W16D4 Pratica

Giacomo di Giacinto

EPICODE

Esercizio
Traccia e requisiti

Traccia:

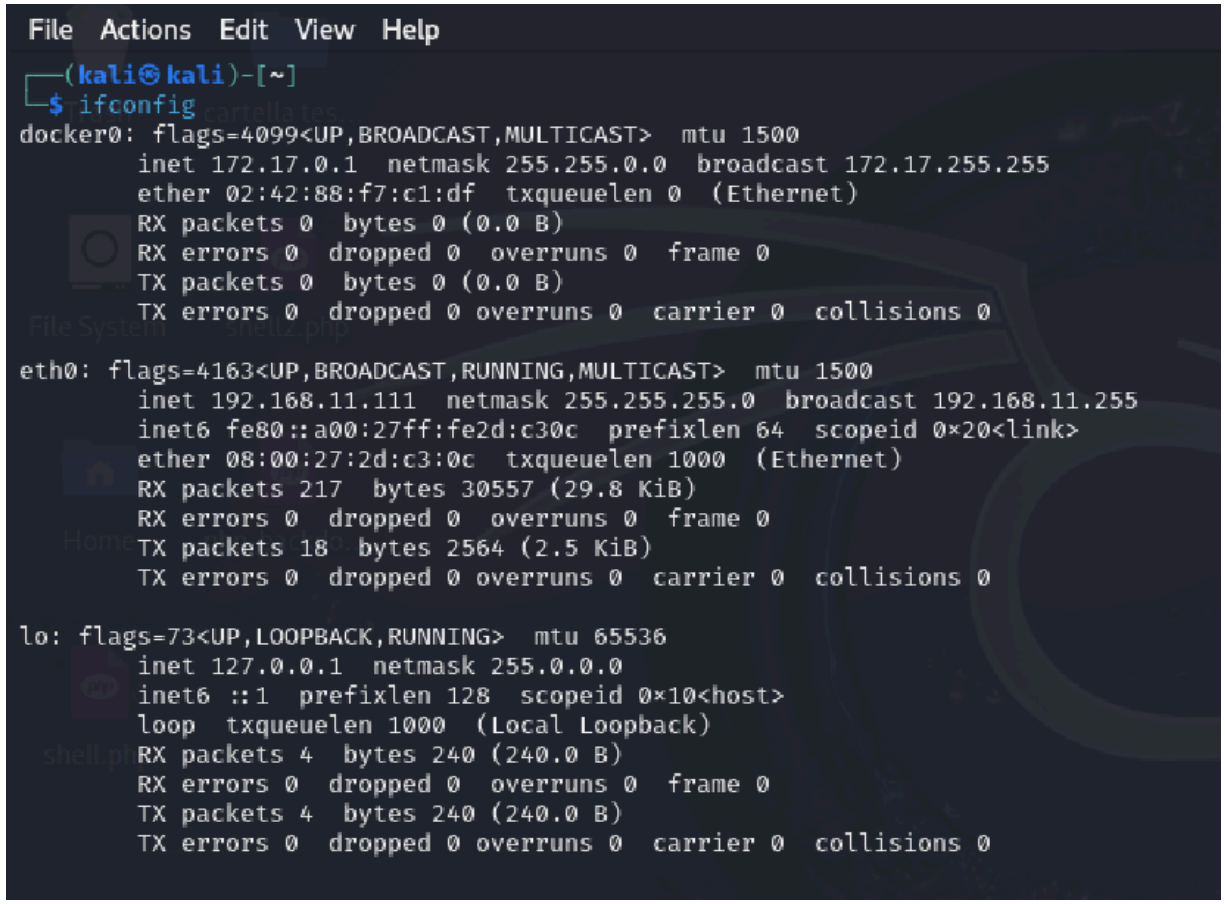
La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente, ripercorrendo gli step visti nelle lezioni teoriche, di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

