-5: *"Migración de IPv4 a Ipv6 en el Ecuador", (Google, 2018)*

c) Seguridad de Internet (IPSec)

Es un conjunto de protocolos el cual asegura las comunicaciones del Protocolo de Internet (IP), incluyendo soporte para IPv4 e IPv6, TCP, UDP, ICMP.

Por otro lado el autor (Valdivia Miranda, 2015) argumenta que para asegurar la comunicación mediante este protocolo, se realiza mediante la autenticación y/o cifrado de paquete IP en el flujo de datos.

IPSec se basa en una serie de protocolos como AH[9], ESP[10], e IKE[11], los cuales ayudan a implementar su arquitectura global mediante la confidencialidad, integridad, autenticación de datos incluyendo que los paquetes no se encuentren duplicados dentro de una VPN(Anti-Replay).

En fin, el principal objetivo de este protocolo es asegurar que el contenido que desea transmitir no sufra cambios desde que fue enviado por su emisor y llegue intacto a su destino.

d) Mensajes de Control de Internet (ICMP)

Es un protocolo que se encarga de manejar los errores que se puedan ocasionar en los paquetes IP, básicamente son generados con el propósito de diagnosticar y enrutar.

ICMP se utiliza mensajes de estado o de error para comunicar que es lo que sucede con un datagrama dentro de los dispositivos de red; por lo cual hace uso de los servicios IP.

El típico mensaje de este este protocolo, es cuando se busca diagnosticar la conectividad, ciertos dispositivos envía un mensaje “echo” con la expectativa de que se reciba una respuesta, en el caso de

[9] **Autentication Header (AH):** Brinda autenticación a la información.
[10] **Encapsulating Security Payload (ESP):** Brinda autenticación y encriptación de la información.
[11] **Internet Key Exchange (IKE):** Define modos de cambios de claves

que no exista, se sobreentiende que la conexión entre host a nivel de red se encuentra perdida.

3.3.4 Capa de Transporte

Es la cuarta capa del modelo OSI, corazón de la jerarquía de protocolos, y responsable de entregar un mensaje de manera transparente, confiable, eficiente, libre de errores y ordenada a su hacia su destino.

Siendo su unidad más básica de datos el segmento, estos se preparan para enviarse a través de medios en partes manejables y de esta manera más fácil de administrarlos.

(Molina Robles, 2014) explica su funcionamiento de la siguiente manera: este nivel toma los mensajes del nivel de sesión, los distribuye en segmentos y los pasa al nivel de red, asegurando que llegue correctamente al nivel de sesión del otro extremo.

Entre otras funcionalidades de esta capa tenemos segmentación de datos reensamblaje de datos, identificación de aplicaciones, control de flujo, y calidad de servicio.

3.3.4.1 Protocolos

a) Datagrama de Usuario (UDP)

Es un protocolo basado en IP, no orientado a conexión, siendo su función básica proteger cada segmento individuamente.

UDP se define como no fiable por que los mensajes pueden llegar dañados, duplicados o no llegar por que no existe un mecanismo que evite este tipo de problemas.

Este protocolo es muy sencillo y gracias a esto su velocidad de transferencia es muy alta sin ofrecer ningún tipo de garantía; además es usado para conexiones que no necesitan corrección de errores o continuidad de flujo, dejando al programa de aplicación una responsabilidad muy grande, el de fiabilidad.

Un ejemplo de UDP es la trasmisión de voz y video, es decir cuando se está viendo o escuchando a otra persona en tiempo real porque no se puede perder tiempo en reenviar datos perdidos.

b) Control de Transmisión (TCP)

Es un protocolo orientado a conexión, permite controla el estado de conexión entre el emisor y receptor. A diferencia del protocolo UDP, es muy fiable ya que el receptor controla, ordena y confirma la entrega de segmentos.

Todos los segmentos viajan protegidos por un control de errores de esta manera verifica que la información no llegue corrupta o alterada.

Su principal objetico es proveer un flujo controlado y fiable de datos entre los emisores y receptores añadiendo funciones de corrección de errores, seguridad y libre de pérdidas.

c) Capa de Puertos Seguros (SSL)

Es un protocolo de seguridad que permite la comunicación entre el usuario y el servidor de tal manera que exista confidencialidad, fiabilidad e integridad de los datos.

SSL asegura que la información que se ha transmitido no pueda ser interceptada ni modificada por factores externos por lo que trabaja con otros protocolos especialmente sobre TCP.

Dentro de sus funciones específicas tenemos seguridad criptográfica, interoperabilidad, flexibilidad y eficiencia dentro de un canal seguro para que cualquier información confidencial y personal no pueda ser interceptada, un claro ejemplo de este protocolo es la compra de artículos mediante páginas web.

d) Capa de Seguridad en la Capa de Transporte (TLS)

Es la sucesión del protocolo SSL, siendo un protocolo criptográfico tiene como objetivo garantizar y asegurar el intercambio de datos entre dos computadoras que se encuentren en red.

Permite que la comunicación sea autenticada, integra y fiable, logra que se transmita la información libre de ataques mediante interoperabilidad, extensibilidad y eficiencia. Básicamente es utilizado y compatible con la mayoría de navegadores web.

Como ejemplo de este protocolo tenemos la protección a la falsificación de correos ya que abre canales que son seguros entre sus servidores.

3.3.5 Capa de Sesión

Es la quinta capa del modelo OSI, responsable de establecer, mantener y cerras las sesiones entre equipos, por ejemplo, sesiones TCP.

Este nivel recibe y mejora los servicios de la capa de transporte y ofrece servicios a la capa de presentación; siendo una sesión el nombre que reciben las conexiones establecidas.

Dentro de sus funcionalidades tenemos reanudaciones de sesiones en caso de interrupción o fallo en la red, gestionar sesiones, sincronización y control de dialogo.

Es uno de los niveles orientados a la aplicación; por lo que con mucha frecuencia las funciones de esta capa se combinan con las de la capa de la aplicación y ambas se implementan como un solo protocolo.

3.3.5.1 Protocolos

a) NetBIOS

Es un protocolo desarrollado por IBM el cual permite que las aplicaciones de distintas computadoras se comuniquen a través del compartimiento de recursos dentro una red LAN.

Utiliza los siguientes puertos: 137(nombres), 138 (datagramas) y 139 (sesión), además necesita el apoyo de otros protocolos para poder trabajar como IPC/IPX y NetBEUI.

b) Llamada de Procedimiento Remoto (RPC)

Es un protocolo muy básico que permite ejecutar códigos en otro equipo sin tener que preocuparse por la comunicación.

(Santos Gonzáles, 2014) manifiesta que a cada dispositivo de red de le asigna un nombre de 15 caracteres, y además no es un protocolo enrutable, por tal motivo no se usa en redes LAN.

3.3.6 Capa de Presentación

Es la sexta capa del nivel OSI, es la responsable de que el emisor y receptor de la información comprendan y entiendan el dialogo que se establezca. Se encarga de la sintaxis y semántica del lenguaje que se está trasmitiendo.

(Baca Urbina, 2016) considera que los datos manejados en este nivel se deben comprimir sin perder sus propiedades lingüísticas y que no pierdan su significado. Sin embargo, cuando toma los datos que han sido entregados por la capa de aplicación, realiza su propia conversión en un formato que pueda ser entendido y comprendido, los formatos habituales que usa son MP3, MPEG, JPEG, GIF, entre otros.

Las funciones básicas de la capa de presentación son conversión (BCD, EBCDIC, ASCII, Unicode), encriptación y comprensión de datos los cuales se basan en el estándar ANSI y X.209.

Al igual que la capa de sesión, es uno de los niveles orientados a la aplicación; por lo que se implementan como un solo protocolo para poder funcionar correctamente.

3.3.7.1 Protocolos

a) Notación Sintáctica Abstracta 1 (ANSI.1)

Es un protocolo usado para representar datos, define la manera de cómo se debe transmitir la información, de tal forma que cualquier maquina pueda interpretarlos. Además, establece la estructura de un correo electrónico.

b) Representación de Datos Externos (XDR) Sintáctica Abstracta 1 (ANSI.1)

Es un protocolo que permite transferir archivos entre diferentes arquitecturas y sistemas operativos que son incompatibles mediante el ordenamiento de caracteres, y conversiones.

Los tipos de datos que soporta son integer, boolean, string, float incluyendo matrices, cadenas que son similares al lenguaje de programación C.

c) Extensiones de Multipropósito de Correo Internet (MIME)

Es un protocolo que agrega estructura al cuerpo del mensaje, de tal manera que define reglas codificadas para enviar textos con formato no ASCII a través del Internet. MIME puede enviarse a través de diferente programas y protocolos de la capa de aplicación de correo electrónico existentes.

3.3.7 Capa de Aplicación

Es la séptima y última capa del modelo OSI, es responsable de garantizar que absolutamente todas las aplicaciones de un equipo tengan acceso a los servicios que ofrecen los 6 niveles anteriores del modelo OSI, todo esto se logra gracias a los protocolos ya mencionados.

Todas las aplicaciones poseen su propio protocolo que utilizan para interactuar directamente con el usuario; estos se manejan de manera automática en el momento que se llama a una determinada aplicación existen.

En este apartado se mencionará la mayoría de protocolos principales, debido a que en los últimos años existen una infinidad de nuevas aplicaciones que permiten a los usuarios el uso de correos electrónicos, aplicaciones en tiempo real, navegación por internet, entre otros.

3.3.7.2 Protocolos

a) Sistema de Nombres de Dominio (DNS)

Es un sistema que asocia direcciones IP con direcciones alfanuméricas, es decir: 192.194.56.17 con www.wikipedia.com.ec.

Las direcciones alfanuméricas deben estar separadas por puntos y siguiendo una jerarquía, para reconocer algunas direcciones que aparecen en última posición, por ejemplo: “com”, “org”, “edu”, “net”; y otros asignados por países como: “es” (España), “ec” (Ecuador), “br” (Brasil)…

Varios autores (Carceller Cheza, Campos Saborido, García Marcos, & Gonzáles Lorenzo, 2013) , lo consideran como una base de datos jerárquica y distribuida, permitiendo localizar cualquier equipo y servicio a través de direcciones alfanuméricas, las cuales sean muy fáciles de recordar.

b) Red de Telecomunicaciones (TELNET)

Es un protocolo que permite el acceso de forma remota a un equipo, como si estuviese trabajando de manera directa sobre él; su acceso en por medio de consola usando comando del sistema operativo en uso.

Su arquitectura se basa en cliente-servidor, usa el puerto 23 para acceder al equipo remoto. Una de las desventajas de este protocolo es que no usa cifrado de daros, por lo que cuando una persona este escuchando en red puede conocer fácilmente su usuario y contraseña.

La mayoría de sistemas operativos ya no lo permiten ni en redes LAN (Windows), esto se debe a que las comunicaciones no se encuentran cifradas.

c) Trasferencia de Archivos (FTP)

Es un protocolo de arquitectura cliente – servidor, tiene como función principal el uso compartido de archivos por medio de programas de servidores remotos.

Su transferencia es muy rápida y no posee las seguridades adecuadas, debido a esto no usa dos puertos para su transmisión; el 20 para viaje de datos y 21 para información de control o dialogo.

Obviamente, FTP posee ciertas desventajas como la falta de encriptación, por lo que con el tiempo se han desarrollado otros protocolos de transferencia de fichero de modo seguro como FTP sobre SSH, FTPS o SCP.

d) Secure Shell (SSH)

Es un protocolo de arquitectura cliente - servidor que proporciona altos estándares de seguridad mediante la encriptación de 128 bits; facilitando la comunicación entre dos sistemas.

Es muy similar al protocolo Telnet, siendo su principal función acceder a máquinas de manera remota mediante una red; usa un intérprete de comandos para poder tomar el control completamente.

Actualmente, existe dos tipos de versiones la cual una es mejor que otra debido a que soluciona todos los problemas de seguridad, un ejemplo claro es OpenSSH, es la versión libre de este protocolo ya que proporciona herramientas para un control seguro, remoto y encriptado.

e) Protocolo Simple de Trasferencia de Correo Electrónico (SMTP

Es un protocolo de arquitectura cliente – servidor, relacionado con correos electrónicos el cual permite que circulen a través del internet; utiliza el puerto 25 y exige de autenticaciones para poder trabajar.

Su principal función es permitir la comunicación con un servidor usando líneas de texto o codificado en ASCII con un máximo de 1000 caracteres para ofrecer instrucciones necesarias.

f) Protocolos de Oficina de Correos (POP)

Es un protocolo usado para descargar mensajes que se encuentren almacénanos en un servidor de correo sin necesidad de conexión. Es diseñado con el objetivo de recibir gestionar, acceder y transferir correos entre un servidor y un cliente local.

Usa el puerto 110 en su última versión más usada POP3 ya que es soportado por casi todos los clientes de correo electrónico; este protocolo es ideal cuando no se desea saturar servidores o gestionar cuentas simultáneamente.

g) Protocolo Simple de Administración de Red (SNMP)

Es un protocolo de arquitectura cliente – servidor que supervisa dispositivos en red, servidores, estaciones de trabajo; de tal manera que busque y resuelva problemas para planear su crecimiento.

Actualmente, este protocolo ofrece su última versión 3, la cual detalla ventajas en el tema de seguridad ya que es de gran importancia en el estudio y gestión de redes.

h) Protocolo de Trasferencia de Hipertexto (HTTP)

Es un protocolo de arquitectura cliente – servidor, sin estado ya que no guarda información de ninguna conexión anterior, permite distribuir y compartir información mediante páginas web. Es usado en el servicio de Internet WWW (WorldWideWeb).

Usa el puerto 80 por defecto, siendo su función principal el transferir información de texto con formato o sin formato, sonido, video, imágenes, entre otros. Los archivos que maneja este protocolo son planos a través de comandos HTML (Lenguaje de Marcas de Hipertexto) que son interpretados por el navegador como formateo de datos.

Por otro lado, tiene su versión HTTPS, se trasmite usando el puerto 443 ofreciendo mayor seguridad al momento de navegar por internet ya que confirma si nos encontramos en una página segura o no.

i) Protocolo de Configuración Dinámica de Host (DHCP)

Es un protocolo de arquitectura cliente – servidor que usa los puertos 67 UDP y 68 UDP respectivamente. Su función principal es asignar parámetros de una configuración IP dinámicamente a todos

los dispositivos que se encuentren dentro de una red local y así lograr simplificar la administración de una red.

Básicamente, es diseñado con el objetivo de sustituir al protocolo BooTP con algunas mejoras las cuales incluye el ahorro de tiempo mediante la gestión de direcciones IP, estas asignaciones son temporales ya que tienen cierto tiempo de validez y renegociando los paramentos de red.

j) Protocolo de Acceso a Mensajes de Internet (IMAP)

Es un protocolo que permite el acceso a mensajes de correo electrónico que se encuentran en un servidor a través del internet.

Actualmente, empresas como Google, Yahoo, Hotmail, entre otros; ofrecen este servicio de manera gratuita y sin ánimos de lucro. No necesita de aplicaciones para consultar correos, ni usar discos duros locales ya que toda la información se guarda en servidores hasta que el usuario decida tomar acciones como eliminarlos.

3.4 Ataques Comunes en los 7 Niveles en el Modelo de Interconexión de Sistemas Abiertos (OSI)

3.4.1 Capa Física

Además de ser el nivel más bajo del modelo OSI, este nivel no se encuentra exento de ataques físicos que pueden provocar grandes daños directa o indirectamente hacia la empresa.

Los entornos físicos pueden llegar a ser muy inciertos por lo que generalmente para un atacante va a resultar más fácil vulnerarlo afectando uno de los principales pilares de la información la disponibilidad. Dentro de este apartado existe amenazas de tipo factores naturales (incendios, inundaciones, terremotos, huracanes), factores humanos (robo y/o perdida de información, energía, dispositivos informáticos, entre otros), destrucción de propiedad privada, sabotajes internos y externos.

Los ataques hacia las autenticaciones y controles de acceso de dan por daños provocados por factores humanos internos ya sea de manera intencional o fortuita hacia el entorno informático, no conciencia de seguridad informática, vandalismo, estafas, elevación y abuso de privilegios que buscan corromper la disponibilidad, confidencialidad e integridad de la información.

Para los medios de trasmisión los principales ataques son hacia los canales guiados e inalámbricos por la cual viaja la información porque puede ser interrumpido u obstaculizado por el entorno, es decir pinchados de cables,

interferencias que destruyen señales, atenuación que limitan distancias, perturbaciones en la trasmisión (ruido), intercepción de cables, entre otros.

Para los medios físicos de almacenamiento y procesamiento de información como los servidores, cintas magnéticas, USB, y otros; pueden ser robados, perdidos y/o destruidos por factores humanos de manera intencionada.

Mientras que en “Cloud Computing” puede existir pérdida o fuga de información, secuestro de sesiones, accesos no autorizados, denegaciones de servicios, entre otros.

3.4.2 Capa Enlace de Datos

3.4.2.1 ARP Spoofing

Es una técnica usada para infiltrarse en una red Ethernet conmutada, la cual permite al atacante monitorizar paquetes de datos en una red de área local, además de poder modificar el tráfico. (Costas Santos, Seguridad y Alta Disponibilidad, 2014).

El principal objetivo de ARP Spoofing es enviar mensajes ARP falsos o falsificados a los equipos de una LAN, asociando la dirección MAC del atacante con la dirección IP de otro equipo, como una puerta de enlace (Gateway). De esta manera cualquier tráfico dirigido a la dirección IP de este equipo suplantado (Gateway), será enviado al atacante, en lugar de su destino real. El atacante, puede elegir entre reenviar el tráfico a el equipo real o modificar los datos antes de reenviarlos.

3.4.2.2 ARP Poisoning

Es un ataque de tipo envenenamiento el cual genera peticiones y respuestas ARP las cuales se encuentran modificadas, el principal objetivo es asociar la dirección MAC del atacante con su respectiva dirección IP, de esta manera el trafico pasara por la máquina del atacante y redirigirlo hacia la maquina final.

3.4.2.3 ARP Hijacking o Proxying

Este tipo de ataque se basa en ARP Spoofing, su principal objetivo es redirigir el flujo de las tramas entre dos dispositivos hacia un equipo propio.

Para realizar un ARP Hijacking, el atacante debe hacer creer a la víctima que la dirección MAC de la máquina con la que se quiere comunicar es el atacante directo; después hace creer a la otra víctima (destino) que la MAC de la máquina con la que se quiere comunicar es la del atacante y finalmente, reenviar la información a sus respectivos destinos una vez procesada por él. (Inteco, 2016).

3.4.2.4 Hombre en el Medio (MitM)

MitM, es un ataque basado en Spoofing, consta como un caso específico de interceptación y modificación de identidad. Un atacante supervisa la comunicación entre dos partes, falsifica las identidades de los extremos y por la tanto recibe el tráfico en los dos sentidos (Costas Santos, Seguridad y Alta Disponibilidad, 2014).

3.4.2.5 Denegación de Servicio ARP

(Inteco, 2016) es un ataque basado en Spoofing; siendo su función principal hacer creer a la víctima que su dirección IP se encuentra asociada a una dirección MAC la cual es falsa, entonces cada vez que la víctima desee comunicarse con dicha dirección IP; el dispositivo switch hace que el tráfico se dirija a un sistema que no existe y por tanto que no llegue a su destino, de esta manera la victima perderá la comunicación con esa dirección IP en la red interna; sin embargo, si dicha dirección IP es la de su puerta de acceso, perderá la conexión con el exterior.

En otras palabras, este es el ataque más básico, y para esto tan solo el atacante debe enviar de forma regular paquetes de respuesta ARP especialmente manipulados, con una asociación que sea falsa.

3.4.2.6 ARP Sniffing

(Inteco, 2016) es un ataque basado en Spoofing, consiste en hacer pensar a la víctima que una determinada dirección IP se encuentra asociada a la su propia dirección MAC.

El atacante indica a la víctima que una dirección IP está asociada a su MAC, por lo tanto, todo ese tráfico es redirigido a el mismo, normalmente en un ataque ARP Sniffing, la tarjeta de red rechaza estos datos. Sin embargo, aunque la dirección MAC coincida, la dirección IP del atacante es completamente diferente a la del destino con el que la víctima quiere ponerse en contacto.

En esta parte, donde entra el modo promiscuo de la tarjeta de red; ya que si el atacante, aparte de enviar de manera regular los paquetes (manipulados) de respuesta ARP, puede ver la información que le llega y procesarla. Es así, como puede obtener la información que la víctima cree estar viendo en otro sistema.

3.4.2.7 MAC Flooding

(Gómez Vietes, 2013) es un ataque que provoca desbordamientos de las tablas de memoria (Content Addresable Memory (CAM)) de un dispositivo switch para conseguir que pase a funcionar como un simple hub, de tal forma que retransmita todo el tráfico que recibe a través de los puertos. En este sentido, al no poder "recordar" que equipo se encuentran conectados a sus distintos puertos por haber sido borrados de sus tablas de memoria.

3.4.2.8 VLAN Hopping

(Gómez López, Castro Simón, & Guillén Núñez, 2014) explican que es una técnica que permite tener acceso al tráfico de red de otra Virtual LAN (VLAN), la cual es normalmente inaccesible cuando se encuentra bien configurada.

Este tipo de ataque se basa en "Switch Spoofing", es decir donde el atacante activa su interfaz en modo troncal e imita el comportamiento de un Switch, sin embargo, para efectuar este ataque, el atacante únicamente tiene que escuchar el tráfico de red filtrando por os paquetes DTP, y en el caso de que existan dichos paquetes, es posible realizar "Saltos" de un VLAN a otra sin restricciones.

3.4.2.9 Doble Etiquetado

Este tipo de método aprovecha una VLAN nativa que se envía sin ninguna etiqueta a través de enlaces trocales conocidas como 802.1Q, entonces cuando crea una VLAN falsa, el atacante envía tráfico unidireccional directo hacia el otro servidor VLAN de esta manera agrega dos etiquetas hacia las VLAN nativas y VLAN destinos. Los Switches realizan un solo nivel de desencapsulación; este tipo de ataque funciona si la VLAN nativa es la misma que la del atacante sin tomar en cuenta si el puerto del atacante esta desactivado el Tracking.

3.4.2.10 Denegación de Servicio basado en STP

Son aquellos que fuerzan a los dispositivos participantes en STP a recalcular sus caminos, debido a esto provoca una gran inestabilidad en la red, cada uno de los switches se ven obligados a consumir tiempo de CPU y memoria. (Dávila, 2012).

3.4.2.11 Inundaciones DHCP

En este tipo de ataques es probable que se produzcan bucles en la red provocando una caída y se empiece duplicar paquetes, congestionando la red y una total degradación.

Este tipo de ataque es simple, ya que se basa en enviar miles de paquetes BPDU con la dirección MAC origen generados aleatoriamente. (Dávila, 2012).

3.4.3 Capa Enlace de Red

3.4.3.1 Recopilación de Información (Networking Footprinting)

(McClure, Scambray, & Kurtz, 2010) explica que la recopilación de información sistemática y metódica permite a los atacantes crear un perfil casi completo de la seguridad de la organización que desean atacar, mediante el uso de herramientas y técnicas.

De esta manera, el atacante sabe a qué se dedica la organización haciendo que los riesgos sean más altos del entorno que los rodea y reduciendo toda esta información a rangos especifico como nombres de dominio, bloques de red, direcciones IP, entre otros.

Las herramientas para realizar este tipo de ataques pueden ser Whois, Google Hacking, People Search, SamSpade, entre otros.

3.4.3.2 IP Spoofing

(Gómez Vietes, 2013) es un tipo de ataque de suplantación de identidad, conocida como enmascaramiento de una dirección IP, mediante la cual un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático paras simular que proceden de un equipo distinto al que verdaderamente los ha originado.

Las herramientas para realizar este tipo de ataques pueden ser Netcat, Etherchange, los cuales hacen una búsqueda profunda de toda la información que pueda existir en la red.

3.4.3.3 Nuke

(Areitio, 2008) este tipo de ataque es muy antiguo realizando un DoS, se beneficia de alguna vulnerabilidad existente en cualquier servicio del sistema operativo de la víctima provocando un error, colgando el equipo o consumiendo recursos. El atacante no necesita ningún tipo de infraestructura o ancho de banda para poder realizarlo, ya que tan solo con enviar unos pocos paquetes IP logra colgar el sistema remoto.

3.4.3.4 Ping de la Muerte

Este tipo de ataque consiste en que un atacante envía un paquete de ping (IP) de tamaño superior a los 65.536 bytes, provocando que la maquina se reinicie o se cuelgue, como él envió de este paquete es muy grande ocasiona que el buffer de memoria se desborde. (Gómez Vietes, 2013)

3.4.3.5 Land

Este tipo de ataque se da a un error de implementación de protocolos en algunos sistemas Windows, consiste en colgar un equipo vulnerable mediante el envío de una serie de paquetes maliciosamente construidos, en los que la dirección y el puerto de origen son idénticos a la dirección y puerto de destino. (Gómez Vietes, 2013)

3.4.3.6 Supernuke o Winnuke

Es un ataque contra algunos sistemas Windows, que se quedan colgados o disminuyen drásticamente su rendimiento al recibir paquetes

UDP manipulados, es decir fragmentos de paquetes Out of Band dirigidos contra el puerto 137. (Gómez Vietes, 2013)

3.4.3.7 Teardrop

(Gutiérrez del Moral, 2014) es un tipo de ataque que consiste en el envío de paquetes fragmentados de manera incorrecta. Los equipos vulnerables que no hayan sido convenientemente parcheados se cuelgan al recibir este tipo de paquetes maliciosos.

3.4.3.8 ICMP Flood

(Gutiérrez del Moral, 2014) es una técnica Denied of Service, siendo su principal objetivo agotar el ancho de banda de la víctima; consiste en enviar de forma continua un número elevado de paquetes ICMP Echo request (ping) hacia la víctima, de manera que esta responde con paquetes ICMP Echo reply (pong); suponiendo una gran sobrecarga de la red y el sistema de la víctima.

3.4.3.9 Smurf o Pitufo

(Gutiérrez del Moral, 2014) es una variación de ICMP Flood, amplifica considerablemente los efectos de un ataque ICMP; se divide en tres partes denominados atacante, intermediario y víctima. Este tipo de ataque tiene por objetivo enviar grandes cantidades de tráfico ICMP a la dirección de broadcast.

Entonces, el atacante dirige paquete ICMP de tipo “Echo request” (ping) a una dirección IP de broadcast, usando como dirección IP origen, la

dirección de la víctima; se espera que los equipos conectados respondan a tal petición usando un “Echo Reply” al equipo de la víctima.

Cuando se mencionó que el ataque era amplificado lo que se explica es que la cantidad de respuestas obtenidas, es la cantidad de equipos de red que pueden responder; estas respuestas son dirigidas a la víctima intentando colapsar los recursos de la red.

3.4.4 Capa Enlace de Transporte

3.4.4.1 Fingerprinting

(Gómes Vieites, 2014) es un conjunto de técnicas y habilidades que permiten extraer toda la información posible sobre un sistema. Los atacantes usan esta información para tratar de explorar las vulnerabilidades potenciales del sistema en cuestión.

3.4.4.2 TCP Connect Scanning

(Gómes Vieites, 2014) , es la técnica más sencilla de escaneo, consiste en el envío de un paquete de intento de conexión al puerto de servicio que se pretende investigar para comprobar, de este modo el sistema responde aceptando la conexión o denegándola. Sin embargo, esta técnica es fácilmente detectable, por lo que se puede configurar al sistema informático para que no responda a este tipo de acciones.

3.4.4.3 TCP SYN Scanning

(Gómes Vieites, 2014), es una técnica de escaneo que intenta abrir la conexión con un determinado puerto para que en cuanto se confirma que

dicho puerto está abierto, envíe un paquete “RST” que solicita terminar la conexión. Esta técnica no es registrada por algunos servidores.

3.4.4.4 TCP FIN Scanning

(Gómes Vieites, 2014), conocida como “Escaneo Oculto de Puertos”, ha sido propuesta como una técnica de escaneo que trata de evitar ser registrada por los cortafuegos y servidores de una organización.

Es una técnica muy avanzada, el cual consiste en el envío de un paquete “FIN” de exploración, de forma que si el puerto esta abierto, el servidor ignorara este paquete, mientras que, si el puerto está cerrado, el servidor responderá con un paquete “RST” ante un paquete “FIN”, independiente de si el puerto encuentra abierto o cerrado.

3.4.4.5 TCP NULL Scanning

(Gómes Vieites, 2014), esta técnica que envía un paquete TCP con todos los Flags a cero en su cabecera

3.4.4.6 TCP ACK Scanning

(Gómes Vieites, 2014), esta técnica permite determinar si el cortafuego actúa como un filtro de paquetes o mantiene el estado de las sesiones.

3.4.4.7 TCP Fragmention Scanning

(Gómes Vieites, 2014), es una técnica de escaneo que recurre a la fragmentación de paquete TCP.

3.4.4.8 TCP Windows Scanning

(Gómes Vieites, 2014), permite reconocer determinados puertos abiertos a través del tamaño de la ventana de los paquetes TCP.

3.4.4.9 Inundación UDP

(Castro , 2013), son ataques de denegación de servicios sobre los UDP, siendo estos no orientados a la conexión; si se inunda a la víctima con paquetes UDP enviados a puertos aleatorios, este tendrá que responder a ellos con paquetes ICMP Destination Unreachable.

3.4.4.10 SYN Flood

(Gómez Vietes, 2013) se basa en el incumplimiento de las reglas básicas del protocolo TCP por parte del cliente. Al establecer la conexión, se envía una petición de conexión al equipo de la víctima, pero no se responde a la aceptación de la conexión por parte de este equipo (se facilita la dirección IP falsa).

El equipo de la víctima deja la conexión en estado de "semi - abierta", consumiendo de este modo recursos de la máquina. Las conexiones "semi – abiertas" caducan al cabo de cierto tiempo, libreando sus recursos. Sin embargo, si se envían muchas peticiones de conexión siguiendo el ataque SYN Flood, se colapsarán los recursos del equipo víctima, que no podrá atender nuevas conexiones legitimas.

3.4.4.11 Connection Flood

(Gómez Vietes, 2013) es un tipo de ataque que consiste en intentar establecer cientos o miles de conexiones simultaneas contra un determinado servidor víctima del ataque, con lo que se consumen sus recursos y se degrada de forma notable su respuesta ante usuarios legítimos.

