

S7.L2 Telnet exploit

Traccia: 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

Fase 1: Configurazione laboratorio virtuale

```
(kali㉿kali)-[~]  
$ 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:feb8:31a2 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:b8:31:a2 txqueuelen 1000 (Ethernet)  
    RX packets 10973 bytes 7890898 (7.5 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 10117 bytes 1617222 (1.5 MiB)  
    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 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 6077 bytes 1582319 (1.5 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 6077 bytes 1582319 (1.5 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:65:34:13  
          inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe65:3413/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
          RX packets:2808 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:2441 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:371169 (362.4 KB) TX bytes:1930963 (1.8 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:5305 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:5305 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:2561839 (2.4 MB) TX bytes:2561839 (2.4 MB)
```

```
(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=7.38 ms
64 bytes from 192.168.1.40: icmp_seq=2 ttl=64 time=0.769 ms
64 bytes from 192.168.1.40: icmp_seq=3 ttl=64 time=0.746 ms
64 bytes from 192.168.1.40: icmp_seq=4 ttl=64 time=0.750 ms
64 bytes from 192.168.1.40: icmp_seq=5 ttl=64 time=0.733 ms
^C
— 192.168.1.40 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4068ms
rtt min/avg/max/mdev = 0.733/2.075/7.378/2.651 ms
```

Configurazione delle Interfacce di Rete

ho configurato le interfacce di rete delle macchine Kali Linux e Metasploitable per garantire che possano comunicare tra loro. Ecco i dettagli dei passaggi che ho seguito:

Verifica delle Configurazioni di Rete con ifconfig

Ho utilizzato il comando ifconfig su entrambe le macchine (Kali Linux e Metasploitable) per visualizzare le configurazioni di rete attuali.

- Kali Linux:
 - Interfaccia eth0 con indirizzo IP 192.168.1.25, netmask 255.255.255.0.
 - Interfaccia di loopback lo con indirizzo IP 127.0.0.1.
- Metasploitable:
 - Interfaccia eth0 con indirizzo IP 192.168.1.40, netmask 255.255.255.0.
 - Interfaccia di loopback lo con indirizzo IP 127.0.0.1.

Riavvio delle Interfacce di Rete

Dopo aver verificato le configurazioni di rete, ho riavviato le interfacce di rete per applicare eventuali modifiche e assicurarmi che le configurazioni siano attive. Questo è stato fatto con il comando:

sudo /etc/init.d/networking restart

Verifica della Connessione tra le Macchine

Test della Connessione con ping

Ho utilizzato il comando ping da Kali Linux per verificare la connessione con la macchina Metasploitable. Ecco il comando e il risultato:

ping 192.168.1.40

- Il comando ping ha inviato pacchetti ICMP alla macchina Metasploitable (192.168.1.40) e ha ricevuto risposte positive.
- Il risultato ha mostrato che i pacchetti sono stati trasmessi con successo, confermando che le due macchine sono in grado di comunicare tra loro sulla rete configurata.

Fase 2. Scansione e Avvio di Metasploit

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.40
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 10:52 EDT
Nmap scan report for 192.168.1.40
Host is up (0.00083s latency).
Not shown: 979 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)
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
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 65.67 seconds
```

```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt

IIIIII dTb.dTb
II      4' v 'B
II      6. .P
II      'T;. ;P'
II      'T; ;P'
IIIIII 'YvP'

I love shells --egypt

      =[ metasploit v6.3.55-dev ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

Scansione della Rete con Nmap

ho eseguito una scansione della rete utilizzando nmap per identificare i servizi attivi sulla macchina Metasploitable. Questo passaggio è essenziale per raccogliere informazioni sul target prima di tentare qualsiasi exploit.

