

Attacco sul servizio “Telnet” con “Metasploit”

- Indice:
 - Introduzione
 - Configurazione Ip
 - Scanning
 - Utilizzo di Metasploit

Introduzione

Che cos'è un attacco hacker sul servizio Telnet?

Il servizio Telnet è un protocollo che è stato creato per l'interazione tra computer remoti e viene utilizzato tramite interfaccia a riga di comando ed è bidirezionale ed orientato ai byte.

Questo protocollo ha alcuni problemi di sicurezza tra cui la mancanza di uno schema di autenticazione che renda sicura la comunicazione tra due host e non intercettabile; la non decriptazione dei dati inviati tramite la connessione (nemmeno le password) ed è quindi banale catturare i dati scambiati ed usare la password per scopi malevoli.

A causa di queste vulnerabilità gli hacker possono utilizzarle per entrare nel sistema. Oggi andremo a vedere il tool "Metasploit". Utilizzeremo la macchina Kali per fare l'attacco verso la macchina Metasploitable.

Configurazione Ip

- Prima di sferrare un attacco bisogna conoscere l'indirizzo ip e nel nostro caso andiamo a settare gli indirizzi delle nostre macchine virtuali.

File Actions Edit View Help

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

root@metasploitable:/home/nsfadmin# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0<link>
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 61 bytes 7320 (7.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 37 bytes 4038 (3.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.5 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::db46:ef7d:3163:c23d prefixlen 64 scopeid 0<link>
    ether 08:00:27:36:82:25 txqueuelen 1000 (Ethernet)
    RX packets 5 bytes 1360 (1.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27 bytes 3604 (3.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 9 bytes 800 (800.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9 bytes 800 (800.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



metasploitable [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
root@metasploitable:/home/nsfadmin# ifconfig
eth0
    Link encap:Ethernet HWaddr 08:00:27:1a:9a:84
    inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
    inet6 addr: fe80::a00:27ff:fe1a:9a84/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:19 errors:0 dropped:0 overruns:0 frame:0
    TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:1550 (1.5 KB) TX bytes:6460 (6.3 KB)
    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:113 errors:0 dropped:0 overruns:0 frame:0
    TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:0
    RX bytes:29705 (29.0 KB) TX bytes:29705 (29.0 KB)

root@metasploitable:/home/nsfadmin#
```

Scanning

- Per conoscere quali sono i servizi aperti andiamo a fare uno scanning di rete con il tool “Nmap”.

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.1.40  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-05 07:12 EST  
Nmap scan report for 192.168.1.40  
Host is up (0.0016s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE          VERSION  
21/tcp    open  ftp              vsftpd 2.3.4  
22/tcp    open  ssh              OpenSSH 4.7p1 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             netkit-rsh rexecd  
513/tcp   open  login?  
514/tcp   open  shell           Netkit rshd  
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  
8009/tcp  open  ajp13           Apache Jserv (Protocol v1.3)  
8180/tcp  open  http            Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 52.78 seconds
```

Utilizzo di Metasploit

- Dopo aver avviato il tool con il comando “msfconsole” andiamo a ricercare il servizio che vogliamo “ackerare” tramite il comando “search telnet_version”.

```
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 auxiliary/scanner/telnet/telnet_version`

```
msf6 > use 1
```

```
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.

Utilizzo di Metasploit

- Dopo aver visto tramite il comando “show options” quali sono le impostazioni necessarie le vado ad implementare.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOST 192.168.1.40
```

RHOST ⇒ 192.168.1.40

```
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	192.168.1.40	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) > exploit
```

```
[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
) | _ _ _ _ _ \x0a| ' _ _ _ _ _ / _ _ _ _ _ / _ _ _ _ _ / _ _ _ _ _ \x0a| | | | | _ / || (_\ _ _ _ _ ) | | | | | (-
|| (_ | | |_) | | _// _/ \x0a| | | | | \_ \_ \_ , _ _ _ . _/ | | | _/ | _ \_ \_ , _ . _/ | | | _ _ _ | \x0a
                                     \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfad
min/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Utilizzo di Metasploit

- Come si è visto dalla figura precedente possiamo dire che il nostro attacco è andato a buon fine. Siamo riusciti ad ottenere user-Id e password.

Grazie