



Departamento de Ciencias de la Computación  
Universidad de las Fuerzas Armadas - ESPE

## Práctica de Laboratorio No. 1

Análisis de Amenazas y vulnerabilidades en un  
servidor Web

**Nombres:**

Yeshua Amador Chiliquinga Amaya

Cesar Ignacio Loor Mercado

**Carrera / Asignatura:** Ingeniería de Software / Ingeniería de  
Seguridad de Software

**NRC:** 23358

**Nombre del profesor:** Walter Fuertes, PhD

**Fecha de presentación:** 24 de mayo del 2025

# Índice

<b>1. Objetivo</b>	<b>2</b>
<b>2. Requerimientos</b>	<b>2</b>
<b>3. Entorno Virtual de Red</b>	<b>2</b>
<b>4. Desarrollo</b>	<b>2</b>
4.1. 1. Reconocimiento de red . . . . .	2
4.1.1. 1.1 Escaneo de puertos con Nmap . . . . .	2
4.2. 2. Identificación de vulnerabilidades . . . . .	3
4.2.1. 2.1 Uso de Nmap para detección de vulnerabilidades . . . . .	4
4.2.2. Escaneos dirigidos a vulnerabilidades específicas . . . . .	4
<b>5. 3. Explotación de una vulnerabilidad con Metasploit</b>	<b>5</b>
5.1. 3.1 Uso de Metasploit para explotar una vulnerabilidad . . . . .	5
<b>6. Investigación</b>	<b>6</b>
<b>7. Discusión y conclusión</b>	<b>7</b>
7.1. ¿Qué amenazas se identificaron? . . . . .	7
7.2. ¿Qué vulnerabilidades fueron explotadas? . . . . .	7
7.3. ¿Cuál es el riesgo de no mitigar estas vulnerabilidades? . . . . .	7
7.4. ¿Cuál herramienta es mejor, NMAP, Metasploit, OpenVAS o Nikto? . . . .	7
<b>8. Resumen de la Actividad</b>	<b>7</b>
<b>9. Conclusiones</b>	<b>8</b>

# 1. Objetivo

El objetivo de esta actividad es introducir a los estudiantes en el proceso de identificación de amenazas, vulnerabilidades y riesgos en un entorno controlado, utilizando Kali Linux y un escenario de red virtualizado en VirtualBox.

## 2. Requerimientos

- Kali Linux (instalado en una máquina virtual en VirtualBox).
- Equipo servidor vulnerable (puede ser una máquina vulnerable como Metasploitable2 o OWASP Broken Web Applications).
- Equipo cliente, puede ser Ubuntu Desktop 24.04.2 LTS.
- VirtualBox o cualquier otra herramienta de virtualización para gestionar las máquinas virtuales.
- Acceso a Internet para descarga de herramientas y recursos.

## 3. Entorno Virtual de Red

- Máquina 1: Kali Linux (máquina atacante)
- Máquina 2: Ubuntu Server - Máquina vulnerable (Metasploitable2 o un servidor web vulnerable)
- Máquina 3: Ubuntu Desktop 24.04.2 LTS.

## 4. Desarrollo

### 4.1. 1. Reconocimiento de red

En Kali Linux, vamos a realizar un escaneo de la máquina vulnerable para identificar los servicios abiertos, lo que nos ayudará a identificar posibles puntos débiles.

#### 4.1.1. 1.1 Escaneo de puertos con Nmap

En Kali Linux, abre una terminal y utiliza Nmap para realizar un escaneo de puertos:

```
1 $ nmap -sV -T4 192.168.112.137
```

Listing 1: Escaneo básico con Nmap

```

j nmap -SV -T4 192.168.112.137
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 11:41 EDT
Nmap scan report for 192.168.112.137
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 6ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.3
80/tcp    open  http         Apache/2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rshbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshcd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1888/tcp  open  java-rmi     GNU Classpath gmicregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu3
5432/tcp  open  postgresql   PostgreSQL 9B 8.3.8 - 8.3.7
5986/tcp  open  vnc          VNC (protocol 3.3)
6880/tcp  open  X11          (access denied)
6887/tcp  open  irc          UnrealIRCd
8888/tcp  open  sftp         Apache Jserv (Protocol v1.0)
8188/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:0C:29:93:EE:30 (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Linux, 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 11.60 seconds

```

Figura 1: Resultado del escaneo Nmap

#### Explicación:

- **Amenaza:** Los servicios en la máquina vulnerable son posibles vectores de ataque.
- **Vulnerabilidad:** Algunos servicios, como HTTP o SSH, pueden estar desactualizados o mal configurados, lo que los hace vulnerables a ataques.
- **Riesgo:** Si un atacante logra explotar una vulnerabilidad en uno de esos servicios, podría comprometer la máquina vulnerable.

#### Referencia Nmap:

- Nmap Documentation: <https://nmap.org/docs.html>

## 4.2. 2. Identificación de vulnerabilidades

En esta etapa, utilizaremos Nmap (con sus scripts NSE) para buscar vulnerabilidades conocidas en los servicios detectados durante el escaneo previo.

