



Consultoría para la adopción del protocolo
IPv6 en la red del Centro Industrial de
Mantenimiento Integral – SENA CIMI

ANEXO APENDICE E.
RECOMENDACIONES DE
SEGURIDAD PARA LA RED CIM.

EDGARDO JAVIER RÚA RANGEL



Tabla de Contenido

INTRODUCCIÓN	3
1. Estadísticas de ataques	4
1.1 Ingeniería social en el SENA 2018	5
1.2 Defensa tradicional	7
1.3 Tecnología FIREEYE	7
1.4 DEFENSA TRADICIONAL VS ANÁLISIS DINÁMICO	8
1.5 La propuesta de FIREEYE	8
1.6 DESPLIEGUE SEGURIDAD PERIMETRAL RED SENA	8
2. Ataques y medidas preventivas a nivel de capa 2	9
2.1 MAC Flooding Attack	9
2.2 DHCP SPOOFING	10
2.3 ARP Spoofing	14
3. Ataques empleando Fragmentación	18
3.1 Medidas a tomar para ataques de fragmentación	19
3.2 Extensiones de privacidad en Sistemas operativos Windows	20
4. Monitoreo 7x24	22
4.1 Recomendaciones contra las amenazas informáticas y AMENAZAS AVANZADAS	22



Tabla de Figuras

Figura 1. Pruebas de Seguridad SENA 2018	5
Figura 2. Resultado de las pruebas de ingeniería social en el SENA 2018.	6
Figura 3. TECNOLOGÍA FIREEYE	7
Figura 4. Modelos de defensa.	8
Figura 5. DESPLIEGUE SEGURIDAD PERIMETRAL RED SENA	8
Figura 6. Instalación de dsniiff.	9
Figura 7. Ejecutar macof.....	10
Figura 8. Topología de DHCP Spoofing.....	11
Figura 9. Herramienta Yersinia.....	11
Figura 10. Lanzar ataque DHCP Spoofing.	12
Figura 11. Ejecutando el ataque.....	12
Figura 12. Inundación de direcciones IP en el Router.	13
Figura 13. Configuraciones IPv4 e IPv6 en dispositivo atacante.	14
Figura 14. Accediendo a la servidor web de Router.....	15
Figura 15. Página web del Router.....	15
Figura 16. Captura Wireshark de tráfico.....	16
Figura 17. Ejecución de ataque Arp Spoofing.	16
Figura 18. Captura tráfico entre víctima y servidor Web.	16
Figura 19. Acceso al servidor web.....	17
Figura 20. Captura de información de la víctima.	17
Figura 21. Verificación Overlapping.....	18
Figura 22. Topología para aplicar contramedidas para fragmentación.....	19
Figura 23. opciones de configuración en un Router Cisco 2901	19
Figura 24. Verificación de Virtual-Reassembly.	20
Figura 25. Direcciones IPv6 Windows.	20
26. Deshabilitar generación aleatoria de la ID.	20
Figura 27. Configuración direcciones IPv6 temporales y habilitado el formato EUI-64	21
Figura 28. Deshabilitar direcciones temporales Windows.	21
Figura 29. Configuración de IPv6 en Windows sin direcciones temporales.	21
Figura 30. Centro de Monitoreo de seguridad.	22



INTRODUCCIÓN

En esta sección se pretende mencionar tipos de ataques maliciosos de los muchos que se encuentran y que pueden afectar el rendimiento de una red tanto IPv4 e IPv6, y como hemos mencionado anteriormente la red CIMI trabajará de forma Dual y por lo tanto habrá que tomar medidas preventivas de seguridad que pueden suceder sobre todo dentro de la misma entidad. Cabe resaltar que para producir estos tipos de ataques no se necesita ser un experto en manejo de técnicas de hackeo. A continuación, se enumeran los tipos de ataques más comunes que se pueden ejecutar.

- El SENA tiene un alto nivel de exposición, por lo cual se requiere un servicio excelente y seguro.
- Sus recursos de cómputo y capacidad de red son apetecidos en el mercado negro para ser usados por demanda por atacantes oportunistas.
- Los atacantes generan muestras de malware y variantes más rápido de lo que las compañías de antivirus pueden generar firmas para su detección.
- La WEB compromete más del 80% de los ataques.
- Los ataques también pueden provenir de equipos propios, de proveedores o de aprendices.
- El filtrado de proxy bloquea grandes grupos de categorías o páginas sin suficiente granularidad, dinamismo y altos falsos positivos.
- Una vez comprometidos los controles tradicionales existentes, no es posible detectar lo que ocurre.
- El tiempo entre nuevos ataques dificulta desplegar actualizaciones de manera oportuna de las soluciones tradicionales.



1. Estadísticas de ataques

Podemos encontrar tipos de ataques comunes en la red del SENA como son:

- **Amenaza Avanzada Persistente (APT):** Va desde secretos nacionales, información gubernamental, robo de propiedad intelectual corporativa, estrategias militares, infraestructura nacional, entre otros. Estas amenazas están desarrolladas hacia objetivos muy específicos y típicamente están siendo patrocinados por algún gobierno u organización.
- **Ataque de Día Cero:** Estos explotan vulnerabilidades desconocidas no descubiertas o no reveladas dentro de una red.
- **Ataques dirigidos por correo electrónico. (Spear – Phishing):** Ataques generalmente ejecutados contra ejecutivos o empleados, comúnmente son ataques de ingeniería social. Correos dirigidos para robo de información o infección.
- **Programas de Extorsión:** Un ransomware (del inglés ransom, extorsión', y ware, por software) es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esta restricción.

Terminología para nuevas amenazas

- **Malware:** programa (software) con comportamientos malignos.
- **Ataque:** un movimiento directo y hostil de fuerzas contra el enemigo, en un intento por abatirlo.
- **Cyber ataques:** uso no autorizado de herramientas o métodos para realizar un ataque hacia los recursos de la organización, que por lo general son ejecutados por medio de computadores conectados a la Internet.
- **Muestra de malware:** archivo binario que contiene código maligno.



