

Exploit Telnet con Metasploit

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**.

Svolgimento dell'esercizio

Passo 1: Avvio di Metasploit

Il primo passo è avviare Metasploit. Questo può essere fatto tramite il comando `msfconsole` nel terminale. Una volta avviato, ci si trova all'interno dell'interfaccia di Metasploit, pronti per eseguire comandi.

```
(kali㉿kali)-[~]  
$ msfconsole  
Metasploit tip: The use command supports fuzzy searching to try and  
select the intended module, e.g. use kerberos/get_ticket or use  
kerberos forge silver ticket
```

Passo 2: Ricerca del Modulo Telnet

Utilizzando il comando **search telnet**, si cerca il modulo appropriato per la scansione Telnet.

```
msf6 > search telnet
```

Passo 3: Selezione del Modulo Telnet

Dopo aver identificato il modulo desiderato, si utilizza il comando **use** **auxiliary/scanner/telnet/telnet_version** per selezionare il modulo di scansione Telnet.

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

Passo 4: Configurazione delle Opzioni

Prima di eseguire la scansione, è necessario configurare le opzioni del modulo. Utilizzando il comando **show options**, si visualizzano le opzioni disponibili.

```
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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.
```

La principale opzione da configurare è **RHOSTS**, che specifica l'indirizzo IP del target. In questo caso, l'indirizzo IP che utilizzeremo è **192.168.40.101**.

Il comando **set RHOSTS 192.168.40.101** imposta questa opzione.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.40.101
RHOSTS => 192.168.40.101
```

Passo 5: Esecuzione della Scansione

Una volta configurato il modulo, si esegue la scansione con il comando **exploit** così da ottenere le credenziali di accesso di **metasploitable**.

```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
[*] 192.168.40.101:23 - 192.168.40.101:23 TELNET
[*] 192.168.40.101:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Passo 6: Esecuzione del comando telnet

Utilizzando il comando telnet seguito dall'IP del target, entreremo al suo interno e potremo inserire le credenziali di accesso ottenute in precedenza.

```
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.40.101
[*] exec: telnet 192.168.40.101

Trying 192.168.40.101...
Connected to 192.168.40.101.
Escape character is '^]'.

metasploitable
VBox_GA__

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:
```