CS0424IT — S7/L1 HACKING CON METASPLOIT

Noemi de Martino

GitHub

TRACCIA

Partendo dall'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio vsftpd (lo stesso visto in lezione teorica). L'unica differenza sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: 192.168.1.149/24.

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit.

SVOLGIMENTO

Impostazione dell'Indirizzo IP per Metasploitable

Per prima cosa, dobbiamo configurare la macchina Metasploitable con un indirizzo IP specifico. L'indirizzo scelto è 192.168.1.149/24. Questa configurazione è fondamentale per assicurarsi che la macchina target sia correttamente inserita nella rete e possa essere raggiunta dalla macchina Kali

```
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

Figura 1: Nuova configurazione di rete di Metasploitable2.

Configurazione di Pfsense

Successivamente, utilizziamo Pfsense come router gateway. Questo passaggio è cruciale per consentire la comunicazione tra la macchina Kali, da cui condurremo l'attacco, e la macchina Metasploitable. Configurare Pfsense attraverso la sua interfaccia web permette di creare un ponte tra le due reti, facilitando così la connessione necessaria per l'esercizio.

```
Pfsense [In esecuzione] - Oracle VM VirtualBox
                                                                                  File Macchina Visualizza Inserimento Dispositivi Aiuto
The IPv4 LAN address has been set to 192.168.50.1/24
ou can now access the webConfiqurator by opening the following URL in your web'
prowser:
                 http://192.168.50.1/
Press <ENTER> to continue.
'irtualBox Virtual Machine - Netgate Device ID: 4f987c0c90f53fe9bb01
** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)
                   -> em0
                                   -> v4/DHCP4: 10.0.2.15/24
                                   -> v4: 192.168.50.1/24
-> v4: 192.168.1.1/24
LAN (lan)
                      em1
OPT1 (opt1)
                      em2
```

Figura 2: Risultato della scansione con Nmap.

Verifica della Connessione

Prima di procedere con l'attacco vero e proprio, è essenziale verificare che la macchina Kali possa comunicare con la macchina Metasploitable. Questo si fa eseguendo un semplice comando ping all'indirizzo IP di Metasploitable (192.168.1.149) dalla macchina Kali. Se la connessione è attiva, possiamo proseguire con i passaggi successivi.

```
(kali® kali)-[~]
$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=1.26 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=1.04 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=1.49 ms
^X64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.952 ms
```

Figura 3: Risultato del ping da Kali a Metasploitable2.

Scansione delle Porte con Nmap

Dopo aver verificato la connessione, eseguiamo una scansione delle porte sulla macchina Metasploitable per identificare i servizi in esecuzione e le loro versioni. Utilizziamo il comando sudo nmap -sV -sT 192.168.1.149 -p 21 per focalizzarci sul servizio FTP, specificamente sulla porta 21.

```
sudo nmap -sV -sT 192.168.1.149 -p 21
```

Questa scansione ci fornisce informazioni dettagliate sulla versione del servizio FTP in esecuzione, confermando la presenza di vsftpd vulnerabile.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 12:52 CEST
Nmap scan report for 192.168.1.149
Host is up (0.00085s latency).

PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
MAC Address: 08:00:27:6D:5F:CB (Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 13.25 seconds
```

Figura 4: Risultato della scansione.

Avvio di Metasploit

A questo punto, sulla macchina Kali, avviamo la console di Metasploit digitando msfconsole nel terminale. Metasploit è una piattaforma potente utilizzata per sviluppare, testare e utilizzare exploit contro vulnerabilità conosciute. L'interfaccia msfconsole ci fornisce tutti gli strumenti necessari per condurre l'attacco.

Figura 5: Avvio di Metasploit.

Exploit vsftpd

Dopo aver trovato il modulo di exploit appropriato, lo selezioniamo con il comando use exploit/unix/ftp/vs Questo comando carica il modulo exploit e ci permette di configurarlo per il nostro attacco.

Figura 6: Ricerca dell'exploit

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Figura 7: Scelta dell'exploit

Dopo aver scelto exploit e payload ed aver configurato le opzioni per entrambi, bisogna lanciare l'attacco con il comando exploit. Se l'attacco è riuscito, ci si ritrova con un prompt dei comandi che rappresenta la riuscita della sessione. Dando alcuni comandi base come pwd, 1s e ifconfig, si verifica la riuscita dell'attacco. Configuriamo l'exploit impostando l'indirizzo IP della macchina target. Questo si fa con il comando set RHOSTS 192.168.1.149. Questo passaggio è fondamentale perché indica a Metasploit quale macchina attaccare.

Figura 8: Setting RHOSTS

Selezione del Payload

Visualizziamo i payload disponibili con il comando show payloads. Un payload è il codice che viene eseguito una volta che l'exploit ha avuto successo. Dopo aver visualizzato i payload compatibili, selezioniamo quello più adatto al nostro scopo con set payload generic/shell_reverse_tcp.

Lancio dell'Attacco

Con l'exploit e il payload configurati, siamo pronti a lanciare l'attacco. Utilizziamo il comando exploit per avviare il processo. Se tutto è configurato correttamente, Metasploit tenterà di sfruttare la vulnerabilità e di eseguire il payload sulla macchina target.

Figura 9: Creazione della cartella test_metasploit e relativa verifica.

Verifica della Riuscita dell'Attacco e Creazione della cartella

Dopo il lancio dell'attacco, dobbiamo verificare se ha avuto successo. Questo si fa eseguendo comandi come 1s e if config nella sessione ottenuta sulla macchina Metasploitable. Se vediamo l'output previsto, significa che l'attacco ha avuto successo e abbiamo ottenuto l'accesso alla macchina target. Una volta ottenuto l'accesso alla macchina Metasploitable, creiamo una cartella chiamata "test_metasploit" nella directory root utilizzando il comando mkdir /test_metasploit. Questo passaggio dimostra che abbiamo il controllo della macchina target.

Verifica della Creazione della Cartella

Infine, verifichiamo la creazione della cartella "test_metasploit" sulla macchina Metasploitable. Questo conferma che l'attacco è stato completato con successo e che abbiamo raggiunto l'obiettivo dell'esercizio.



Figura 10: Creazione della cartella test_metasploit.

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

Figura 11: Verifica della cartella creata.

CONCLUSIONE

Questo esercizio ha illustrato i passaggi necessari per sfruttare una vulnerabilità nel servizio vsftpd su una macchina Metasploitable, utilizzando la piattaforma Metasploit. Abbiamo configurato correttamente la rete, eseguito l'exploit e il payload, e verificato il successo dell'attacco. La creazione della cartella "test_metasploit" ha dimostrato il nostro controllo sulla macchina target, completando così l'esercizio con successo.