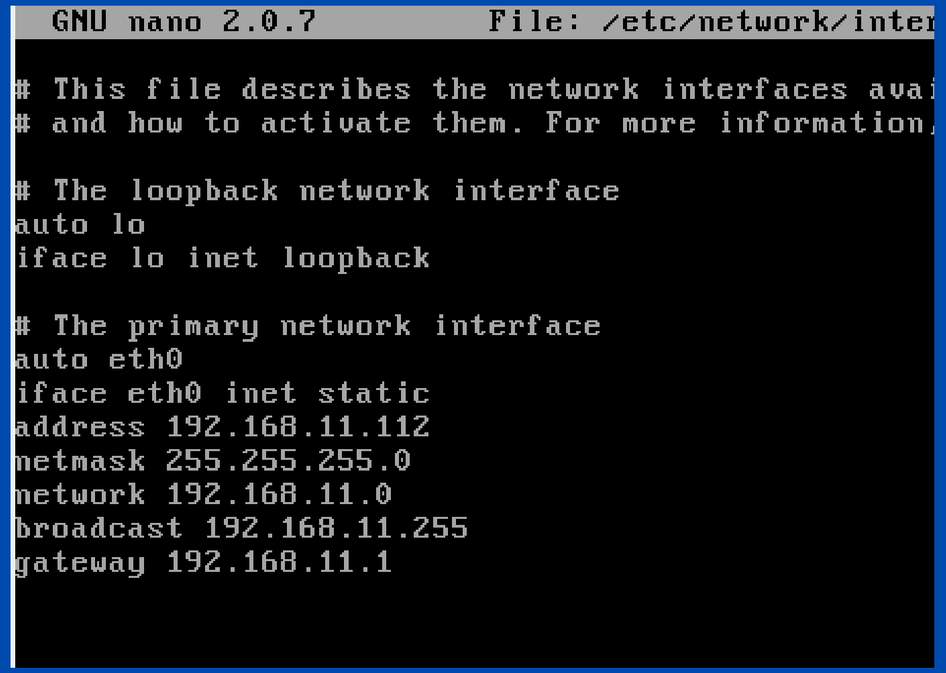
METASPLOIT

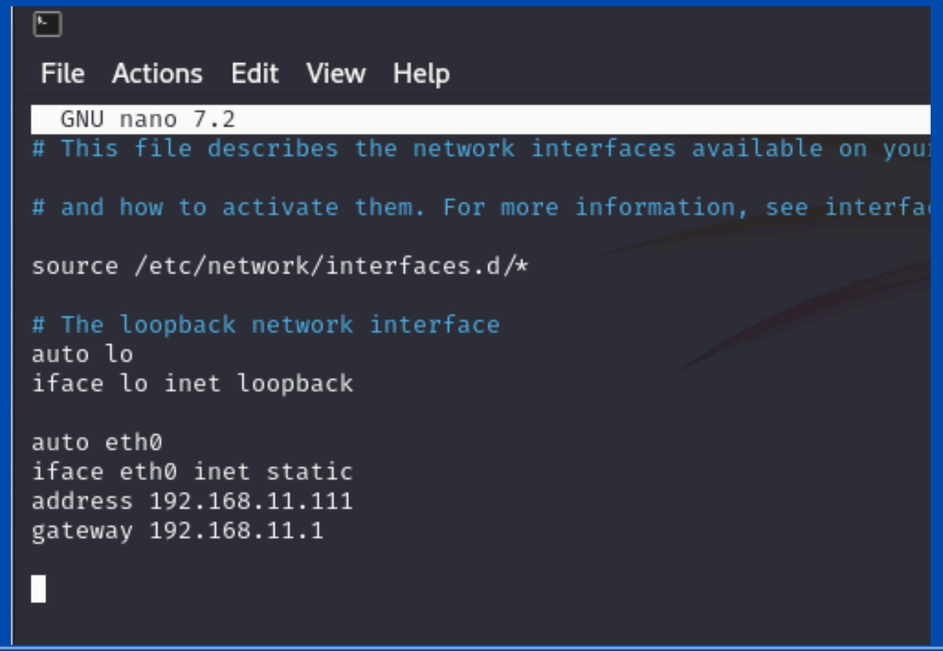
Metasploit è un framework di sicurezza informatica utilizzato per il penetration testing e lo sviluppo di **exploit**. Grazie ai **moduli** e ai **payload** è possibile fare pentesting in maniera più semplice ed automatizzata. Mette a disposizione una libreria con una vasta gamma di exploit ed è spesso utilizzato per testare la robustezza dei sistemi, la velocizzazione del lavoro e la ricerca e lo sviluppo di nuovi exploit. In questo caso lo utilizzeremo per sfruttare una vulnerabilità presente sulla macchina **Metasploitable** sulla porta 1099, **Java RMI** per ottenere una sessione di **Meterpreter** sulla macchina remota. Meterpreter è una shell che ci permette di **interagire direttamente sul sistema target**.