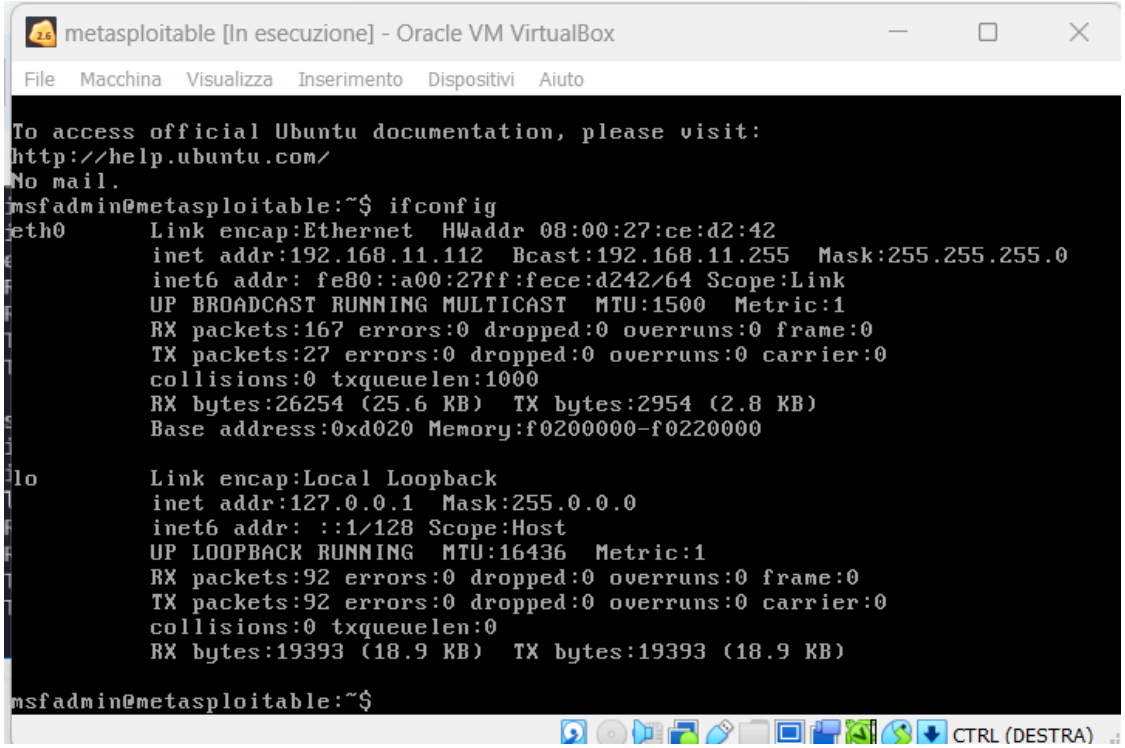
I requisiti dell'esercizio sono:

- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: **192.168.11.111**
- La macchina vittima (Metasploitable) deve avere il 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 3) altro...

Soluzione

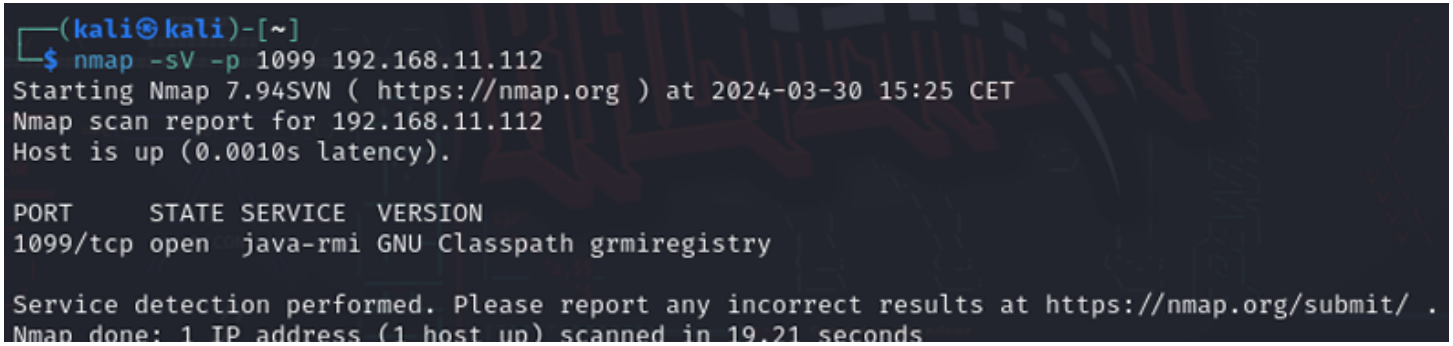
1. Imposto gli IP delle macchine come da esercizio