Esecuzione della Scansione

Ho utilizzato il comando nmap con le opzioni -sV per identificare le versioni dei servizi attivi sulla macchina con l'indirizzo IP 192.168.1.40:

```
nmap -sV 192.168.1.40
```

Risultati della Scansione

Il risultato della scansione nmap ha mostrato una lista di porte aperte e i servizi corrispondenti, insieme alle versioni dei software in esecuzione. Ecco alcuni dei servizi identificati:

- Porta 21 (FTP): ProFTPD 1.3.1
- Porta 22 (SSH): OpenSSH 4.7p1 Debian
- Porta 23 (Telnet): Servizio Telnet attivo
- Porta 80 (HTTP): Apache httpd 2.2.8
- Porta 139 e 445 (SMB): Samba smbd 3.X
- Porta 3306 (MySQL): MySQL 5.0.51a
- Porta 5432 (PostgreSQL): PostgreSQL DB 8.3.0

Questi risultati indicano che il servizio Telnet è attivo sulla porta 23, il che è cruciale per l'esecuzione dell'exploit pianificato.

Avvio di Metasploit

Dopo aver completato la scansione della rete, ho avviato Metasploit.

Esecuzione di Metasploit

Ho avviato Metasploit utilizzando il comando msfconsole:

```
msfconsole
```

Interfaccia di Metasploit

Al lancio di Metasploit, ho visualizzato la schermata iniziale con il logo ASCII e informazioni sulla versione di Metasploit in uso, che in questo caso è la v6.3.55-dev.

L'interfaccia di Metasploit (msfconsole) fornisce accesso a vari moduli come Exploit

Fase 3: Ricerca e Configurazione del Modulo Telnet

```
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 B
anner Detection

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet
_version

msf6 > |
```

```
msf6 > use 1
msf6 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 <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                                                                                                                                                                     |



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

Ricerca del Modulo Telnet

ho utilizzato Metasploit per cercare un modulo specifico che mi permettesse di interagire con il servizio Telnet sulla macchina Metasploitable.

Comando di Ricerca

Ho utilizzato il comando search per trovare i moduli disponibili per Telnet:

```
search telnet_version
```

Risultati della Ricerca

Il risultato della ricerca ha mostrato diversi moduli disponibili. Tra questi, ho scelto il modulo auxiliary/scanner/telnet/telnet_version che è progettato per rilevare le versioni dei servizi Telnet.

-Utilizzo del Modulo Telnet

-Selezione del Modulo

Ho selezionato il modulo desiderato utilizzando il comando use:

```
use auxiliary/scanner/telnet/telnet_version
```

Questo comando ha caricato il modulo selezionato, pronto per essere configurato e utilizzato.

Visualizzazione delle Opzioni del Modulo

Per vedere quali parametri erano necessari per eseguire il modulo, ho utilizzato il comando show options:

Configurazione delle Opzioni del Modulo

Il comando show options ha visualizzato i parametri che devono essere configurati prima di eseguire il modulo. I parametri richiesti includono:

- PASSWORD: La password per il login (non obbligatorio per questo modulo specifico)
- RHOSTS: L'indirizzo IP del target, necessario per eseguire la scansione (in questo caso, 192.168.1.40)
- RPORT: La porta su cui il servizio Telnet è in ascolto (di default, 23)
- THREADS: Il numero di thread concorrenti da utilizzare per la scansione
- TIMEOUT: Il tempo di attesa per una risposta dal servizio Telnet
- USERNAME: Il nome utente per il login (non obbligatorio per questo modulo specifico)

Fase 4: Configurazione Dettagliata del Modulo Telnet

```
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 <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                                                                                                                                                                     |



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

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

ho proseguito con la configurazione dettagliata del modulo auxiliary/scanner/telnet/telnet versione in Metasploit per assicurarmi che tutti i parametri necessari siano correttamente impostati prima di eseguire l'exploit.

Conferma del Target

Ho impostato l'indirizzo IP del target (RHOSTS) utilizzando il comando:

```
set RHOSTS 192.168.1.40
```

Questo comando specifica che la scansione sarà diretta verso la macchina Metasploitable con l'indirizzo IP 192.168.1.40.

Visualizzazione delle Opzioni del Modulo

Comando di Visualizzazione

Ho utilizzato di nuovo il comando `show options` per verificare che tutti i parametri necessari siano correttamente configurati:

show options

Parametri del Modulo

Il comando ha visualizzato i parametri configurabili del modulo auxiliary/scanner/telnet/telnet version, specificando quello di nostro interesse (RHOSTS)

- **RHOSTS:** (yes) 192.168.1.40, l'indirizzo IP del target.