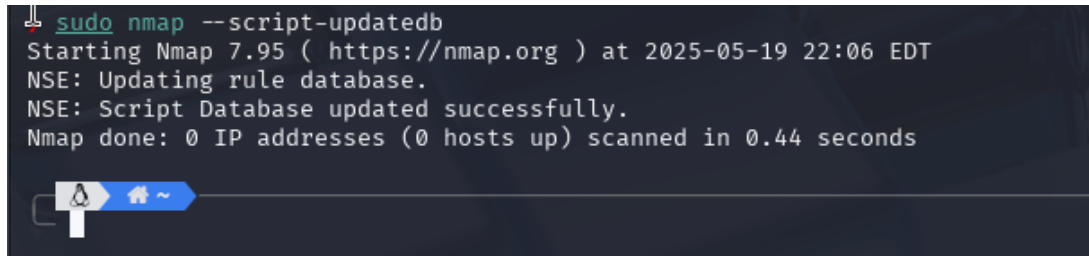
### 4.2.1. 2.1 Uso de Nmap para detección de vulnerabilidades

#### Preparar entorno en Kali Linux

Verifica que Nmap esté instalado (por defecto Kali lo incluye). Actualiza la base de datos de scripts NSE para asegurarte de contar con las últimas comprobaciones:

```
1 $ sudo nmap --script-updatedb
```

Listing 2: Actualización de scripts NSE



```
1 sudo nmap --script-updatedb
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-19 22:06 EDT
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.44 seconds
```

Figura 2: Actualización de scripts NSE

#### Escaneo de versiones y vulnerabilidades con el agrupador "vuln"

```
1 $ sudo nmap -sV --script=vuln -oN nmap_vuln_scan.txt 192.168.112.137
```

Listing 3: Escaneo de vulnerabilidades con NSE

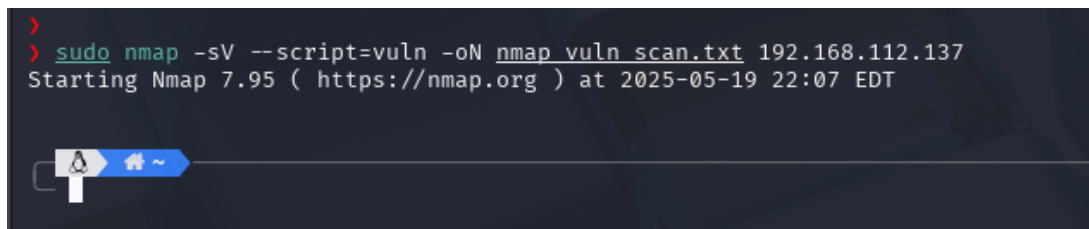
- -sV - Detecta la versión de cada servicio en puertos abiertos.
- --script=vuln - Ejecuta todos los scripts NSE categorizados como "vuln".
- -oN nmap\_vuln\_scan.txt - Guarda el resultado en un archivo de texto.

### 4.2.2. Escaneos dirigidos a vulnerabilidades específicas

#### Comprobación de SSL/TLS (Heartbleed, Poodle, etc.)

```
1 $ sudo nmap -p 443 --script ssl-heartbleed,ssl-poodle -oN nmap_ssl_vulns.txt 192.168.112.137
```

Listing 4: Escaneo de vulnerabilidades SSL/TLS



```
> sudo nmap -sV --script=vuln -oN nmap_vuln_scan.txt 192.168.112.137
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-19 22:07 EDT
```

Figura 3: Resultado del escaneo de vulnerabilidades SSL/TLS

#### Verificación de SMB (MS08-067, MS17-010/EternalBlue, etc.)

```
1 $ sudo nmap -p 139,445 --script smb-vuln-ms08-067,smb-vuln-ms17-010 -oN nmap_smb_vulns.txt 192.168.112.137
```

Listing 5: Escaneo de vulnerabilidades SMB

```
cat smb_vuln.txt
0 Map Scan initiated Mon May 19 21:50:43 2020 as: /usr/lib/nap/nap -p 139,445 --script smb-vuln-ms08-602,smb-vuln-ms17-010 --db map_smb_vulns.txt 192.168.112.117
Map scan report for 192.168.112.117
Host is up (0.0001s latency).
0MB: STATE: SNIFF
139/tcp open: netbios-ssn
445/tcp open: microsoft-ds
MAC Address: 08:00:27:9C:1E:10 (VMware)
0 Map done at Mon May 19 21:50:46 2020 -- 1 IP address (1 host up) scanned in 6.41 seconds
```

Figura 4: Resultado del escaneo de vulnerabilidades SMB

## 5. 3. Explotación de una vulnerabilidad con Metasploit

Una vez identificadas las vulnerabilidades, vamos a intentar explotarlas usando Metasploit, una herramienta de explotación automatizada.