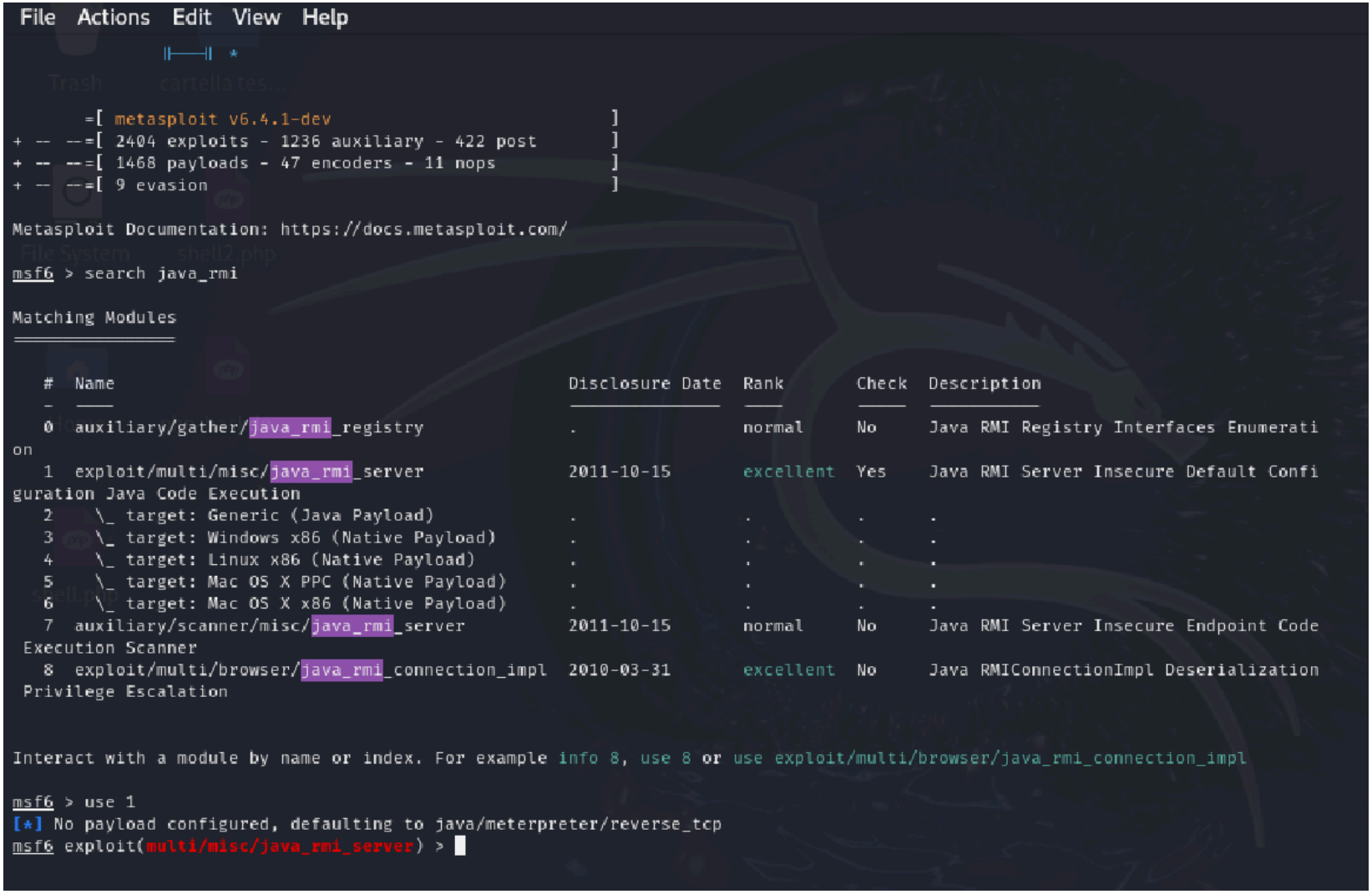

metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 08:00:27:ce:d2:42
inet addr:192.168.11.112 Bcast:192.168.11.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fece:d242/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:167 errors:0 dropped:0 overruns:0 frame:0
TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:26254 (25.6 KB) TX bytes:2954 (2.8 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:92 errors:0 dropped:0 overruns:0 frame:0
TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)
msfadmin@metasploitable:~$
CTRL (DESTRA)

2. Verifica della porta

con il comando Nmap verifico che la porta oggetto dell’attacco sia aperta e verifico che il servizio collegato sia Java RMI

