

Esercizio S7-L2

Un exploit è un codice malevolo che agisce su una vulnerabilità già presente nel sistema, che essa sia nota o non nota.

L'obiettivo di oggi era sfruttare una vulnerabilità del protocollo telnet. Con la corretta esecuzione potremmo prendere il controllo della macchina vittima.

Dopo aver confermato la corretta connessione usando il ping, ho eseguito una scansione nmap per assicurarmi che la porta telnet fosse la 23 e che versione ci fosse.

L'ip corretto è 192.168.1.40, questo screen è frutto di un test precedente).

```
(gimp@kali)-[~]
$ nmap -sV 192.168.1.20
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 17:57 CET
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service S
Service scan Timing: About 90.91% done; ETC: 17:58 (0:00:02 remaining)
Stats: 0:01:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Sc
NSE Timing: About 97.92% done; ETC: 17:58 (0:00:00 remaining)
Nmap scan report for 192.168.1.20
Host is up (0.0025s 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
```

Poi ho aperto msfconsole:

```
-search auxiliary telnet_version
```

```
-use      ""
```

```
-show options
```

```
-set rhosts 192.168.1.40
```

-run

```
msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.40
rhosts => 192.168.1.40
msf6 auxiliary(scanner/telnet/telnet_version) > run

[+] 192.168.1.40:23 - 192.168.1.40:23 TELNET
- . _ _ _ _ _ \x0a      | | _ _ _ _ _ | | _ _ _ _ _ | | _ _ _ _ _ \x0a|
_ / _ _ _ _ _ \x0a    / _ _ _ _ _ \x0a  / _ _ _ _ _ \x0a  / _ _ _ _ _ \x0a|
( | _ _ _ _ _ ) | | ( | | ( | | ) | | _ // _ / \x0a| | | | \x0a , _ _ _ _ _ / _ / | |
\x0a / _ _ _ _ _ \x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aCon
tact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0ame
tasptailable login:
[*] 192.168.1.40:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > ifconfig
```

È possibile vedere che vengono fornite le credenziali di accesso a metasploitable.

Avviando il protocollo telnet 192.168.1.40 connettendolo all'ip vittima si potrà agire sul sistema vittima da remoto.

[illegible]