3.4.5 Capa Enlace de Sesión

3.4.5.1 NetBIOS

Es un ataque que permite compartir recursos de una computadora a otra siempre y cuando tengan habilitado los puertos 137,138 o 139; de tal manera que los atacantes ingresan de manera sencilla y obtener un control total permitiendo que los mensajes puedan pasar de ida y regreso en la red.

3.4.5.2 Llamada de Procedimiento Remoto

Esta tecnología creada por Sun MicroSystems ayuda puede ser vulnerable desde equipos "Unix" los cuales permiten realizar procedimientos y acciones de manera remota desde otro equipo.

Para realizar este tipo de ataque tan solo se debe obtener la lista de servicios activos mediante el comando "#rpcinfo –p (Dirección IP a Atacar)".

3.4.6 Capa Enlace de Presentación

3.4.6.1 Fuerza Bruta

Es un tipo de ataque que intenta romper cifrados mediante pruebas de todas las posibles combinaciones, es posible descifrar usuarios y contraseñas para autenticar un usuario. Este tipo de ataque requiere tiempo y diferentes recursos por lo que, si su contraseña es larga, esta tiende a crecer de manera exponencial.

3.4.6.2 Diccionario

Es similar al ataque de fuerza bruta, con la diferencia que para descifrar o conseguir una contraseña se usan posibles palabras, generalmente son tomadas de un glosario de palabras y nombres. Si dicha clave se encuentra en el diccionario se consigue reducir el tiempo necesario para encontrarla.

3.4.6.3 Textos Cifrados

El atacante dispone de varios textos cifrados y su principal objetivo es recuperar los textos claros y buscar claves utilizadas en diferentes sistemas criptográficos.

3.4.6.4 Textos Claros Conocidos

El atacante conoce o puede adivinar alguna parte de textos cifrados, siendo su principal objetivo determinar la clave utilizada para descifrar el resto del texto, entre los más habituales textos conocidos tenemos cabeceras de paquetes, cabeceras en mensajes de correos electrónicos, entre otros.

3.4.7 Capa Enlace de Aplicación

3.4.7.1 Sniffing

Es una técnica basada en “escucha” la cual permite obtener grandes cantidades de información que circulan por una red; todo este proceso se lo realiza mediante aplicaciones los cuales capturan, interpretan y almacenan los paquetes de datos para proceder a su análisis como contraseñas, correos electrónicos, datos crediticios, bancarios, entre otros.

3.4.7.2 Denegaciones de Servicios (DoS)

Es un ataque cuyo principal objetivo es lograr que un servicio o recurso quede completamente inaccesible o colapse completamente para usuarios legítimos dentro de una red.

Puede ser realizado de muchas maneras derivándolos en dos situaciones; la primera es denegar servicio por saturación, es decir inundar a un equipo con solicitudes para que no puedan responder a las reales y la segunda es denegar mediante la explotación de vulnerabilidades los cuales se aprovechan de estas para hacer inestable al sistema.

3.4.7.3 Denegaciones Distribuidas de Servicios (DDoS)

Este tipo de ataques se basa en inhabilitar un servidor, infraestructura o servicio mediante la sobrecarga del ancho de banda del mismo servidor o agotar sus recursos disponibles; para lograr esto, se envían múltiples peticiones desde varios puntos de la red.

3.4.7.4 SMPT Flood

Es un ataque que se basa en él envió masivo de mensajes de correos provocando saturaciones de los servidores de correo electrónico derivando en DDoS.

3.4.7.5 DNS Spoofing

Es un ataque que permite alterar las direcciones de los servidores DNS para mantener un control total de las consultas que realiza la víctima y así lograr que apunten a servidores maliciosos. Uno de los más grandes impactos que puede realizar este tipo de ataques es la falsificación de sitios para robar credenciales de la víctima.

3.4.7.6 Telnet

Es un ataque que permite la autenticación de una víctima mediante solicitudes de usuarios y contraseñas que se transmiten a atreves de la red. Para lograr este tipo de ataque se debe usar técnicas de Sniffing los cuales verifiquen que los puertos de "Telnet" se encuentren abiertos y de esta manera lograr su acceso.

3.4.7.7 Ataque al protocolo SSH

Es un ataque equivalente a "Telnet" pero de manera segura, sin embargo, el hecho de cifrar el usuario y contraseña no impide que un atacante que las conozca acceda al servicio.

3.4.7.8 Ataque por Inyección

Es un ataque que permite la modificación de una cadena de consulta de base de datos mediante la "inyección" de código en su consulta. Es muy fácil de ejecutar ya que tan solo requiere de una sola computadora y conocimientos sólidos en bases de datos.

3.4.7.9 Ataque HTTP y HTTPS

Este tipo de ataque posibilita la entrega de información por parte de los usuarios mediante el puerto 80 y la ejecución remota de código en la parte del servidor. Realizar este tipo de ataque puede desembocar en denegaciones de servicios, inestabilidad o invalidez a todo un sistema.

3.5 Aplicación de los ataques más comunes en los 7 Niveles en el Modelo de Interconexión de Sistemas Abiertos (OSI)

Partiendo de la importancia de los recursos informáticos para todo tipo de empresas se realiza un análisis de los ataques más comunes que se puede producir en el modelo OSI. A continuación, se detalla cómo se producen y sus maneras de prevenirlas.

3.5.1 ARP Poisoning – Hombre en el Medio

ARP Poisoning y MitM se producen a nivel 2 del Modelo OSI (Enlace de Datos), ambos se encuentran estrechamente ligados para producir ataques de tipo de falsificación de direcciones MAC dentro de una red LAN. Como resultado, el atacante vincula la dirección MAC con la dirección IP de la víctima.

Se ha utilizado el sistema operativo “Kali Linux” como atacante y la máquina virtual “Windows 7” como víctima, siendo estas herramientas útiles para simular cualquier tipo de ataque hacia la red.

“Kali Linux” posee diversas herramientas para provocar cualquier tipo de ataque en este caso se usará “Ethercap” debido a que cuenta con variedad de ataques que deben pasar por MitM con el objetivo de interponerse entre la comunicación de dos máquinas y que todo el tráfico pase por la máquina del atacante y poder desencriptar cualquier tipo de información.

Cuando el ataque inicia se debe seleccionar las direcciones IP objetivos (victimas) ya que la herramienta Ethercap es capaz de identificar cualquier dirección IP que se encuentre en la red; se realiza un “Sniff” profundo a dichas direcciones seleccionadas. Como se puede observar en la Ilustración 3-6, se utiliza el analizador de tráfico “Wireshark” el cual permitirá observar toda la información que atraviesa por la red; de esta manera se realiza un filtro de los paquetes ARP enviados a la maquina víctima.

A continuación se demuestra que el ataque se realizó con éxito ya que la dirección MAC de la víctima fue falsificada sin ningún inconveniente (VER ANEXO 8.1). Todas estas acciones desembocan en diversos ataques como denegar servicios, secuestros de sesiones, interceptación o modificación en el tránsito de datos, entre otros.

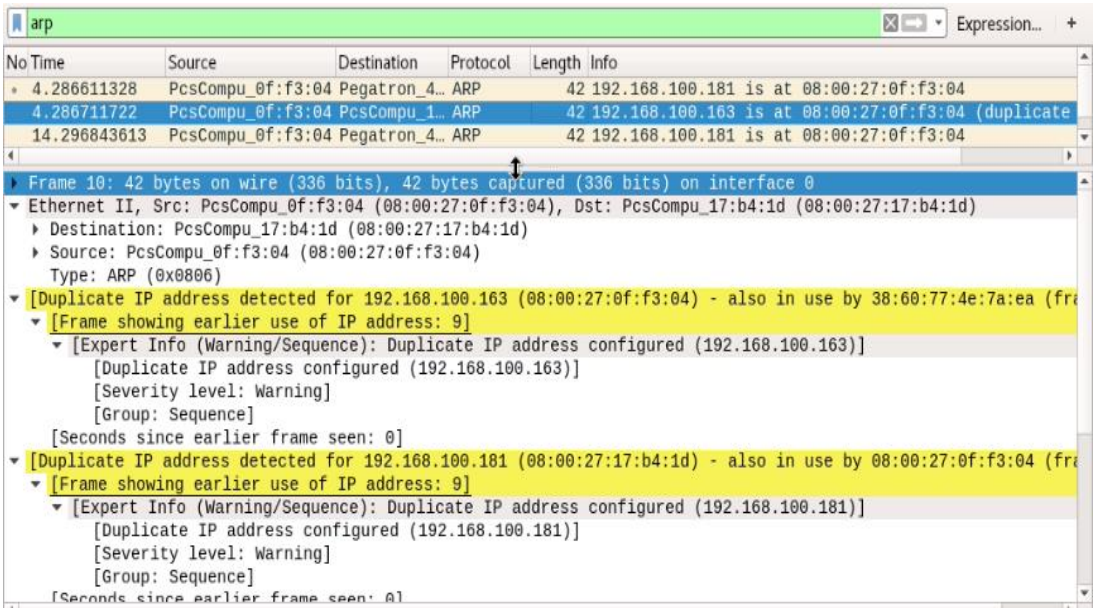


Ilustración 3-6: *"Visualización del ataque MitM y ARP Spoofing en Wireshark",*

3.5.1.1 Medios de Prevención

3.5.1.1.1 Trabajar con rutas estáticas con los equipos de red de tal manera que logre invalidar cualquier tipo de información que trata de cambiar la cache ARP, a pesar de que es una solución simple esta asegura que la puerta de enlace predeterminada sea realmente la de la red y no de un atacante. Se debe tomar en cuenta que esta media se usa en redes pequeñas y no tan complicadas debido a que muchas veces una red puede tener grandes cantidades de terminales que sería muy laborioso ingresar cada una de las direcciones IP y MAC; si embrago, brinda una alta seguridad para el protocolo ARP. Para configurar las tablas ARP (VER ANEXO 8.1).

3.5.1.1.2 Dividir la red en subredes a través de los routers o redes virtuales, de tal forma que se pueda reducir y controlar el tráfico de un

equipo hacia otro mejorando el rendimiento de la misma, brindando mayor seguridad, controlando su crecimiento, entre otros.

3.5.1.1.3 Usar protocolos de tipo RARP[12] el cual permite realizar consultas de las direcciones MAC con el objetivo de devolver sus respectivas direcciones IP, en el caso de que devuelva más de una dirección IP quiere decir que dicha MAC fue clonada.

3.5.1.1.4 Cuando se utiliza los diferentes dispositivos de red la mayoría de switchs y routers ya cuentan con funcionalidades y características de seguridad contra este tipo de ataques, por lo que es necesario contar con personal capacitado para realizar las configuraciones y monitoreo respectivo.

3.5.1.1.5 Usar herramientas como "Arpwatch" que son soluciones libres para todo tipo de sistemas GNU/Linux la cual realiza un seguimiento de las direcciones IP y MAC, esta aplicación realiza un tipo de lo de los incidentes sospechosos, además se puede configurar para recibir cualquier tipo de alarma por medio de correo electrónico.

3.5.1.1.6 Usar herramientas como "Arpon" de tal manera que asegure el protocolo ARP, además esta aplicación evita ataques de enrutamiento usando tres tipos de técnicas de suplantación ARP

[12] **RARP:** Protocolo de Reverso ARP

conocidos como redes configuradas como SARPI[13], DARPI[14], HARPI[15].

3.5.1.1.7 Cabe resaltar que existen varias herramientas las cuales no son muy utilizadas pero ayudan de manera potencial la mitigación de este tipo de ataque como XArp[16].

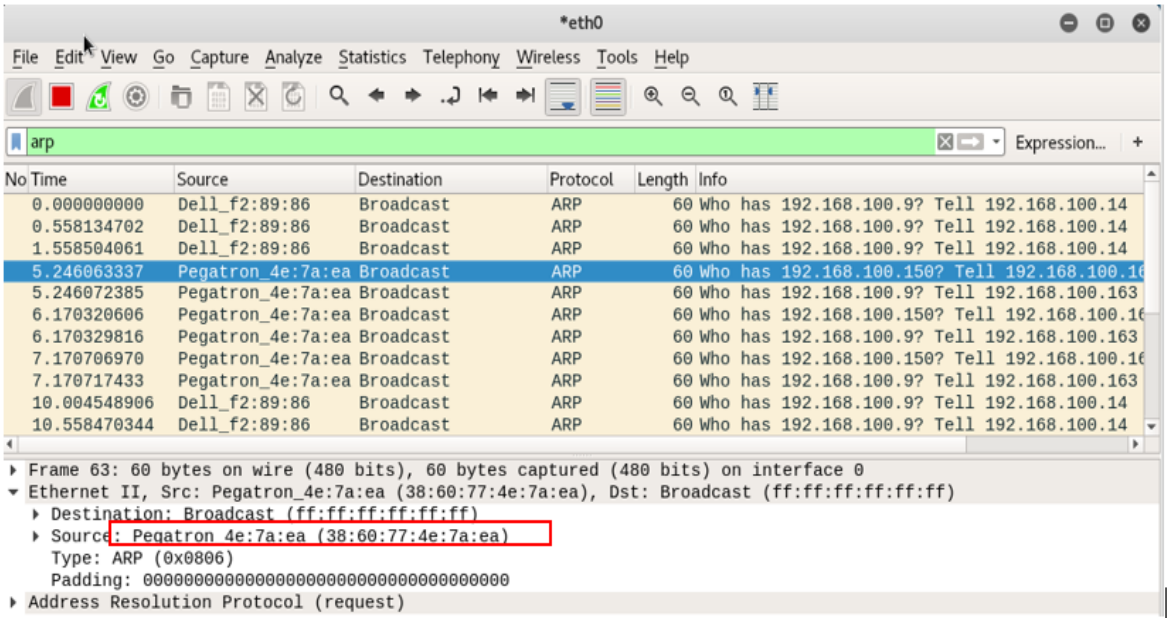


Ilustración 3-7: *"Visualización de la Mitigación MitM y ARP Spoofing a través de rutas estáticas"*

Como se puede observar en la Ilustración 3-7 se ha capturado el tráfico de la máquina a la cual se busca atacar nuevamente (victima), esta vez no ha tenido éxito ya que se ha establecido direcciones estáticas para que no pueda ingresar ninguna maquina diferente a las establecidas. (VER ANEXO 8.1).

[13] **SARPI:** Redes configuradas estáticamente.
[14] **DARPI:** Redes configuradas dinámicamente.
[15] **HARPI:** Redes configuradas estáticamente y dinámicamente.
[16] **XArp:** Advanced ARP Spoofing Detection (Detección de Suplantación de ARP Avanzada)

3.5.1.2 Resultados

Antes de realizar el ataque con su respectiva mitigación, se puede observar en la Tabla 3-2 cuales son las direcciones IP y MAC respectivamente:

	Dirección IP	**Dirección MAC**	**Sistema Operativo**
Atacante	192.168.100.166	38:60:77: 4E:7A: EA	Kali Linux
Victima	192.168.100.181	38:60:77: 4E:7A: EA	Windows 7

Tabla 3-2: *"Direcciones IP y MAC antes del Ataque MitM y ARP Spoofing"*

Sin embargo, después del ataque se suplanta la dirección MAC de la víctima, quedando de la forma:

	Dirección IP	**Dirección MAC**	**Sistema Operativo**
Atacante	192.168.100.166	38:60:77: 4E:7A: EA	Kali Linux
Victima	192.168.100.181	38:60:77: 4E:7A: EA	Windows 7

Tabla 3-3: *"Direcciones IP y MAC después del Ataque MitM y ARP Spoofing"*

Cuando la mitigación se realiza podemos observar Ilustración 3-7 que después de establecer direcciones estáticas por más que se intente el ataque no cambiará las direcciones originales quedando de la forma:

	Dirección IP	**Dirección MAC**	**Sistema Operativo**
Atacante	192.168.100.166	38:60:77: 4E:7A: EA	Kali Linux
Victima	192.168.100.181	38:60:77: 4E:7A: EA	Windows 7

Tabla 3-4*: "Direcciones IP y MAC después de la mitigación del Ataque MitM y ARP Spoofing"*

3.5.2 CDP –Denegación de Servicio

Este tipo de ataque se produce a nivel de enlace de datos, sin embargo, también involucra a varias capas como de aplicación para denegar cualquier tipo de servicio en salidas a Internet y capa de red debido a que el tránsito de datos pasa por routers. El diseño de red que se usará para este tipo de ataque se muestra en la Ilustración 3-8.

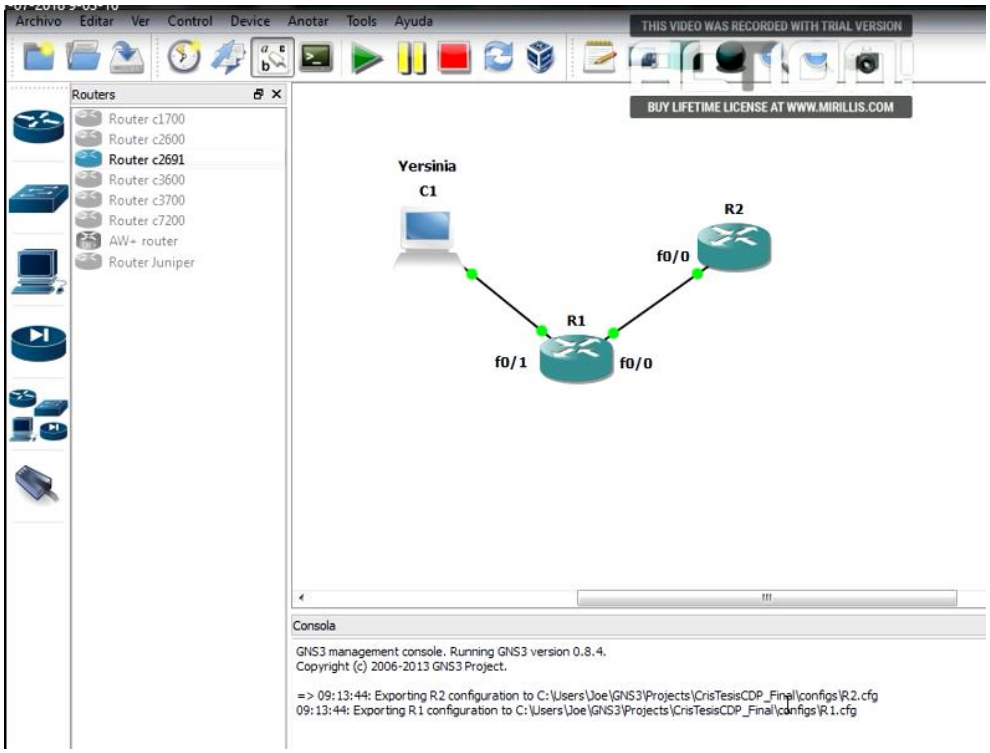


Ilustración 3-8: *"Diseño de Red CDP "*

Para simular este tipo de ataque, se utiliza el sistema operativo "Kali Linux" el cual es utilizado como atacante mientras que los routers serán las víctimas; cabe recordar que se utiliza la herramienta GNS 3 en su versión 1.4 para realizar la correcta configuración y manipulación de dichos routers. (VER ANEXO 8.2).

Por otro lado, Yersinia es la herramienta que ayudará a realizar una inundación de tabla CDP, los paquetes enviados no se encuentran encriptados entonces tienden a aumentar rápidamente lo que provoca una denegación de servicios. La mayoría de routers y switches tienen su CDP habilitado por default lo que provoca una vulnerabilidad muy grande para cualquier tipo de empresa.

Como se muestra a continuación, después de haber realizado este tipo de ataque con éxito, la Ilustración 3-9 e Ilustración 3-10 despliega toda la información que tiene CDP tomando en cuenta que este contiene toda la información sobre un dispositivo como las direcciones IP, versión de software, plataforma, VLAN nativa lo cual es de relevancia para el atacante.

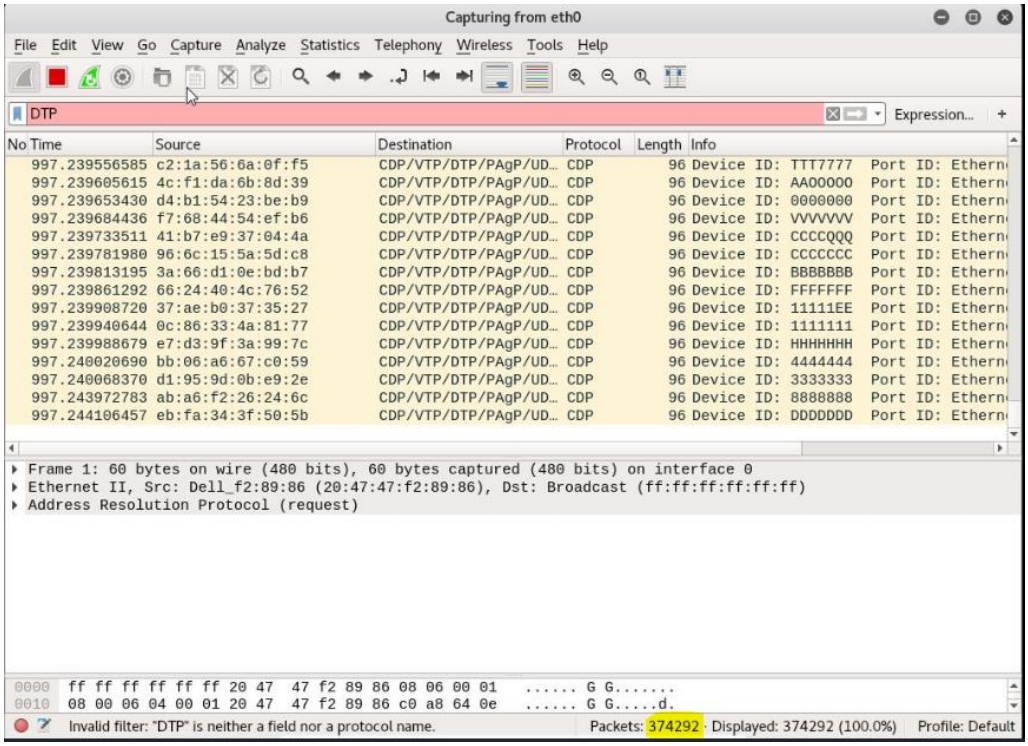


Ilustración 3-9: *"Ataque CDP y Denegación de Servicios"*

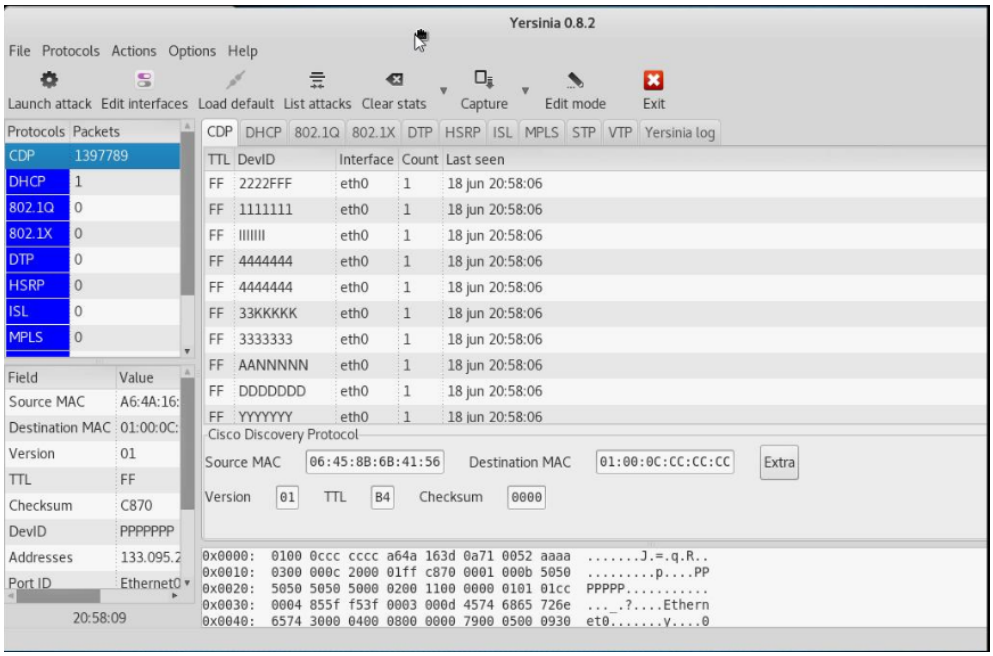


Ilustración 3-10: *"Log Ataque con Yersinia"*

3.5.2.1 Medios de Prevención

3.5.1.1.1 Para prevenir este tipo de ataque se debe deshabilitar las tablas CDP de los routers, para realizar estas acciones se digita los siguientes comandos *"no cdp run"* o *"no cdp enable"*. Sin embargo, en la actualidad no se ha mejorado dicho protocolo desde el punto de vista de seguridad (VER ANEXO 8.2).

3.5.1.1.2 Utilizar herramientas que permita analizar y observar todo el tráfico que pasa por los dispositivos de red, por ejemplo "Wireshark", este analizador permitirá observar cual es el comportamiento de las tramas, protocolos, origen y destino de cada uno de los paquetes.

3.5.1.1.3 Conocer profundamente cuales son los dispositivos de red más importantes para que se pueda configurar de manera correcta los routers y máquinas de tal forma que se reconozca rápidamente este punto vulnerable y corregirlo a tiempo, ya que puede provocar una gran inestabilidad en el sistema.

3.5.1.1.4 Reconocer cuales son dispositivos de red que necesiten tener habilitado este protocolo ya este es necesario para conocer cuál es la información de los routers y switches que se encuentran conectadas localmente.

3.5.1.1.5 Cabe destacar que la persona que realiza la configuración de los routers o switches debe tener conocimiento sobre lo que está realizando y sobre cómo funciona el protocolo CDP ya que sin esta información simplemente al momento de realizar configuraciones puede dejar inválido a los dispositivos.

Como se puede observar en la Ilustración 3-11, se ha mitigado con éxito este tipo de ataque, la herramienta “Wireshark” capturó el trafico un antes y un después de realizar estas acciones. El sistema se ha estabilizado y no permitirá ningún tipo de inundación CDP.

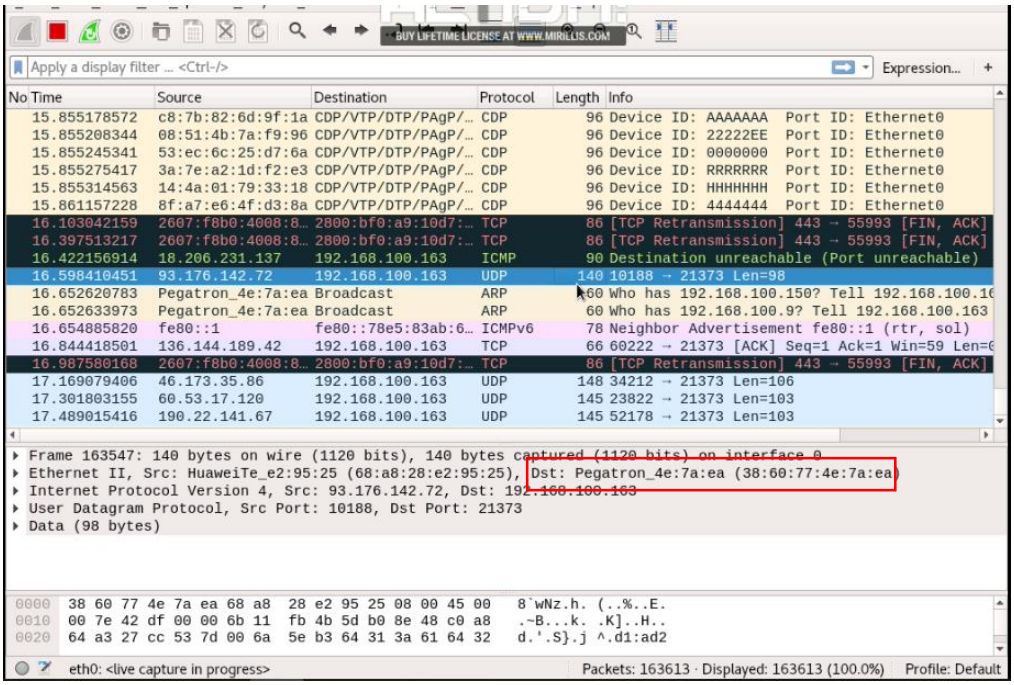


Ilustración 3-11: *"Visualización de la mitigación del Ataque CDP – Denegación de Servicios"*

3.5.2.2 Resultados

La Ilustración 3-9 muestra cómo las tablas CDP de los routers se inunda con información no relevante causando inestabilidad en el sistema incluso denegaciones de servicios, debido a que envía cantidades de información a gran velocidad. Sin embargo, cuando se toma medidas sobre este ataque se observa en la Ilustración 3-11 que se estabiliza el sistema tan solo digitando los comandos mencionados en las medidas preventivas y el tráfico en la red continua su curso con normalidad, detallándonos direcciones MAC, IP, versiones de protocolo, origen y destino de los paquetes, entre otros.

3.5.3 DHCP – Hombre en el Medio

Este tipo de ataque se produce a nivel de enlace de datos, involucra a la capa de aplicación para denegar servicios, la capa de red ya que se debe configurar routers y switchs que trabaja conjuntamente para poder simular este ataque como muestra la Ilustración 3-12.

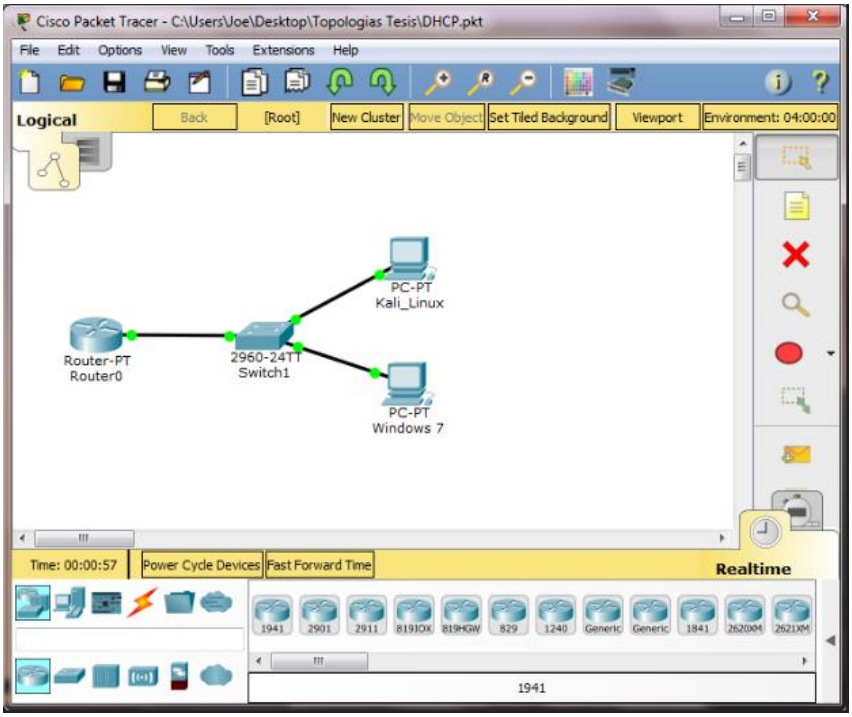


Ilustración 3-12: *"Diseño de Red DHCP – Denegación de Servicio"*

Para simular un ataque de tipo DHCP se utiliza el sistema operativo "Kali Linux" y la herramienta Yersinia con el objetivo de solicitar direcciones simplemente hasta que el servidor se sature como se observa en la Ilustración 3-13.

