Meterpreter – Metasploitable

Obiettivo: La nostra macchina Metasploitable presenta un servizio vulnerabile sulla porta 1099 – Java RMI. Si richiede allo studente di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota

Indice:

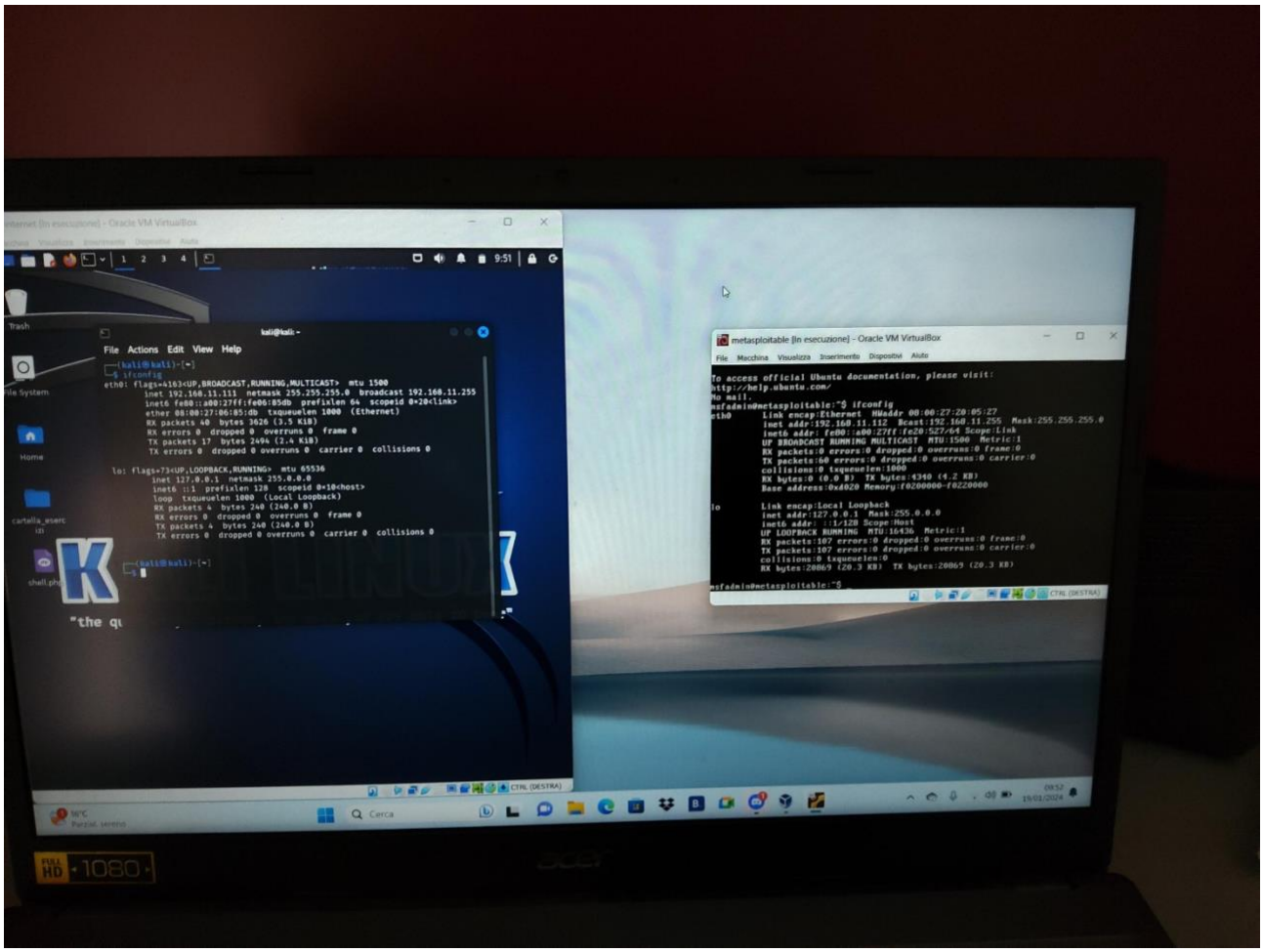
- Collegare le due macchine
- Scannerizzare Metasploitable per trovare la vulnerabilità
- Sfruttare la vulnerabilità per ottenere la configurazione di rete e le informazioni sulla tabella di routing della macchina della vittima

Svolgimento:

In questa prima task andremo a recuperare dati come la tabella di routing e la configurazione di rete utilizzando msfconsole per creare una sessione di meterpreter sulla,macchina target

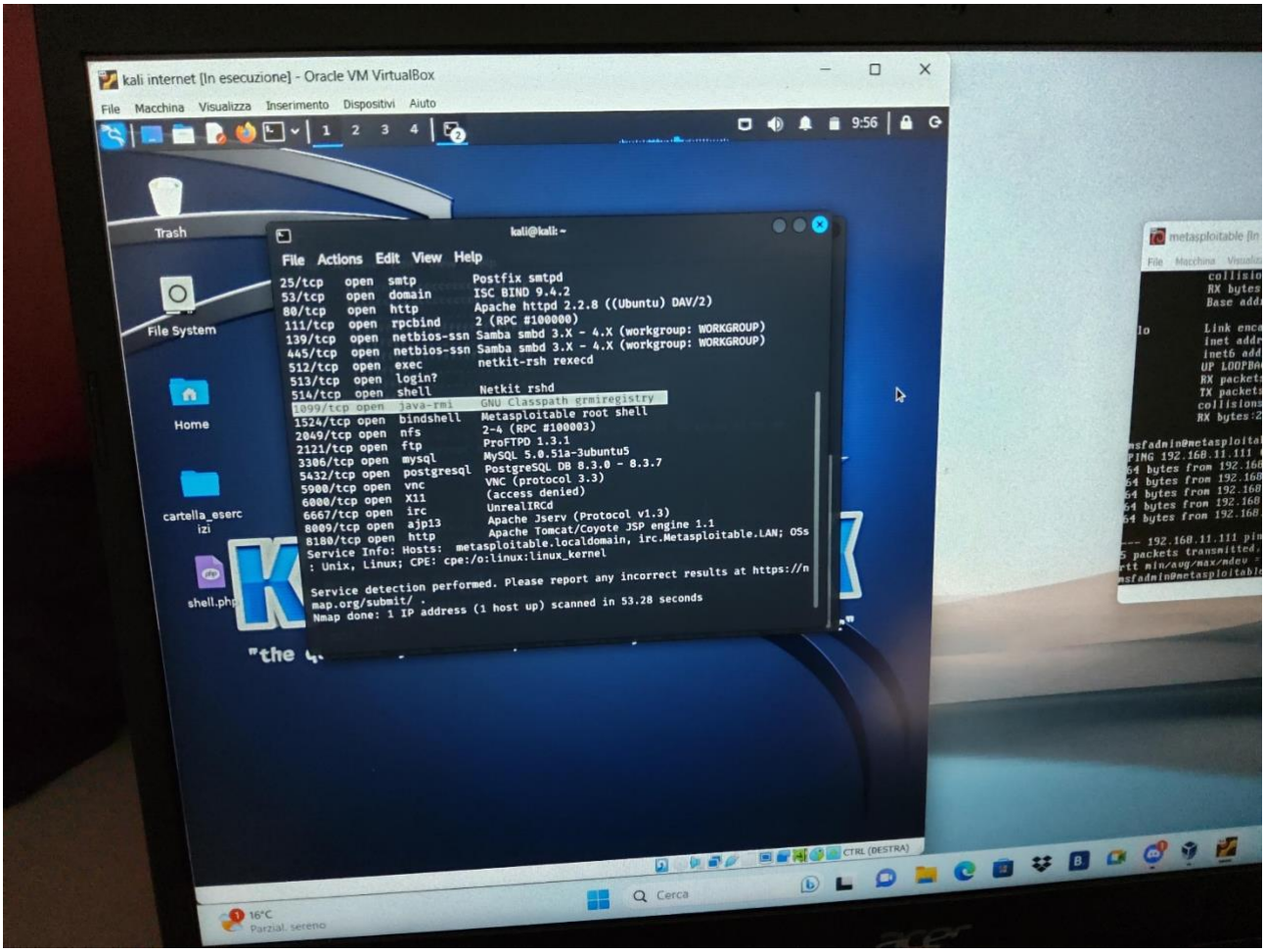
Collegare le due macchine

Collegare kali (la macchina attaccante) e metasploitable (la macchina target) utilizzando il comando ping e l'indirizzo IP sul terminale, si possono trovare gli indirizzi IP tramite il comando "ifconfig"