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
Anexo recomendaciones de seguridad para la Red CIMI

1.1 Ingeniería social en el SENA 2018

- Email, spam, phishing aleatorio
- Email, spam, phishing plenamente identificado (spear phishing)
- LinkedIn
- Facebook
- Resultados pruebas ingeniería social SENA 2018

PRUEBA	EXITOSA	ALCANCE DE LA PRUEBA	ÁREA / FUNCIONARIOS (En cantidades de áreas o funcionarios)	NIVEL COMPROMETIDO (En cantidades de áreas o funcionarios)	NIVEL COMPROMETIDO (En porcentajes)
Phishing de Campaña Agencia de Viajes (Página WEB Fraudulenta de viajes a Cancún)	SI	Funcionarios	17	5	23%
Llamadas Telefonicas (Llamadas con pretexto de Agencia de Viajes)	NO	Funcionarios	9	0	0%
Suplantación (Con las credenciales adquiridas suplantamos los ingresos de un funcionario)	SI	Funcionarios	17	1	6%
Tailgating (colados) (Ingreso no autorizado a áreas)	SI	Área	1	1	100%
Información desatendida (Recolección de Información desatendida y dispositivos)	SI	Área	1	1	100%
Acceso no autorizado a PCs o Laptops (Acceso no autorizado a portátiles y equipos de funcionarios)	SI	Área	17	8	32%

Figura 1. Pruebas de Seguridad SENA 2018



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
Anexo recomendaciones de seguridad para la Red CIMI

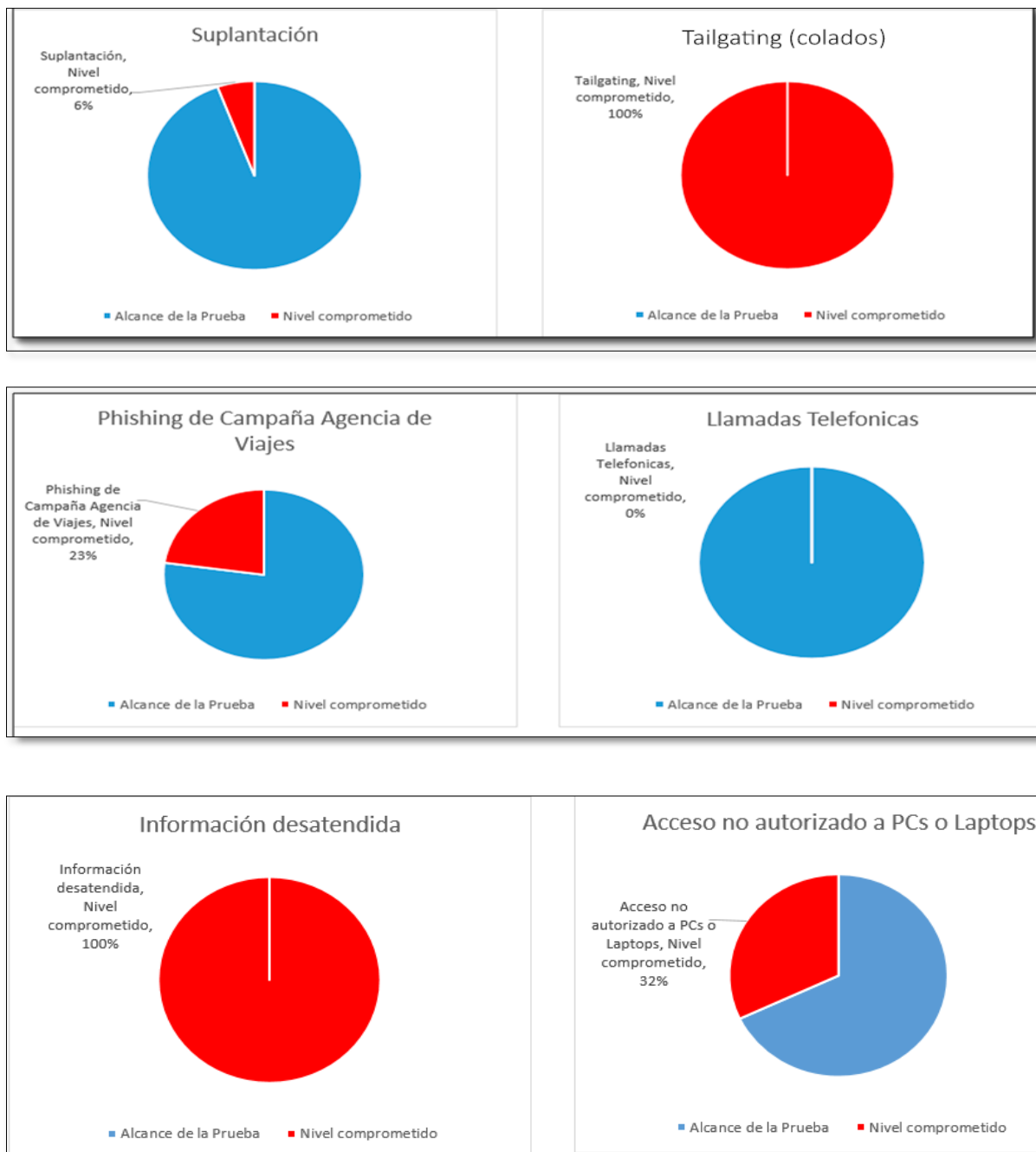


Figura 2. Resultado de las pruebas de ingeniería social en el SENA 2018.



1.2 Defensa tradicional

Las técnicas y estrategias de defensa tradicional están fallando en su detección y contención del malware avanzado por varias razones; la principal es que estas herramientas están basadas en firmas, lo cual significa que ellos solo pueden detectar lo que ya conocen, no tienen la capacidad de detectar y contener el malware y cualquier amenaza emergente.

Para mitigar estas amenazas emergentes, se puede tratar de realizar ajustes de configuración en dispositivos como Firewall, IPS y Proxys, pero por lo general al no ser algo dinámico genera muchos falsos positivos.

La respuesta es seguridad de manera no tradicional prevenir, detectar, contener y resolver.

1.3 Tecnología FIREEYE

Plataforma para prevenir, detectar, contener y resolver las nuevas generaciones de cyber ataques. Identifican incluso lo nuevo y desconocido en tiempo real. FireEye es pionero en las soluciones de protección de amenazas avanzadas APTs, provee una protección completa y continua contra las amenazas más sofisticadas de la actualidad. Sus Principales características:

- Provee visibilidad en todas las etapas del ciclo de vida del ataque y bloqueo en tiempo real de amenazas.
- Previene evasión de máquina virtual.
- Protección completa y correlación por medio de múltiples vectores.
- Analiza código desconocido y objetos WEB sospechosos.

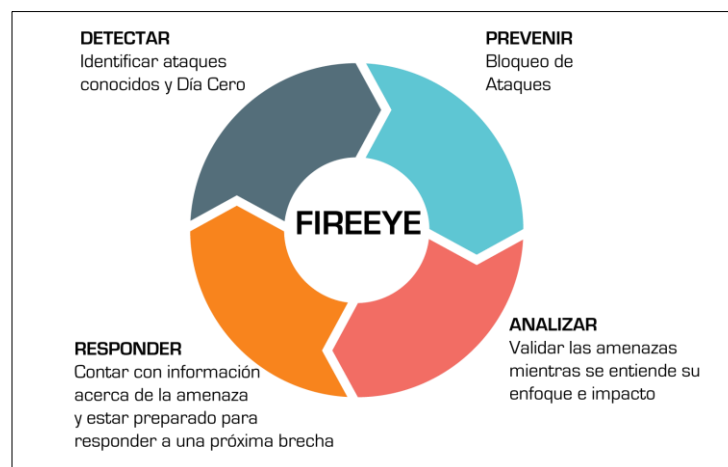


Figura 3. TECNOLOGÍA FIREEYE



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
Anexo recomendaciones de seguridad para la Red CIMI