Este ataque simplemente tiene como objetivo producir bucles en la red provocando caídas e inestabilidades en el sistema, además congestiona la red enviando miles de paquetes BPDU con la dirección MAC origen generados aleatoriamente generando denegaciones de servicios, inestabilidad en los recursos incluso dejar invalido cualquier dispositivo de red. (VER ANEXO 8.3).

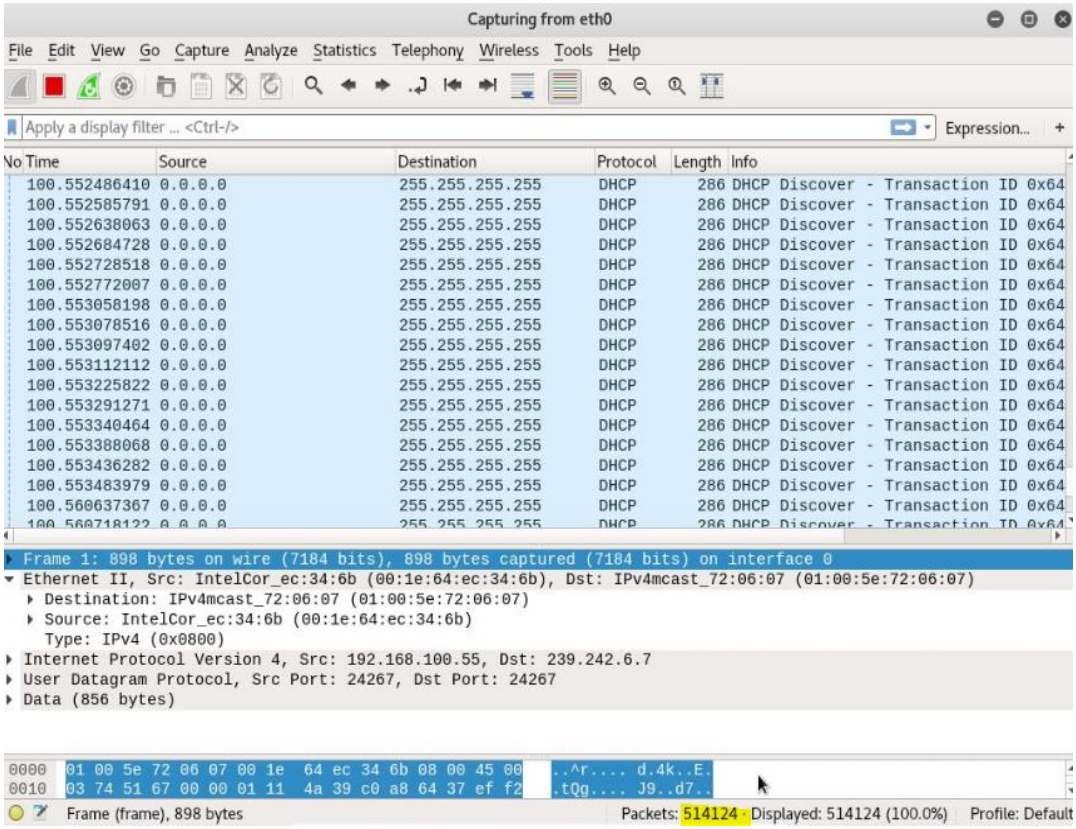


Ilustración 3-13: *"Ataque con Yersinia DHCP – Denegación de Servicio"*

3.5.3.1 Medios de Prevención

3.5.1.1.1 Para prevenir este tipo de ataque se debe establecer una cierta característica de seguridad la cual trabaja como un firewall entre dos hosts no confiables y servidores DHCP. Esta mitigación tiene el nombre de "DHCP Snooping" de modo que el flujo de información se pueda estabilizar configurando el switch y las VLAN mediante un conjunto de comandos (VER ANEXO 8.3).

3.5.1.1.2 Actualmente los switches Cisco cuantas con la solución "Snooping" integrada, la cual sirve para mitigar este tipo de ataque, siendo su funcionamiento muy simple ya que solo se debe declarar el puerto al cual se cuenta conectado el DHCP.

3.5.1.1.3 Usar “Listas de Control de Acceso” para poder bloquear el puerto 68, siento este el puerto destino que utiliza el servidor DHCP para poder comunicarse.

3.5.1.1.4 Detener un DHCP falso mediante el bloqueo del puerto 68 por medio de una pasarela de red o firewall.

3.5.1.1.5 Usar analizadores de tráfico como “Wireshark” de tal manera que ayude a alertar sobre cualquier tipo de situación que se pueda presentar realizando varios filtros para buscar paquetes, tramas, protocolos diferentes al configurado a nuestro servidor DHCP.

Como se muestra en la Ilustración 3-14, después de configurar los routers y el switches se puede observar que el ataque se ha mitigado con éxito, se utiliza la herramienta Wireshark para analizar nuevamente el tráfico que pasa por la red deduciendo que empieza a bloquear cualquier DHCP no autorizados.

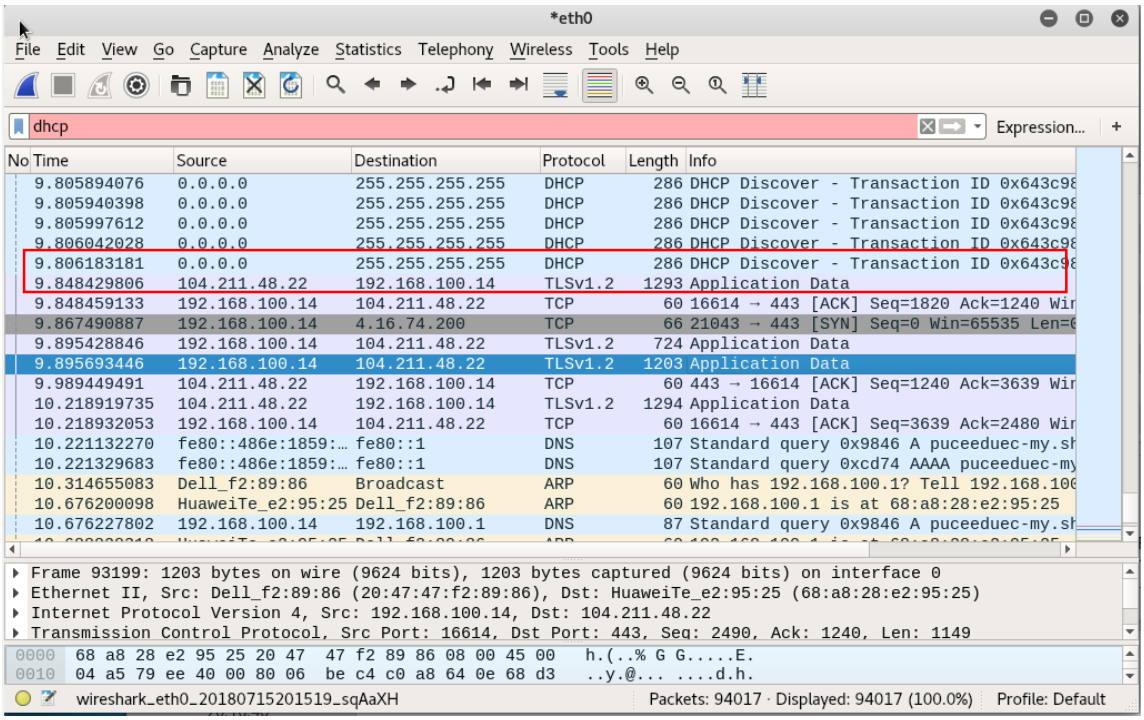


Ilustración 3-14: *"Visualización de la Mitigación del Ataque DHCP – Denegación de Servicio"*

3.5.3.2 Resultados

Al de realizar este ataque con su respectiva mitigación se puede observar en la Ilustración 3-13 cómo se llena las tablas DHCP con direcciones MAC aleatorias y a grandes velocidades causando inestabilidad al sistema. Sin embargo, cuando se toma medidas sobre este ataque se observa en la Ilustración 3-14 que el tráfico en la red se estabiliza y empieza a captar toda la información sin ningún problema. (VER ANEXO 8.3).

3.5.4 Syn Flood

Para realizar este tipo de ataque es necesario realizar un escaneo de los puertos que se encuentre disponibles en la red, se utiliza la herramienta “Zenmap” y de esta manera se lista los puntos más vulnerables de un equipo.

Syn Flood es un tipo de ataque de inundación que se basa en el incumplimiento de las reglas básicas del protocolo TCP en el nivel de trasporte por parte del cliente; debido a que, al establecer una conexión se envía una petición de conexión al equipo de la víctima, enviando muchas peticiones de conexión de esta manera logra colapsar los recursos del equipo víctima y no podrá atender nuevas conexiones legitimas. Todo este ataque desemboca en denegaciones de servicio ya que el sistema consumirá todos sus recursos.

Como se puede observar en la Ilustración 3-15, la herramienta “Wireshark” nos muestra que el equipo victima empezó a consumir todos los recursos de manera desproporcionada logrando que el equipo sea más lento, sin internet y muchas veces que no responda de manera adecuada. (VER ANEXO 8.4)

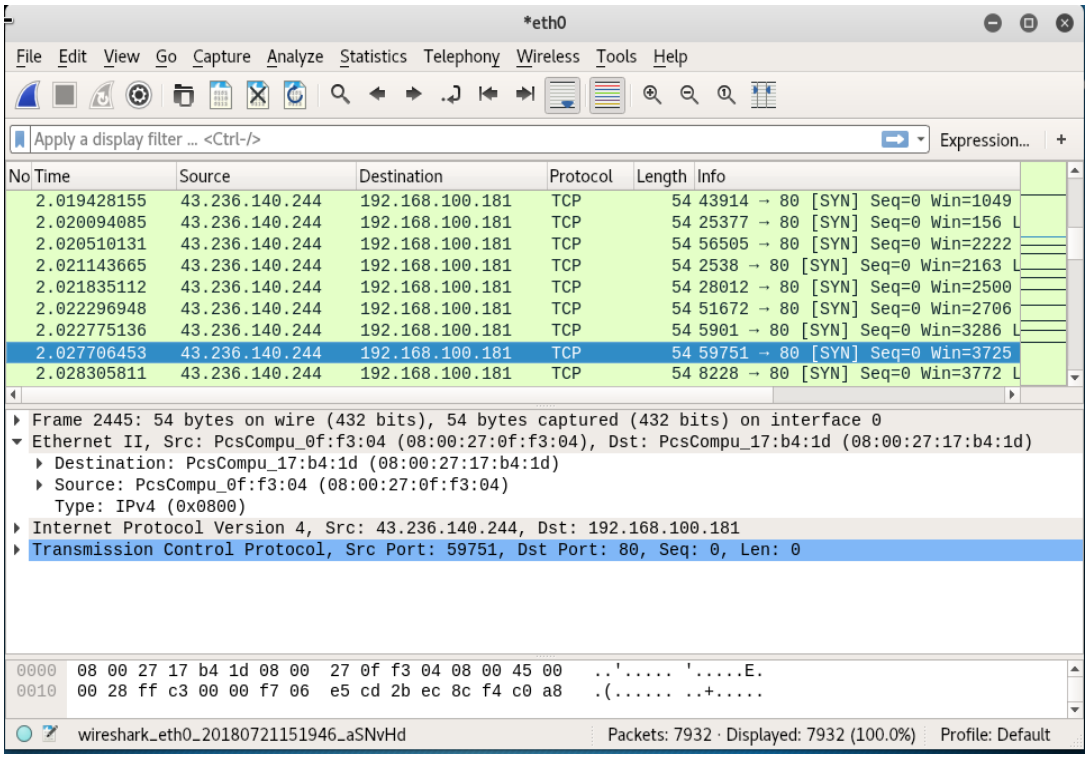


Ilustración 3-15: *"Visualización del Ataque Syn Flood en Wireshark"*

3.5.4.1 Medios de Prevención

3.5.4.1.1 Para prevenir este tipo de ataque se utiliza la herramienta Untagle en la versión de Linux Debian 8, se realiza la configuración de reglas con el objetivo de bloquear el tráfico que pasa por el puerto 80. De considerar pertinente, aquí se puede permitir filtrar el tráfico de cualquier red permitiendo el acceso a cualquier dirección IP. (VER ANEXO 8.4)

3.5.4.1.2 Activar Syn Cookies en las consolas de Windows o Linux respectivamente, siendo usado como una estrategia inteligente para evitar todo tipo de almacenamiento de los estados de los TCP.

3.5.4.1.3 Activar SynProxy en las consolas de Windows y Linux respectivamente, ya que es utilizado para apoderarse de todas las conexiones mientas se genera Syn Cookies de tal manera que se introduce en los paquetes enviados y resuelve el problema de seguridad en páginas web.

3.5.4.1.4 De ser necesario bloquear los puertos abiertos que no se utilice, ya que esto genera que la maquina sea más vulnerable a ciertos tipos de ataques, además utilizar frecuentemente analizadores de tráfico que permitan verificar el estado actual de una determinada red.

En la Ilustración 3-16, la herramienta “Wireshark” nos muestra que el ataque fue mitigado con éxito, ya que se ha estabilizado el sistema mediante la aplicación de reglas a través Untangle, es decir bloquear el paso del tráfico del puerto 80 y redirigirlo hacia otra dirección IP que sea segura. (VER ANEXO 8.4)

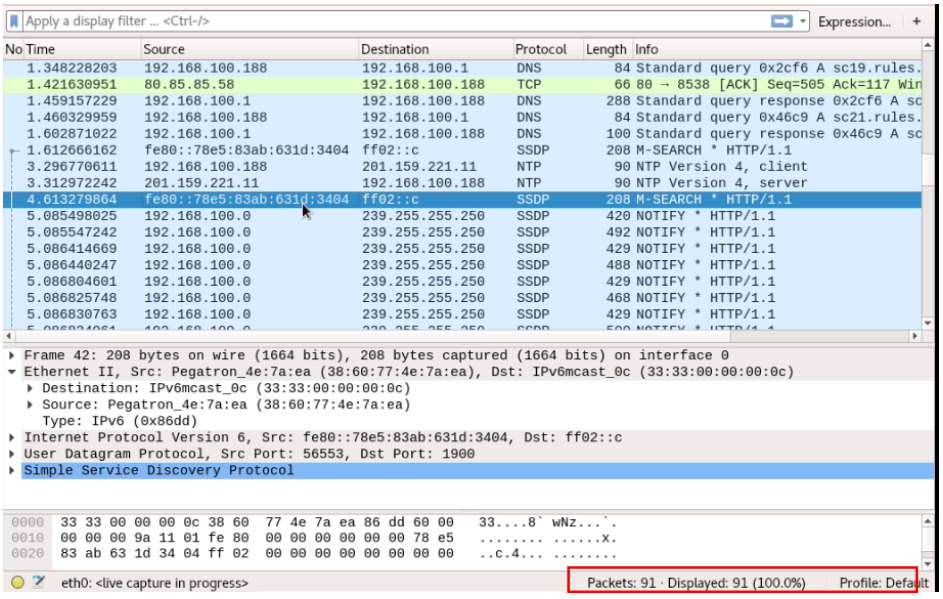


Ilustración 3-16: *“Visualización de la Mitigación del Ataque Syn Flood”*

3.5.4.2 Resultados

Al realizar este ataque con su respectiva mitigación se puede observar en la Ilustración 3-15 que el servidor empieza a realizar inicios de sesión sin finalizar, es decir dejando a la espera de una respuesta. Sin embargo, cuando se toma medidas sobre este ataque a través de un Firewall en este caso Untangle, se observa en la Ilustración 3-16 que cuando filtra la dirección IP establecida, empieza a captar el tráfico de manera estable y sin ninguna complicación debido a que se ha re direccionado el puerto.

3.5.5 Sesiones, contraseñas y aplicaciones

Este tipo de ataque vulnera los niveles superiores del nivel OSI (sesión, presentación y aplicación) debido a que permite el ingreso a cualquier máquina que tenga disponible el acceso al puerto 21.

El robo de contraseñas y sesiones es muy habitual, ya que puede empezar desde descifrar contraseñas por fuerza bruta hasta ingresar aplicaciones que permitan estas acciones. Para simular este tipo de ataque se ha utilizado el aplicativo "John the Ripper" el cual permite descifrar los usuarios y contraseñas para ingresar a cualquier máquina.

Si bien es cierto, esta aplicación es un poco complicada de instalar, aplicar y entender ya que se debe realizar con mucho cuidado debido a que podemos mover dañar algún fichero que sea útil para este aplicativo. Como se puede observar en la Ilustración 3-17, se ha realizado con éxito el ataque, logrando entrar a la maquia víctima y poder realizar cualquier tipo de acción dañina. (VER ANEXO 8.5)

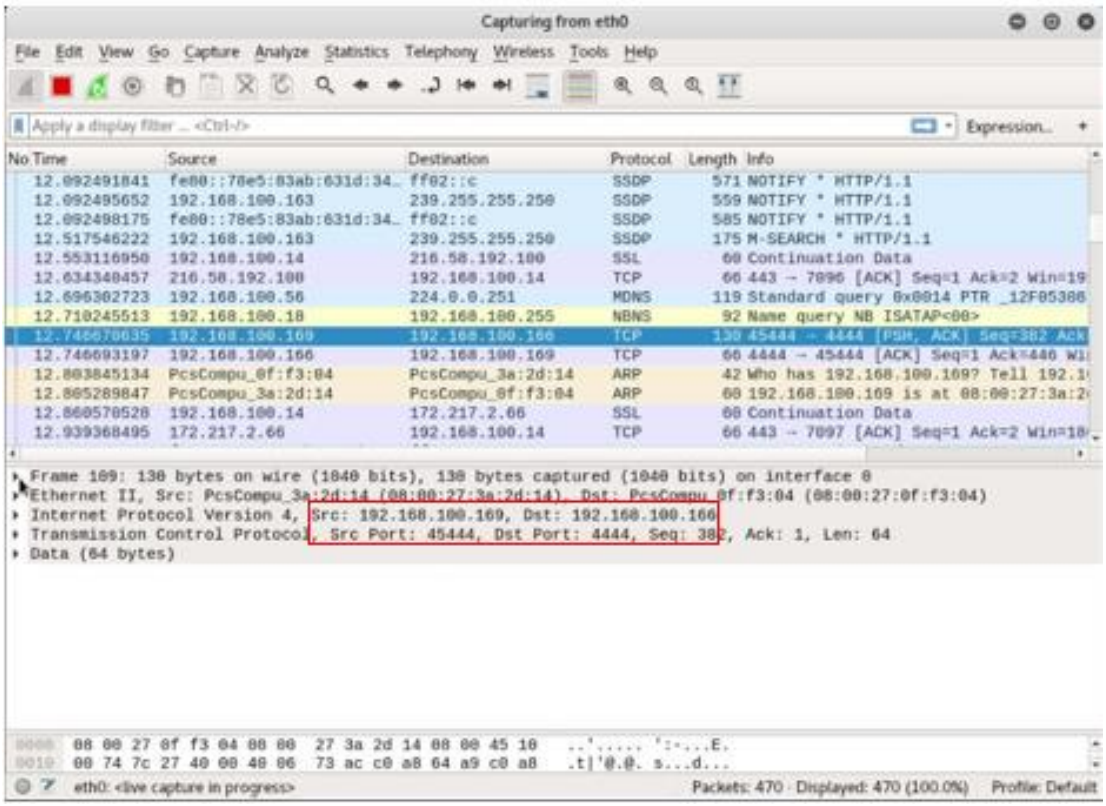


Ilustración 3-17: "Ataque Robo de Sesiones, Contraseñas y Aplicaciones "

3.5.5.1 Medios de Prevención

3.5.5.1.1 Este tipo de ataque secuestra sesiones de un equipo de tal manera que pueda acceder fácilmente, inclusive la instalación de cualquier aplicativo que permita la instalación, modificación o eliminación de archivos. Por este motivo es necesario deshabilitar el puerto 137 (servicios de nombre),138 (servicios de datagrama),139 (servicios de sesión) y 445 (servicios de sesión) mediante la activación del firewall con el que trabaje nuestro sistema operativo, configurando las reglas necesarias de filtrado y de esta manera impedir la publicación de estos protocolos susceptibles a través de internet. (VER ANEXO 8.5)

3.5.5.1.2 Instalar en sistemas operativos Linux un firewall que se encuentra vinculado al kernel llamado “iptables”, este cortafuego puede soportar infinitas reglas permitiendo analizar todo el tráfico que circula por la red y de esta manera saber qué información, datos, paquetes pueden o no ingresar al equipo; sin embargo, para manipular este cortafuego es necesario tener permisos privilegiados.

3.5.5.1.3 Cuando se realice la instalación del sistema operativo en una empresa, se debe configurar correctamente ya que este servicio se debe habilitar para poder compartir los recursos a través de una red local y por defecto también en Internet por lo cual es necesario el uso de contraseñas en todos los archivos incluyendo los compartidos de una computadora de tal manera que cuando se realice un ataque, este sea un impedimento más.

3.5.5.1.4 Actualmente, en la mayoría de empresas usan el sistema Operativo “Windows” independientemente de sus versiones, por tal motivo una solución manual a este tipo de ataques es desactivar la “NetBIOS” mediante: “Panel de Control, Redes e Internet, Centro de Redes y Recursos Compartidos, Cambiar configuración del Adaptador, Propiedades, Protocolo de Internet versión 4 (TCP/IPv4), Propiedades, Opciones Avanzadas, Pestaña (WINS) y Deshabilitamos NetBIOS de TCP/IP”.

Como se puede observar en la Ilustración 3-18, la herramienta “Wireshark” nos muestra que el ataque fue mitigado con éxito, ya que se puede observar que la dirección 192.168.100.169 se está dirigiendo a 192.168.100.181 lo que se deduce que el protocolo 21 ya redirige tu tráfico hacia esta dirección. (VER ANEXO 8.5)

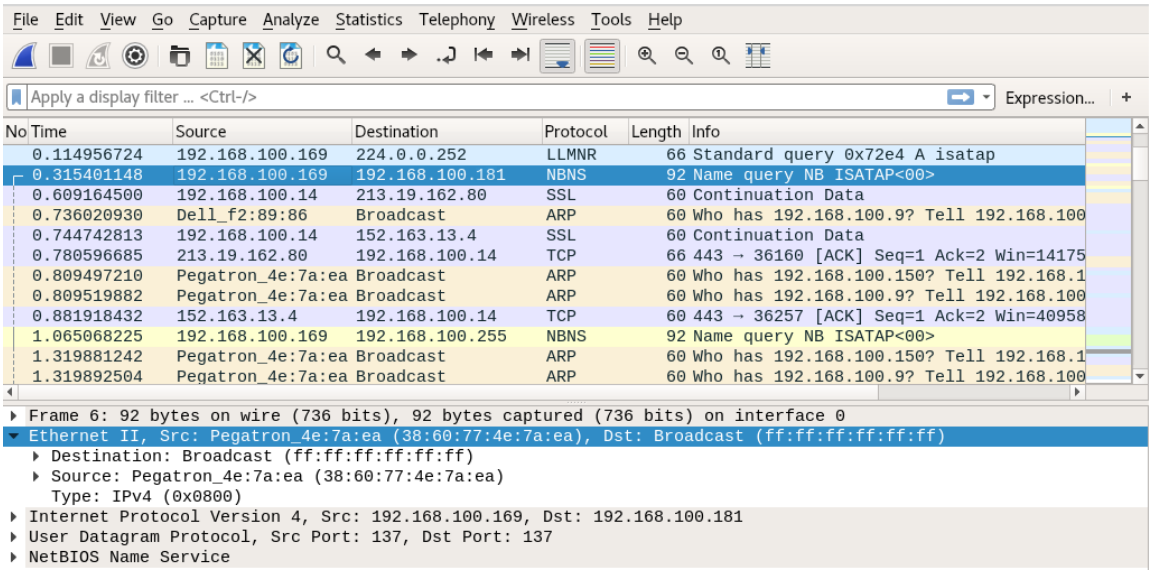


***Ilustración 3*-18:** “Ataque Robo de Sesiones, Contraseñas y Aplicaciones”

3.5.4.3 Resultados

Al realizar este ataque con su respectiva mitigación se puede observar en la Ilustración 3-17 que la sesión fue robada y a partir de esta vulnerabilidad puede tomar el control total de todo un sistema; sin embargo, cuando se realiza la mitigación a través de Firewalls (Untangle) se puede observar que el tráfico se redirige hacia una determinada dirección establecida por el usuario como segura Ilustración 3-18.

4. CAPÍTULO IV: DESCRIPCIÓN DEL MODELO OSI Y TCP

4.1 Definición de las Capas de los Modelos de Referencia

En la actualidad el estudio de los modelos de protocolos es muy relevante debido a que proporciona una referencia en común para mantener una estabilidad y seguridad entre sus tipos de protocolos y los servicios que proporciona a la red.

Estos modelos además de ser estándares para mantener una comunicación entre computadoras, tiene por objetivo definir bien las funciones en cada nivel propuesto y los procesos que se involucran para dicha comunicación.

Por otra parte, en el estudio de las redes los dos modelos que son fundamentales para permitir una excelente comunicación independientemente de los protocolos que se utilicen son “Modelo OSI” y “Modelo TCP/IP” por lo que entenderlos y conocerlos es muy importante para facilitar su comprensión e interrelación.

Independientemente del modelo que se utilice, este se encuentra dividido en niveles, los cuales se comunican con la capa mediamente superior e inferior de la misma pila por medio de interfaces que representan a los protocolos.

4.1.1 Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI)

Es un modelo de referencia definido por la ISO con el objetivo de establecer estándares que permitan la comunicación de computadoras entre diferentes fabricantes. Consta de siete niveles los cuales brinda servicio a la capa inmediatamente superior apoyándose de la capa inferior.

4.1.2 Modelo de Referencia de Control y Transmisión / Protocolo de Internet (TCP/IP)

Es un modelo de referencia desarrollado por Vinton Cerf, proviene de dos protocolos importantes TCP e IP, tiene como objetivo la comunicación entre computadoras de diferentes fabricantes. Consta de cuatro niveles que brindan servicio a la capa inmediatamente superior apoyándose de la capa inferior.

Como se ha mencionado anteriormente, ambos modelos son usados para permitir la comunicación entre computadores basándose en el concepto de pila de protocolos siendo su funcionalidad de capas parecida pero no igual. Sin embargo, existen ciertas características entre uno y otro que los hace completamente diferentes, independientemente del propósito con el que fueron creados.

El modelo OSI posee 7 niveles a diferencia del modelo TCP/IP con tan solo 4, como se puede observar en la siguiente imagen, cada uno de los noveles se encuentran bien definidos para cumplir con una función en específico.

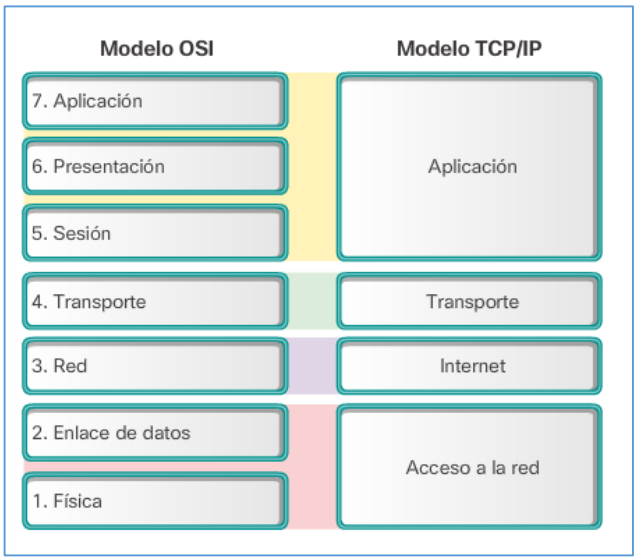


Ilustración 4-1:*"Modelo OSI y Modelo TCP/IP" (Interpolados, 2017)*

4.2 Definición de los Niveles de los Modelos de Referencia

El modelo TCP/IP se compone de 4 niveles los cuales cumplen con la misma funcionalidad del modelo OSI, con la diferencia que en el nivel Físico está compuesto por el nivel de enlace de datos, al igual que en la capa de aplicación se encuentra compuesto por la capa de sesión y presentación.

Las unidades básicas que trabajan en el modelo TCP/IP se comparan a las del modelo OSI, es decir:

- Trama: Unidad que se usa en la capa de acceso a la red.
- Paquete: Unidad que se usa en la capa de Internet.
- Segmento: Unidad que se usa en la capa de Transporte
- Datos: Unidad que se usa en la capa de Aplicación

MODELO OSI		**MODELO TCP/IP**	
NIVELES	**FUNCIONALIDAD**	**NIVELES**	**FUNCIONALIDAD**
Físico	Encargada de la señal y transmisión binaria	**Físico**	Encargada de la señal y transmisión binaria y del Direccionamiento Físico (MAC y LLC)
Enlace de Datos	Encargada del Direccionamiento Físico (MAC y LLC)		
Red	Determina una ruta adecuada y direccionamiento lógico	**Internet**	Determina una ruta adecuada y direccionamiento lógico
Transporte	Conexión extremo a extremos y fiabilidad de datos	**Transporte**	Conexión extremo a extremos y fiabilidad de datos
Sesión	Comunicación entre los dispositivos de red	**Aplicación**	Comunicación entre los dispositivos de red, Representa a los datos, brinda servicios de red a las aplicaciones
Presentación	Representa a los datos		
Aplicación	Brinda servicios de red a las aplicaciones		

Tabla 4-1: *"Modelo OSI vs Modelo TCP/IP"*

El proceso que realiza este modelo es descender por la pila de protocolos emisor y escalar en la del receptor, cada nivel de la pila añade datos y cabeceras a enviar a la capa inferior de tal manera que se encapsulen para poder trabajar; sin embargo, cuando los datos se reciben realiza un proceso inverso, es decir cuando la información asciende se va eliminando las cabeceras correspondientes.

