

Datos Generales

Título: Análisis de vulnerabilidades y medidas de protección en sistemas operativos: Práctico en Linux

Alumnos: Diego Raúl Montes – Ramiro Morales - Comisión 2025-04

Materia: Arquitectura y Sistemas Operativos

Profesor/es: Martín Aristiaran

Tutor: Sofia Lemos

Fecha de Entrega: 5/06/2025

Índice

1. Introducción
2. Marco Teórico
3. Caso Práctico
4. Metodología
5. Resultados
6. Conclusiones
7. Bibliografía
8. Anexos

1. Introducción

La seguridad en sistemas operativos es un pilar crítico en la era digital. De acuerdo con el OWASP TOP 10, los ataques a servicios expuestos como DNS o SSH representan el 40% de las brechas de seguridad. Este trabajo se enfoca en analizar

vulnerabilidades y aplicar medidas de protección en Linux, utilizando herramientas como *iptables* y *Nmap*, con un enfoque práctico en el bloqueo de puertos maliciosos.

¿Por qué se eligió este tema?

La seguridad en sistemas operativos es esencial en la actualidad, debido a amenazas como el ransomware (ej. WannaCry) o vulnerabilidades explotables (ej. EternalBlue). Elegimos este tema para aprender a protegernos y aplicar herramientas como *Nmap* y *firewalls* en entornos reales.

¿Qué importancia tiene en nuestra formación como técnicos en programación?

Como futuros técnicos en programación, debemos desarrollar software seguro y proteger servidores. Entender conceptos como configuración de *iptables* o ataques de *phishing* es clave para nuestro perfil profesional.

Objetivos del trabajo:

1. Simular un ataque MITM con *Nmap* para capturar tráfico no cifrado.
2. Implementar reglas de *iptables* para cerrar puertos críticos (como el 445).
3. Validar la eficacia del bloqueo mediante escaneos con *Nmap* antes y después.

2. Marco Teórico

2.1. Tipos de ataques

Ataque	Descripción	Ejemplo
Phishing	Suplantación de identidad para robar credenciales o información confidencial.	Páginas falsas de bancos que imitan el diseño original. (principal.pdf, Fig. 2)
DDoS	Sobrecarga de redes o servidores con tráfico falso.	Uso de botnets para colapsar un servidor. (principal.pdf, p. 16)
MITM	Intercepción de comunicaciones entre dos partes sin su conocimiento.	Atacante en red local que lee o modifica mensajes. (principal.pdf, p. 6)

2.2. Herramientas de protección

 Bloqueo de puertos con *iptables*:

Comando de ejemplo:

```
sudo iptables -A INPUT -p tcp --dport 445 -j DROP
```

Explicación técnica:

1. **-A OUTPUT**: Agrega una regla a la cadena de salida. Es el tráfico que sale por el puerto
2. **-p tcp**: Aplica solo a paquetes TCP.
3. **--dport 445**: Objetivo: puerto 445 (SMB).
4. **-j DROP**: Descarta el paquete sin respuesta (estado "filtered" para *Nmap*).

Impacto:

- El atacante recibirá un *timeout* al intentar conectarse.
- Los servicios internos seguirán funcionando.

Firewalls:

- *iptables*: Configuración avanzada de reglas de red en Linux.
- *firewalld*: Alternativa más simple con zonas y servicios predefinidos.

Nmap:

- Herramienta de escaneo de red para identificar puertos y servicios activos.
- Ejemplo: **nmap -sV IP** permite descubrir puertos abiertos en un host.

3. Caso Práctico

Título: Mitigación con firewall en Linux

Descripción del problema:

Un atacante en la misma red local logra interceptar comunicaciones entre dos equipos.

Herramientas utilizadas:

- *Nmap*: Captura de tráfico y detección de puertos.
- *iptables*: Bloqueo de puertos vulnerables.

Capturas de pantalla:

- Resultado del comando: `nmap -sV -O [IP]` mostrando servicios y sistema operativo.