1.4 DEFENSA TRADICIONAL VS ANÁLISIS DINÁMICO

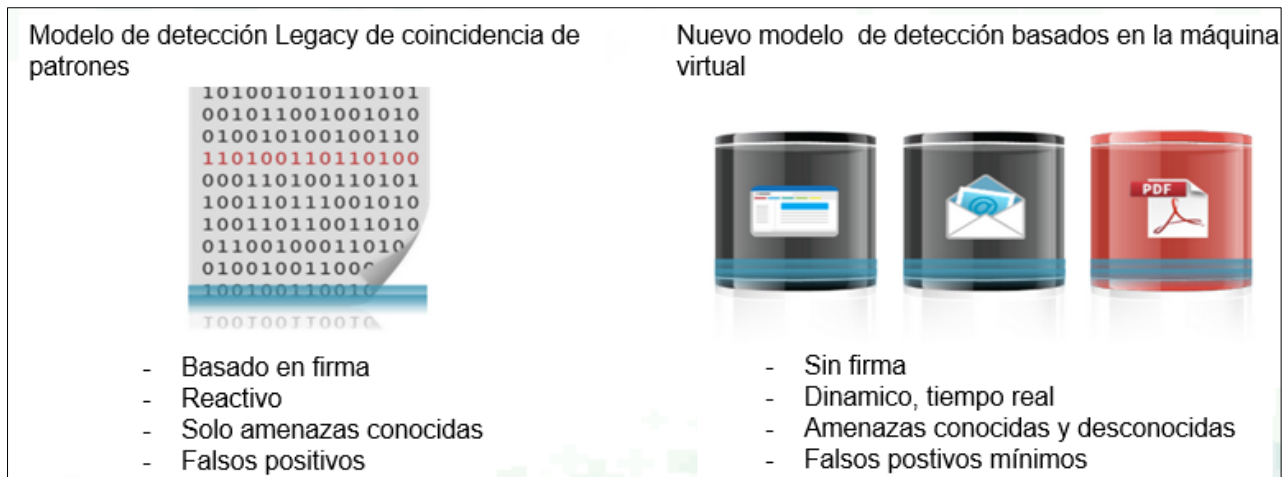


Figura 4. Modelos de defensa.

1.5 La propuesta de FIREEYE

Detener los ataques WEB que las herramientas tradicionales tales como Firewalls, IPS, AV y Web Gateways no pueden contener:

- Exploits de día cero
- Callbacks (comunicaciones con sus servidores).
- APT
- Protección de clics a enlaces
- Protección de ingreso a un sitio WEB comprometido.

1.6 DESPLIEGUE SEGURIDAD PERIMETRAL RED SENA

En la figura siguiente se muestra el sistema de seguridad implementado en el SENA en todas sus sedes.

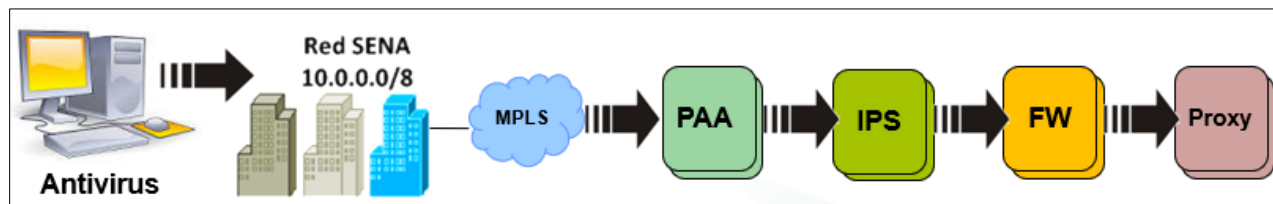


Figura 5. DESPLIEGUE SEGURIDAD PERIMETRAL RED SENA



2. Ataques y medidas preventivas a nivel de capa 2

El objetivo es enumerar los diferentes ataques que se pueden presentar a nivel de capa 2 del modelo OSI, y las medidas de seguridad que se deben aplicar a través de los Switches de acceso para evitar vulnerabilidades.

2.1 MAC Flooding Attack

Este ataque lo pretende es inundar la red local de direcciones Mac de forma aleatoria esto puede provocar que algunos Switches entren en modo “Hub” facilitando el Sniffing de toda la red, con este método de ataque se pretende sabotear el dispositivo y dejarlo inhabilitado.

Para producir este ataque se debe trabajar bajo un entorno Linux, en este caso se utiliza Ubuntu 16.04 se debe instalar la herramienta “dsniff” y se ejecuta “macof” y se debe colocar el número de direcciones MAC que va a generar de forma aleatoria para que inunde el Switch de acceso de la red. Se muestra los comandos que para instalar la herramienta y ejecutarla. Ver la Fig. 6.

```
# apt-get install dsniff  
  
# macof -i eth0 -n 10000
```

```
root@nla:/home/nla# apt-get install dsniff  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
dsniff is already the newest version (2.4b1+debian-22.1).  
0 upgraded, 0 newly installed, 0 to remove and 330 not upgraded.  
root@nla:/home/nla# macof -i enp0s3 -n 1
```

Figura 6. Instalación de dsniff.



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
Anexo recomendaciones de seguridad para la Red CIMI

En la Figura 7 se muestra la herramienta ejecutándose y generándose múltiples direcciones MAC.

```
Building dependency tree
Reading state information... Done
dsniff is already the newest version (2.4b1+debian-22.1).
0 upgraded, 0 newly installed, 0 to remove and 330 not upgraded.
root@nla:/home/nla# macof -i enp0s3 -n 10
52:4e:12:3:97:ee 11:6d:a2:1a:c8:1f 0.0.0.0.59264 > 0.0.0.0.21792: S 1408938400:140893
8400(0) win 512
4c:4c:4f:4d:1b:6 49:4a:ed:6f:95:a5 0.0.0.0.2768 > 0.0.0.0.38266: S 901290983:90129098
3(0) win 512
86:17:97:41:96:ca 8d:23:7a:47:c4:27 0.0.0.0.8592 > 0.0.0.0.35444: S 1786697588:178669
7588(0) win 512
9b:6e:15:7f:58:93 f1:4b:13:7:63:f5 0.0.0.0.29126 > 0.0.0.0.6818: S 1695138832:1695138
832(0) win 512
43:1c:1a:d:b5:42 fc:56:7f:26:94:e3 0.0.0.0.35169 > 0.0.0.0.29466: S 1090680472:109068
0472(0) win 512
15:41:c:1c:b7:90 71:90:27:15:28:c8 0.0.0.0.46143 > 0.0.0.0.23052: S 717909066:7179090
66(0) win 512
1b:82:5d:3c:c5:4 e0:5a:ab:2e:7d:11 0.0.0.0.58742 > 0.0.0.0.60398: S 1047697627:104769
7627(0) win 512
d4:91:7c:51:ac:0 5a:76:eb:5a:cc:60 0.0.0.0.748 > 0.0.0.0.28065: S 193601824:193601824
(0) win 512
a2:1e:1:2a:cb:89 71:df:cd:6b:3c:ee 0.0.0.0.64220 > 0.0.0.0.34355: S 543964507:5439645
07(0) win 512
94:59:d2:22:40:1c a4:e0:11:36:f2:5 0.0.0.0.17054 > 0.0.0.0.37684: S 439771799:4397717
99(0) win 512
root@nla:/home/nla#
```