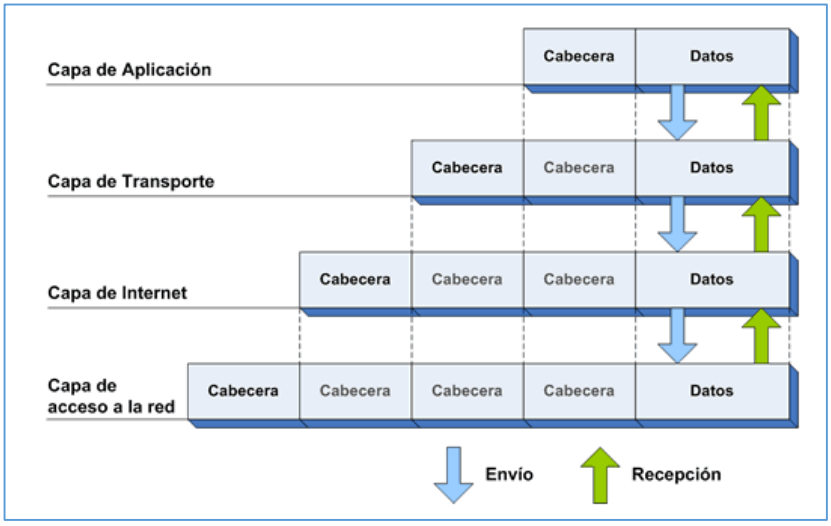


Ilustración 4-2: "Proceso del Modelo TCP/IP" (Textoscientificos.com, 2006)

4.3 Definición de los Protocolos de los Modelos de Referencia

El modelo TCP/IP como se puede observar es mucho más sencillo que el modelo OSI por lo que el conjunto de protocolos en los que se basa este modelo es el TCP e IP siendo los primeros en definirse y los más utilizados de esta familia. No obstante, no se descarta a los demás protocolos pudiendo llegar a más de 100, entre los más importantes tenemos a HTTP, FTP, Telnet, entre otros.

Ahora, TCP como se mencionó anteriormente es uno de los protocolos más importantes ya que se encarga de las conexiones entre sí para crear flujo de datos garantizando que los datos sean entregados sin errores, ordenados y distinguir las

aplicaciones en un mismo dispositivo; mientras que el protocolo IP se encarga de enviar y recibir los datos en bloques, este envío se realiza mediante la elección de la mejor ruta sin garantizar que llegue a su destino.

En fin, estos dos protocolos trabajan conjuntamente para resolver la trasmisión de datos que se genera en una red independientemente si es interna o externa, asegurando que la información llegue correctamente, sin errores y por la mejor ruta. A continuación, detalla los protocolos más usados en los modelos de referencia OSI y TCP/IP:

Modelo OSI		**Modelo TCP/IP**	
Niveles	**Protocolos**	**Niveles**	**Protocolos**
Físico	Dispositivos físicos que conectan a una red	**Físico**	PPP, ETHERNET, Controladores de Interfaz
Enlace de Datos	HDLC,PPP,CSMA/CD, ETHERNET, LAN,STP, VLAN,ARP,		
Red	IPv4, IPv6, IPSec, ICMP	**Internet**	ARP, NAT, ICMP, RIP, OSPF,EIGRP,BGP
Transporte	UDP, TCP, TLS, SSL	**Transporte**	UDP, TCP
Sesión	NetBIOS, RPC	**Aplicación**	DNS, BOOTP, DHCP, SMTP, POP, IMAP, FTP, TFTP, HTTP
Presentación	ANSI.1, XDR, MIME		
Aplicación	DNS, Telnet, FTP, SSH, SMPT, POP, SNMP,HTTP, DHCP,IMAP		

Tabla 4-2: *"Protocolos del Modelo OSI vs Modelo TCP/IP"*

4.4 Principales Ventajas del Modelo OSI y TCP/IP

MODELO OSI	MODELO TCP/IP
Evita problemas de compatibilidad.	Se encuentra diseñado para enrutar.
Divide y detalla sus niveles en 7 para facilitar su compresión en partes más simples.	Brinda abstracción de capas, dividiéndose y detallándose sus niveles en 4.
Brinda al fabricante un conjunto de estándares para asegurar su compatibilidad e interoperabilidad.	Es compatible con herramientas estándares el cual utilizan para analizar su funcionamiento en la red
El cambio que se realice en una capa no afecta en las demás.	Se usa en redes grandes y medianas incluidas redes empresariales.
Simplifica su aprendizaje.	Es muy fiable en cuanto a seguridad
Permite a los distintos tipos de hardware y software de red comunicarse entre sí de una manera totalmente definida.	Imprescindible para el Internet por lo que en la actualidad es el modelo más utilizado.
Proporciona un lenguaje en común para describir las funciones y capacidades de las redes.	Es flexible y se encuentra disponible para todo tipo de sistemas operativos y hardware.
Realiza una comunicación no orientada y orientada a la comunicación.	Puede realizar una comunicación sin conexión, considerando en la capa de transporte una comunicación con o sin conexión.
Tiende a definir claramente las diferencias entre los servicios, las interfaces, y los protocolos	No tiene definida claramente las diferencias entre los servicios, las interfaces, y los protocolos

Tabla 4-3: *"Protocolos del Modelo OSI vs Modelo TCP/IP"*

4.5 Principales desventajas del Modelo OSI y TCP/IP

MODELO OSI	MODELO TCP/IP
Sus capas posee actividades que son redundantes como el control de errores que realiza cada capa	Afecta el diseño de nuevas tecnologías ya que no tiene definido claramente sus protocolos, interfaces, servicios.
Es interpretado como "calidad pobre" debido a la gran cantidad de código en su implementación.	Posee el peor rendimiento para el uso de servidores como por ejemplo en ficheros de impresión
Mala sincronización	No distingue entre la capa física y la de enlace de datos, de igual manera entre la de aplicación, sesión y presentación.
Posee tecnología desactualizada ya que su modelo y protocolos son imperfectos	Es difícil de configurar y mantener a pesar de su reducido número de capas

Tabla 4-4: *"Principales Ventajas del Modelo OSI y TCP/IP"*

5. CAPITULO V: MODELO DE SEGUIRDAD APLICADA AL MODELO OSI

5.1 Seguridades en los Niveles del Modelo de Referencia de Interconexión de Sistemas Abiertos

5.1.1 Capa Física

5.1.1.1 Existen soluciones innovadoras que sustituye a los Data Center, los "Cloud Computing". Esta es una manera óptima de almacenar, asegurar, garantizar, acceder rápida y eficazmente a la información en tiempo real. Sin embargo, el este recurso informático se basa desde aplicaciones hasta un centro de datos a través del Internet y en un modelo de pago por uso.

5.1.1.2 Los medios guiados y no guiados a utilizarse dentro de LAN dependen de la persona que estructure la red por lo cual deben realizar un análisis profundo del entorno físico que va a rodear los equipos informáticos. Sin embargo, se recomienda utilizar cables de fibra óptica ya que poseen divisores ópticos que hace imposible su interceptación, aunque su instalación debe ser cuidadosa debido a que es un cable muy sensible que puede romperse y ser inservible.

5.1.1.3 La seguridad en los medios guiados es muy simple, pero difícil de asegurar al 100% , si la elecciones es un cable de tipo par trenzado se debe resguardar que el cableado cumpla con las normativas y calidad necesaria como el CAT 5[17] o CAT 7[18].

[17] **CAT 5:** Cable Par Trenzado de Categoría 5, descritos en el estándar EIA/TIA 568B
[18] **CAT 7:** Cable Par Trenzado de Categoría 7, descritos en el estándar ISO/IEC 11801:2002

5.1.1.4 Crear planos de red los cuales identifique claramente los canales hacia donde se dirigen los cables de red, se debe incluir los puestos de trabajos conectados, su numeración, cada uno de sus extremos, entre otros.

5.1.1.5 Identificar los tramos más complicados, es decir se debe analizar en la empresa cuales son los canales de comunicación más importantes y brindar mayor seguridad para que no exista ningún tipo de interceptación ya sea de tipo internos o externos.

5.1.1.6 Asegurar que el suministro de energía sea estable y continuo mediante el uso de sistemas UPS[19]con el objetivo de que los dispositivos informáticos no se apaguen de manera brusca en el caso de que existe cortes eléctricos.

5.1.1.7 Realizar periódicamente un inventario de los equipos fiscos de red detallando su ubicación, claves de acceso, permisos de acceso, habilitación de puertos de puertos, entre otros; teniendo en cuenta a los dispositivos que necesiten mayor seguridad y resguardarlos en gabinetes de comunicaciones que brinden mayores seguridades.

5.1.1.8 Instalar, actualizar y mantener dispositivos de control de acceso hacia la empresa y dispositivos físicos mediante el uso de tarjetas únicas para los usuarios, sistemas biométricos, dactilares, ópticos entre otros.

5.1.1.9 Cuando se realice modificaciones físicas de la red, este debe estar establecido y aprobado como un control de cambios, la cual debe

[19] **UPS**: Sistema Ininterrumpido de Energía

encontrarse bien documentada y controlada periódicamente después de su implementación.

5.1.1.10 Realizar backups periódicamente de la información que se considera relevante para la empresa con el objetivo de evitar robo y/o perdida de la misma. Se recomienda realizar esta acción mensualmente o dependiendo del responsable de infraestructura.

5.1.1.11 Actualmente, para realizar cualquier tipo de backups se puede realizar una nube privada la cual sea pagada y la información se encuentre disponible en tiempo real.

5.1.1.12 Realizar un análisis profundo de la topología de la red, ya que, al implementarla, este impondrá la lógica de transmisión de la información.

5.1.1.13 El crecimiento de la red en una empresa es inevitable, por lo que se debe realizar estrategias de expansión, se debe tomar en cuenta que estas deben ser bien diseñadas desde el inicio debido a que si realiza esta acción incorrectamente ocasionará grandes problemas en el futuro.

5.1.1.14 Se debe auditar los puntos de acceso a la red, es decir que la puerta de acceso a la red se encuentre correctamente documentado y justificado.

5.1.1.15 Implementar, desarrollar y aplicar políticas de seguridad dentro de la empresa entre las más importantes de identificación y acceso, de contraseñas, de accesos remotos, de manteniendo de la red, entre otros.

5.1.1.16 Realizar planes de contingencia contra factores naturales los cuales aseguren y prevengan cualquier tipo incidente fortuito. De ser posible detallar con exactitud cada procedimiento a seguir.

5.1.1.17 Realizar constantes auditorias de seguridad física. En la actualidad existen empresas especializadas las cuales brindan un servicio completo, ya que buscan las más grandes dificultades que puede tener una empresa hasta posibles riesgos y poderlos prevenir en el futuro.

5.1.1.18 Capacitar y concientizar al personal para saber qué hacer en caso de desastres naturales, de ser posible realizar cada cierto tiempo simulaciones de evacuación.

5.1.2 Capa de Enlace de Datos

5.1.2.1 Este nivel como tiene acceso a absolutamente toda la información de la red es muy importante aplicar un alto nivel de seguridad, por tal motivo se debe utilizar distintas herramientas como analizadores de protocolos.

a) Wireshark: Es el analizador de paquetes más conocido a nivel mundial, básicamente trabaja como un Sniffer que permite ver todo el tráfico que circula por la red en momentos específicos. Es open source y multiplataforma. Por otra parte, permite capturar cookies, contraseñas, direcciones IP, direcciones MAC, entre otros.

b) Dripcap: Es un nuevo analizador de protocolos para observar paquetes en tiempo real. Su interfaz es moderna y amigable al usuario por lo que se

podrá encontrar rápidamente la información necesaria. Es gratuita, multiplataforma y de código abierto.

c) AppSniffing: Es un analizador de protocolos con una interface gráfica amigable que permite diagnosticar rápidamente problemas y anormalidades que pueda existir en la red.

d) Microsoft Message Analyzer: Permite capturar paquetes en una red local en tiempo real o remota de tal manera que permita analizar el tráfico de los diferentes protocolos. Incluye capturar tráficos realizados anteriormente para un análisis en detalle.

Las herramientas mencionadas, son las más utilizadas para realizar un análisis de tráfico en la red, tomando en cuenta que algunas de ellas no poseen una gran estabilidad para ser utilizadas o no son multiplataforma como lo es Wireshark ya que además se ser conocida mundialmente, se puede instalar en cualquier sistema operativo, siendo amigable al usuario, fácil de entender y utilizar. Aunque Microsoft Message Analyzer no se queda atrás, a pesar de solo ser para Windows esta herramienta es muy completa incluso permite la evolución de eventos del sistema y otros mensajes de componentes Windows.

5.1.2.2 Realizar controles de direcciones de Hardware, es decir efectuar una lista completa del direccionamiento IP y MAC con el objetivo de auditar periódicamente estas direcciones para evitar falsificaciones o intrusiones de factores externos. Las herramientas más usadas para realizar este control es IP Address Manager, la cual usa un escaneo activo para detectar, rastrear subredes con sus respectivas direcciones. Sin embargo, en la actualidad

Advanced IP Scanner aparte de escanear los dispositivos de red, asocia direcciones IP con las direcciones MAC incluso presenta los fabricantes de las tarjetas de red para dar acceso a carpetas compartidas y servidores FTP.

5.1.2.3 Establecer direcciones IP estáticas con sus respectivas MAC para evitar ataques de suplantación, esto se realiza manualmente independientemente del número de direcciones que se encuentre en red.

5.1.2.4 Escoger correctamente los dispositivos que van a trabajar en la red, de acuerdo al tipo de empresa que va a utilizarlo. Entre los mejores switchs tenemos a TP-Link TL-SG108E (empresas pequeñas), soporta el estándar 802.1Q VLAN, previene ataques de tipo "DHCP", mientras que un switch de tipo Cisco SG200-26 26 (empresas multinacionales) trabaja rápidamente e incluye todo tipo de seguridades de protocolos a nivel de enlace de datos y red, es recomendado como uno de los mejores switches de ethernet.

5.1.2.5 Realizar correctas configuraciones de los dispositivos de red, especialmente de los switches, se debe bloquear todo tipo de acceso a puertos que no se están utilizando de esta manera se puede evitar cualquier tipo de escucha que se encuentre en la red.

5.1.2.6 Crear y configurar correctamente las Vlan[20] ya que ayudan a segmentar la red de tal forma que exista separación de tráfico y poder realizar un rápido análisis de lo que sucede a cada momento en la red.

[20] **VLan:** Red de Area Local, no existe a nivel físico, pero si lógico.

5.1.2.7 Diseñar las diferentes topologías de red mediante el uso de las herramientas GNS3 O Cisco Tracer Packet, este mecanismo ayuda a simular como será implementada la red para en un futuro ponerla en marcha. Entre estas dos herramientas, Cisco Tracer Packet posee características y funcionalidades muy parecidas a las de un switch real; sin embargo, se debe conocer bien el funcionamiento y comandos para poder realizar cualquier configuración. Por otra parte, GNS3 es amigable al usuario y más fácil de manejar sus características debido a que no siempre se tiene que realizar configuraciones manuales.

5.1.3 Capa de Red

5.1.3.1 En este nivel se direcciona correctamente la información a través de los routers, por tal motivo es de vital importancia que la seguridad en estos dispositivos sea muy alta con respecto al control adecuado de contraseñas, su configuración debe ir desde el acceso a Telnet, hasta la interfaz gráfica mediante http.

5.1.3.2 Realizar las configuraciones necesarias dentro del router, ya que muchas veces los detalles de la configuración no son empleados como los subnetting, broadcast, puertos, rutas, entre otros.

5.1.3.3 Utilizar un firewall especializado y dedicado a la protección de los dispositivos en red, entre las herramientas más utilizadas es el propio Firewall de Windows ya que mantiene controlada y segura a una máquina, posee actualizaciones automáticas lo que hace al sistema operativo utilizar los últimos parches que libera Microsoft, por otra parte para el sistema

operativo Linux en cualquiera de sus versiones tenemos la aplicación Untagle, la cual sirve como una pasarela de red de código abierto especializado para empresas pequeñas ofreciendo desde bloqueos de correo electrónico hasta Pishing[21].

5.1.3.4 Implementar el protocolo IPSec, ya que esta suite de protocolo brinda funcionalidades de seguridad al protocolo IP para redes virtuales privadas o VPN, se la puede implementar de dos maneras en modo túnel[22] y modo transporte[23] .

5.1.3.5 Al igual que en la capa de enlace de datos, utilizar un analizador de protocolos la cuales pueda devolver directamente las direcciones IP con sus respectivas MAC. Sin embargo, se puede utilizar varias herramientas de detección de intrusos en una red como lo es Snort ya que posee un monitor de detección de ataques y escaneo de puertos la cual ayuda a prevenir cualquier tipo de ataque a través del registro y alerta del mismo.

5.1.3.6 Utilizar protocolo SSL[24] y TLS[25] los cuales proporcionen una comunicación segura y confiable debido a que se basan en la funcionalidad de TCP brindando confidencialidad e integridad en la información en los servidores y páginas web.

[21] **Pishing:** Suplantar identidades que tiene como objetivo estafar y obtener información
[22] **Modo Túnel:** Cada paquete IP se cifra y encapsula dentro de otro.
[23] **Modo Transporte:** Los extremos de una comunican cifran el contenido del paquete
[24] **SSL:** Secure Socket Layer
[25] **TLS:** Transport Layer Security

5.1.4 Capa de Transporte

5.1.4.1 Se debe realizar altos controles en el establecimiento de sesiones y puertos, debido a que este nivel es el responsable de entregar el paquete o no mediante los protocolos TCP o UDP. Para realizar un escaneo de puertos se debe usar Zenmap ya que es una aplicación completa que nos ayuda a realizar un escáner profundo de una determina red o subred permitiendo establecer los quipos activos y poder sacar la información necesaria. Sin embargo, no descartamos otras herramientas útiles como Nessus, Netcat, Dmitry ya que permiten hacer un análisis completo de vulnerabilidades incluyendo escaneo de puertos, direcciones IP, entre otros.

5.1.4.2 No usar siempre el protocolo UDP por que se necesita mayor control debido a que no es orientado a conexión y es más complicado regular el ingreso seguro en la red. Por otra parte, el protocolo TCP se puede regular mediante proxys y por medio de firewalls cerrando la mayoría de puertos que no emplee.

5.1.4.3 Usar protocolos SSL, TLS o SSH las cuales permiten la protección de los datos mediante técnicas de cifrado, estos deben ser considerados cuando se establece una conexión y lograr administrar remotamente los dispositivos.

5.1.5 Capa de Sesión

5.1.5.1 Deshabilitar protocolos inseguros los cuales no sean requeridos en nuestra red por ejemplo NetBIOS, mediante un análisis profundo escaneo de puerto utilizando herramientas mencionados anteriormente (Zenmap, Nmap, Nessus).

5.1.5.2 Evitar que personas externas o no autorizadas puedan inyectar datos en sesiones activas e incluso puedan modificar tablas de rutas de tal manera que pueda obtener información relevante.

5.1.5.3 Utilizar firewalls mediante la configuración de reglas de filtrado de manera que impida publicar protocolos susceptibles a enumeración que no cumplan con funciones públicas (NetBIOS).

5.1.5.4 Seleccionar correctamente los protocolos de autenticación para garantizar confiabilidad de cualquier contraseña que pueda trasmitirse a través de la red.

5.1.5.5 Realizar constates auditorías a los accesos remotos los cuales solo se permita a personas autorizadas previamente con las autenticaciones establecidas por la empresa.

5.1.5.6 Habilitar los servicios de auditoría a nivel de sistema operativo de tal forma que se lleve un control rígido mediante la revisión de los registros de log.

5.1.6 Capa de Presentación

5.1.6.1 Utilizar protocolos seguros los cuales ayuden a cifrar los datos para que puedan ser trasmitidos a la capa de aplicación.

5.1.6.2 Utilizar diferentes técnicas de criptografía de tal forma que se lleve un control adecuado de claves utilizadas por el usuario. Sin embargo, se pueden crear políticas de seguridad de contraseñas mediante ciertos criterios de complejidad como su longitud, sensibilidad a mayúsculas o minúsculas, caracteres especiales, alfanuméricos.

5.1.6.3 Implementar políticas de bloqueo de contraseñas con el objetivo de que, si existe cierto número de intentos, automáticamente se bloquee la máquina y alerte al administrador.

5.1.7 Capa de Aplicación

5.1.7.1 Implementar Firewalls que brinden un alto nivel de seguridad (Untangle) y permita el control del tráfico en la red debido a que obligatoriamente tiene que pasar por estas aplicaciones para saber si se niega o admite el tránsito en la red.

5.1.7.2 Realizar filtros de acceso mediante el uso de los analizadores de tráfico como Wireshark ya que este permite incluso inspeccionar los paquetes de los niveles superiores del modelo OSI (Sesión, Presentación y Aplicación) de tal forma que se pueda observar el contenido de cada uno de los protocolos utilizados.

5.1.7.3 Mantener los Firewalls actualizados y monitorizados día a día, con el objetivo de que protejan al sistema frente a diversos ataques intencionales o fortuitos.

5.1.7.4 Bloquear y redirigir el tráfico de los puertos a través de Firewalls de manera que lleguen a un destino seguro y no pueda ser interceptado en el camino.

5.1.7.5 Todas las aplicaciones que deseen ser instaladas dentro de una máquina, deben pasar por varios filtros de seguridad, incluido tener permisos de

administrador de modo que puedan funcionar correctamente, tomar en cuenta que se debe solicitar actualizaciones periódicas de las mismas.

6. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

6.1.1 Utilizar una arquitectura en capas es indispensable para que dos sistemas se puedan comunicar entre si independientemente de sus fabricantes, por tal motivo el modelo OSI fue una de las primeros en desarrollarse definiendo bien sus características y funcionalidades en cada uno de sus niveles brindando seguridad a través de sus protocolos.

6.1.2 El modelo OSI es la base fundamental para realizar estudios avanzados en materia de redes de datos incluso de telecomunicaciones debido a que se encuentra desarrollado en 7 niveles los cuales detallan una definición simple y concisa de cada protocolo y cuál es el funcionamiento en cada uno de ellos.

6.1.3 En ninguna infraestructura de red existe seguridad y garantía del 100% cuando se comunican los dispositivos de red, debido a que la tecnología avanza y factores tanto internos como externos buscan agujeros de seguridad para vulnerar cualquier sistema.

6.1.4 Dentro de los 7 niveles OSI, se concluye que el nivel físico es el más vulnerable debido a que se encuentra expuesto a factores humanos que pueden ocasionar daños de manera fortuita o intencional ocasionando daños graves.

6.1.5 Los 7 niveles del modelo OSI trabajan conjuntamente para brindar integridad, confidencialidad e integridad de los datos; sin embargo, estos no solo trabajan en una capa en específico debido a que se valen de los niveles inferiores para dar servicio a los niveles superiores.

6.1.6 Un diseño de seguridad debe ser construido de acuerdo a las posibles vulnerabilidades que pueda presentar la empresa, por este motivo se debe realizar un análisis general para encontrar cuales son los puntos débiles y establecer medidas preventivas brindando soluciones efectivas frente a estos problemas.

6.1.7 Mediante el análisis de los ataques y sus posibles mitigaciones que pueda tener dentro de una red se concluye que se debe diseñar, implementar y mantener un Sistema de Gestión de Seguridad de la Información para las empresas independientemente de su tamaño, estas deben encontrarse enmarcadas dentro de la norma ISO 27000 que establece las mejores prácticas recomendadas para una alta seguridad de la información.

6.1.8 El sistema operativo Kali Linux es una de las mejores herramientas que existe a nivel de seguridad de información, debido a que es diseñada especialmente para auditorias, mantenimiento y monitorización de redes. A pesar de ser distribuida para GNU/Linux es muy útil para realizar análisis completos encontrando el origen y destino de un ataque, vulnerabilidad.

6.1.9 Realizar un profundo análisis de vulnerabilidad en cada una de las capas del modelo OSI se puede determinar con varias herramientas como lo es Kali Linux, Nessus, Wireshark que permite determinar detenidamente lo que ocurre dentro de la red con sus posibles mecanismos de protección.

6.1.10 Las mejores herramientas dentro de Kali Linux que se pueden encontrar para simular ataques y encontrar vulnerabilidades en los diversos protocolos hacia

la red son Yersinia, Ettercap, Hydra, Wireshark, Zenmap, John the Ripper y Metasploit Framework.

6.1.11 Kali Linux fue creada con objetivos educativos y éticos, sin embargo, muchos hackers utilizan este sistema operativo para realizar ataques directos hacia la red, gracias a que las aplicaciones son fáciles de entender y aplicar.

6.1.12 Encontrar distintas medidas preventivas para cada uno de los ataques que se pueden producir en la red es complicado, ya que cada uno de ellos se relacionan entre sí, solo basta entender el ataque y deducir por que se producen para encontrar sus posibles soluciones.

6.2 Recomendaciones

6.2.1 Actualizar con frecuencia los sistemas operativos y softwares de los diferentes dispositivos informáticos, prestando especial atención en las actualizaciones que se presenten ya que muchas veces estos pueden presentar fallas y ser aprovechadas por atacantes informáticos. Se debe estar pendientes de las actualizaciones, parches de seguridad recomendados por fabricantes para prevenir todo tipo de virus e intrusiones no deseadas.

6.2.2 Utilizar firewall como dispositivo de seguridad de tal manera que pueda monitorear el tráfico que circule por una red estableciendo reglas para poder permitir, bloquear o re direccionar cualquier tipo de conexión. Sin embargo, no hay que olvidar que esta herramienta pueda trabajar como software o hardware siendo totalmente configurable para las peticiones del usuario.

6.2.3 Usar herramientas de escaneo de puertos como “Zenmap”, disponible para los distintos sistemas operativos Windows, Linux y MAC; de tal forma que permita realizar un análisis completo de cualquier equipo conectado a la red determinando cuáles son sus puntos vulnerables y poder prevenir a tiempo cualquier situación fortuita. Además, “Zenmap” es un aplicativo muy completo ya que incluso puede mostrar la topología y detallar información completa dependiendo del tipo de escaneo que se realice dentro de la red.

6.2.4 Utilizar routers y switches modernos como Cisco ya que ayudan a mitigar los problemas tipo broadcast y de seguridad. Son diseñados específicamente para mitigar cualquier tipo de problemas Ethernet.

6.2.5 Antes de realizar cualquier tipo de ataque o mitigación hacia una red se debe tener conocimientos sobre lo que se está realizando, de igual manera los simuladores de red se deben encontrarse bien instalados y configurados para que puedan cumplir con las funciones programadas.

6.2.6 Para poder simular cualquier tipo de ataque y sus posibles mitigaciones, es necesario realizarlo en un ambiente donde exista mayor tránsito de información ya que de esta manera se puede analizar y observar de mejor manera cual es el comportamiento de cada dispositivo informático.

6.2.7 Dar mantenimiento frecuentemente a los equipos informáticos revisando su estado físico ya que estos cumplen con cierto tiempo y calidad de vida.

6.2.8 Para simular estos ataques es recomendable utilizar el sistema operativo “Kali Linux” (maquina atacante), “Metasploitable”, “Windows 7”, “Windows XP” en cualquiera de sus versiones; estos son utilizados con el objetivo de realizar pruebas de seguridad.

6.2.9 Para realizar pruebas de hacking ético, se recomienda utilizar softwares de virtualización como Virtual Box o VMWare. Estas aplicaciones son muy reconocidas a nivel mundial y posee características de fácil configuración (tarjeta de red, sonido, procesador, entre otros) gracias a esto se realizó las simulaciones de máquinas atacantes o víctimas recreando cualquier sistema operativo necesitado.

6.2.10 Utilizar y cambiar las contraseñas de los dispositivos informáticos cada 3 meses de tal manera que sea difícil de descifrar y menos predecible para el atacante, esta es una buena práctica para el buen funcionamiento de la empresa debido a que factores humanos no puedan perjudicar o extraer información relevante y necesaria.

6.2.11 Actualmente, el correo electrónico es la herramienta más utilizada en todas las empresas; sin embargo, no se encuentra exento a cualquier tipo de ataque, por tal motivo se recomienda no responder o abrir correos spam, abrir vínculos extraños inclusive suscribir correos empresariales en páginas web desconocidas.

6.2.12 Contar con múltiples métodos de autenticación ya sea tipo usuario, maquina o dispositivo informático que permita identificar quien dice ser. Se recomienda permitir y dar accesos tan solo los sistemas o aplicaciones en concreto y a los necesarios.

6.2.13 Realizar periódicamente backups de toda la información de una empresa, de tal forma que si existe pérdida o robo de información; se pueda recuperar fácilmente. Aunque actualmente existe la famosa “Cloud Computing” logrando ser la manera más óptima de almacenar, asegurar, garantizar, acceder rápida y eficazmente a la información en tiempo real.

6.2.14 Diseñar cualquier tipo de plan de acción que pueda hacer frente a diferentes situaciones fortuitas de forma que pueda responder rápidamente tras sufrir un ataque. Se sugiere designar un responsable para gestionar dicho plan.

6.2.15 Realizar periódicamente auditorías se seguridad interna la cual de una visión más profesional sobre posibles vulnerabilidades de los sistemas utilizados. En la actualidad existen varias empresas especializadas en realizar este tipo de auditorías las cuales prestan abiertamente sus servicios como el caso de “ClaveiSystems”.

6.2.16 Todos los empleados que trabajen para una empresa deben capacitarse en materia de Seguridad de la Información abarcando puntos relevantes como las causas y consecuencias de un ataque, autenticaciones, inseguridad de contraseñas, ciberataque entre otros; los cuales permitan garantizar cierta seguridad por factor humano.

7. BIBLIOGRAFÍA

7.1 20 COMPUTING? (20 de Noviembre de 2017). *¿QUÉ ES EL CLOUD COMPUTING? - SETEINFO DEL ECUADOR*. Recuperado el 03 de Julio de 2018, de SETEINFO DEL ECUADOR: http://seteinfo.com/que-es-el-cloud-computing/

7.2 Abad Domingo, A. (2013). *Redes Locales.* Madrid: McGraw-Hill España.

7.3 Aguilera, P. (2011). *Seguridad Informática.* Editex.

7.4 Álvarez Marañon, G., & Pérez García, P. P. (2004). *Seguridad Informática para Empresas y Particulares.* Madrid: Mc Graw Hill.