Setup Ambiente

Abbiamo utilizzato **Metasploit** sulla nostra macchina Kali Linux per eseguire un attacco contro Metasploitable, la nostra macchina target. **Entrambe le macchine sono collocate sulla stessa rete interna, con gli indirizzi IP 192.168.11.111 per Kali e 192.168.11.112 per Metasploitable.**

Per garantire la connettività e la configurazione di rete corrette, è stato sufficiente eseguire il comando **sudo nano /etc/network/interfaces** su entrambe le macchine, permettendo la modifica delle configurazioni di rete direttamente dai file di interfaccia di rete.

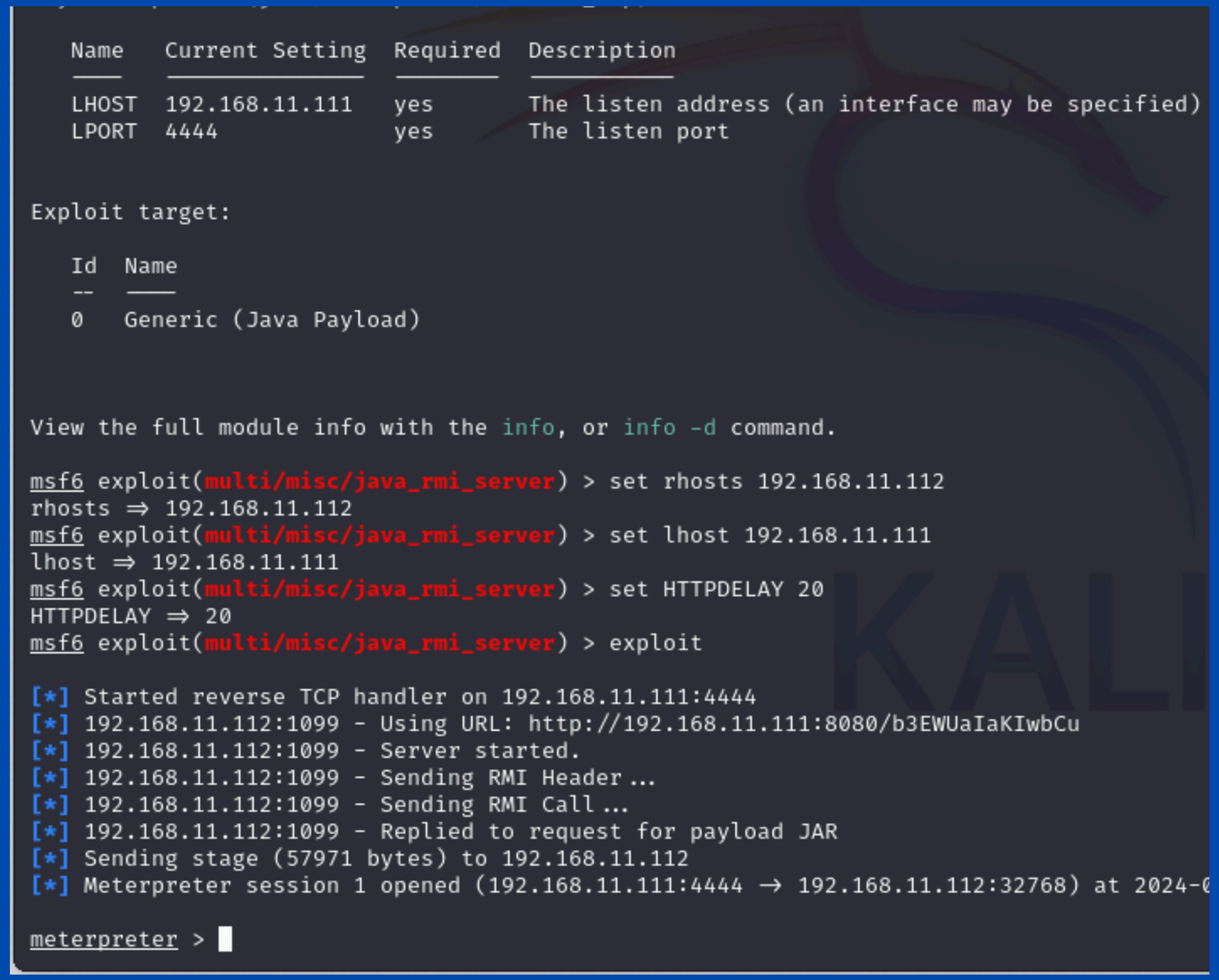




MSFCONSOLE

Questa è la schermata di lancio di metasploit, ottenuta con il comando **‘mfsconsole’.**

Ad ogni avvio ci darà un messaggio di benvenuto diverso! Ci sono diversi comandi utili come ad esempio **“search”** per cercare gli exploit, payload e moduli di ausilio; **“use”** per caricare un modulo specifico per l’uso, **“info”** per dettagli completi sui moduli, etc. Nello screen è visibile l’utilizzo del comando ‘’search’’ per andare a cercare la vulnerabilità di nostro interesse JAVA RMI, che ci permetterà di proseguire con l’exploit.



Con il comando **"show options"** possiamo andare a controllare quali sono i parametri modificabili, come l'**host remoto e l'host locale, le porte, l'HTTP delay ed altre impostazioni di configurazione.**

Noi andremo a configurare:

- **RHOST :** con l'indirizzo IP della macchina target
- **LHOST:** con l'indirizzo iP della macchina attaccante
- **HTTP DELAY:** per aumentare la quantità di tempo che il server deve attendere la richiesta del payload dato che un valore troppo basso (10 secondi) potrebbe causare una chiusura precoce della connessione. Per questo motivo setteremo l'HTTP DELAY a 20.