Figura 7. Ejecutar macof.

continuación, se muestra los comandos que se deben ejecutar.

```
SwAcceso (Config-if)Switchport mode Access
SwAcceso (Config-if)Switchport port -security
SwAcceso (Config-if) Switchport port -security máximo 1
SwAcceso (Config-if) Switchport port -security violation shutdown
```

2.2 DHCP SPOOFING

En la siguiente topología se muestra un DHCP falso en la red el cual está instalado en Ubuntu 16.04, los demás equipos de la red normalmente tomaran IPv4 e IPv6 del server DHCP configurado en el Router CPECIMI. Ver la Fig. 8.



SERVICIO NACIONAL DE APRENDIZAJE SENA

Procedimiento de Desarrollo Curricular

Anexo recomendaciones de seguridad para la Red CIMI

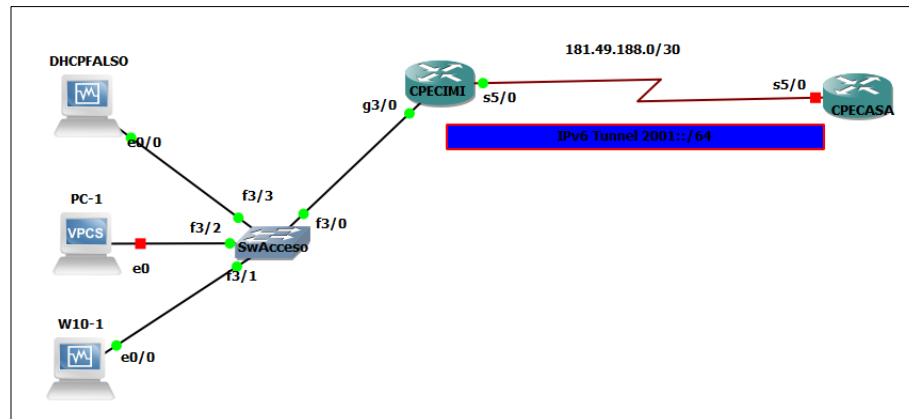


Figura 8. Topología de DHCP Spoofing.

Para poder simular este ataque se debe instalar una herramienta en Ubuntu llamada Yersinia

```
#apt-get install yersinia
```

```
#yersinia -G
```

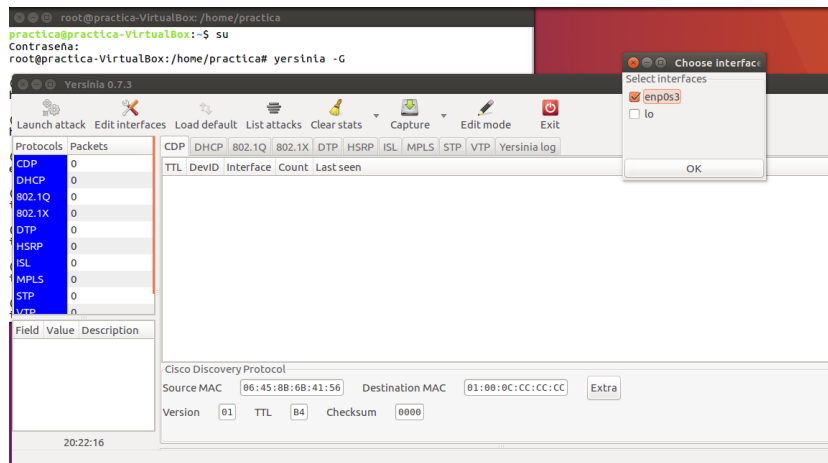


Figura 9. Herramienta Yersinia.



SERVICIO NACIONAL DE APRENDIZAJE SENA

Procedimiento de Desarrollo Curricular

Anexo recomendaciones de seguridad para la Red CIMI

Este ataque tiene como finalidad inundar de direcciones IPv4 e IPv6 de manera aleatoria e indiscriminada, hasta que el Router agote el direccionamiento de IP que pueden ofrecer dentro de la red, y cuando un dispositivo final quiera acceder por primera vez a la red solicitara al Router una dirección IP este no podrá tomar su solicitud ya que agotado su pool de direcciones y el servidor DHCP falso en la red le suministrara una dirección falsa con la cual podrá acceder y hasta tomar el control del equipo. Ver la Fig. 10.

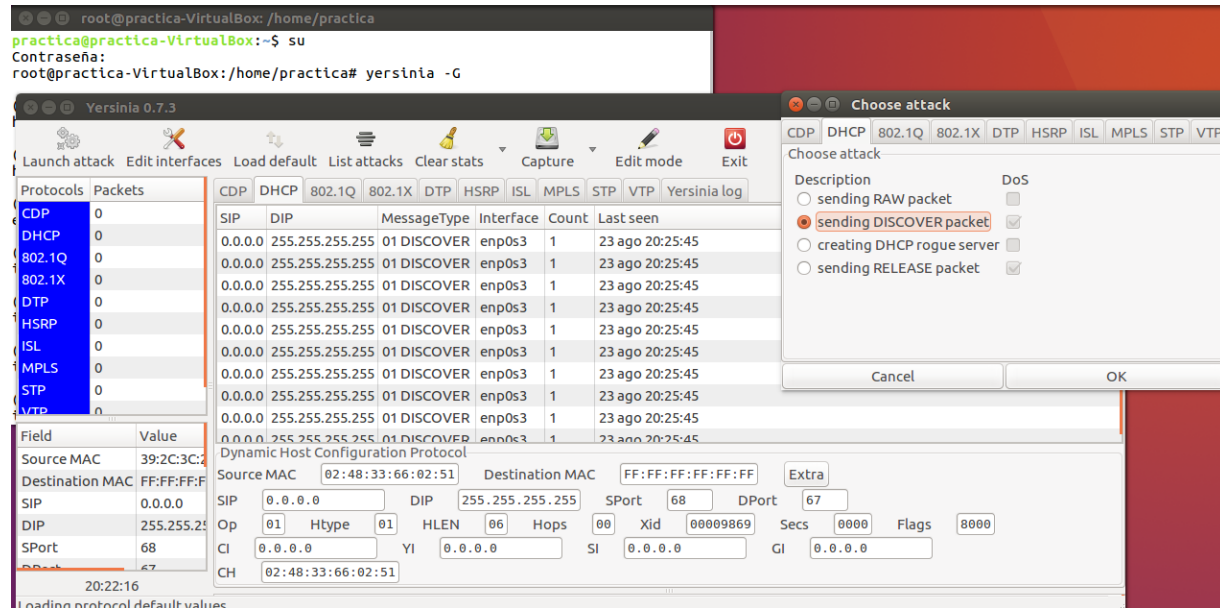


Figura 10. Lanzar ataque DHCP Spoofing.