7.5 Areitio, J. (2008). *Seguridad de la Información: Redes, Informática y Sistemas de Información.* Madrid: PARANINFO.

7.6 Baca Urbina, G. (2016). *Introducción a la seguridad informática.* Mexico: Grupo Editorial Patria.

7.7 Carceller Cheza, R., Campos Saborido, C., García Marcos, C. J., & Gonzáles Lorenzo, J. (2013). *Servicios en Red.* Madrid: Macmillan Iberia, S.A.

7.8 Castaño Ribes, R. J., & López Fernández, J. (2013). *Redes Locales.* MacMillan Iberia, S.A.

7.9 Castellanos Sandoval, E. J. (2011). Ingenieria Social: Corrompiendo la mente humana. *REVISTA .SEGURIDAD.*

7.10 Castro , C. R. (10 de Diciembre de 2013). *Flooding.* Obtenido de Flooding: http://www.tic.udc.es/~nino/blog/lsi/reports/flood.pdf

7.11 Castro Gil, M. A., Díaz Orueta, G., Alzórriz Armandáriz, I., & Sancristóbal Ruiz, E. (2014). *Proceso y Herremientas para la Seguridad en Redes.* Madrid: UNED - Universidad Nacional de Educación a Distancia.

7.12 Cisco Systems. (01 de Mayo de 2012). *Blog.utp.edu.co.* Obtenido de CAPITULO 5 Capa de red de OSI: http://blog.utp.edu.co/ee973/files/2012/04/capitulo05-capa-de-red.pdf

7.13 Conecta Software. (17 de Octubre de 2017). *Hackers y Crackers no son galletas - Definiendo tipos de intrusos - Conecta Software*. Recuperado el 03 de Febrero de 2018, de Conecta Software: https://conectasoftware.com/ciberseguridad/hackers-crackers-no-galletas-definiendo-tipos-intrusos

7.14 Corletti Estrada, A. (2011). *Seguridad por Niveles.* Madrid: darFE.

7.15 Costas Santos, J. (2014). *Seguridad Informática.* RA-MA Editorial.

7.16 Costas Santos, J. (2014). *Seguridad y Alta Disponibilidad.* Madrid: Ra-Ma.

7.17 Dávila, A. (2012). *Seguridad en redes a nivel de capas del modelo OSI*. Obtenido de ATAQUES SOBRE EL NIVEL 2 DEL MODELO OSI (III): SPANNING TREE PROTOCOL: https://www.s21sec.com/es/blog/2009/06/ataques-sobre-el-nivel-2-del-modelo-osi-iii-spanning-tree-protocol/

7.18 Escrivá Gascó, G., Romero Serrano, R. M., & Ramada, D. J. (2013). *Seguridad informática.* Macmillan Iberia, S.A.

7.19 Gómes Vieites, Á. (2014). *Gestión de Incidentes de Seguridad Informática.* Madrid: Ra-Ma.

7.20 Gómez López, J., Castro Simón, M. Á., & Guillén Núñez, P. (2014). *Hackers. Aprende a atacar y a defenderte* (2da. Actualizada ed.). Madrid: Ra-Ma.

7.21 Gómez Vieites, Á. (2011). *Enciclopedia de la Seguridad Infomática.* Madrid, España: Ra-Ma. Recuperado el 2018, de https://books.google.com.ec/books?id=Bq8-DwAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=true

7.22 Gómez Vietes, Á. (Diciembre de 2013). *Tipos de ataques e intrusos en las redes informáticas.* Obtenido de Tipos de ataques e intrusos en las redes informáticas: http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

7.23 Google. (25 de Mayo de 2018). *IPv6 – Google*. Obtenido de Google.com: https://www.google.com/intl/es/ipv6/statistics.html

7.24 Gutiérrez del Moral, L. (2014). *Curso de Ciberseguridad Y Hacking Etico.* Punto Rojo Libros, S.L.

7.25 IBM Cloud. (07 de Junio de 2017). *IBM : ¿Qué es cloud computing? - España*. Obtenido de Ibm.com: https://www.ibm.com/cloud-computing/es-es/learn-more/what-is-cloud-computing/

7.26 Inteco. (2016). *Envenenamiento ARP*. Obtenido de Egov.ufsc.br: http://www.egov.ufsc.br/portal/sites/default/files/envenenamiento_arp.pdf

7.27 Interpolados. (01 de Marzo de 2017). *COMPARACIÓN ENTRE EL MODELO OSI Y EL MODELO TCP/IP*. Obtenido de Interpolados: https://interpolados.wordpress.com/2017/03/01/comparacion-entre-el-modelo-osi-y-el-modelo-tcpip/

7.28 Mamani Quisbert, D. J. (2013). Fases de un Ataque Hacker. *Revistas Bolivianas*, http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a29.pdf.

7.29 MazeLabs. (2013). *IT Security – ARP Poisoning.* Obtenido de Itsecurity.telelink.com: http://itsecurity.telelink.com/arp-poisoning/

7.30 McClure, S., Scambray, J., & Kurtz, G. (2010). *Hackers 6. Secretos y Soluciones de Seguridad en Redes.* Mc Graw Hill.

7.31 Microsoft. (2018). *¿Qué es la informática en la nube? Guía para principiantes | Microsoft Azure*. Obtenido de Azure.microsoft.com: https://azure.microsoft.com/es-es/overview/what-is-cloud-computing/

7.32 Molina Robles, F. J. (2014). *Redes locales.* Madrid: RA-MA Editorial.

7.33 Muspratt, A. (31 de jULIO de 2017). *Tapping into SaaS, PaaS and IaaS - An Introduction to Cloud*. Obtenido de Crozdesk Software Blog: https://blog.crozdesk.com/tapping-saas-paas-iaas/

7.34 Navarro Lacoba, R. (2014). *La guía exprés de redes.*

7.35 OWASP. (02 de Febrero de 2017). *Identificar a los atacantes en Servidores Web.* Obtenido de Owasp.org: https://www.google.com.ec/search?biw=681&bih=617&tbs=cdr%3A1%2Ccd_min%3A2016%2Ccd_max%3A2018&ei=Byt2WtTrIqOL5wK956CYAg&q=que+son+lammers&oq=que+son+lammers&gs_l=psy-ab.3..0i22i30k1.1215762.1218155.0.1218408.15.11.0.1.1.0.296.1798.0j1j7.8.0....0...1c.1.64.

7.36 Pérez Luna, A. (2014). *Instalaciones de Telecomunicaciones.* Madrid: Paraninfo .

7.37 Roa Buendía, J. (2013). *Seguridad informática.* McGraw-Hill España. Obtenido de http://puceftp.puce.edu.ec:2057/lib/pucesp/detail.action?docID=10692460

7.38 Romero Ternero, M. d., Barbancho Concejero, J., Benjumea Mondéjar, J., Rivera Romero, O., Ropero Rodríguez, J., Sanchez Antón, G., & Sivianes Castillo, F. (2014). *Redes Locales.* Madrid: Parainfo.

7.39 Santos Gonzáles, M. (2014). *Sistemas Telemáticos.* Madrid: Ra-Ma.

7.40 Socialetic. (01 de Julio de 2018). *¿Qué es el Hacking Ético y para qué sirve? | Socialetic*. Obtenido de Socialetic.com: https://www.socialetic.com/que-es-el-hacking-etico-y-para-que-sirve.html

7.41 Tanenbaum, A. S., & Wetherall, D. J. (2012). *Redes de Computadoras* (Quinta ed.). Mexico: Pearson.

7.42 Textoscientificos.com. (02 de Octubre de 2006). *TCP/IP y el modelo OSI | Textos Científicos*. Obtenido de Textoscientificos.com: https://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

7.43 Valdivia Miranda, C. (2015). *Redes Telemáticas.* Madrid: Ediciones Paraninfo, S.A.

8. ANEXOS

8.1 Desarrollo del Ataque y Mitigación de ARP Poisoning – MitM

8.1.1 Averiguar la dirección IP y MAC del atacante (Kali Linux) usando el comando *"ifconfig"*.

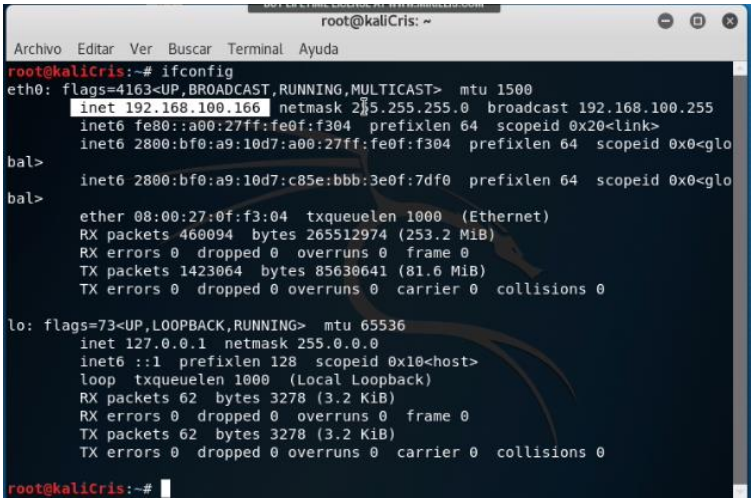


***Ilustración 8.1**: "Dirección IP y MAC del atacante ARP Poisoning – Hombre en el Madio"*

8.1.2 Se usa la máquina virtual "Kali Linux" y buscamos la herramienta "Ettercap".

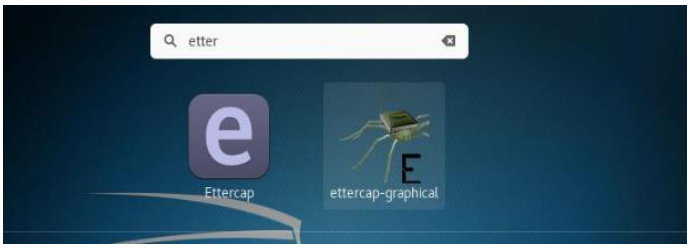


***Ilustración 8.2**: "Herramienta Grafica Ettercap"*

8.1.3 Se despliega la interfaz gráfica de la aplicación



***Ilustración 8.3**: "Despliegue Gráfico de Ettercap"*

8.1.4 Ir a la pestaña "Sniff", a continuación "Unified Sniffing" para buscar la interfaz de red con la que va a trabajar.

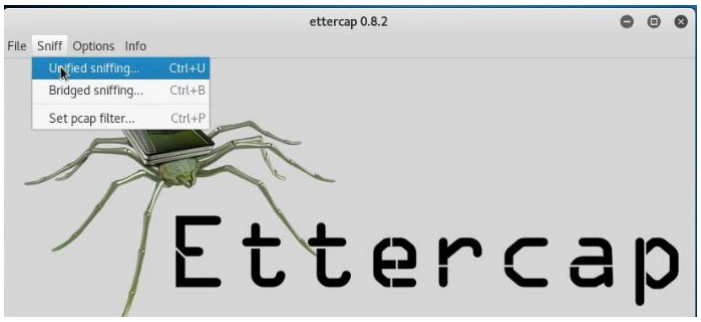


***Ilustración 8.4**: "Búsqueda de interfaz de red a trabajar"*

8.1.5 Se selecciona la interfaz de red "eth0".

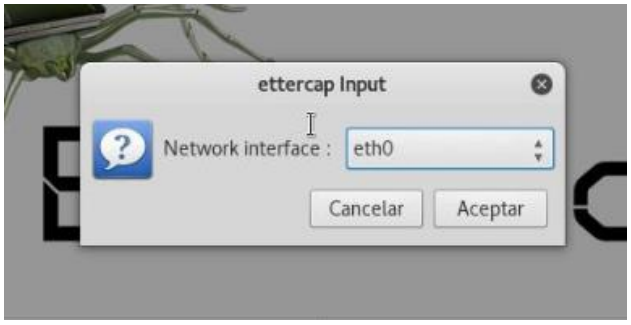


***Ilustración 8.5**: "Selección de interfaz de red"*

8.1.6 Se despliega la información actual de la máquina como dirección MAC y direcciones IP con las cuales trabajará. Además, se carga plugins, puertos…



***Ilustración 8.6**: "Información actual de la Máquina Atacante"*

8.1.7 Se realiza un escaneo de los equipos que se encuentre conectados a la red

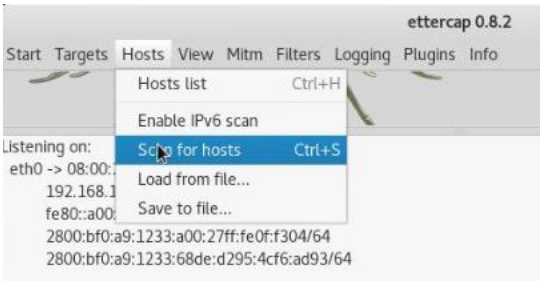


***Ilustración 8.7**: "Escaneo de Equipos Disponibles en la Red"*

8.1.8 Se han encontrado 7 equipos en la red, los cuales incluye los equipos victimas para realizar este ataque.

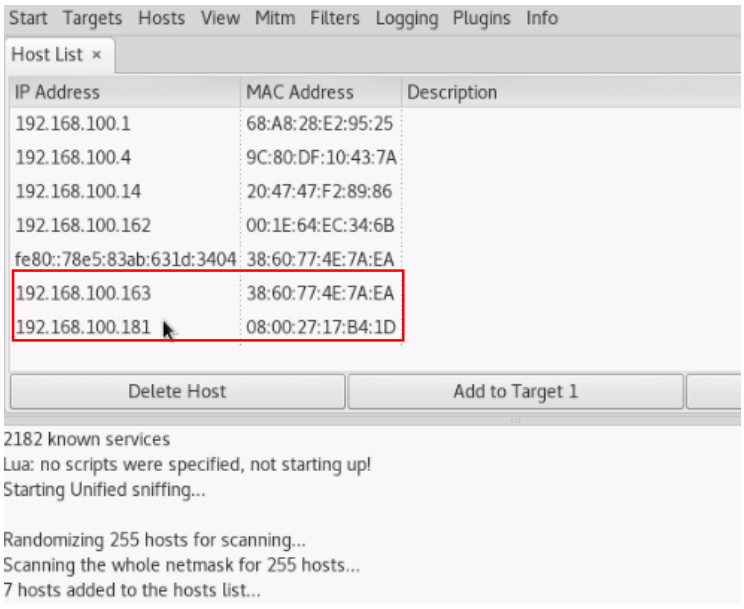


***Ilustración 8.8**: "Búsqueda de equipos victimas en la red "*

8.1.9 En la pestaña Hosts, seleccionar la opción "Host list", de esta manera se registran todos los hosts disponibles en red.

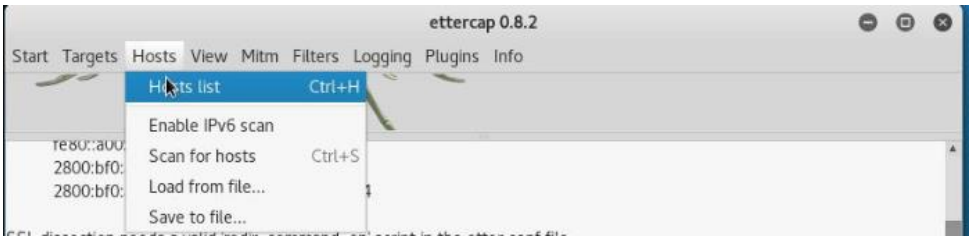


***Ilustración 8.9**: "Registro de Posibles Máquinas Victimas "*

8.1.10 Verificar cuales son las direcciones IP de las maquinas objetivos, en este caso la máquina virtual "Metasploitable" trabajará como una puerta de enlace y "Windows 7" como la maquina a atacar. Tomar en cuenta que para averiguar esta información es necesario utilizar los comandos *"ifconfig"* (Linux) e *"ipconfig"* (Windows)

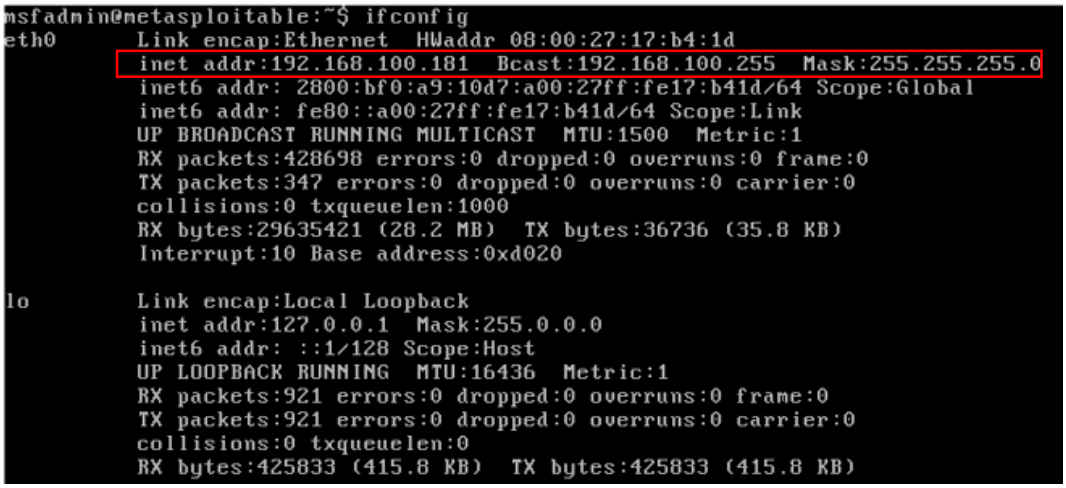


***Ilustración 8.10**: "Dirección IP de Metasploitable "*

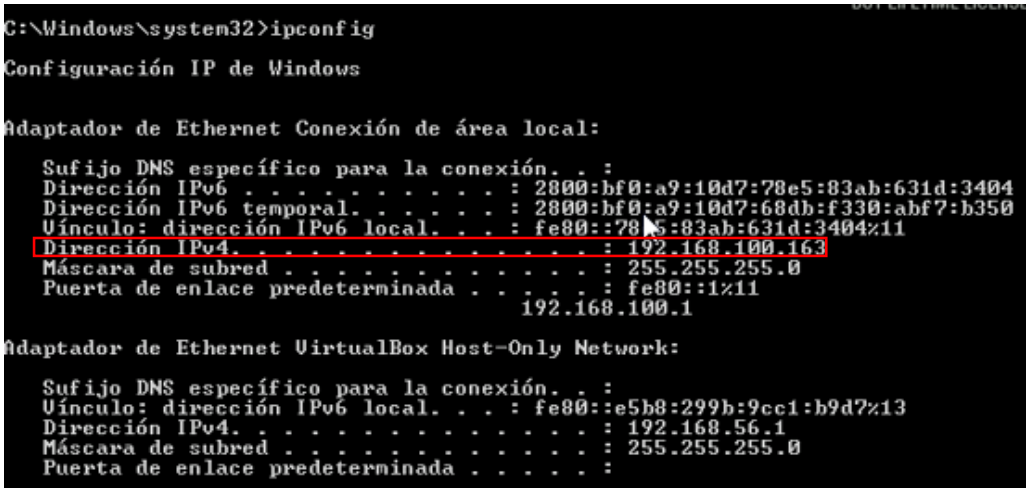


***Ilustración 8.11**: "Dirección IP de Windows "*

8.1.11 Seleccionar las maquinas objetivos para el ataque

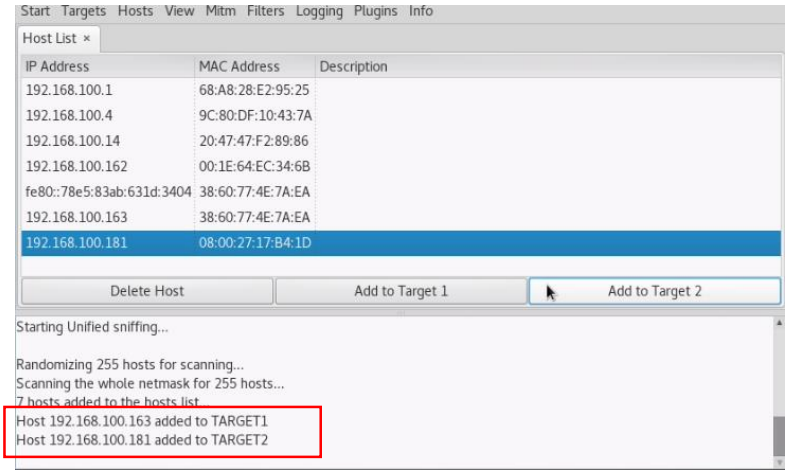


***Ilustración 8.12**: "Selección maquinas victimas"*

8.1.12 Nos dirigimos a la pestaña MitM (Man in the Middle), y seleccionamos en "ARP Poisoning"

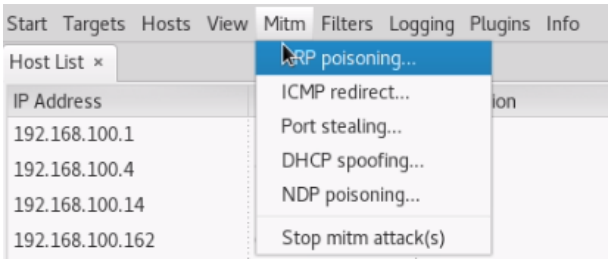


***Ilustración 8.13**: "Selección ataque ARP Poisoning mediante MitM"*

8.1.13 En el cuadro de dialogo que se despliega, se marca "Sniff remote conections", seguido de "Aceptar".



***Ilustración 8.14**: "Sniff remote connections"*

8.1.14 Como se observa, se realiza la asociación de las direcciones MAC con sus respectivas direcciones IP.

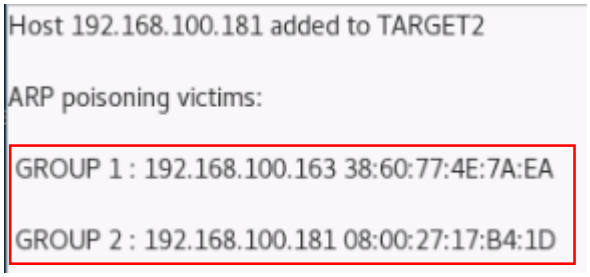


***Ilustración 8.15**: "Asociación de direcciones MAC e IP"*

8.1.15 A continuación, se selecciona en el menú principal "Plugins", el cual dirige a una serie de posibles plugins a usarse, en este caso será *"remote_browser"* (ver páginas web de la maquina a victima), de esta manera tomará toda la información que atraviese por la red. Para un monitoreo profundo, se trabaja con la dirección IP 192.168.100.163 con dirección MAC 38:60:77: 4E:7A: EA.

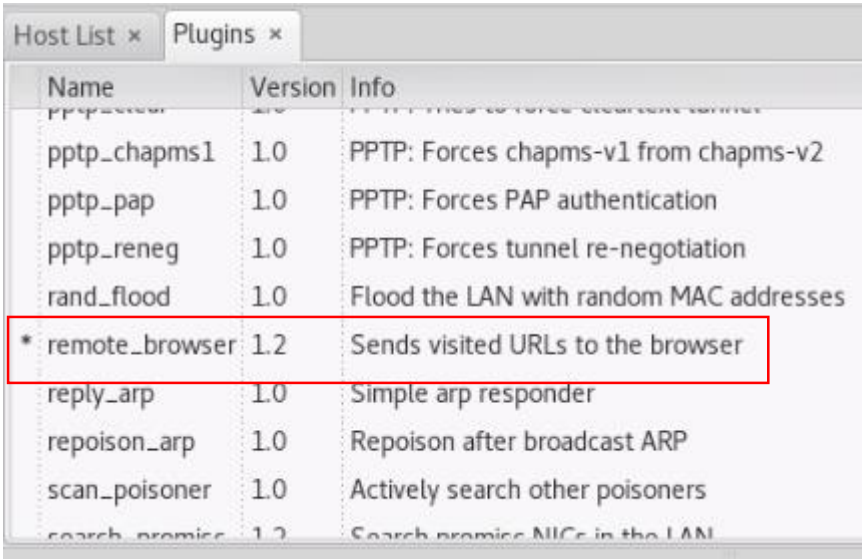


***Ilustración 8.16**: "Selección de Plugin remote_browser"*

8.1.16 Nos dirigimos al log de la aplicación y como se puede observar, el ataque se realizó con éxito

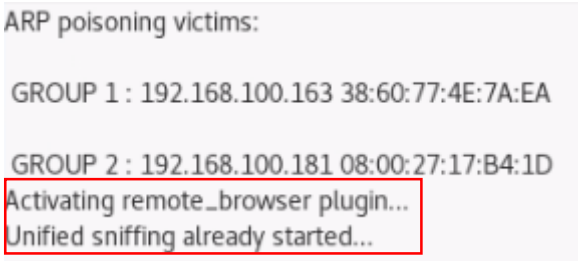


***Ilustración 8.17**: "Log de Ettercap"*

8.1.17 Para verificar que las direcciones MAC se encuentran suplantadas, utilizamos el cmd con el comando *"arp -a"*

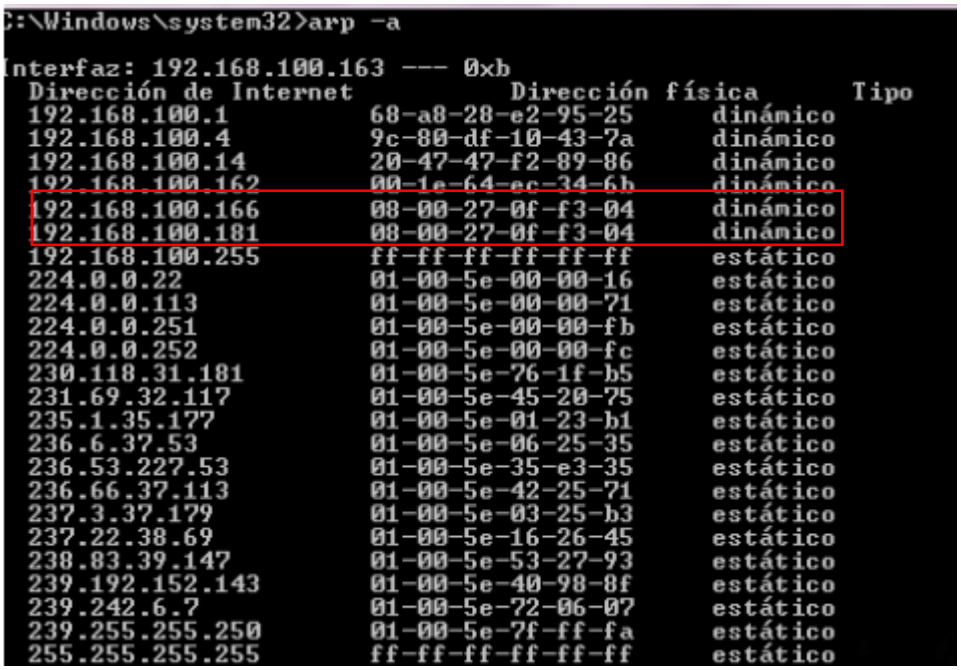


***Ilustración 8.18**: "Ataque direcciones MAC"*

8.1.18 Como medida preventiva para este tipo de ataque se usa entradas estáticas, es decir permitir que ciertos equipos con sus respectivas direcciones IP y MAC puedan ingresar en las máquinas. Tomando en cuenta que la configuración de esta mitigación en los equipos es muy fácil cabe recalcar que es muy útil.

8.1.19 Para configurar, estas direcciones y que solo permitan pasar información se debe abrir un CMD en modo de administrador y agregar las rutas estáticas necesarias con el comando *"arp –s (dirección IP) (dirección MAC)"*.

8.1.20 Sin embargo, otros comandos que aseguran la asignación de estas direcciones es "*netsh", "interface", "ipv4" "add neighbors "Conexión de área local" (dirección IP) (dirección MAC)".* Como se puede ver en la Ilustracion 7-19, se ha agregado la entrada estática correctamente.

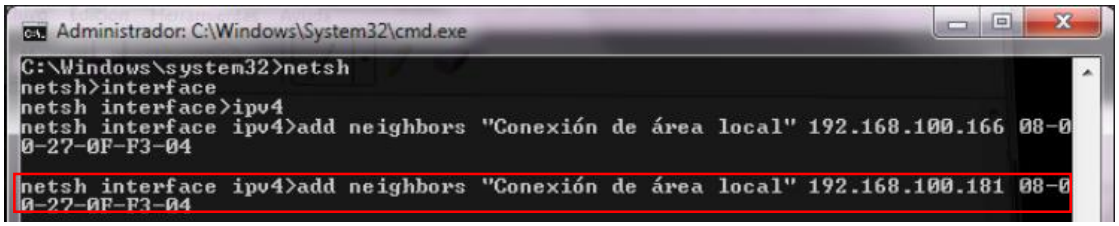


***Ilustración 8.19**: "Asignación de Direcciones Estáticas"*

8.1.21 Verificamos que la entrada estática se agregara correctamente, utilizando el comando *"arp -a"*.

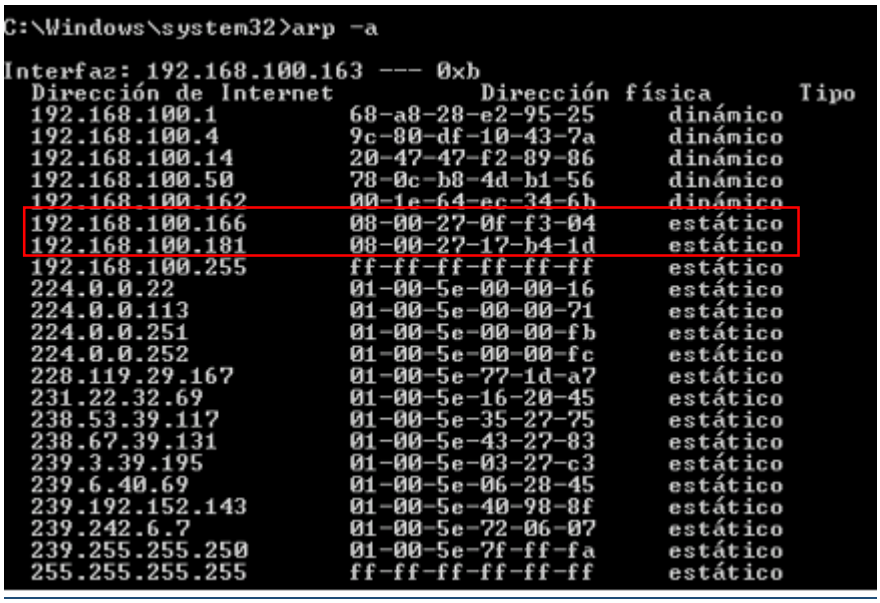


***Ilustración 8.20**: "Asignación de Rutas Estáticas"*

8.1.22 Realizamos nuevamente el ataque (paso 7.1 - 7.1.16). Se captura nuevamente el tráfico con la herramienta “Wireshark” y cómo podemos observar en la Ilustración 7-21 el ataque se encuentra mitigado correctamente debido a que la dirección MAC no cambia en lo absoluto.

