Pratica S7/L1

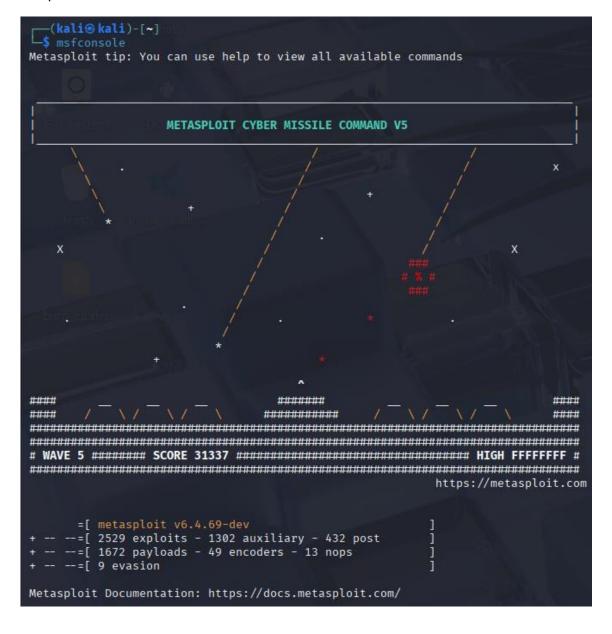
Introduzione: l'obiettivo di questo esercizio era identificare e sfruttare una vulnerabilità nota nel servizio FTP (vsftpd) di una macchina virtuale vulnerabile al fine di ottenere un accesso non autorizzato e dimostrare la compromissione del sistema tramite la creazione di una cartella.

Configurazione del laboratorio:

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

Fase di attacco

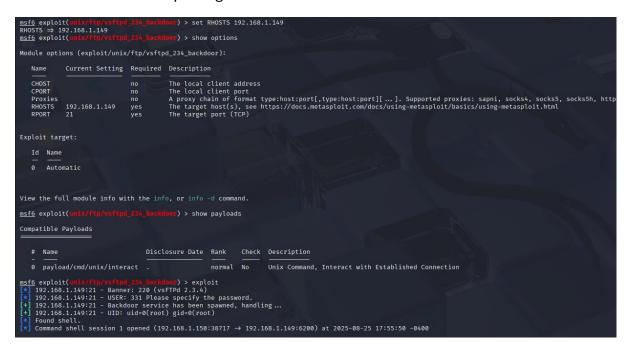
Dopo aver verificato la connettività tra le due macchine e aver eseguito una scansione nmap sulla porta 21, la fase di attacco è iniziata con la preparazione del framework Metasploit su Kali Linux.



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.



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.



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.

```
nsfadmin@metasploitable:~$ ifconfig
          Link encap:Ethernet HWaddr 08:00:27:e6:1c:91 inet addr:192.168.1.149 Bcast:192.168.1.255
eth0
                                                          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
             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
             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 /
       dev
             initrd
                          lost+found
bin
                                       nohup.out
                                                  root
                                                         sys
boot
       etc
             initrd.img
                          media
                                                              _metasploit
                                       opt
                                                  sbin tes
                                                                           var
                                                                           vmlinuz
drom
       home
             lib
                          mnt
                                       proc
                                                         tmp
                                                   srv
nsfadmin@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.