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:

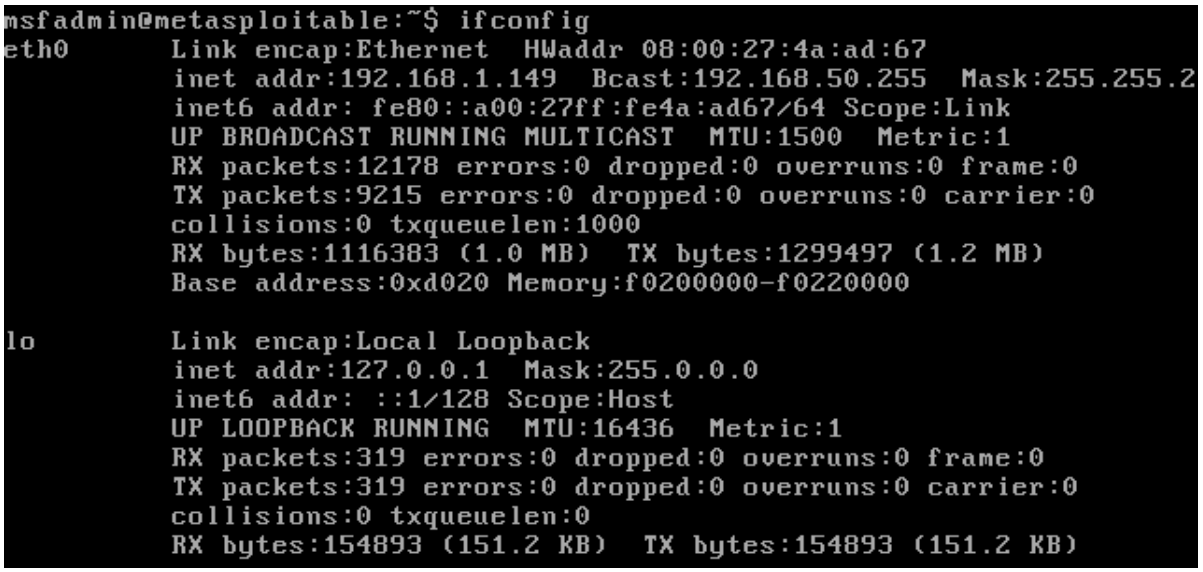
- manuale, quando si usano dei siti che contengono già dei codici malevoli (CVE, ExploitDB). In pratica, scarico il codice e poi con Netcat lo uso sul target. C'è da dire che l'exploit manuale è consigliato farlo solo su una rete di piccole dimensioni, dato che richiederebbe molto tempo;
- automatico,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



Poi controllo se l’attaccante riesce a raggiungerlo

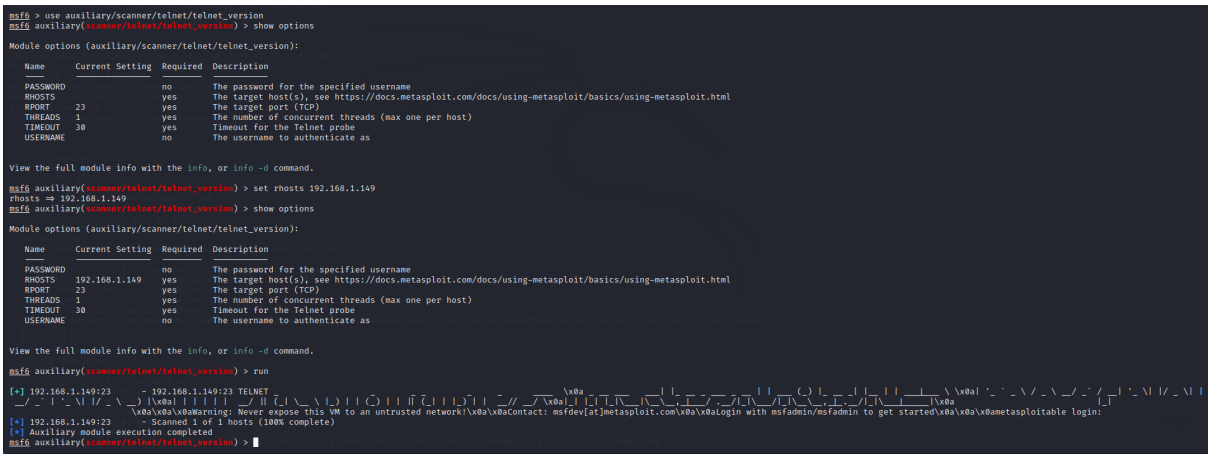
```
┌──(natalino㉿kali)-[~]
└─$ ping 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data.
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=5.40 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=11.4 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.789 ms
64 bytes from 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

ed effettuo il mio exploit utilizzando un modulo ausiliario



Infine controllo se le credenziali che ho carpito sono corrette