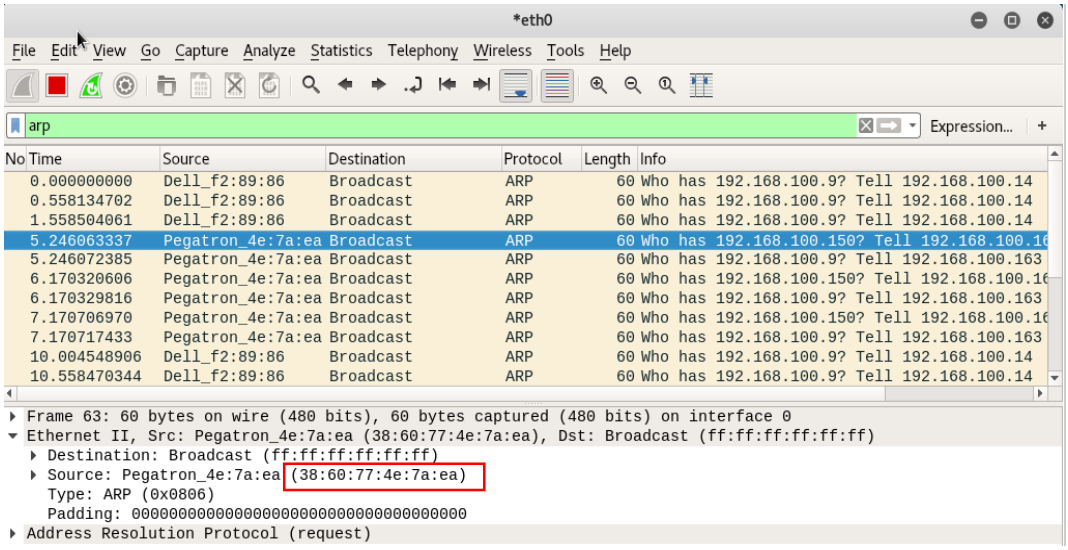


***Ilustración 8.21**: “Mitigación después del Ataque”*

8.2 Desarrollo del Ataque y Mitigación de CDP –Denegación de Servicio

8.2.1 Para realizar este ataque es necesario utilizar una aplicación que ayude a la simulación de routers y switchs, llamada GNS31. Se ha realizado la siguiente topología para simular este tipo de ataque, cabe recalcar que se ha utilizado subredes dentro de la red 192.168.100.0/24.

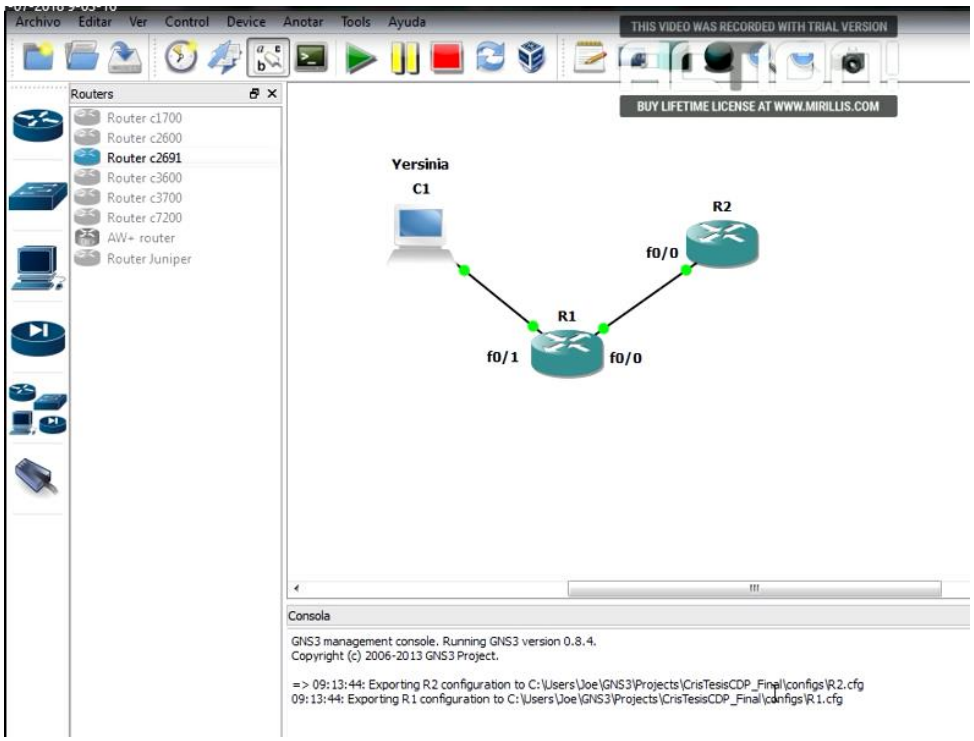


***Ilustración 8.22**: "Diseño de Red para Ataque de red CDP – Denegación de Servicios"*

8.2.2 Se abre una consola en el sistema operativo Kali Linux, y se digita el comando *"sudo yersinia -G"*, de tal manera que se abra la aplicación gráfica.

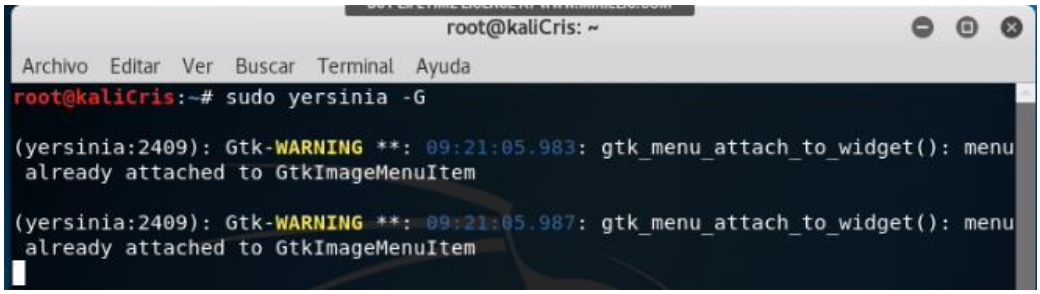


***Ilustración 8.23**: "Llamar Modo Gráfico de Yersinia"*

8.2.3 Se despliega la siguiente interfaz, el cual es muy amigable para el usuario y realizar diferentes tipos de ataques

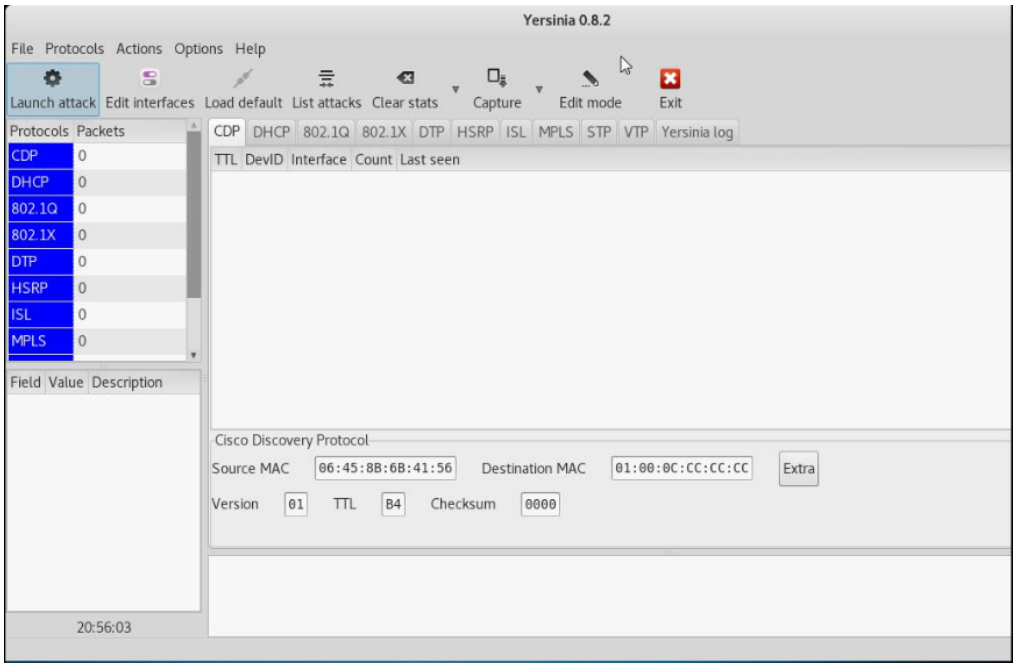


***Ilustración 8.24**: "Interfaz de la herramienta Yersinia de Kali Linux"*

8.2.4 Seleccionar la pestaña CDP seguido de "Launch Attack", para observar las opciones y realizar este tipo de ataque.

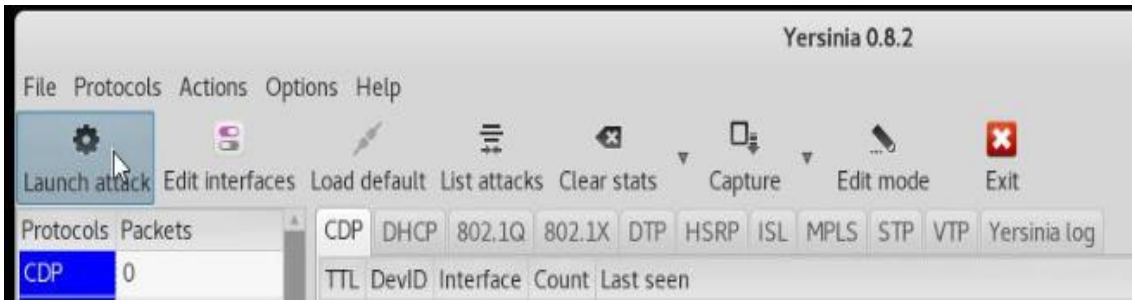


***Ilustración 8.25**: "Cargar tipo de ataque CDP"*

8.2.5 Seleccionar la pestaña CDP, seguido de "Flooding CDP table"

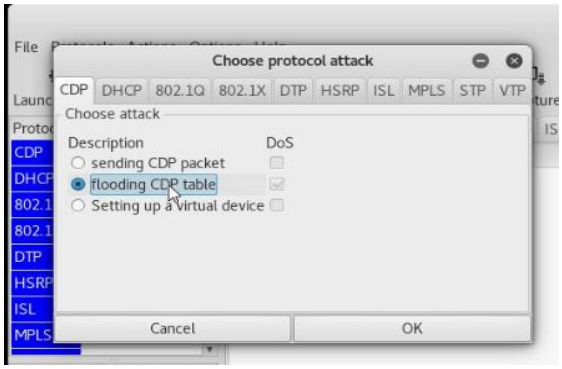


***Ilustración 8.26**:* "Cargar ataque de Inundación de tabla CDP"

8.2.6 El ataque ha empezado a realizarse con éxito, como se puede observar aumenta rápidamente el número de CDP enviados, generando Denegaciones de Servicio.

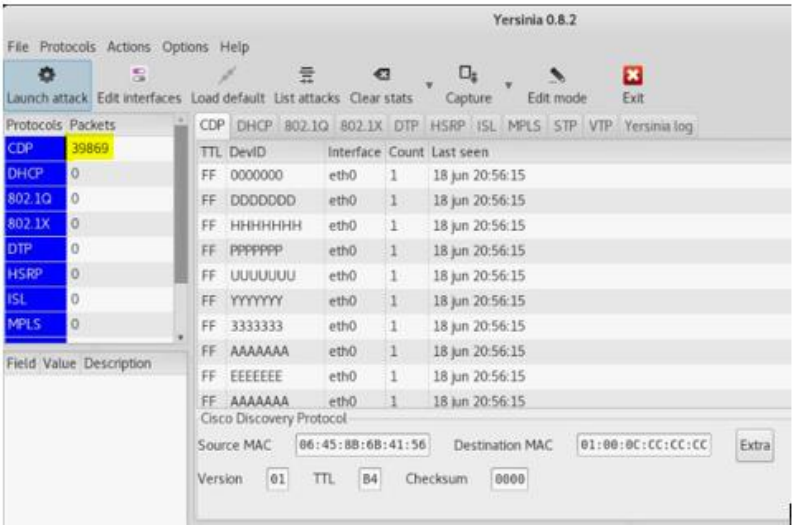


***Ilustración 8.27**:* "Incremento notable de paquetes CDP"

8.2.7 La pestaña "Yersenia Log", nos indica si el ataque ha sido efectuado con normalidad



***Ilustración 8.28**: "Log Yersinia"*

8.2.8 Además, para comprobar este tipo de ataque, se realiza un filtro en la aplicación "Wireshark" con la dirección 192.168.100.163.

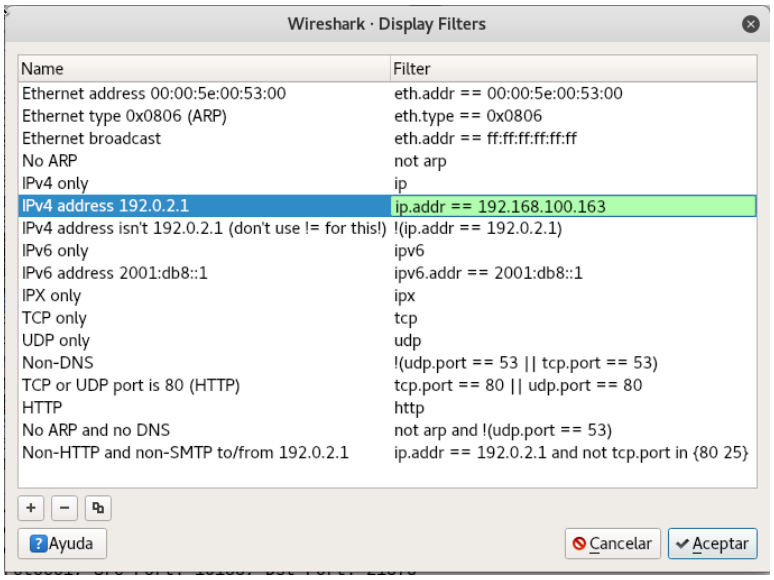


***Ilustración 8.29**: "Filtrado de dirección IP en Wireshark"*

8.2.9 Como se puede observar existe un ataque de inundación CDP

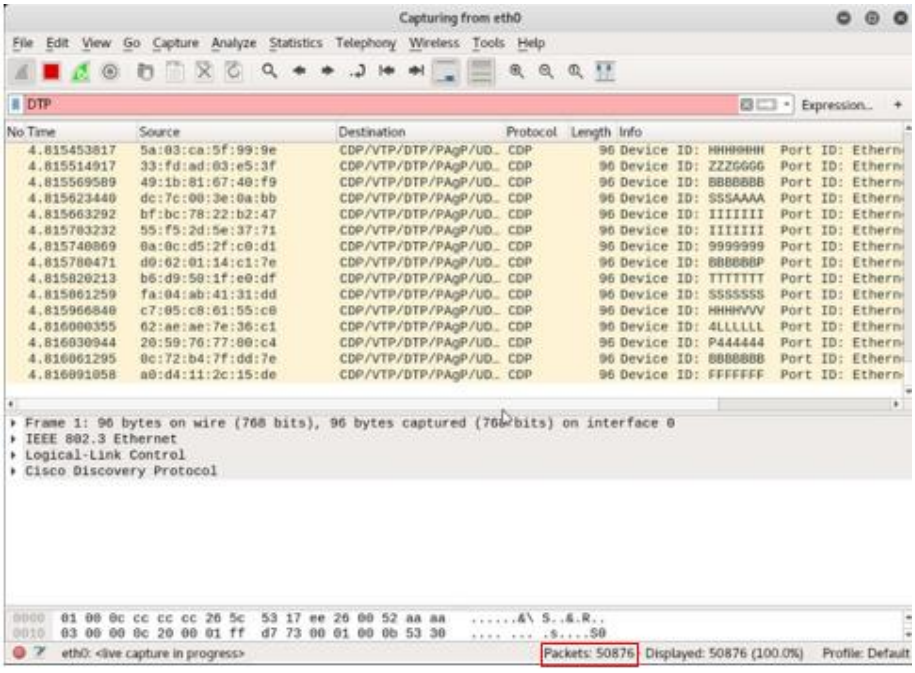


***Ilustración 8.30**: "Captura de paquetes CDP en Wireshark"*

8.2.10 Finalmente, podemos observar en el Log de Yersinia que el ataque en pocos minutos puede llegar a llenar la tabla CDP rápidamente

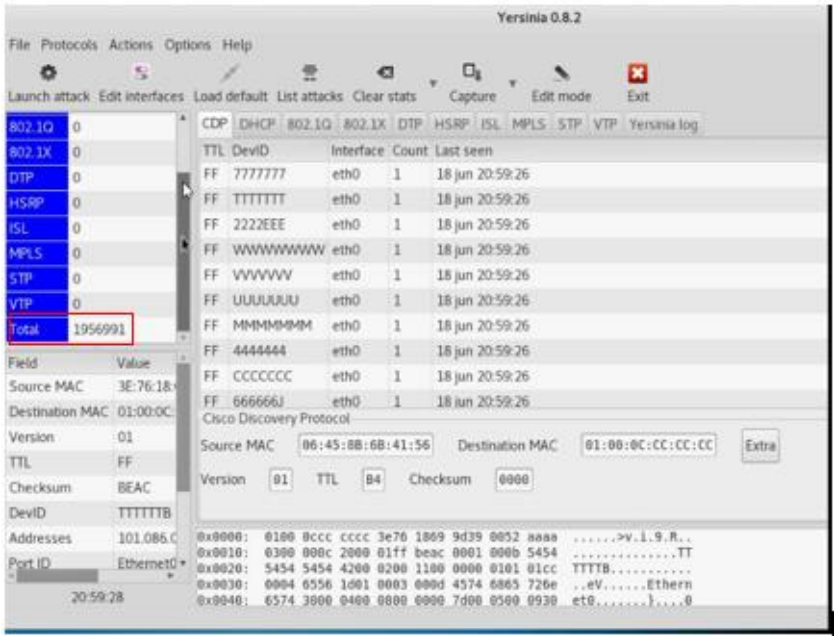


***Ilustración 8.31**: "Log de Yersinia"*

8.2.11 Para mitigar este tipo de ataque es necesario realizar las respectivas configuraciones en los routers que se muestran a continuación. Seleccionamos el modo consola de cada uno de los dispositivos de red.



***Ilustración 8.32**: "Log de Yersinia"*

8.2.12 Establecemos las direcciones IP y la máscara de cada uno de los routers Ilustración 7-33 para realizar esto se digita en la consola de GNS 3 los siguientes comandos *"conf t", "interface (nombre de la interface)", "ip add (dirección IP)", "no sh"*



***Ilustración 8.33**: "Configuración Router 1"*

8.2.13 Se configura el enlace del Router 1 al Router 2 con los comandos mencionados anteriormente:

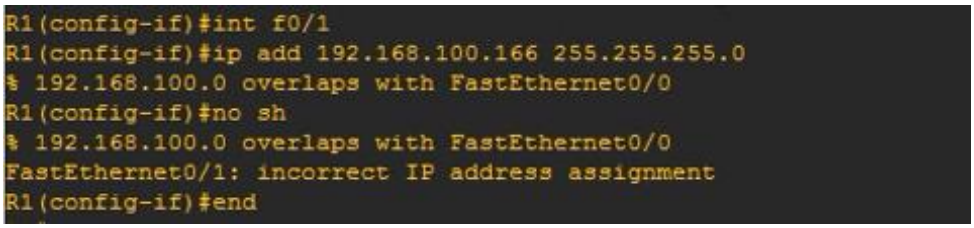


***Ilustración 8.34**: "Configuración enlace Router 1 a Router 2"*

8.2.14 Para la configuración del router 2 se tiene:

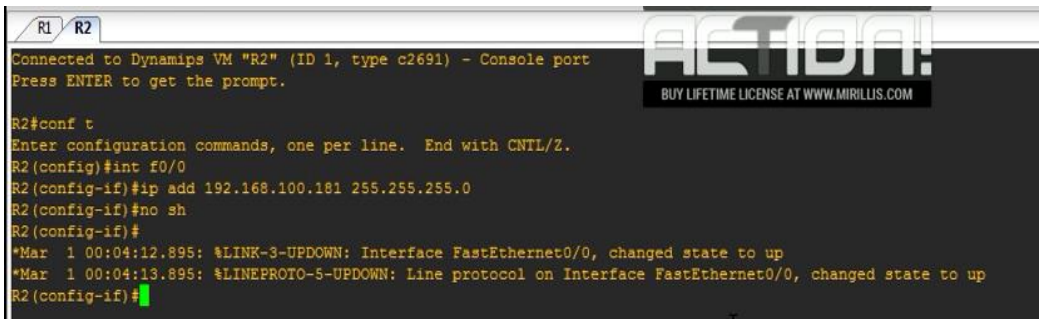


***Ilustración 7.35**:* "Configuración Router 2"

8.2.15 Para mitigar este ataque se debe deshabilitar el protocolo CDP en la misma consola del Router 1, se realiza esta acción con el comando *"no cdp enable" y "no cdp run"*, para visualizar que se realizará esta acción se digita el comando *"show cdp"*, tomar en cuenta que para este comando debe estar fuera del modo de configuración digitando el comando *"exit"*.

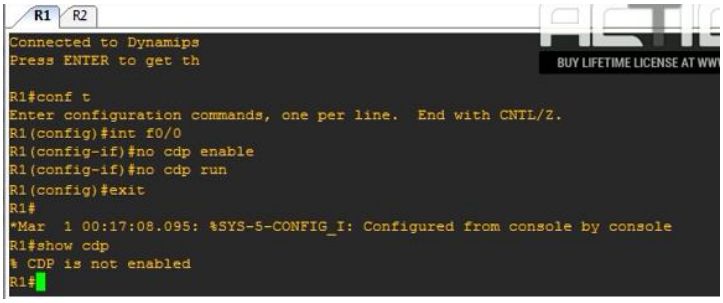


***Ilustración 8.36**: "Configuración Router 2"*

8.2.16 Realizamos los pasos 7.2.1 hasta 7.2.10, de manera que simule el ataque nuevamente. Capturamos el tráfico con la herramienta "Wireshark" y como se puede observar el sistema se estabiliza nuevamente (observar el número de paquetes en aumento). Por otro lado, como podemos ver el ataque se ha mitigado ya que no está enviado información irrelevante por que el tráfico de la maquina víctima se regulariza detallando su dirección IP, MAC, protocolos…

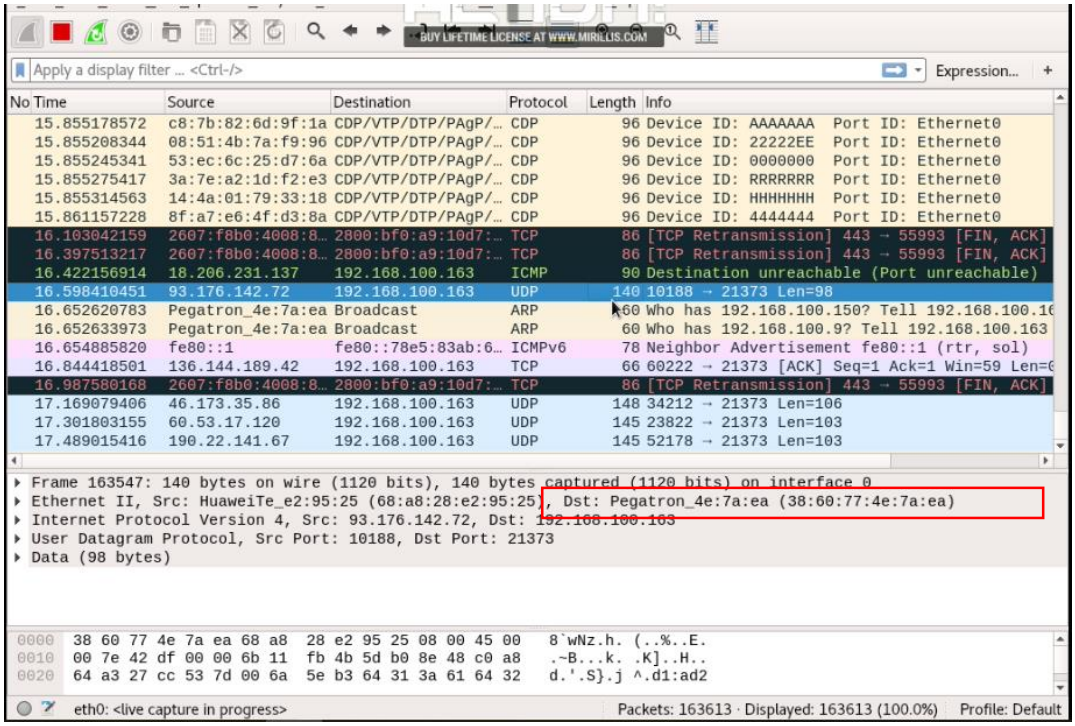


***Ilustración 8.37**: "Captura de Mitigación del Ataque CDP- Denegación de Servicio"*

8.3 Desarrollo del Ataque y Mitigación de DHCP – Hombre en el Medio

8.3.1 Para realizar este ataque es necesario utilizar la aplicación Cisco Packet Tracer que ayude a simular routers y switchs dentro de una red. Se ha realizado la siguiente topología para simular este tipo de ataque, cabe recalcar que se ha utilizado subredes dentro de la red 192.168.100.0/24.