### 5.1. 3.1 Uso de Metasploit para explotar una vulnerabilidad

Por ejemplo, si descubrimos que un servicio HTTP es vulnerable a un Remote Code Execution (RCE), podemos usar Metasploit para explotarlo.

```
1 $ msfconsole
```

Listing 6: Iniciando Metasploit

```
> msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

Trace program: running

wake up, Neo...
the matrix has you
follow the white rabbit.

knock, knock, Neo.

(
X
Q
)
```

Figura 5: Consola de Metasploit

Buscamos un exploit relacionado con el servicio identificado (por ejemplo, un servicio HTTP):

```
1 msf6 > search apache
```

Listing 7: Buscando exploits en Metasploit

```
msf6 > search apache
```

#	Name	Disclosure Date	Rank	Check	Descr
0	exploit/multi/http/apache_apisix_api_default_token_rce	2020-12-07	excellent	Yes	APISI
1	exploit/linux/http/atutor_filemanager_traversal	2016-03-01	excellent	Yes	ATuto
2	exploit/multi/http/apache_activemq_upload_jsp	2016-06-01	excellent	No	Activ
3	auxiliary/scanner/http/apache_userdir_enum	.	normal	No	Apach
4	exploit/multi/http/apache_normalize_path_rce	2021-05-10	excellent	Yes	Apach
5	exploit/multi/http/apache_normalize_path_rce	.	.	.	.
6	exploit/multi/http/apache_normalize_path_rce	.	.	.	.
7	exploit/multi/http/apache_normalize_path_rce	.	.	.	.
8	exploit/multi/http/apache_normalize_path_rce	.	.	.	.
9	exploit/multi/http/apache_normalize_path_rce	.	.	.	.

Figura 6: Resultado de búsqueda de exploits en Metasploit

### Explicación:

- **Amenaza:** Si el atacante explota la vulnerabilidad, puede ejecutar comandos remotos en el servidor.
- **Vulnerabilidad:** El servidor web tiene una vulnerabilidad de ejecución remota de código debido a una mala configuración.
- **Riesgo:** El riesgo es que el atacante pueda tomar control total del servidor.

### Referencia Metasploit:

- Metasploit Documentation: <https://docs.metasploit.com/>

## 6. Investigación

En lugar de Metasploit, realiza la explotación de una vulnerabilidad con Nikto.

```
1 $ nikto -h 192.168.112.137
```

Listing 8: Escaneo con Nikto

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.112.137	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

```
Exploit target:
```

Id	Name
0	Automatic

Figura 7: Resultado del escaneo con Nikto

Nikto documentation: <https://www.kali.org/tools/nikto/>

## 7. Discusión y conclusión

### 7.1. ¿Qué amenazas se identificaron?

Se identificaron varias amenazas potenciales, incluyendo la posibilidad de que un atacante ejecute código remoto en el servidor web, acceda a información sensible o realice ataques de denegación de servicio.

### 7.2. ¿Qué vulnerabilidades fueron explotadas?

Entre las vulnerabilidades identificadas se encuentran servicios desactualizados, configuraciones inseguras en servicios web, y posibles vulnerabilidades en servicios como SMB y SSL/TLS.

### 7.3. ¿Cuál es el riesgo de no mitigar estas vulnerabilidades?

Si no se corrigen estas vulnerabilidades, un atacante podría obtener acceso completo al sistema, robar información confidencial, instalar malware o utilizar el sistema comprometido como punto de partida para ataques a otros sistemas en la red.

### 7.4. ¿Cuál herramienta es mejor, NMAP, Metasploit, OpenVAS o Nikto?

Cada herramienta tiene un propósito específico:

- **NMAP:** Excelente para descubrimiento de hosts y servicios en una red.
- **Metasploit:** Potente para explotación de vulnerabilidades y pruebas de penetración.
- **OpenVAS:** Especializado en escaneo de vulnerabilidades con una base de datos extensa.
- **Nikto:** Específico para análisis de vulnerabilidades en servidores web.

## 8. Resumen de la Actividad

- **Amenaza:** Es cualquier posible evento o situación que podría comprometer la seguridad de la red o los sistemas.
- **Vulnerabilidad:** Es una debilidad que puede ser explotada por una amenaza, como un servicio desactualizado o una mala configuración.
- **Riesgo:** Es la probabilidad de que una amenaza explote una vulnerabilidad, lo que puede resultar en daño al sistema o acceso no autorizado.



## 9. Conclusiones

Los participantes habrán aprendido cómo identificar, analizar y explotar vulnerabilidades en una red, comprendiendo la relación entre las amenazas, las vulnerabilidades y los riesgos. Utilizando herramientas como Nmap, Metasploit y Nikto en Kali Linux, habrán ganado experiencia práctica en pruebas de penetración y evaluación de seguridad en un entorno controlado.

## Referencias Bibliográficas

1. OpenVAS: The Open Vulnerability Assessment System. (2012). Syngress Publishing. ISBN: 978-1-59749-574-5.
2. Nikto: A Web Server Scanner. (2010). Packt Publishing. ISBN: 978-1-84951-019-3.
3. The Penetration Tester's Guide. (2011). No Starch Press. ISBN: 978-1-59327-288-3
4. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. (2009). Insecure Publishing. ISBN: 978-0-9799587-1-7.
5. Nmap in the Enterprise: Your Guide to Network Scanning. (2008). Syngress Publishing. ISBN: 978-0-08-055874-5.