En la figura 11 se muestra la ventana de escogencia de qué tipo de ataque se puede generar en este caso se escoge “sending Discover packet”.

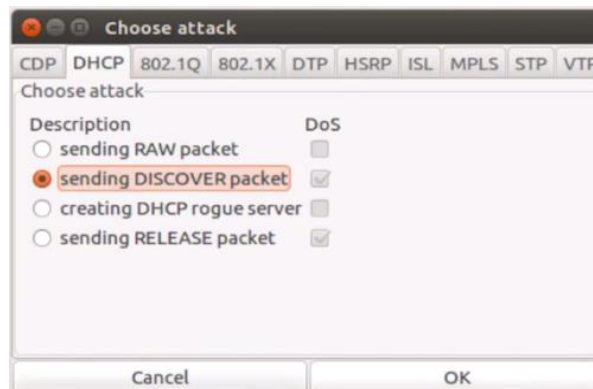


Figura 11. Ejecutando el ataque.



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
Anexo recomendaciones de seguridad para la Red CIMI

En la figura 12 se muestra el comando “*show ip dhcp binding*”, y se puede observar múltiples direcciones inundando el Router, dejándolo sin pool para generar si en llegado caso otro equipo quiere recibir una IP.

```
R1#show ip dhcp binding
```

192.168.10.201	0100.5079.6668.02	Infinite		Automatic
192.168.10.202	24d1.7d06.36cd	Feb 23 2017 10:17 AM		Automatic
192.168.10.203	c6d4.4c3c.da90	Feb 23 2017 10:17 AM		Automatic
192.168.10.204	758f.ee1e.7d36	Feb 23 2017 10:17 AM		Automatic
192.168.10.205	20fc.5423.2f63	Feb 23 2017 10:17 AM		Automatic
192.168.10.206	ee37.5f0e.b693	Feb 23 2017 10:17 AM		Automatic
192.168.10.207	829c.564b.ccdc	Feb 23 2017 10:17 AM		Automatic
192.168.10.208	e90e.654b.d15d	Feb 23 2017 10:17 AM		Automatic
192.168.10.209	0b8d.ac58.2688	Feb 23 2017 10:17 AM		Automatic

Figura 12. Inundación de direcciones IP en el Router.

Para poder contrarrestar este ataque se deben tomar medidas en el Switch de acceso el cual se hace a través de DHCP Snooping con los siguientes comandos.

```
SwAcceso(Config) ip dhcp snooping
```

```
SwAcceso (Config) ip dhcp snooping Vlan 10,20
```

En este caso se está activando para las Vlan 10 y 20, esto lo que permite que solo el tráfico que provenga de esas Vlan se tendrá que autenticar por decirlo de alguna forma solo con el puerto que conecta al Router que está en modo troncal.

Se debe configurar el siguiente comando en la interfaz que conecta el Router con el Switch y la pone como modo confiable para recibir los mensajes DISCOVER Packet, y si ese mensaje viene de otro dispositivo que no esté conectado a dicho puerto será descartado.

```
SwAcceso(Config)#ip dhcp snooping trust
```



2.3 ARP Spoofing

Siguiendo con la topología planteada anteriormente se pretende simular este ataque que viene a modificar el flujo de los datos enviados desde un PC víctima que pasa a través de un Gateway para hacer un ataque de tipo MITM (Man in the Middle) consiguiendo que el tráfico de la víctima pase por una máquina atacante de forma inadvertida para la víctima.

El atacante que se debe encontrar dentro de la misma red para poder lanzar el ataque va a conseguir ver el flujo de tráfico de manera bidireccional.

Primero realizar un ping desde el computador con el sistema operativo Linux con una IPv4 192.168.150.10 /24 e IPv6 con 2001:db8:60:968::10/64, para comprobar conectividad.

Entrar al navegador y escribir la IP LOOPBACK 200.1.1.1 que será la del Servidor HTTP. Ver la Fig. 13.

```
root@practica-VirtualBox:/home/practica# ifconfig
enp0s3  Link encap:Ethernet  direcciónHW 08:00:27:98:79:6b
        Direc. inet:192.168.150.10  Difus.:192.168.150.255  Másc:255.255.255.0
        Dirección inet6: 2001:db8:60:968::10/64 Alcance:Global
        Dirección inet6: fe80::a00:27ff:fe98:796b/64 Alcance:Enlace
        ACTIVO DIFUSIÓN FUNCIONANDO MULTICAST MTU:1500 Métrica:1
        Paquetes RX:0 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:78989 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1000
        Bytes RX:0 (0.0 B)  TX bytes:22575487 (22.5 MB)

lo      Link encap:Bucle local
        Direc. inet:127.0.0.1  Másc:255.0.0.0
        Dirección inet6: ::1/128 Alcance:Anfitrión
        ACTIVO BUCLE FUNCIONANDO MTU:65536 Métrica:1
        Paquetes RX:19973 errores:0 perdidos:0 overruns:0 frame:0
        Paquetes TX:19973 errores:0 perdidos:0 overruns:0 carrier:0
        colisiones:0 long.colaTX:1
        Bytes RX:1478417 (1.4 MB)  TX bytes:1478417 (1.4 MB)
```

Figura 13. Configuraciones IPv4 e IPv6 en dispositivo atacante.

Configuración del servidor HTTP en el Router CPECIMI para la simulación de tráfico WEB.

```
CPECIMI (config)#ip http authentication local
CPECIMI (config)#username admin privilege 15 password admin123
```



SERVICIO NACIONAL DE APRENDIZAJE SENA

Procedimiento de Desarrollo Curricular

Anexo recomendaciones de seguridad para la Red CIMI

En la figura 14 se muestra el acceso al servidor WEB configurado en el Router.

