

# Esercizio 2 Settimana 7

## Metasploit Telnet

Oggi andremo ad utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet sulla macchina Metasploitable. Il servizio Telnet è in ascolto sulla porta 23 ed è relativo alla connessione remota tra host di una rete (ormai sostituito con i protocolli SSH più sicuri).

Iniziamo con la scansione aggressiva della macchina vittima per andare a vedere se la porta è effettivamente aperta dopodiché apriamo Metasploit su Kali con il comando `'msfconsole'`.

```
root@Andrea: ~  
File Actions Edit View Help  
root@Andrea: ~  
# nmap -A -T4 192.168.1.17  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 14:45 CET  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 2.54 seconds  
root@Andrea: ~  
# nmap -A -T4 192.168.1.149  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 14:45 CET  
Nmap scan report for LAPTOP-4COMA36N.station (192.168.1.149)  
Host is up (0.00038s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp           vsftpd 2.3.4  
| ftp-syst:  
|  STAT:  
|  FTP server status:  
|    Connected to 192.168.1.33  
|    Logged in as ftp  
|    TYPE: ASCII  
|    No session bandwidth limit  
|    Session timeout in seconds is 300  
|    Control connection is plain text  
|    Data connections will be plain text  
|    vsFTPd 2.3.4 - secure, fast, stable  
|_ End of status  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
22/tcp    open  ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
| ssh-hostkey:  
|  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)  
|  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)  
23/tcp    open  telnet        Linux telnetd  
25/tcp    open  smtp          Postfix smtpd  
| sslv2:  
|  SSLv2 supported  
|  ciphers:  
|    SSL2_DES_192_EDE3_CBC_WITH_MD5  
|    SSL2_DES_64_CBC_WITH_MD5
```

A questo punto andiamo a cercare l'exploit con il comando `'search + parametri di ricerca'` e con `'use 1'` selezioniamo il numero dell'exploit (si può inserire anche il path) che vogliamo utilizzare. Non serve altro se non settare nel modo corretto le impostazioni inerente all'host tramite `'set rhosts 192.168.1.149'`.

```
root@Andrea: ~  
File Actions Edit View Help  
==[ metasploit v6.3.27-dev ]  
+ -- ==[ 2335 exploits - 1220 auxiliary - 413 post ]  
+ -- ==[ 1385 payloads - 46 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit tip: To save all commands executed since start up  
to a file, use the makerc command  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search telnet_version  
  
Matching Modules  
  
# Name Disclosure Date Rank  
Check Description  
- - - - -  
0 auxiliary/scanner/telnet/lantronix_telnet_version normal  
No Lantronix Telnet Service Banner Detection  
1 auxiliary/scanner/telnet/telnet_version normal  
No Telnet Service Banner Detection  
  
Interact with a module by name or index. For example info 1, use 1 or use auxilia  
ry/scanner/telnet/telnet_version  
  
msf6 > use 1  
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.149  
rhosts => 192.168.1.149  
msf6 auxiliary(scanner/telnet/telnet_version) > exploit
```

Con il comando *'exploit'* andiamo ad eseguirlo e Metasploit andrà a cercare user e password della macchina vittima fino a fare il login.

[illegible]

L'exploit è una tecnica o codice malevolo che permette di sfruttare una vulnerabilità di un determinato sistema o dispositivo informatico per poterne prendere possesso. Inoltre, a differenza dei malware, non hanno bisogno dell'azione diretta dell'utente essendoci la vulnerabilità intrinseca nella macchina vittima.