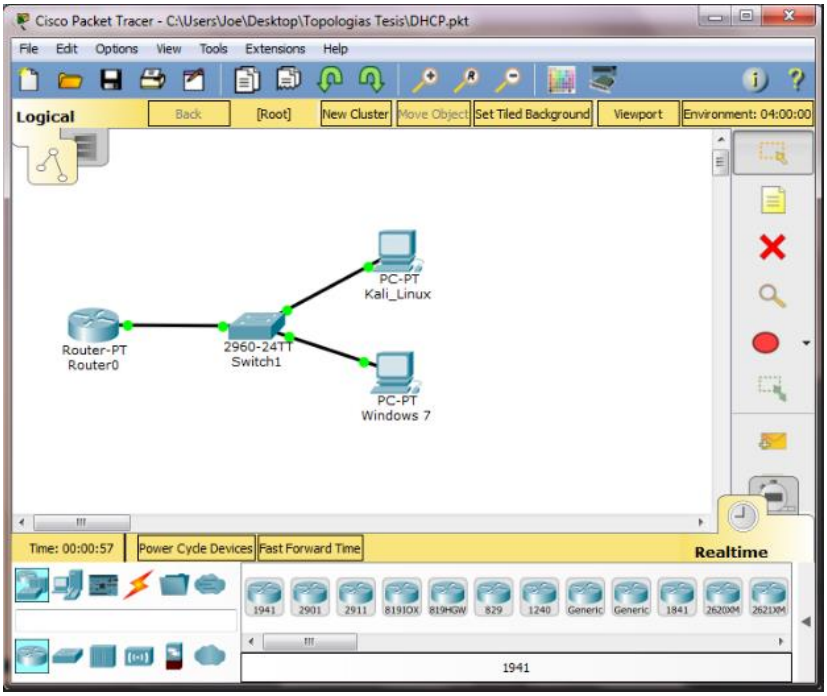


***Ilustración 8.38**: "Diseño de red para realizar ataque DHCP - Denegación de Servicio"*

8.3.2 Abrir una consola en el sistema operativo Kali Linux y digitar el comando "sudo yersinia -G"

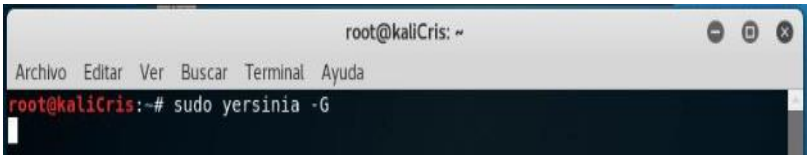


***Ilustración 8.39**: "Desplegar el modo grafico de la herramienta Yersinia"*

8.3.3 Abrir una consola en el sistema operativo Kali Linux y digitar el comando “sudo yersinia -G”

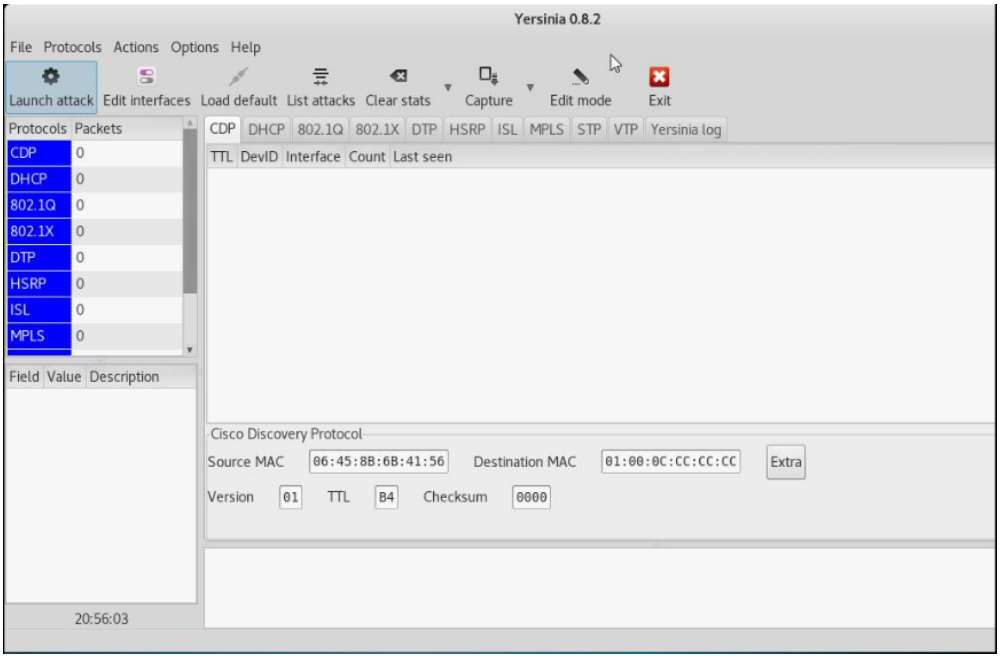


***Ilustración 8.40**: “Modo grafico de la herramienta Yersinia”*

8.3.4 Seleccionar la pestaña DHCP

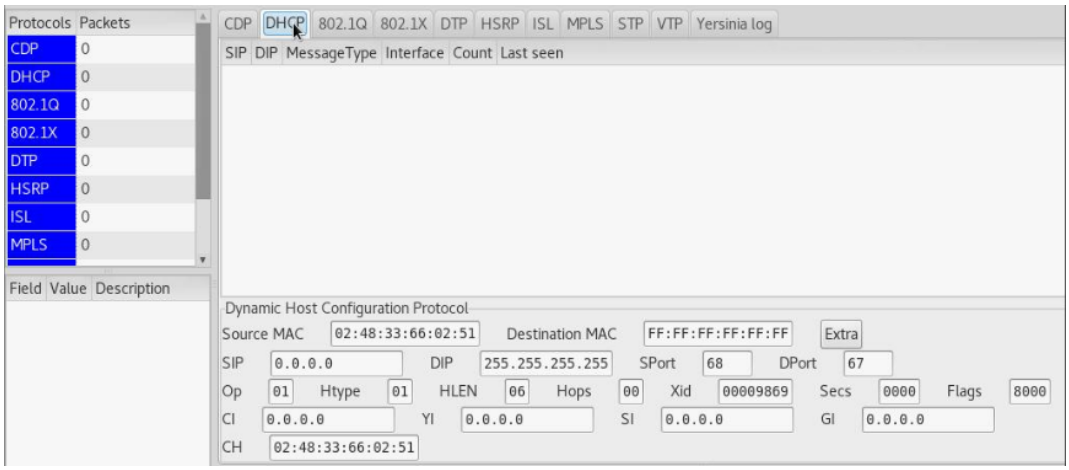


***Ilustración 8..41**: “DHCP en Yersinia”*

8.3.5 Presionar “Launch Attack”

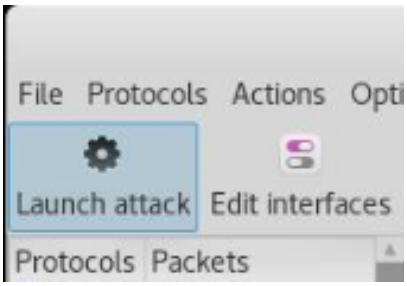


***Ilustración 8.42**: "Cargar Ataque en DHCP Yersinia"*

8.3.6 A continuación, se despliega las siguientes opciones y se selecciona "sending DISCOVER packet"

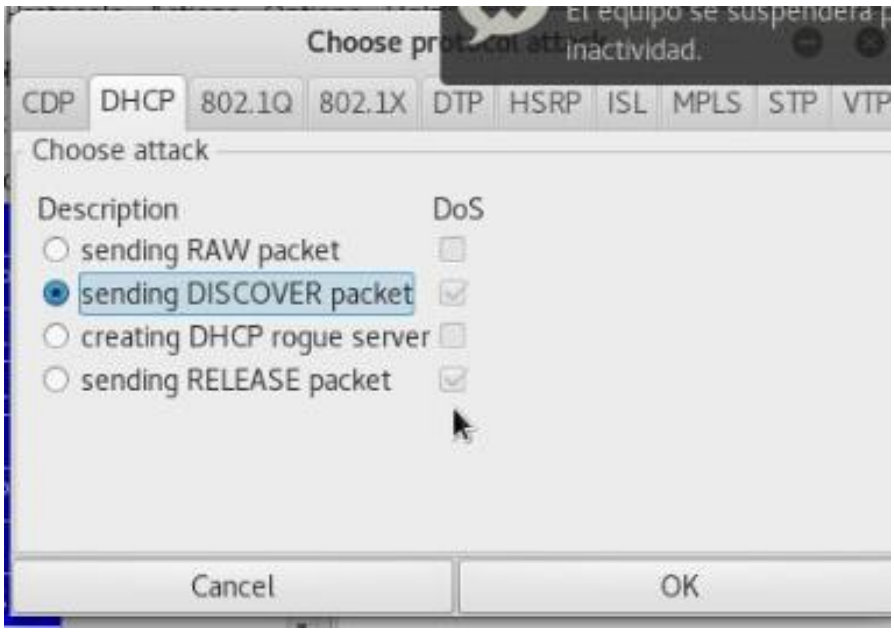


***Ilustración 8.43**: "Seleccionar tipo de Ataque DHCP"*

8.3.7 Se inicia el ataque llenando con direcciones MAC origen, como se puede observar los DHCP se llenan rápidamente

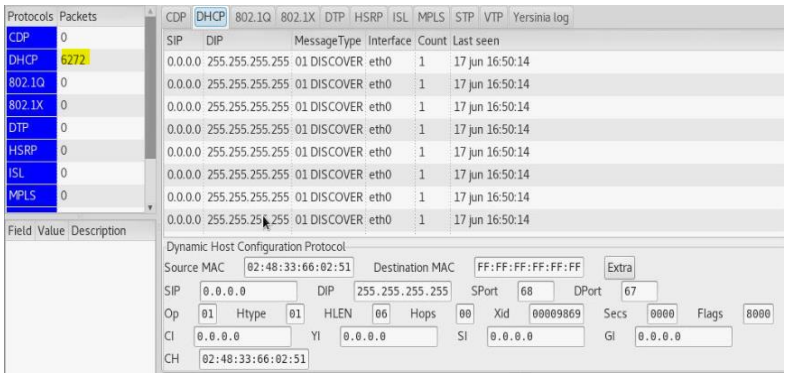


***Ilustración 8.44**: "Inundación de direcciones MAC "*

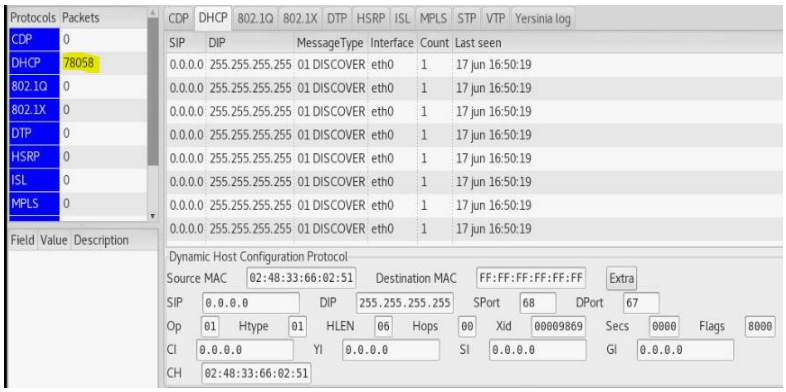


***Ilustración 8.45**: "Crecimiento de paquetes DHCP"*

8.3.8 Para mitigar este tipo de ataque es necesario que el switch se configure en modo "DHCP Snooping".

8.3.9 Buscar máquinas para configurar su IP automático a través del DHCP

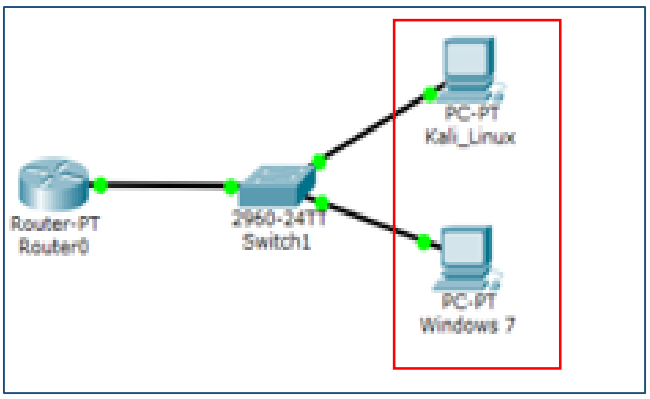


***Ilustración 8.46**: "Maquinas a configurar su IP"*

8.3.10 Ir a las configuraciones de las maquinas antes mencionadas

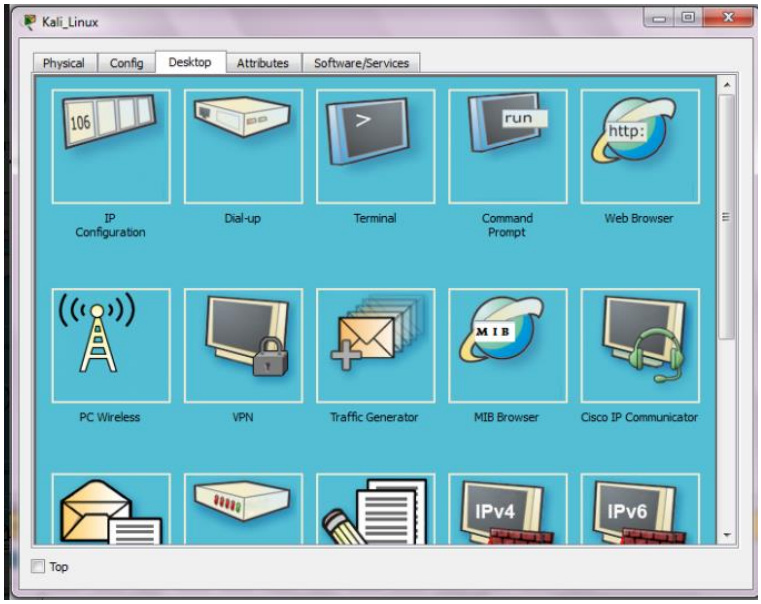


***Ilustración 8.47**: "Configuración IP "*

8.3.11 Seleccionar DHCP y automáticamente establecerá una dirección IP automático dentro de la red.

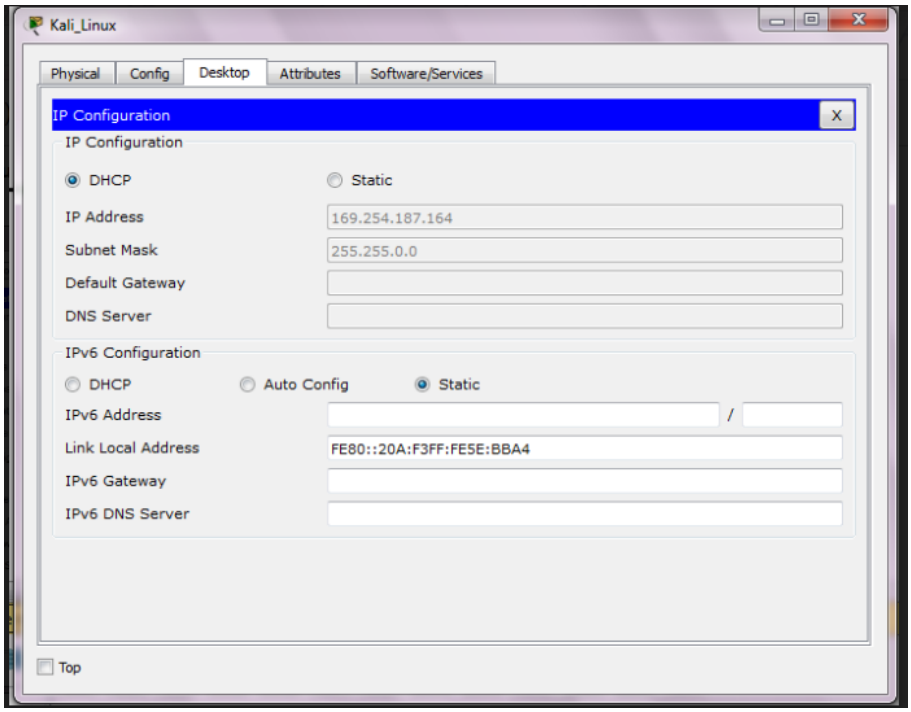


***Ilustración 8.48**: "Establecer Dirección IP mediante DHCP "*

8.3.12 Dentro del switch se digita los siguientes comandos en la consola del switch *“enable”, “configure t”, “ip dhcp snooping”, “ip dhcp snooping vlan 1”, interface f0/1, “ip dhcp trust”, “interface dhcp f0/2”, “ip dhcp trust”.*

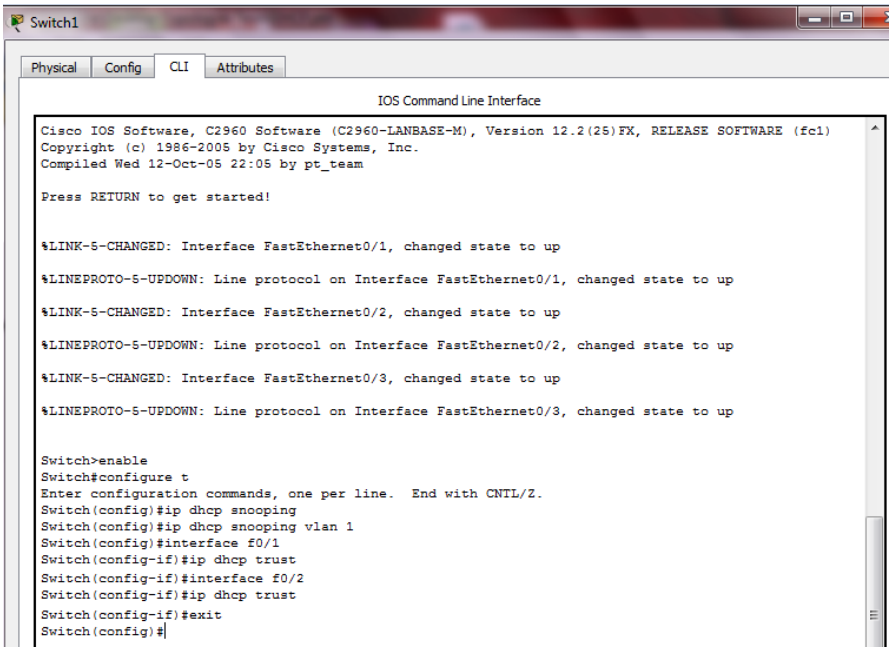


Ilustración 8.49*:* “Configuración switch en modo DHCP Snooping”

8.3.13 Visualizar la mitigación del ataque. Como se puede observar en la Ilustración 7-49, el ataque se ha detenido y empieza a circular de nuevo información sin problemas.

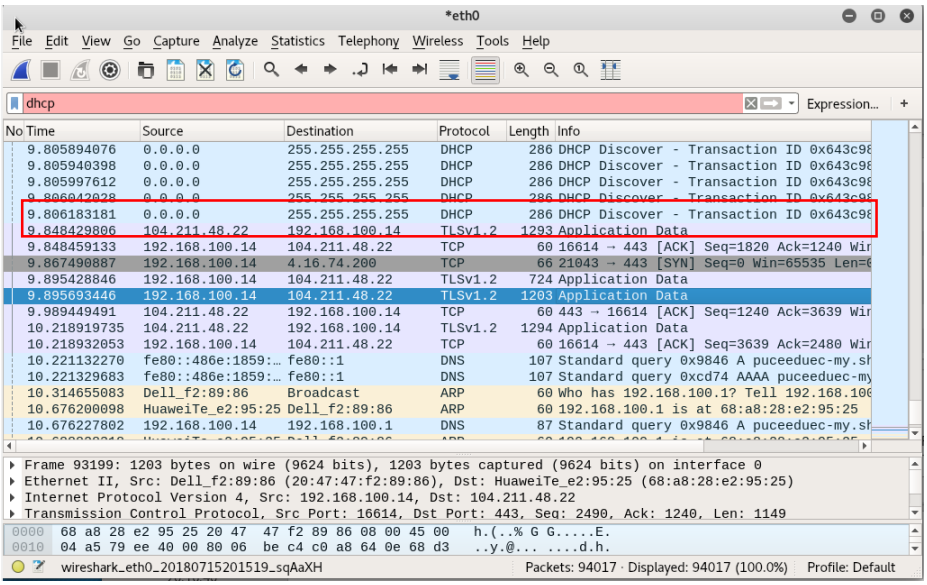


***Ilustración 8.50**: "Visualización de la Mitigación del DHCP-Denegación de Servicios"*

8.4 Desarrollo del Ataque y Mitigación de Syn Flood

8.4.1 Realizar un escaneo de puerto con la aplicación "Zenmap" hacia la subred 192.168.100.181 (Sistema Operativo Metasploitable), se usa la para detallar los puertos vulnerables de la víctima:

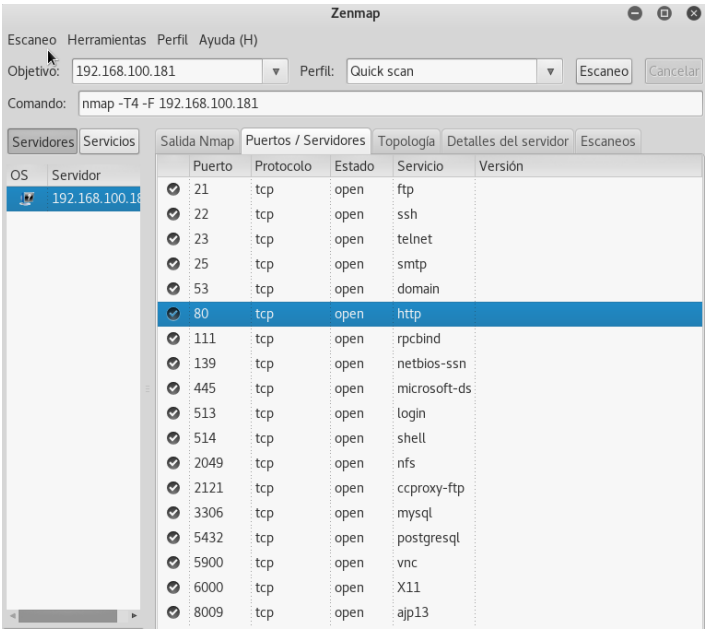


***Ilustración 8.51**: "Escaneo de puerto Zenmap "*

8.4.2 En el sistema operativo Kali Linux, abrir un terminal “Metasploit”

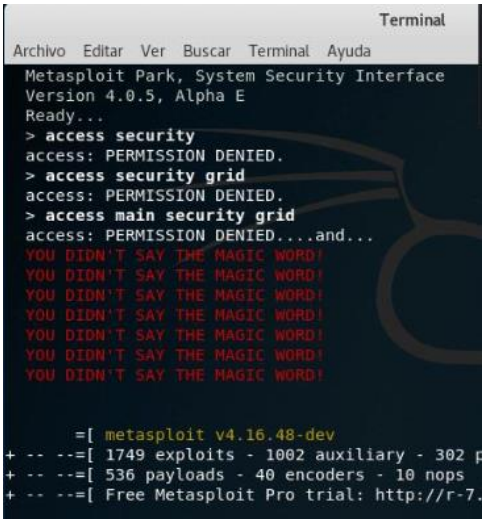


Ilustración 8.52*: “Terminal Metasploit de Kali Linux”*

8.4.3 Se digita el comando *“Search telnet”* de esta manera buscamos el tipo de vulnerabilidades para este puerto:

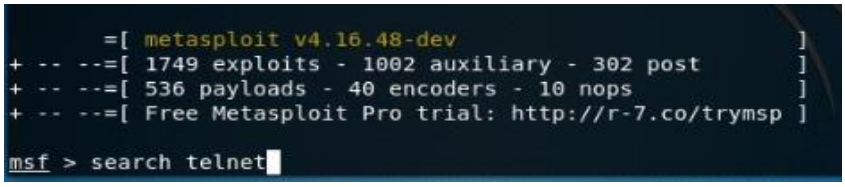


Ilustración 8.53*: “Buscar Tipo de Vulnerabilidades Telnet”*

8.4.4 Se lista todas las vulnerabilidades, tomando en cuenta que para este tipo de ataque utilizamos *“use auxiliary/dos/tcp/synflood”*, adicionalmente mostramos las opciones con el comando *“show options”:*

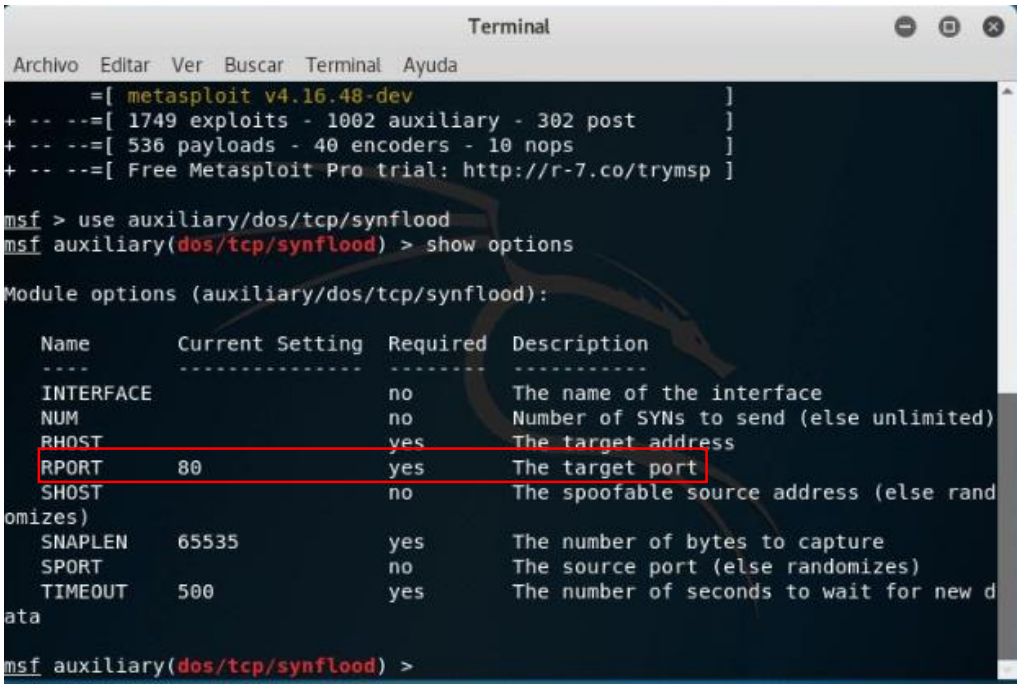


***Ilustración 8.54**: "Buscar Tipo de Vulnerabilidades Telnet"*

8.4.5 Una vez establecido este paso, es necesario establecer la víctima, como podemos observar la Figura… se encuentra vacío la dirección del objetivo:

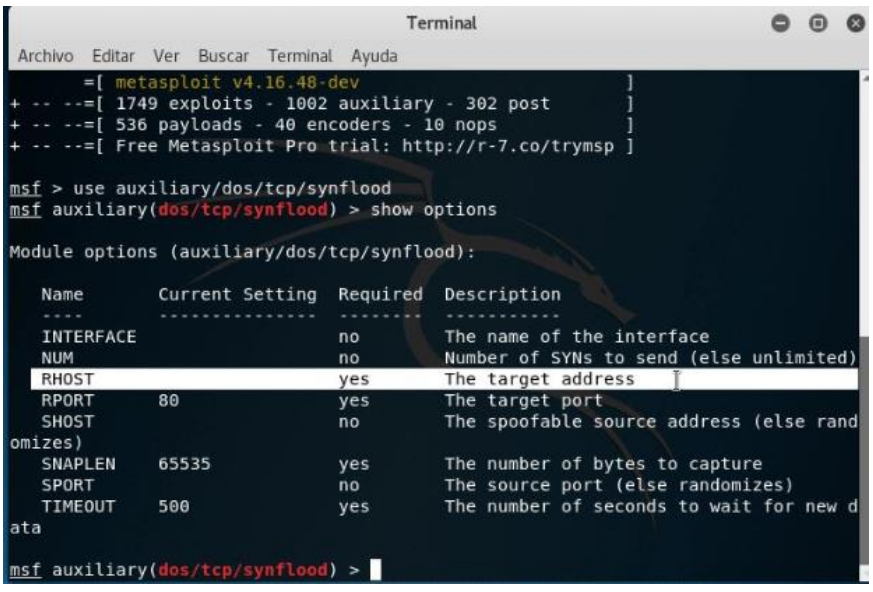


***Ilustración 8.55**: "Dirección Victima Vacío "*

8.4.6 Una vez establecido este paso, se establece la víctima, se usa el comando *"set RHOST (Dirección IP),* y mostramos las opciones para revisar que la dirección se encuentre correctamente con el comando *"show options"*

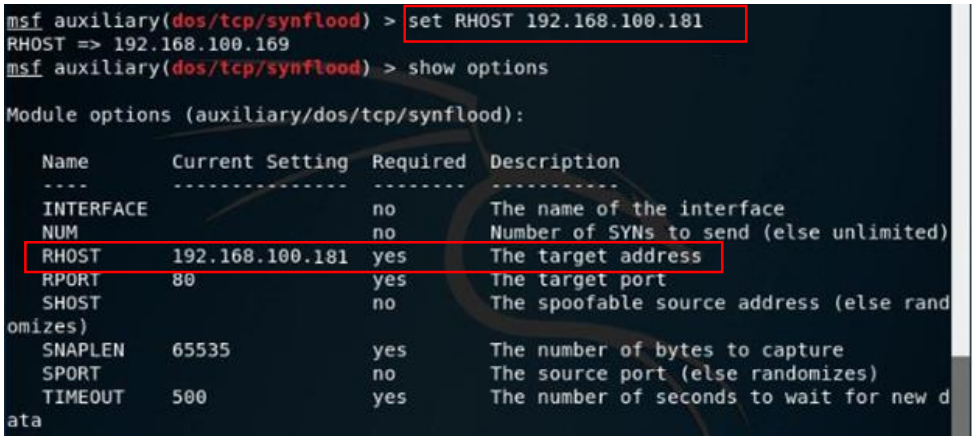


***Ilustración 8.56**: "Dirección Victima Establecida "*

8.4.7 Ejecutar el comando *"run"* y el ataque comenzará



***Ilustración 8.57**: "Inicio del Ataque Syn Flood – Denegación de Servicios "*

8.4.8 Para visualizar el ataque, capturamos el tráfico que atraviesa por la red; como observamos la víctima se empezó a consumir rápidamente sus recursos desembocando en denegaciones de servicios, sin conexión a internet e incluso el equipo era muy lento.

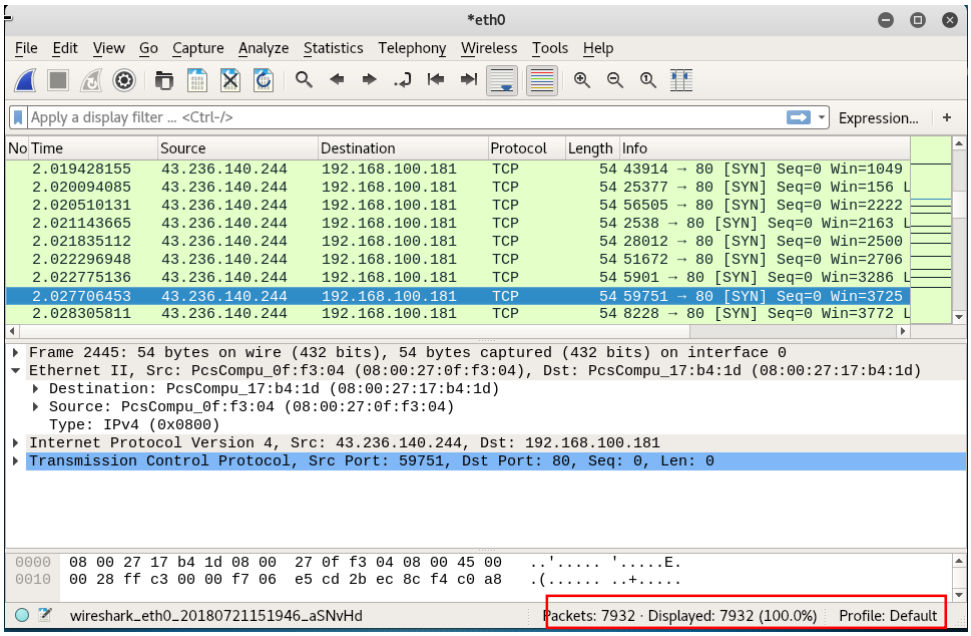


***Ilustración 8.58**: "Inicio del Ataque Syn Flood – Denegación de Servicios "*

8.4.9 Para mitigar este tipo de ataque se realiza la instalación de una pasarela de red la cual permita bloquear el tráfico por el puerto 80 y solo permitir tráfico de direcciones confiables.

