
EXPLOIT TELNET

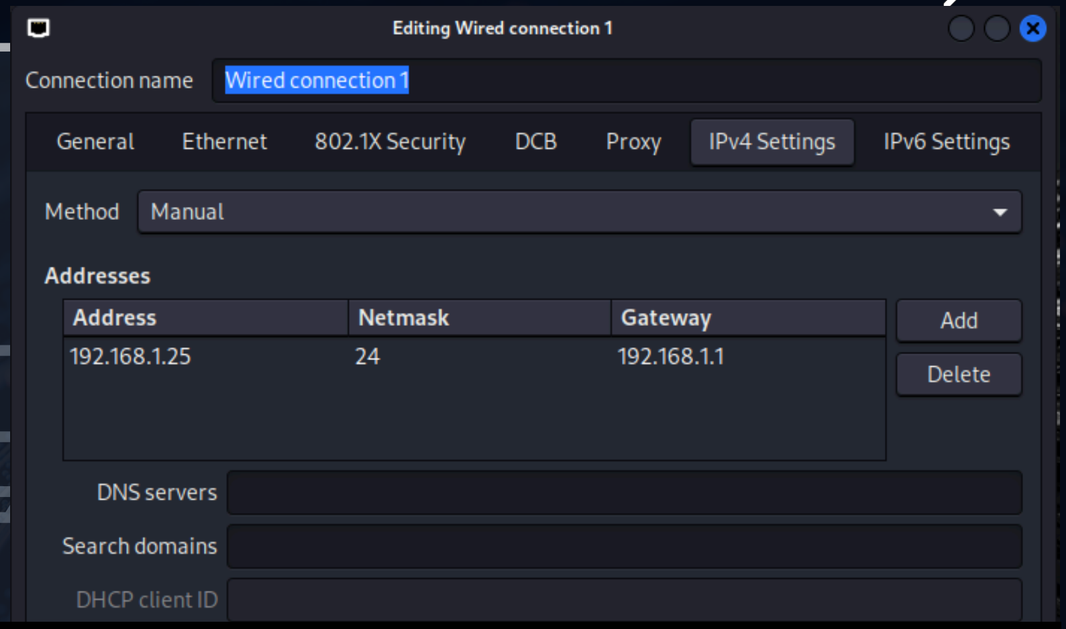
OBIETTIVO

Sulla base dell’esercizio visto in lezione teorica, utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il modulo auxiliary telnet_version sulla macchina Metasploitable.

Requisito:
Seguire gli step visti in lezione teorica. Prima, configurate l’ip della vostra Kali con 192.168.1.25 e l’ip della vostra Metasploitable con 192.168.1.40

IP SETTING

Impostiamo gli IP richiesti, settandoli all'interno delle due macchine.
Kali, da GUI andiamo a compilare l'IPV4 scelto.
Metasploitable, da CLI attraverso il comando
nano /etc/network/interfaces
compiliamo qui l'IPV4 di cui abbiamo bisogno.




```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

auto eth0
iface eth0 inet static
address 192.168.1.40
network 192.168.1.0
netmask 255.255.255.0
gateway 192.168.1.1
```

NMAP

Da Kali, mediante nmap scannerizziamo l'IP bersaglio e analizziamo i servizi attivi.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.40
PING 192.168.1.40 (192.168.1.40) 56(84) bytes of data.
64 bytes from 192.168.1.40: icmp_seq=1 ttl=64 time=1.21 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.774 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.578 ms
^C
── 192.168.1.40 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 0.578/0.855/1.214/0.265 ms

┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 13:57 CET
Nmap scan report for 192.168.1.40
Host is up (0.0024s 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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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 11.41 seconds
```

```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

                                                [ Wrote 15 lines

root@metasploitable:/home/msfadmin# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9
          inet addr:192.168.1.40  Bcast:192.168.
          inet6 addr: fe80::a00:27ff:fe9b:64f6/6
          UP BROADCAST RUNNING MULTICAST  MTU:15
          RX packets:20 errors:0 dropped:0 overr
          TX packets:49 errors:0 dropped:0 overr
          collisions:0 txqueuelen:1000
          RX bytes:1613 (1.5 KB)  TX bytes:4352
          Base address:0xd020 Memory:f0200000-f0

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
          RX packets:108 errors:0 dropped:0 over
          TX packets:108 errors:0 dropped:0 over
          collisions:0 txqueuelen:0
          RX bytes:22641 (22.1 KB)  TX bytes:226

root@metasploitable:/home/msfadmin# _
```

EXPLOIT SETTING

Cerchiamo un exploit lavorante su telnet, nello specifico quell oselezionato ci mostrerà il service banner della macchina bersaglio. Settiamo l'IP di Metasploitable, ci assicuriamo mediante "show options" la corretta compilazione.

```
                                https://metasploit.com

       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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 auxiliary/scanner/telnet/telnet_version

msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 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-metasploi
   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
```

Metasploitable2 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
                                [ Wrote 15 lines ]

root@metasploitable:/home/msfadmin# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:9b:64:f6
          inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.2
          inet6 addr: fe80::a00:27ff:fe9b:64f6/64 Scope:Link
```

EXPLOIT

Avviamo l'exploit. Possiamo leggere il banner in cui troviamo scritte le credenziali di accesso.

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

[+] 192.168.1.40:23       - 192.168.1.40:23 TELNET _                     _          _ _
| | ___ (_) |_ __ _| |__ | | ___|___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \
_ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/
          |_|                                                  \x0a\x0a\x0aWarning: Never exp
t]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasp
[*] 192.168.1.40:23       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) >
```