PROGETTO S7/L5

CYBER SECURITY & ETHICAL HACKING

Yuliya Suvorova, 20/12/2024

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.

## ESECUZIONE ESERCIZIO

Innanzitutto, si devono configurare gli indirizzi ip delle macchine, come da figura 1 (KALI) e 2 (Metasploitable).

Figura 1

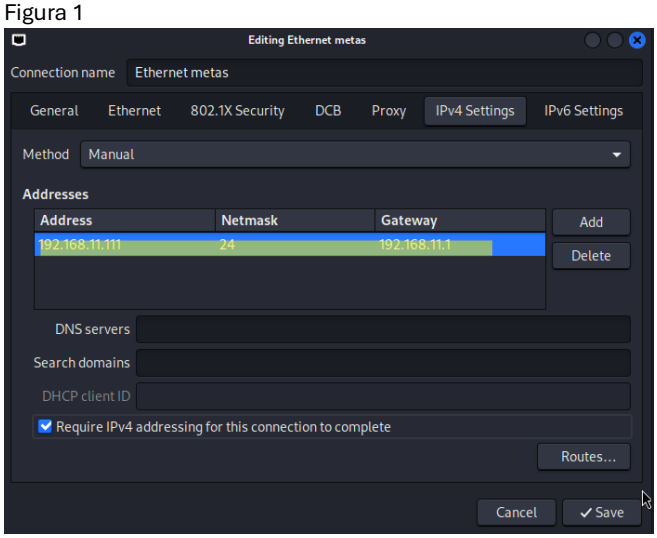
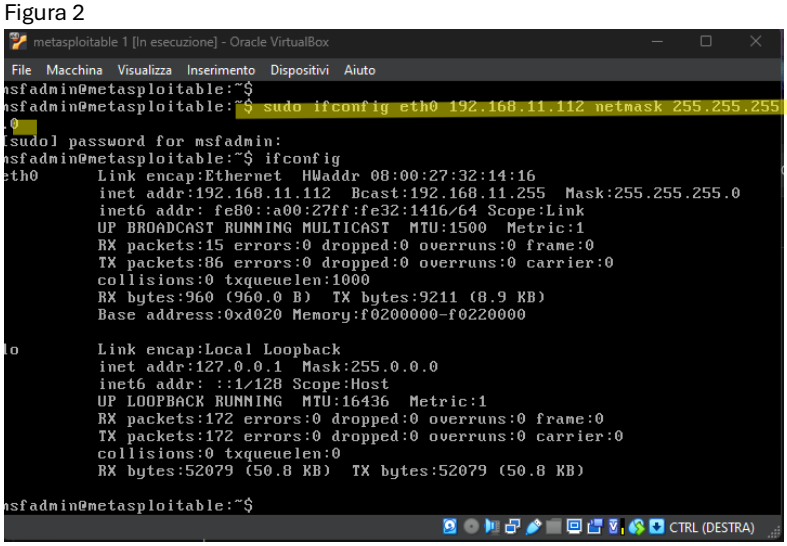



Figura 2



È sempre preferibile testare la comunicazione tra le due macchine tramite il comando **ping**, come in figura 3 e 4.

Figura 3- ping da KALI e Metasploitable.

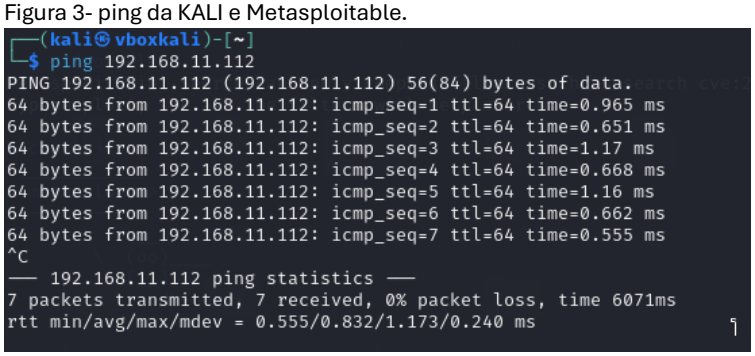
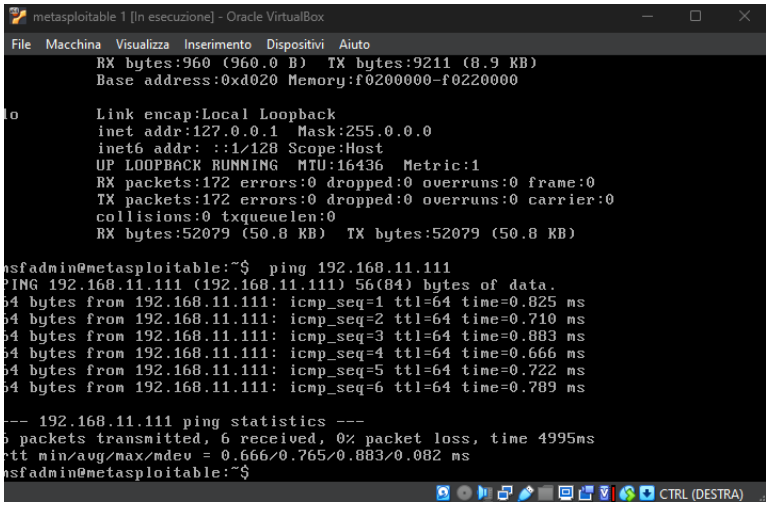