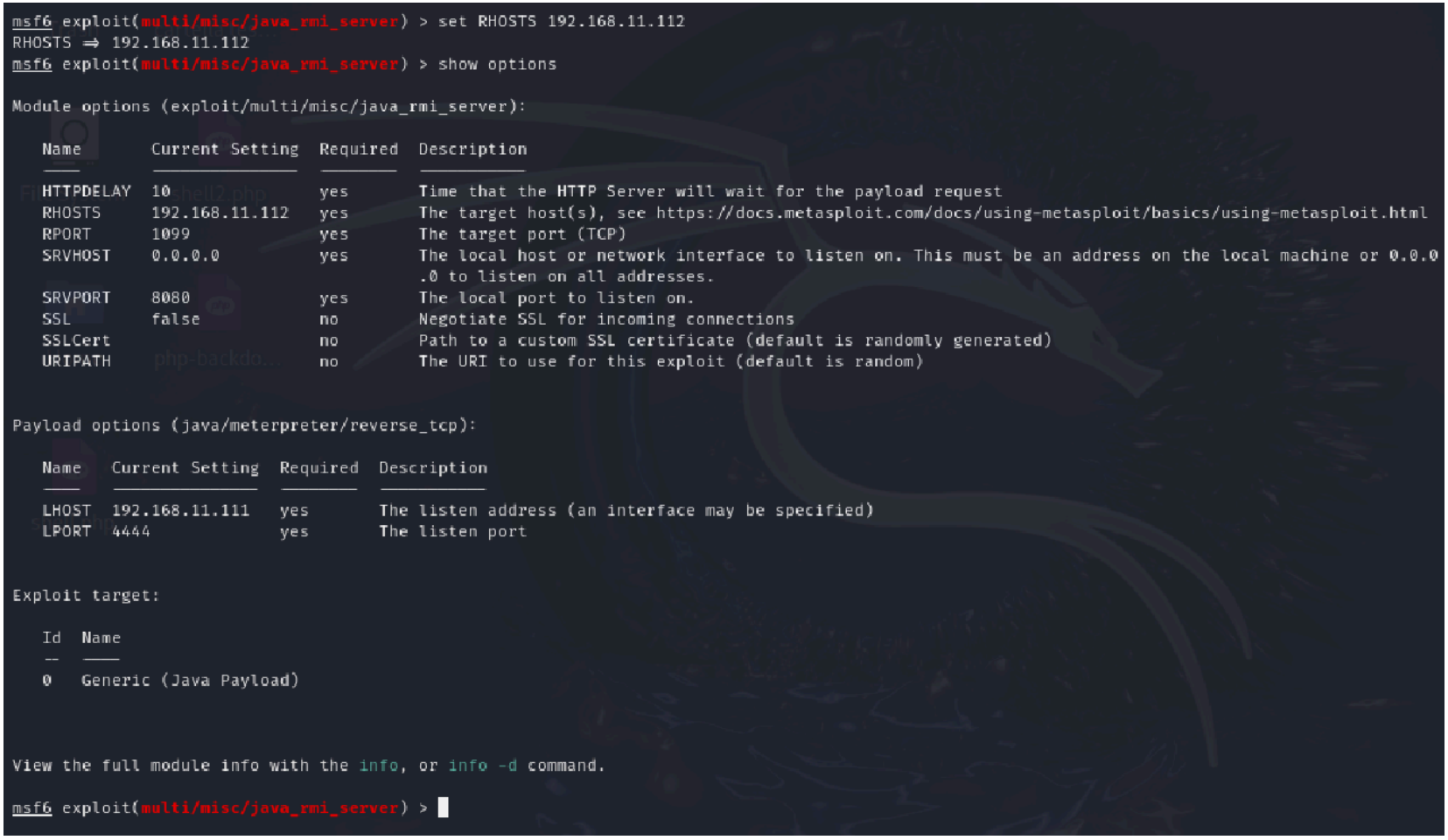


3. Apro Msfconsole e scelgo l'exploit



4. configuro l’exploit

Configuro il parametro RHOST con l’indirizzo IP del ricevente (metasploitable – 192.168.11.111)
Configuro il parametro LHOST con l’indirizzo IP dell’attaccante (kali – 192.168.11.112)



5. Faccio partire l’exploit e verifico di essere dentro la macchina target con il comando ifconfig