Fase 5: Esecuzione dell'Exploit

[illegible]

Esecuzione del Modulo Telnet

ho eseguito il modulo auxiliary/scanner/telnet/telnet versione di Metasploit per rilevare la versione del servizio Telnet sulla macchina Metasploitable. Questo è il passaggio finale per completare la scansione e raccogliere le informazioni necessarie.

Comando di Esecuzione

Ho eseguito il comando exploit per avviare la scansione:

exploit

Risultato dell'Esecuzione

Il risultato dell'esecuzione ha mostrato i seguenti dettagli:

- L'indirizzo IP del target 192.168.1.40 sulla porta 23 (Telnet).
- Conferma che il modulo ha scansionato con successo 1 host (192.168.1.40) e ha completato al 100%.
- Visualizzazione del banner del servizio Telnet, che contiene informazioni utili come avvisi e credenziali di accesso (nel caso specifico, l'accesso è con msfadmin).

Analisi dei Risultati

- Individuazione del Servizio Telnet: Il modulo ha confermato che il servizio Telnet è attivo sulla macchina target e ha rilevato la versione del servizio.
- Banner del Servizio: Il banner recuperato ha fornito informazioni aggiuntive, come il suggerimento di contattare msfdev e le credenziali di default msfadmin/msfadmin per il login. Questo è importante perché può confermare la vulnerabilità e la presenza di configurazioni di default che possono essere sfruttate.

Fase Finale: Accesso alla Macchina Metasploitable

```
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 '^]'.

msf6 (root@kali:~) ssh -p 22 root@192.168.1.40
Warning: Never expose this VM to an untrusted network!
msf6 (root@kali:~) ssh -p 22 root@192.168.1.40
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Mon May 20 14:41:19 EDT 2024 on pts/1
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/
You have new mail.
msfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:65:34:13
      inet addr:192.168.1.40 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe65:3413/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:5882 errors:0 dropped:0 overruns:0 frame:0
      TX packets:5375 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:616793 (602.3 KB) TX bytes:2170744 (2.0 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:5606 errors:0 dropped:0 overruns:0 frame:0
```

Connessione Telnet

Nella fase finale, ho utilizzato le informazioni raccolte nelle fasi precedenti per connettermi alla macchina Metasploitable tramite Telnet, sfruttando le credenziali ottenute.

Comando di Connessione

Ho utilizzato il comando Telnet per connettersi alla macchina Metasploitable:

```
telnet 192.168.1.40
```


Stabilire la Connessione

Il comando Telnet ha tentato di connettersi all'indirizzo IP 192.168.1.40 sulla porta 23 (Telnet). La connessione è stata stabilita con successo, e mi è stato richiesto di inserire le credenziali di accesso.

Accesso con Credenziali

Credenziali Utilizzate

Ho utilizzato le credenziali di default msfadmin per effettuare il login:

- Username: msfadmin
- Password: msfadmin

Login Riuscito

Il login è stato effettuato con successo, confermando che le credenziali ottenute erano corrette. Una volta autenticato, ho avuto accesso alla shell della macchina Metasploitable.

Verifica della Connessione

Esecuzione di Comandi di Verifica

Dopo aver effettuato il login, ho eseguito alcuni comandi per verificare la connessione e raccogliere informazioni sul sistema. Ad esempio:

ifconfig

Output dei Comandi

L'output del comando ifconfig ha mostrato le configurazioni di rete della macchina Metasploitable, confermando la connessione e l'accesso alla shell.

Obiettivi Raggiunti

Nella fase finale, ho completato i seguenti obiettivi:

- Connessione al Servizio Telnet: Ho utilizzato Telnet per connettersi alla macchina Metasploitable.
- Autenticazione: Ho utilizzato le credenziali msfadmin per effettuare il login con successo.
- Accesso alla Shell: Ho ottenuto l'accesso alla shell della macchina target, confermando che l'exploit è stato eseguito correttamente.
- Verifica delle Configurazioni di Rete: Ho utilizzato comandi di sistema per verificare le configurazioni di rete e confermare la mia presenza nella shell del sistema target.

Conclusione

Questa fase finale ha dimostrato il successo dell'attacco, permettendomi di accedere alla macchina Metasploitable tramite Telnet utilizzando le credenziali di default. Ho confermato l'accesso eseguendo comandi di verifica, completando così l'intera esercitazione con successo.