8.4.10 Descarga Untangle de su página oficial debido a que es recomendado trabajar en su última versión, para este tipo de mitigación se usara 14.0.0 (https://www.untangle.com/get-untangle/)

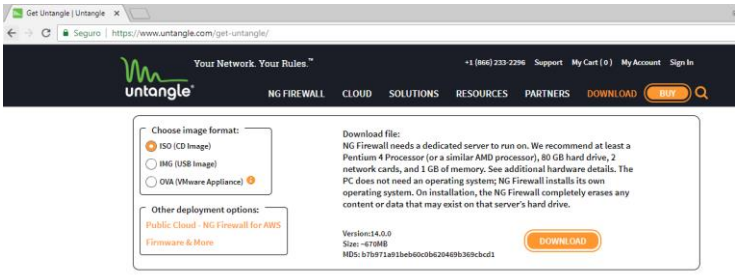


***Ilustración 8.59**: "Descarga de Untangle"*

8.4.11 Utilizar una máquina virtual Oracle VM VirtualBox e instalar Untangle, cuando el proceso de instalación finalice; desplegara lo siguiente:

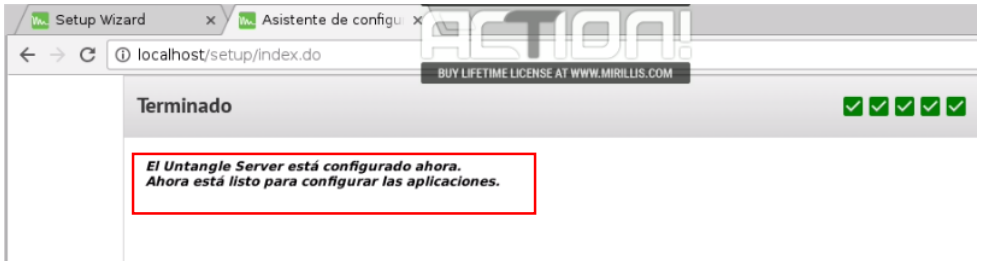


***Ilustración 8.60**: "Finalización de la Instalación de Untangle"*

8.4.12 Crear una cuenta Untagle, caso contario logearse para su ingreso



***Ilustración 8.61**: "Creación de Cuenta Untangle"*

8.4.13 Verificar que la tarjeta de red se encuentre activa, dirigirse a la pestaña Interfaces



***Ilustración 8.62**: "Verificación de Tarjeta de Red"*

8.4.14 Añadir una regla, la cual indique que todo el tráfico de la dirección 192.168.100.181 tiene que bloquearse



***Ilustración 8.63**: "Bloqueo del Puerto 80"*

8.4.15 Añadir una regla, que indique que el tráfico de la dirección 192.168.100.181 deba bloquearse

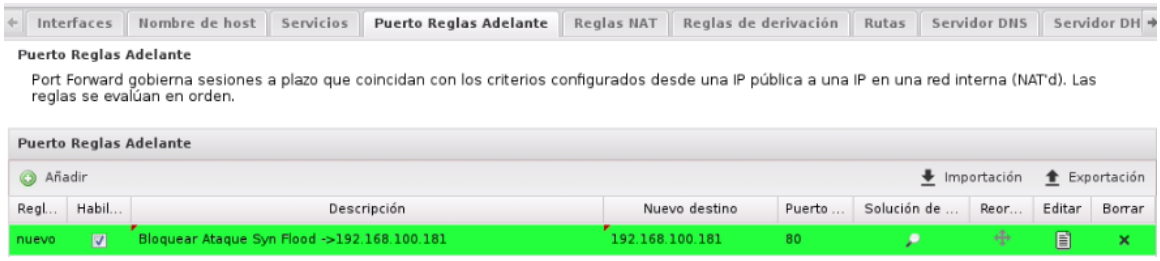


***Ilustración 8.64**:* "Bloqueo del Puerto 80"

8.4.16 Realizamos nuevamente un escaneo con la herramienta "Zenmap" de la dirección IP 192.168.100.181 (maquina victima) y podemos verificar que el puerto 80 se encuentra filtrado

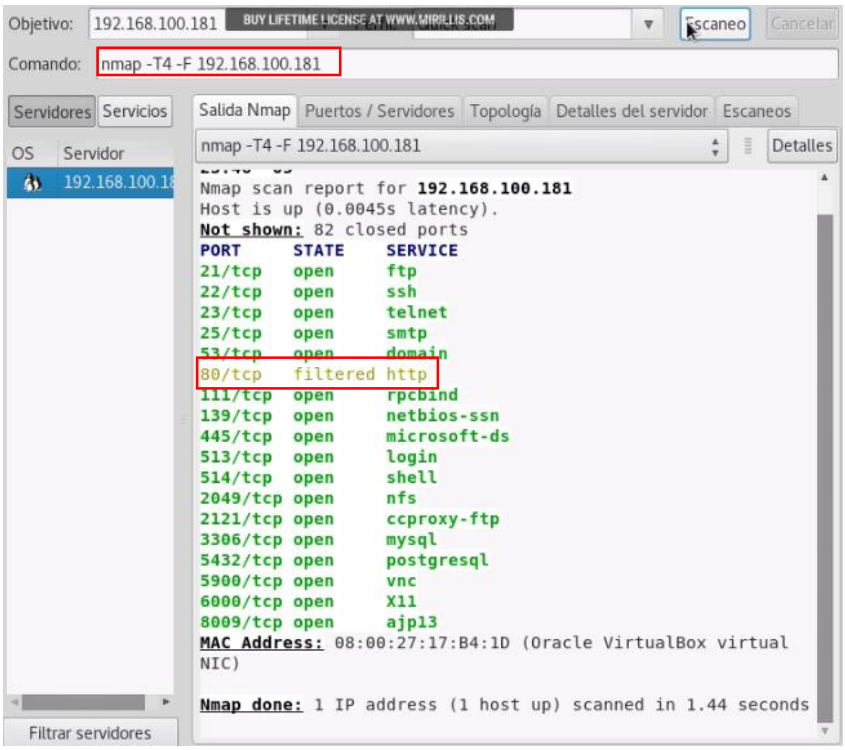


***Ilustración 8.65**: "Verificación del Puerto 80 con Zenmap"*

8.4.17 Después de realizar estos pasos, para comprobar que el firewall se encuentre configurado de acuerdo a lo necesitado, se va a permitir el tráfico de una a una determinada dirección IP (Realizar los pasos 7.4.1 hasta 7.4.8)

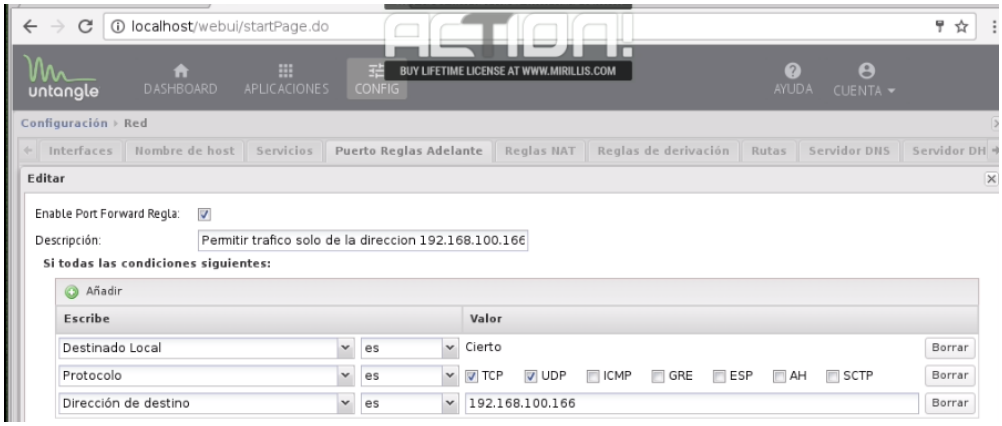


***Ilustración 8.66**: "Configuración para permitir el tráfico de una determinada dirección IP"*

8.4.18 Se utiliza la herramienta Wireshark, realizando un filtrado de la dirección IP 192.168.100.163, como podemos se ha estabilizado el sistema, incluso tomar en cuenta el número de paquetes es mínimo.

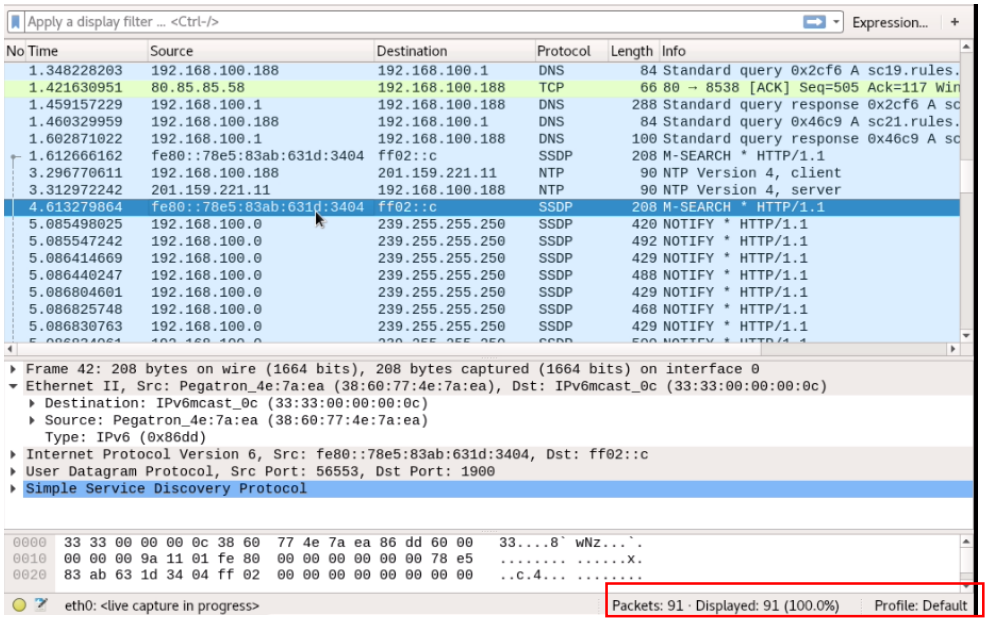


Ilustración 8.67*: "Configuración para permitir el tráfico de una determinada dirección IP"*

8.5 Desarrollo del Ataque y Mitigación de Sesiones, contraseñas y aplicaciones

8.5.1 Para realizar este tipo de ataque se debe levantar los servicios de PostgreSQL mediante el uso de consola (Kali Linux) y dos líneas de código:

- service postgresql start (inicia el servicio para PostgreSQL)
- service postgresql status (verifica que el servicio se encuentre activo)

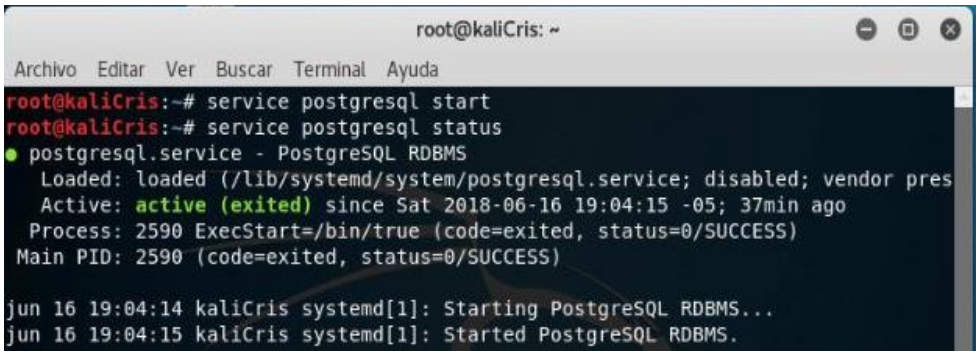


***Ilustración 8.68**: "Levantamiento de servicios PostgreSQL"*

8.5.2 Levantar los servicios "Apache", mediante el uso de la consola (Kali Linux) y dos líneas de código:

- service apache2 start (inicia el servicio Apache)
- service apach2 status (verifica que el servicio se encuentre activo)

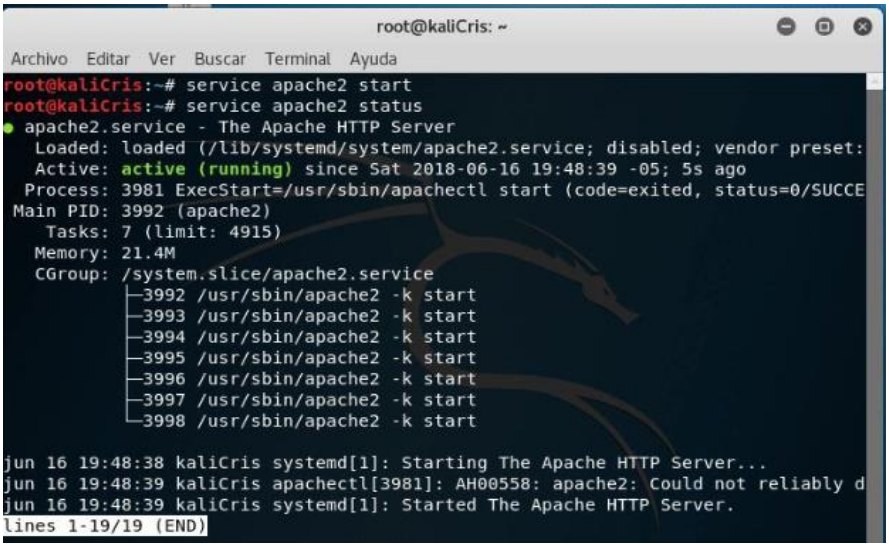


***Ilustración 8.69**: "Levantamiento de servicios Apache"*

8.5.3 Se abre un explorador de Internet y se digita la página por defecto de este servicio (127.0.0.1), comprobando su estado actual y lista para su uso

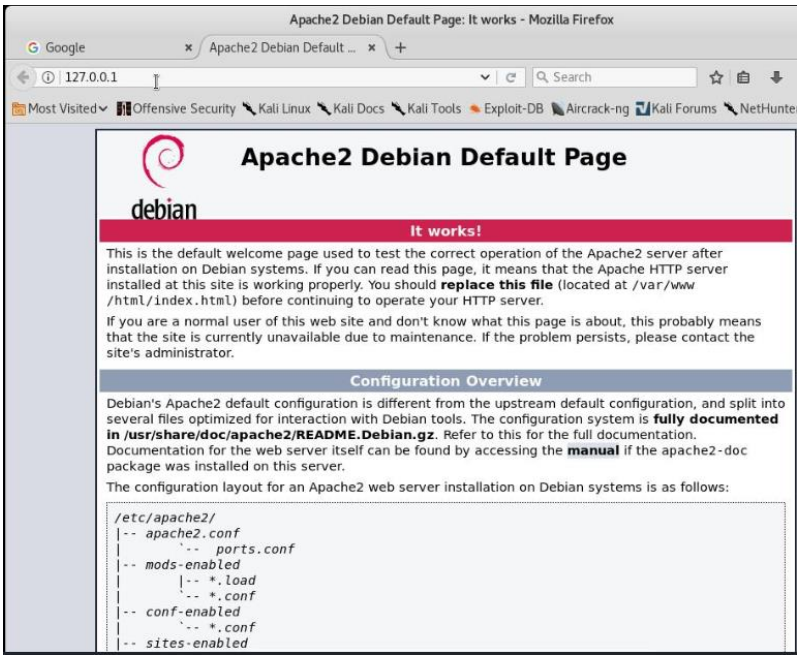


***Ilustración 8.70**: "Verificación Actual de Apache"*

8.5.4 Ahora, para realizar este ataque es necesario descargar el aplicativo llamado "John the Ripper" desde su página oficial (http://www.openwall.com/john/) y lo instalamos en el sistema operativo "Kali Linux":

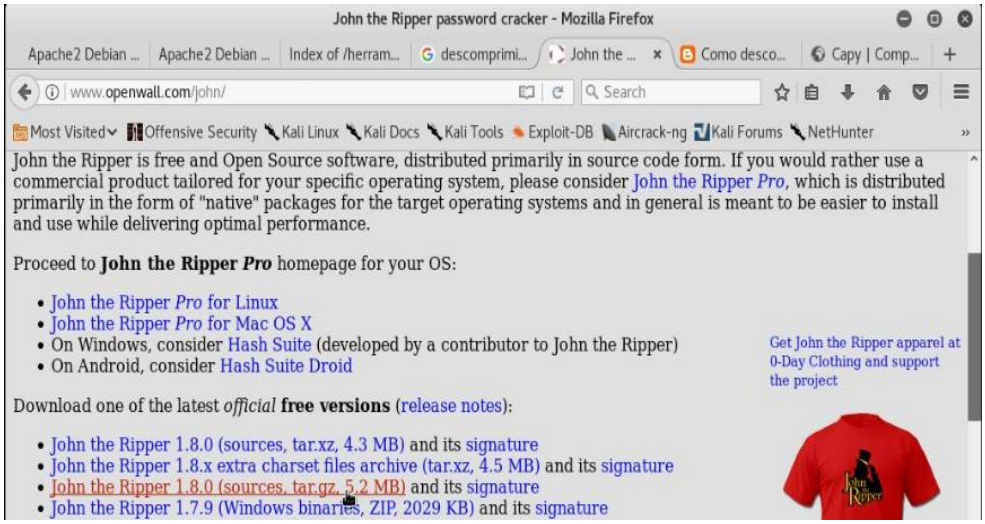


***Ilustración 8.71**: "Descargar Jonh The Ripper"*

8.5.5 Dentro del sistema operativo "Kali Linux", se abre la dirección: "Otras ubicaciones, Equipo, var, log, www, html" y se crea una carpeta llamada toolsTesis y se procede a guardar el aplicativo (John the Ripper)

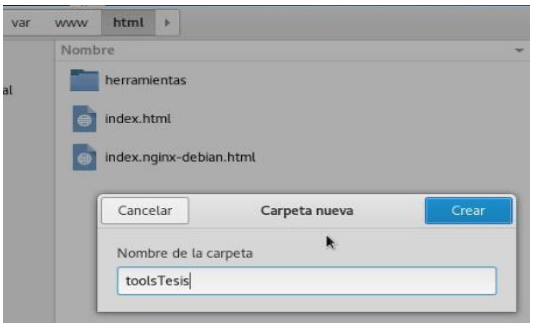


***Ilustración 8.72**: "Creación de Carpeta para guardar aplicativo John the Ripper"*



***Ilustración 8.73**:* "Guardar aplicativo John the Ripper"

8.5.6 Para verificar que la aplicación se encuentre dentro de esta dirección se abre un explorador de Internet y digitamos "127.0.0.1/toolsTesis" y como se observa la aplicación se encuentra guardada correctamente

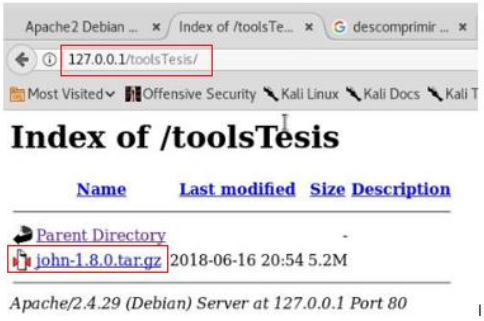


***Ilustración 8.74**: "Verificación de Aplicativo John the Ripper en Apache"*

8.5.7 Siendo la misma dirección local, ingresamos a la dirección 192.168.100.166

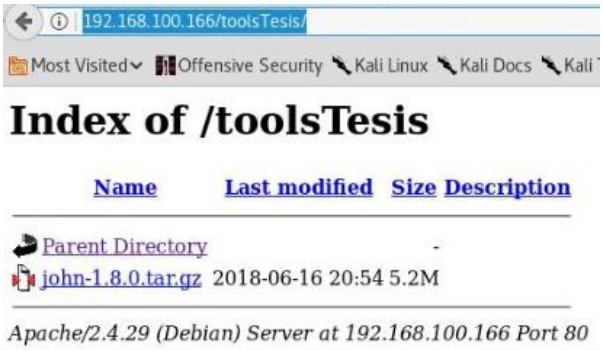


***Ilustración 8.75**: "Ingreso a la dirección 192.168.100.166"*

8.5.8 Abrir una consola e instalar una aplicación que nos ayude a descomprimir ficheros.

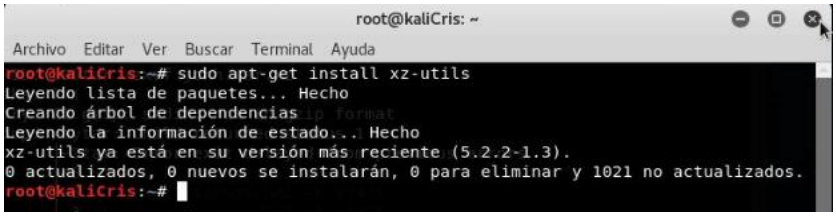


***Ilustración 8.76**: "Descomprimir archivos Jon de Ripper"*

8.5.9 A continuación, se procederá a realizar el ataque abriendo una consola en "Metasploit framework"

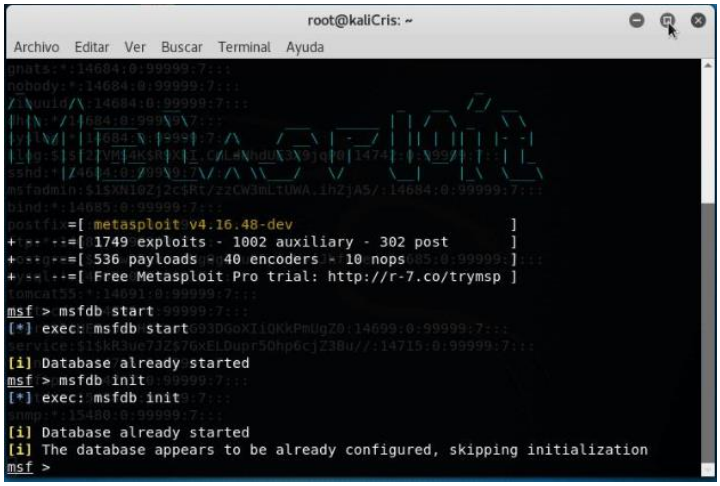


***Ilustración 8.77**: "Abrir consola de Metasploit"*

8.5.10 Se digita el comando "search vsftpd" y podemos observar que la única vulnerabilidad que podemos ingresar



***Ilustración 8.78**: "Búsqueda de Vulnerabilidades al puerto 21"*

8.5.11 Seleccionamos dicha vulnerabilidad



***Ilustración 8.79**: "Selección de vulnerabilidad al puerto 21"*

8.5.12 Configuramos la dirección victima (192.168.100.169) y observamos que esta lista para abrir su sesión y poder controlar la maquina

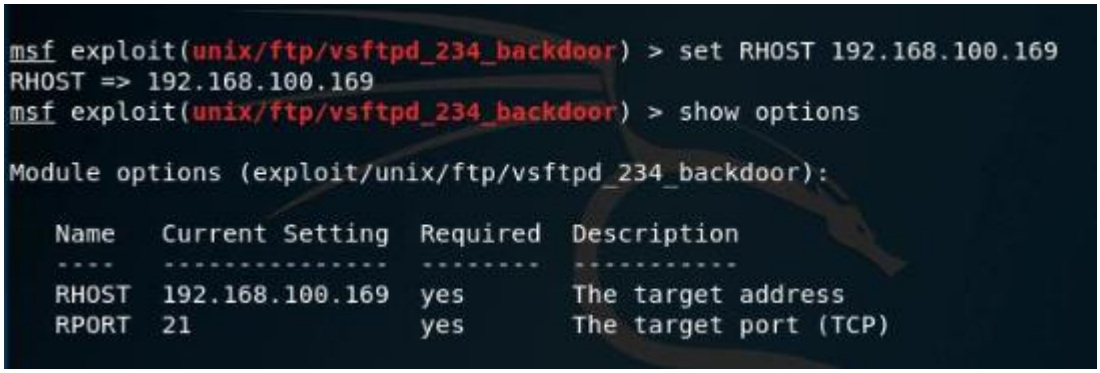


***Ilustración 8.80**: "Configuración de dirección victima"*

8.5.13 Con el comando “exploit” podemos controlar la sesión, la cual ya se encuentra abierta



***Ilustración 8.81**: “Control de Sesión Abierta”*

8.5.14 Como podemos observar, ya tenemos control total a la computadora de la victima



***Ilustración 8.82**: “Control total del equipo victima ”*

8.5.15 Ahora, dentro de la sesión y con el comando *“cat /etc/passwd”,* se puede averiguar todas las contraseñas, tomando en cuenta que se encuentra de manera desordenada

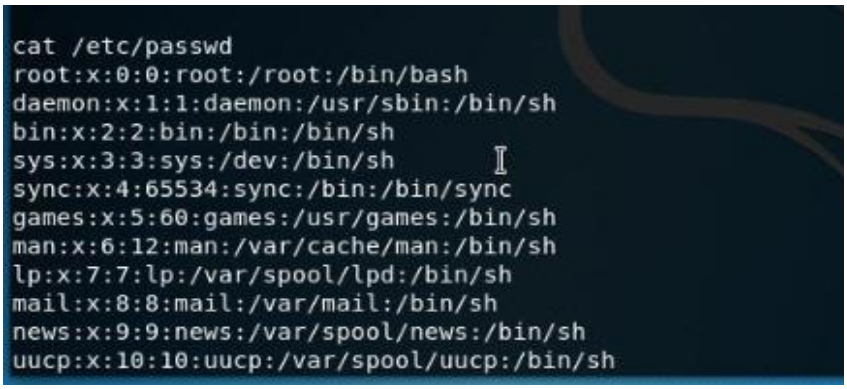


Ilustración 8.83: *"Comando para averiguar contraseñas "*

8.5.16 De igual manera dentro de la sesión y con el comando *"cat /etc/shadow"*, se puede averiguar todos los usuarios, tomando en cuenta que se encuentra de manera desordenada.

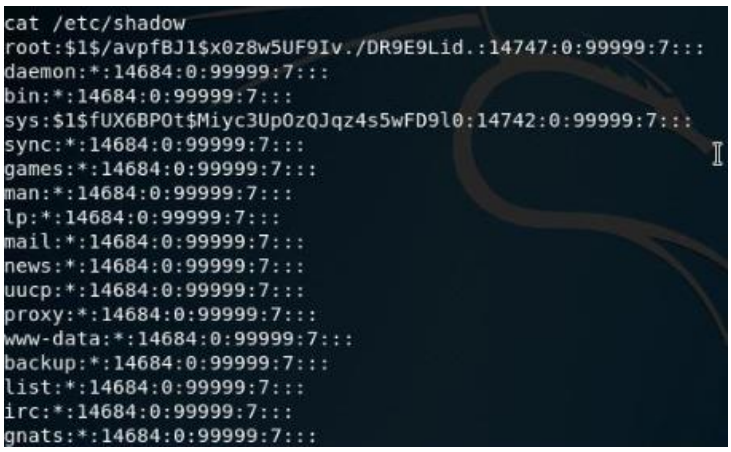


Ilustración 8.84: *"Comando para averiguar usuarios "*

8.5.17 Ahora, para que toda la información se encuentre ordenada y encontrar los usuarios y contraseñas para cada aplicación, se usa el siguiente comando



Ilustración 8.85 *"Abrir directorio de la aplicación John de Ripper"*

8.5.18 Descomprimir el aplicativo John the Ripper a través del comando “tar xvzf (nombre_aplicacion)”



Ilustración 8.86 *“Descomprimir John the Ripper”*

8.5.19 Se ingresa a la aplicación, visualizando sus recursos

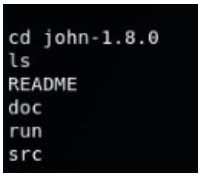


Ilustración 8.87 *“Visualización de recursos - John the Ripper”*

8.5.20 Se ingresa y lista el recurso (src); se usa el comando *“make generic”*; de esta manera empieza a realizar una búsqueda y ordenando las claves y usuarios encontrados.



Ilustración 8.88: "Uso del comando "*make generic"* para ordenar usuarios y contraseñas"

8.5.21 Se llama el archivo ". tockack.txt" donde se encuentra almacena la información requerida mediante los siguientes comandos

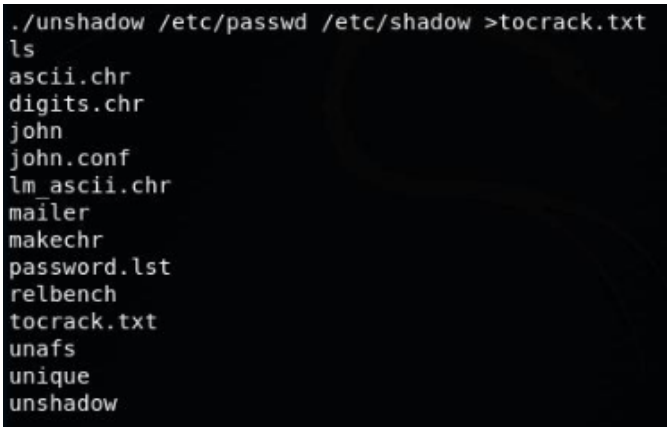


Ilustración 8.89*: "Llamar archivo donde se encuentra la información requerida"*

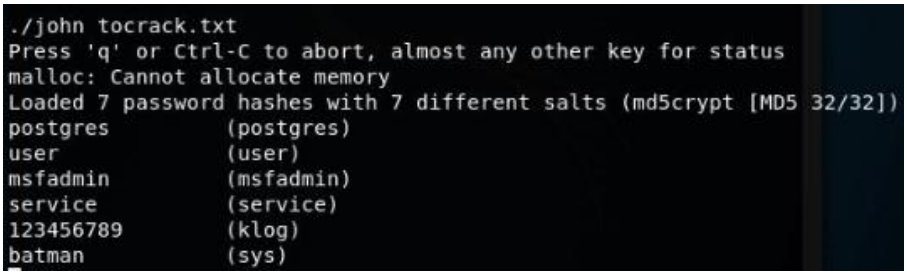


Ilustración 8.90: *"Archivo de claves y contraseñas"*

8.5.22 Configurar las reglas necesarias para mitigar este tipo de ataque se reenvía el puerto 21 puertos hacia una dirección segura.

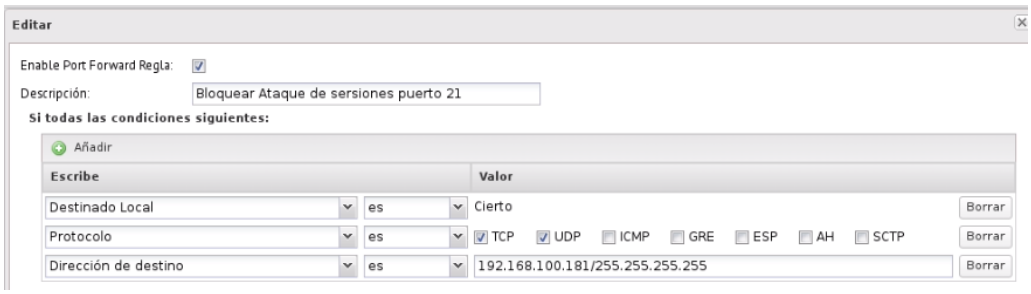


Ilustración 8.91: *"Configuración de reglas para reenvío de puertos"*

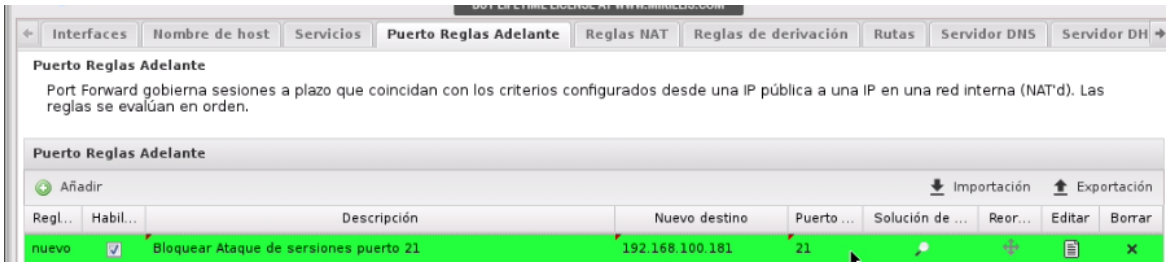


Ilustración 8.92: "Reenvío de puertos a una dirección segura"