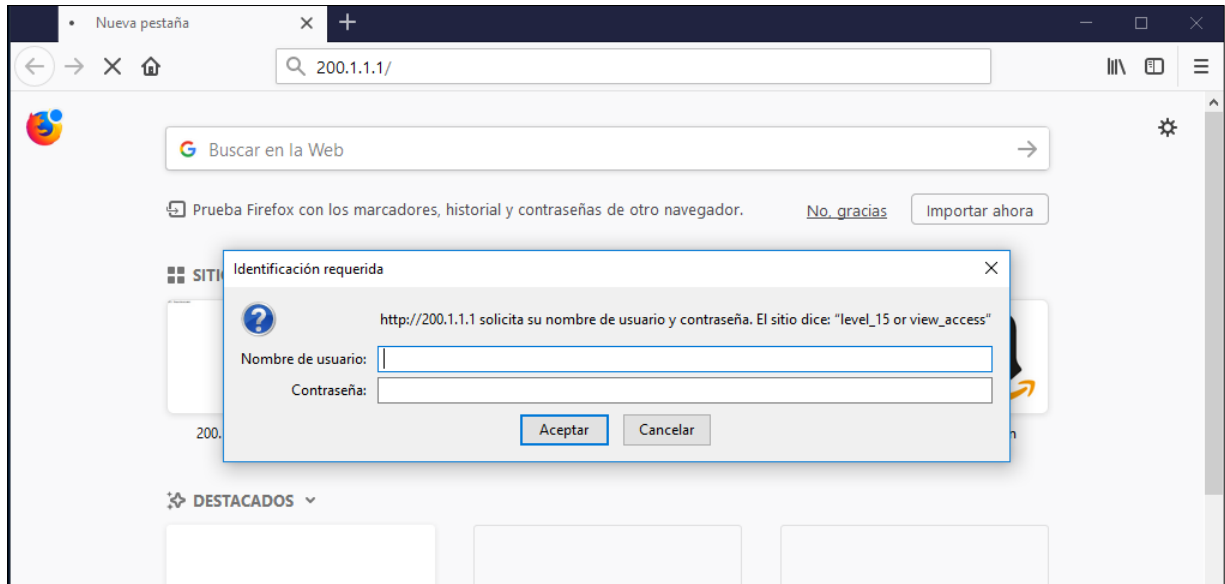


Figura 14. Accediendo a la servidor web de Router

Se observa en la figura 15 el acceso a la página del Router.

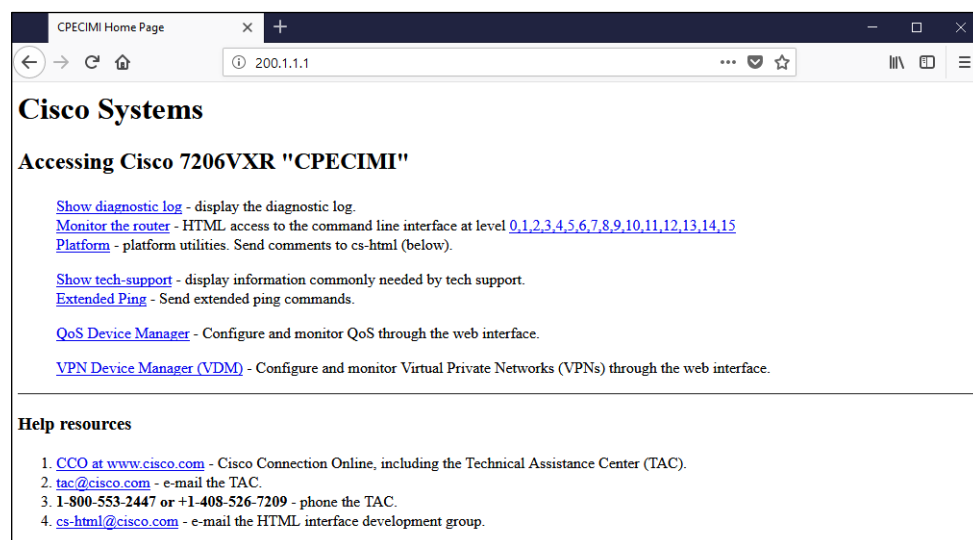


Figura 15. Página web del Router.



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
Anexo recomendaciones de seguridad para la Red CIMI

Se filtra en Wireshark la información del PC víctima y como se observa no hay ningún tipo de tráfico, ya que la conversación entre la víctima y el Router es privada como debe ser. Ver la Fig. 16.

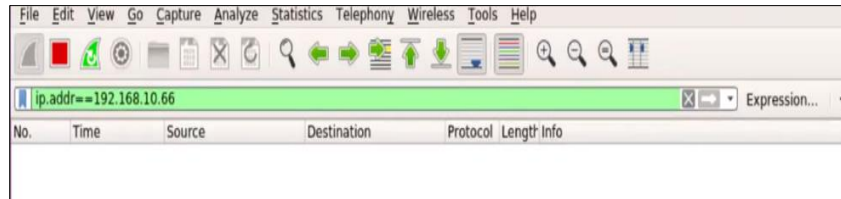


Figura 16. Captura Wireshark de tráfico.

Le voy a decir a la víctima que es la 192.168.10.66, que todo lo que envíe a la dirección IP 192.168.150.1 que es el Gateway lo desvíe a mi MAC local. Ver la Fig. 17.

```
root@practica-VirtualBox:/home/practica# arpspoof -i enp0s3 192.168.10.66 -t 192.168.150.1
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
8:0:27:98:79:6b 0:0:0:0:0:0 0806 42: arp reply 192.168.10.66 is-at 8:0:27:98:79:6b
```

Figura 17. Ejecución de ataque Arp Spoofing.

Se empezó a interceptar tráfico de tipo TCP que va de 192.168.10.66 a 200.1.1.1. Ver la Fig. 18.

No.	Time	Source	Destination	Protocol	Length	Info
452	421.634010180	192.168.10.66	200.1.1.1	TCP	74	33492 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=
454	421.990722289	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33478 → 80 [SYN] Seq=0
455	422.041155283	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33482 → 80 [SYN] Seq=0
456	422.246696227	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33480 → 80 [SYN] Seq=0
457	422.294404417	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33484 → 80 [SYN] Seq=0
458	422.318443961	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33486 → 80 [SYN] Seq=0
459	422.384738246	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33488 → 80 [SYN] Seq=0
460	422.574151286	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33490 → 80 [SYN] Seq=0
462	422.632062028	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33492 → 80 [SYN] Seq=0
466	424.043501465	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33482 → 80 [SYN] Seq=0
467	424.293266809	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33484 → 80 [SYN] Seq=0
468	424.322158894	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33486 → 80 [SYN] Seq=0
469	424.389248724	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33488 → 80 [SYN] Seq=0
472	424.578113581	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33490 → 80 [SYN] Seq=0
473	424.642042085	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33492 → 80 [SYN] Seq=0
477	425.996567419	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33478 → 80 [SYN] Seq=0
478	426.243805137	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33480 → 80 [SYN] Seq=0
482	428.052630994	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33482 → 80 [SYN] Seq=0
483	428.306952421	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33484 → 80 [SYN] Seq=0
484	428.323678140	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33486 → 80 [SYN] Seq=0
485	428.402849462	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33488 → 80 [SYN] Seq=0
486	428.571389052	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33490 → 80 [SYN] Seq=0
487	428.643376465	192.168.10.66	200.1.1.1	TCP	74	[TCP Retransmission] 33492 → 80 [SYN] Seq=0

Figura 18. Captura tráfico entre víctima y servidor Web.