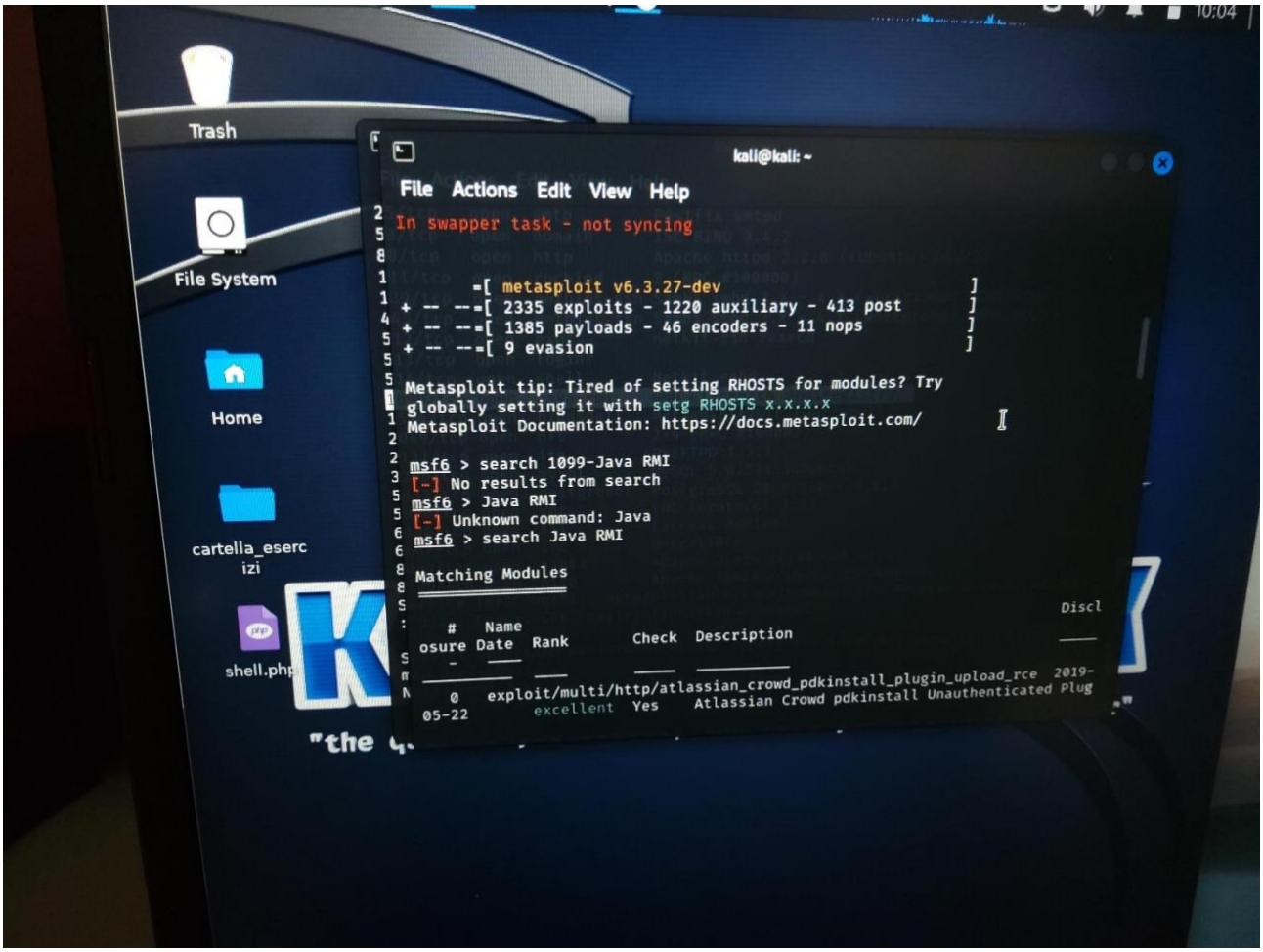
Scannerizzare metasploitable per trovare la vulnerabilità:

Scannerizzare metasploitable tramite il tool nmap per trovare una vulnerabilità all'interno del sistema tramite Il comando "nmap -sV indirizzo IP di metasploitable"