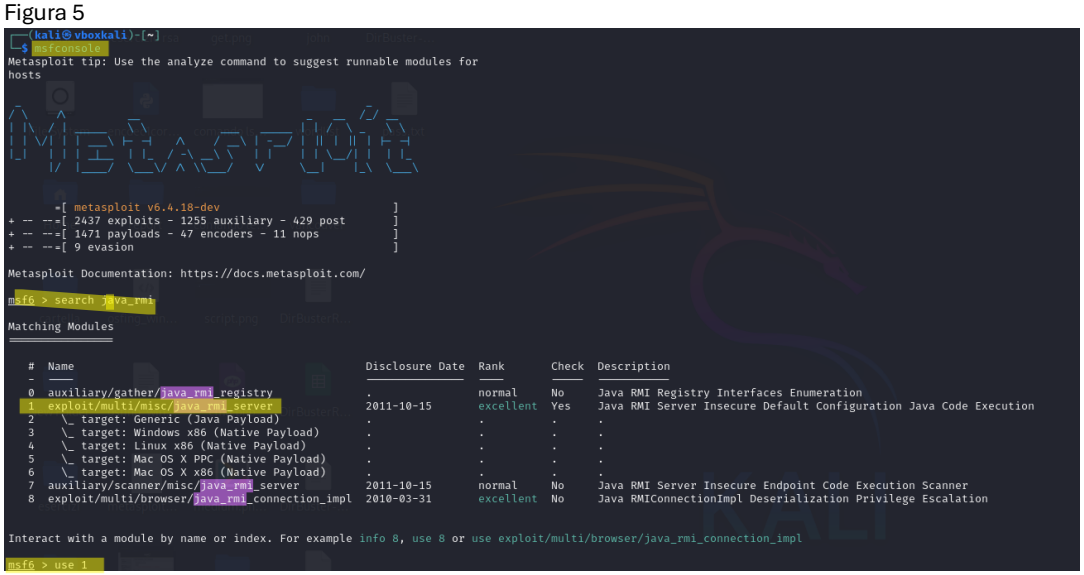

Figura 4- ping da Metasploitable a KALI.




**La comunicazione tra le macchine dunque ha avuto successo.**

A questo punto si deve deve avviare il servizio Metasploit da terminale tramite il comando **msfconsole** e cercare l'exploit java_rmi tramite il comando **search java_rmi** e scegliere l'exploit da utilizzare (come in figura 5).

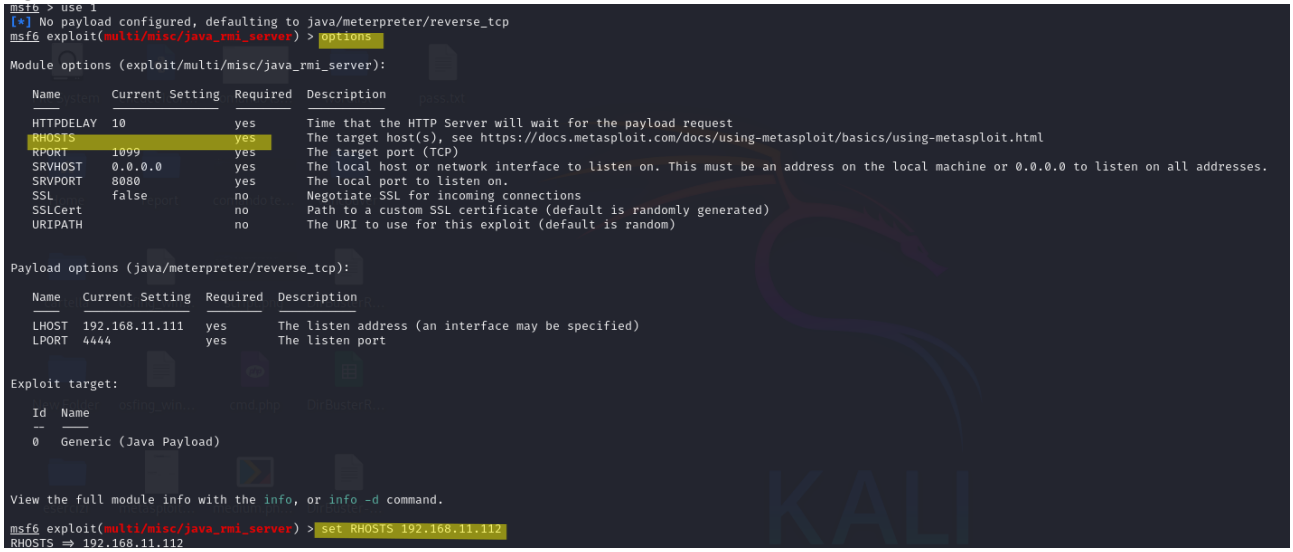
Figura 5



Per l'esercizio è stato scelto l'exploit 1 "exploit/multi/misc/java/rmi_server" poiché ciò che interessa è attaccare un servizio RMI (Remote Method Invocation) vulnerabile esposto su un server e l'exploit sfrutta l'esposizione di questo registro per eseguire un codice arbitrario.

Innanzitutto, si devono configurare i parametri richiesti, visibili tramite il comando "**options**" o "**show options**", nello specifico il parametro RHOSTS, tramite in comando **set** (come in figura 6). In questo caso RHOSTS è 192.168.11.112, indirizzo ip della metasploitable.

Figura 6




Dopo di che si deve lanciare il comando **run** per eseguire l'exploit ed entrare automaticamente in Meterpreter (shell avanzata che permette, tra le altre cose, il controllo remoto della macchina) per poi lanciare i comandi **ifconfig**, per sapere la configurazione di rete della macchina target, e **route**, per ottenere informazioni circa la tabella di routing della macchina, come richiesto dalla traccia (figura 7).

Figura 7