Dopo il successo dell'attacco e l'ottenimento dell'accesso remoto tramite Meterpreter sulla macchina Metasploitable, sono stati raccolti importanti dati di configurazione di rete e routing.

Meterpreter > ifconfig

Analizzando l'output di ifconfig, è stato possibile identificare le interfacce di rete attive sulla macchina, inclusi indirizzi IP, subnet mask e altre informazioni.

```
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 : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fefb:8737
IPv6 Netmask : ::
```

Meterpreter > route

Con il comando route, sono state rilevate le rotte di rete attive sulla macchina vittima. È stato identificato il gateway predefinito utilizzato per instradare il traffico di rete.

```
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  Interfa
    ------                    -------  -------  ------  ------
    ::1                       ::       ::
    fe80::a00:27ff:fefb:8737  ::       ::
```

CONCLUSIONI

Attraverso l'utilizzo di Metasploit e l'exploit della vulnerabilità Java RMI sulla porta 1099 della macchina Metasploitable, siamo riusciti ad **ottenere con successo una sessione Meterpreter sulla macchina remota.** Questo processo ci ha permesso di dimostrare la **gravità delle vulnerabilità** presenti nei servizi di rete e l'importanza di una rigorosa **valutazione della sicurezza.**

Esaminando le informazioni raccolte tramite Meterpreter, abbiamo acquisito una **visione dettagliata della configurazione di rete e delle rotte attive sulla macchina vittima.** Questi dati forniscono preziose informazioni utili per valutare la sicurezza del sistema e identificare potenziali **punti deboli che potrebbero essere sfruttati da attaccanti malevoli.**

Questo evidenzia l'importanza della consapevolezza sulla sicurezza informatica e sottolinea la necessità di adottare misure proattive per proteggere le reti e i sistemi da attacchi informatici.