Regla aplicada:

```
iptables -A INPUT -p tcp --dport 445 -s 10.10.11.69 -j DROP
```

Validación:

- Antes del bloqueo: puerto 445 aparece como "open".
- Después del bloqueo: *Nmap* muestra el puerto 445 como "Operation not Permitted".

Paso a paso del procedimiento:

1. Identificar la IP de la víctima
 - Ejecutar `ip a` o `hostname -I` en la máquina víctima.
2. Escaneo inicial con Nmap (antes del bloqueo)

Desde la máquina atacante:

```
nmap -sV -O [IP_de_la_víctima]
```

- Confirmar que el puerto 445 esté abierto.

3. Aplicar la regla de iptables

En la víctima:

```
sudo iptables -A OUTPUT -p tcp --dport 445 -s [IP_del_atacante] -j DROP
```

4. Verificar la regla aplicada

Ejecutar:

```
sudo iptables -L -n -v
```

5. Escaneo con Nmap (después del bloqueo)

En el atacante:

```
nmap -sV [IP_de_la_víctima]
```

- Confirmar que el puerto 445 (está bloqueado)

6. Capturas recomendadas

- Resultado del escaneo antes y después.
- Comando aplicado de iptables.
- Verificación con `iptables -L`.

4. Metodología

Herramientas:

- *Nmap*
- *iptables*

Reparto de tareas:

- Ramiro: Escaneo y simulación de ataque.
 - Diego: Configuración del firewall en la máquina objetivo.
-

5. Resultados

Logros:

- Se bloqueó exitosamente el puerto 445 mediante *iptables*.
 - Se comprobó el cambio de estado en *Nmap*, de "open" a "operacion no permitted".
-

6. Conclusiones

Configurar un firewall es una medida fundamental para proteger sistemas operativos. Aprendimos que:

- No basta con instalar un sistema: debe configurarse correctamente.
 - Se recomienda complementar con autenticación multifactor (MFA) y actualizaciones constantes.
 - Para futuras prácticas, exploramos herramientas avanzadas como *SELinux*.
-

7. Bibliografía (formato APA)

Roco, D. (2020). *Principales vulnerabilidades en componentes TIC*. UTN Mendoza.

UTN. (2023). *Seguridad en sistemas operativos*. Material de cátedra.

UTN. (2023). *Actividad 2 – Apuntes de clase*.

UTN. (2023). *Escaneo de puertos con Nmap*.

8. Anexos (Capturas)

```
(root@kali)-[/home/kali]
# nmap -sV 10.10.11.69
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 20:32 EDT
Stats: 0:01:33 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 90.91% done; ETC: 20:33 (0:00:05 remaining)
Stats: 0:01:34 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 86.36% done; ETC: 20:33 (0:00:00 remaining)
Nmap scan report for 10.10.11.69
Host is up (0.19s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2025-06-04 07:32:56Z)
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., Site: Defa
ult-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap        Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., Site: Defa
ult-First-Site-Name)
3268/tcp  open  ldap            Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., Site: Defa
ult-First-Site-Name)
3269/tcp  open  ssl/ldap        Microsoft Windows Active Directory LDAP (Domain: fluffy.htb0., Site: Defa
ult-First-Site-Name)
```

```
(root@kali)-[/home/kali]
# sudo iptables -A OUTPUT -p tcp -d 10.10.11.69 --dport 445 -j DROP

(root@kali)-[/home/kali]
# nmap -sV -p-445 10.10.11.69
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-03 20:27 EDT
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.10.11.69, 16) => Operation not permitted
Offending packet: TCP 10.10.14.14:40778 > 10.10.11.69:445 S ttl=56 id=561 iplen=44 seq=1765647030 win
=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 10.10.11.69, 16) => Operation not permitted
Offending packet: TCP 10.10.14.14:40780 > 10.10.11.69:445 S ttl=48 id=25752 iplen=44 seq=1765778100 w
in=1024 <mss 1460>
```