

REPORT UNIT 2 WEEK 7

MODULO 2

Avvio con **msfconsole**.

```
(kali㉿kali)-[~]
$ msfconsole

IIIIII dTb.dTb
II 4' v 'B
II 6. .P
II 'T; . ;P'
II 'T; ;P'
IIIII 'YvP'

I love shells --egypt

      =[ metasploit v6.3.16-dev ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Use sessions -1 to interact with the
last opened session
Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

Con **nmap -sV** vedo le porte aperte.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.50.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-11 18:40 EDT
Nmap scan report for 192.168.50.100
Host is up (0.038s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN;
```

L'esercizio ci chiede di sfruttare telnet (23).
Faccio **search** per la versione telnet richiesta

35	auxiliary/scanner/telnet/telnet_version	normal	No	Telnet Service Banner Detection
36	auxiliary/scanner/telnet/telnet_encrypt_overflow	normal	No	Telnet Service Encryption Key ID Overflow Detection
37	payload/cmd/unix/bind_busybox_telnetd	normal	No	Unix Command Shell, Bind TCP (via BusyBox telnetd)

Scelgo il modulo **scanner/telnet/telnet_version** e faccio show options per vedere i parametri necessari.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  RHOSTS           yes       The password for the specified username
  RHOSTS    RPORT            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     THREADS           yes       The target port (TCP)
  THREADS   TIMEOUT           yes       The number of concurrent threads (max one per host)
  TIMEOUT   USERNAME          no        Timeout for the Telnet probe
  USERNAME
```

Imposto il target host con **set RHOSTS** ed uso exploit.

Non sono presenti payloads.

Testo il risultato collegandomi alla telnet ed inserendo username e password trovate.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.50.100
RHOSTS => 192.168.50.100
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[*] 192.168.50.100:23 - 192.168.50.100:23 TELNET
[*] 192.168.50.100:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.50.100
[*] exec: telnet 192.168.50.100

Trying 192.168.50.100...
Connected to 192.168.50.100.
Escape character is '^['.

msf6@kali:~$ telnet 192.168.50.100
Trying 192.168.50.100...
Connected to 192.168.50.100.
Escape character is '^['.

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
```

Infine, esco con **exit** e torno ai comandi principali con **back**.