SERVICIO NACIONAL DE APRENDIZAJE SENA

Procedimiento de Desarrollo Curricular

Anexo recomendaciones de seguridad para la Red CIMI

El usuario víctima se da cuenta que no tiene conexión a internet. Se abre una tercer terminal y se ejecuta un comando para que el usuario victima pueda seguir navegando y no se dé cuenta que esta hackeado.

Echo 1 > /proc/sys/net/ipv4/ip forward

Lo que hace es ejecutar en el kernel de Linux la opción de envío de trafico de interfaces, por defecto el valor está en 0. Borrar los archivos temporales del navegador para que de nuevo se pida la contraseña de acceso. El usuario victima desea navegar de nuevo por internet.

```
CPECIMI /level/15/exec/show/tech-support/cr
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CPECIMI
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp pool Datos
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
!
ip dhcp pool Voz
network 192.168.150.0 255.255.255.0
default-router 192.168.150.1
option 150 ip 192.168.150.1
!
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
ipv6 dhcp pool Datos
prefix-delegation pool Datos lifetime 3600 3600
```

Figura 19. Acceso al servidor web

En Wireshark filtramos el tráfico HTTP. Ver la Fig. 20.

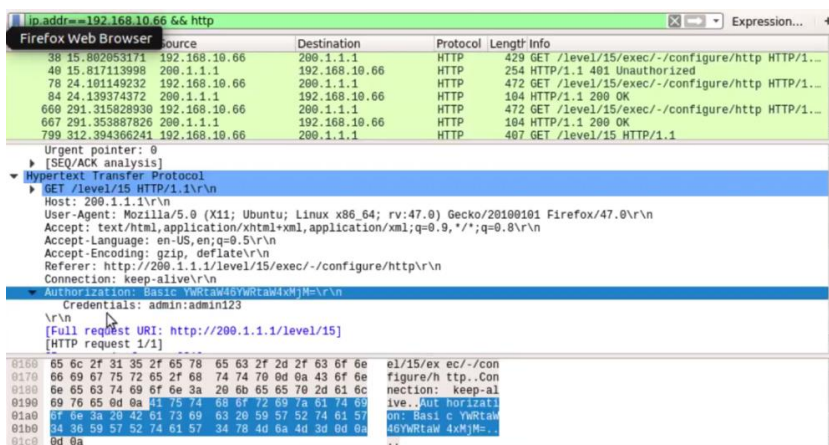


Figura 20. Captura de información de la víctima.



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
Anexo recomendaciones de seguridad para la Red CIMI

Contramedida para evitar ARP Spoofing DAI (Dynamic ARP Inspection)

```
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#ip arp inspection
Switch(config)#ip arp inspection vlan 10
Switch(config)#no ip dhcp snooping information option
```

Se afianza en el dhcp Snooping como medida auxiliar de contrastar la información de las IP y MAC legítimas existentes previamente. De esa manera lo que hará será comparar lo que está guardado en la tabla ip dhcp snooping binding.

3. Ataques empleando Fragmentación

El ataque típico de DoS es contra la memoria del sistema que implementa IPv6. Para cada nuevo fragmento, el sistema reserva algunas estructuras de memoria para el manejo de reensamblado, si un atacante envía una gran cantidad de fragmentos (pretendiendo ser de diferentes paquetes), el sistema puede agotar su memoria y otros fragmentos pueden ser rechazados.

A pesar de que se exige descartar los paquetes que usen la técnica de ataque denominada Overlapping, que se emplea para sobrescribir los números de puertos en los encabezados TCP, en algunos sistemas operativos como Ubuntu 16.04 y OPEN BSD son susceptibles a este ataque, como se demuestra a continuación.

En la figura 21 se quiere observar el tipo de tráfico fragmentado para poderlo identificar en una red.

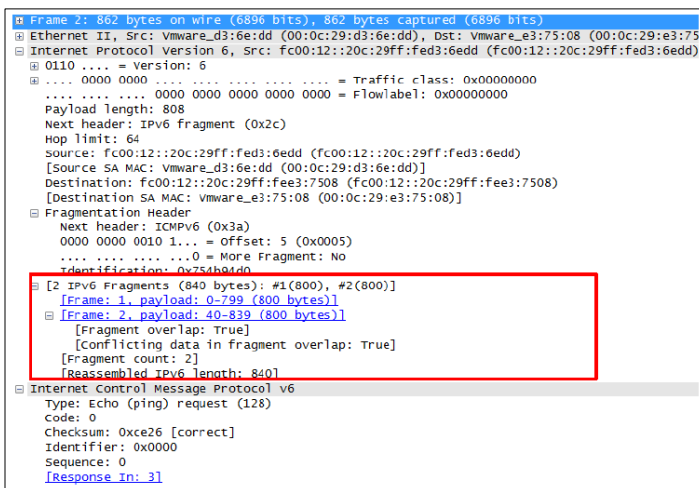


Figura 21. Verificación Overlapping



3.1 Medidas a tomar para ataques de fragmentación

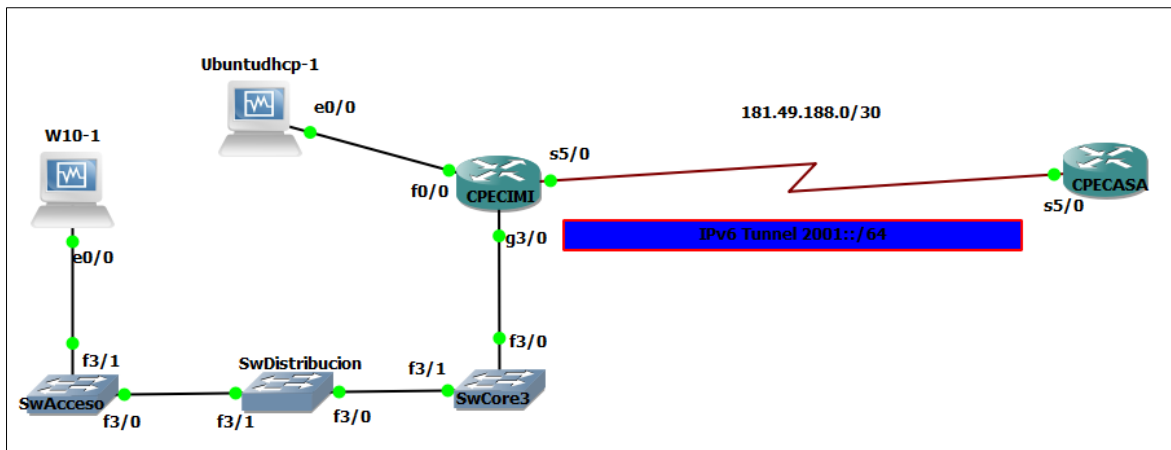


Figura 22. Topología para aplicar contramedidas para fragmentación

Tomando como referencia la topología que se muestra y la interfaz Ethernet conectada a Ubuntu 16.04, se pretende generar reglas de Firewalls que descarten paquetes menores a 1280 bytes que no sean el último fragmento.