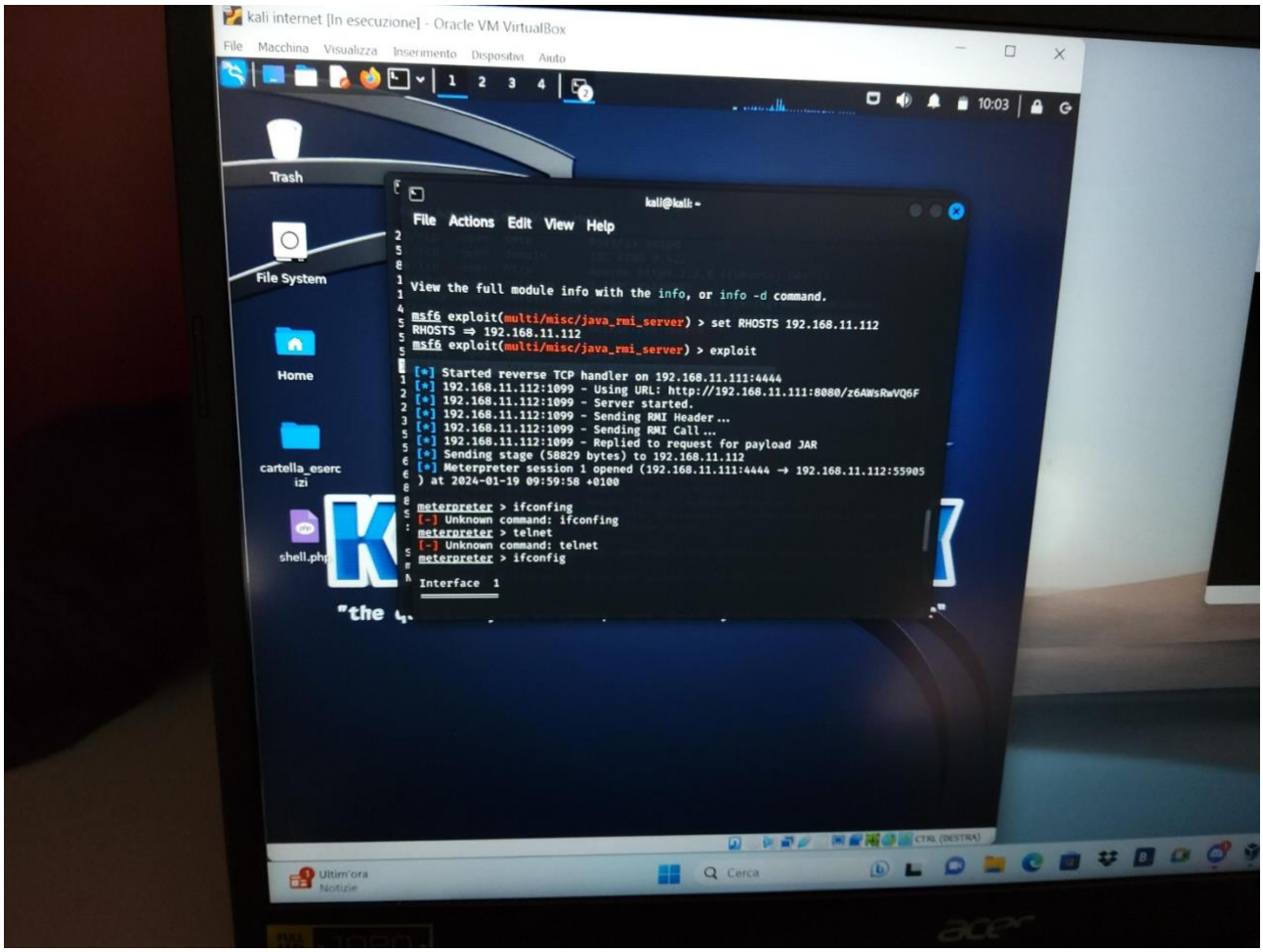
Sfruttare la vulnerabilità per ottenere la configurazione di rete e le informazioni sulla tabella di routing della macchina della vittima:

Aprire msfconsole, tool molto potente utile per cercare e sfruttare le vulnerabilità di un sistema, cercare la vulnerabilità trovata con nmap tramite la funzione “search”



Una volta trovata, utilizzare il comando “use con la vulnerabilità cercata” e impostare tra l’indirizzo IP

Della macchina target (metasploitable) tramite il comando “set hosts con l’indirizzo IP” seguito dal comando “exploit” per attaccare la macchina target



Una volta creata la sessione di meterpreter è possibile recuperare la configurazione di rete tramite il comando “ifconfig” e le informazioni sulla tabella di routing tramite il comando “route”