



EPICODE

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)-[~]
$ sudo 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)
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: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(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-the-framework/setting-rhosts.html
RPORT	23	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max on some targets)
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 192.168.1.149
```

```
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.

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

```
[+] 192.168.1.149:23 - 192.168.1.149:23 TELNET  
_ / _ | ' _ \ | / _ \ | _ / _ | ' _ \ | / _ \ | _ / _ | ' _ \ | / _ \ |  
a      |_|  
       \x0a\x0a\x0aWarning: Never expose this VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/m  
sfadmin to get started\x0a\x0a\x0ametasploitable login:  
[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed
```

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.

Grazie per l'attenzione.