Cisco cuenta con la implementación de la función VRF (Virtual Fragmentation Reassembly). Esta funcionalidad reensambla fragmentos de paquetes, examina fragmentos fuera de secuencia y los ordena. VRF examina los fragmentos de una sola fuente y pasa el paquete final a la capa superior de la pila, si existen problemas con los fragmentos, el paquete es descartado. En la Figura 18 se muestra las opciones de configuración en un Router Cisco 2901 y en la Figura 23 se muestra estadísticas tomadas de un puerto.

```
CPECIMI(config)#interface fastEthernet 0/0
CPECIMI(config-if)#ipv6 enable
CPECIMI(config-if)#ipv6 virtual-reassembly drop-fragments
```

Figura 23. opciones de configuración en un Router Cisco 2901

```
CPECIMI#show ipv6 virtual-reassembly
```



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
Anexo recomendaciones de seguridad para la Red CIMI

```
%Interface FastEthernet0/0
IPv6 configured concurrent reassemblies (max-reassemblies): 64
IPv6 configured fragments per reassembly (max-fragments): 16
IPv6 configured reassembly timeout (timeout): 3 seconds
IPv6 configured drop fragments: ON

IPv6 current reassembly count:0
IPv6 current fragment count:0
IPv6 total reassembly count:0
IPv6 total reassembly timeout count:0
```

Figura 24. Verificación de Virtual-Reassembly.

3.2 Extensiones de privacidad en Sistemas operativos Windows

Por defecto Windows, no utilizan el formato EUI-64 para la generación de las direcciones IPv6, sino que se basan en un algoritmo que las genera en forma aleatoria. Además, siguiendo los lineamientos se generan direcciones IPv6 temporales para conexiones salientes. Ambas características se observan en las Figuras 25.

```
Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . . :
Dirección IPv6 . . . . . : 2001:db8:60:968:ac5f:7b5:5f2:1cf8
Dirección IPv6 temporal. . . . . : 2001:db8:60:968:a572:49fc:450:4bb3
Vínculo: dirección IPv6 local. . . : fe80::ac5f:7b5:5f2:1cf8%5
Dirección IPv4. . . . . : 192.168.150.2
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : fe80::%5
                                           192.168.150.1
```

Figura 25. Direcciones IPv6 Windows.

Es posible deshabilitar esta generación aleatoria y forzar al sistema a que utilice el formato EUI-64. Esto se consigue con la ejecución de los siguientes comandos, mostrados en la Figura 26. En la Figura 22, se puede apreciar las direcciones IPv6 empleando el formato EUI-64.

```
C:\Windows\system32>netsh interface ipv6 set global randomizeidentifiers=disabled
store=active
Aceptar

C:\Windows\system32>netsh interface ipv6 set global randomizeidentifiers=disabled
store=persistent
Aceptar
```

26. Deshabilitar generación aleatoria de la ID.



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
Anexo recomendaciones de seguridad para la Red CIMI

```
Adaptador de Ethernet Ethernet:
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Dirección física. . . . . : 08-00-27-BF-E0-A0
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Dirección IPv6 . . . . . : 2001:db8:60:968:a00:27ff:febf:e0a0(Preferido)
Dirección IPv6 temporal. . . . . : 2001:db8:60:968:a436:2a12:e2ea:8ecc(Preferido)
Dirección IPv6 temporal. . . . . : 2001:db8:60:968:a572:49fc:450:4bb3(Preferido)
Vínculo: dirección IPv6 local. . . : fe80::a00:27ff:febf:e0a0%5(Preferido)
Dirección IPv4. . . . . : 192.168.150.2(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : jueves, 23 de agosto de 2018 6:54:29 p.m.
La concesión expira . . . . . : viernes, 24 de agosto de 2018 6:54:30 p.m.
Puerta de enlace predeterminada . . . : fe80::%5
192.168.150.1
Servidor DHCP . . . . . : 192.168.150.1
IAID DHCPv6 . . . . . : 50855975
DUID de cliente DHCPv6. . . . . : 00-01-00-01-22-CD-B3-CE-08-00-27-BF-E0-A0
Servidores DNS. . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Figura 27. Configuración direcciones IPv6 temporales y habilitado el formato EUI-64

Por otro lado, es posible también deshabilitar la generación de direcciones temporales como se muestra en las Figura 28 y Figura 29.

```
C:\Windows\system32>netsh interface ipv6 set privacy state=disabled store=active
Aceptar

C:\Windows\system32>netsh interface ipv6 set privacy state=disabled store=persistent
Aceptar
```

Figura 28. Deshabilitar direcciones temporales Windows.

```
Adaptador de Ethernet Ethernet:
Sufijo DNS específico para la conexión. . . :
Dirección IPv6 . . . . . : 2001:db8:60:968:a00:27ff:febf:e0a0
Vínculo: dirección IPv6 local. . . : fe80::a00:27ff:febf:e0a0%5
Dirección IPv4. . . . . : 192.168.150.2
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . : fe80::%5
192.168.150.1

Adaptador de túnel isatap.{3459DE7E-564D-47D9-A09C-FCA36207119D}:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
```

Figura 29. Configuración de IPv6 en Windows sin direcciones temporales.

El ID es obtenido tomando los 64 bits de más a la izquierda del Identificador aleatorio computado, y se coloca en 0 el bit 6 (se numera como 0 al bit de más a la izquierda). Esto crea una ID con el bit universal/local teniendo solo significado local.



SERVICIO NACIONAL DE APRENDIZAJE SENA
Procedimiento de Desarrollo Curricular
Anexo recomendaciones de seguridad para la Red CIMI

4. Monitoreo 7x24

- Integración con el servicio de SOC – Centro de Operaciones de Seguridad
- Seguimiento de las amenazas avanzadas detectadas por red, tipo y nivel de amenaza.
- Bloqueo en tiempo real de amenazas WEB



Figura 30. Centro de Monitoreo de seguridad (SOC).

4.1 Recomendaciones contra las amenazas informáticas y AMENAZAS AVANZADAS

- Usar software legal y actualizado.
- Mantener el antivirus activo, actualizado y apuntando a la EPO.
- Seguir las buenas prácticas de navegación segura.
- Navegar con proxy
- Desconfiar de la descarga de archivos adjuntos
- No seguir los enlaces de los correos sospechosos
- Utilizar una solución de protección dinámica de malware
- Usar bloqueador de ventanas emergentes
- Tener el firewall del sistema activo.
- Tener software de seguridad en todos los dispositivos (tabletas, teléfonos, computadores, entre otros).
- Evitar otorgar privilegios de administrador a usuarios (a menos que sea absolutamente necesario).
- Reportar comportamiento extraño a Seguridad de la Información, haciendo uso la Mesa de Servicios.