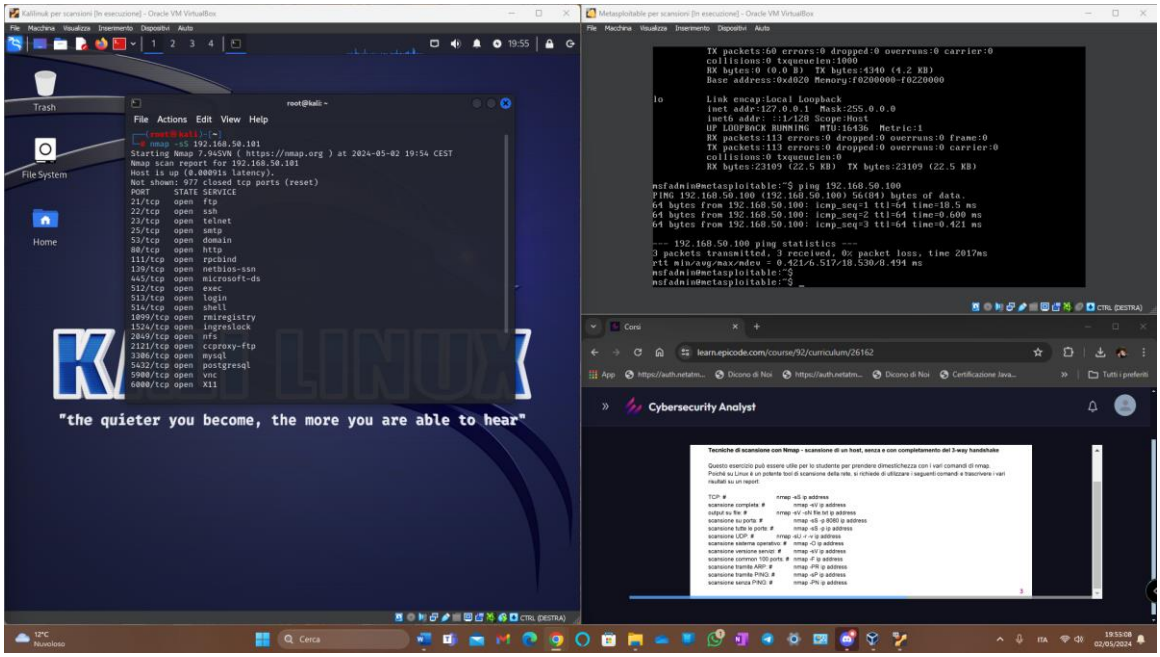
Network Scan Risultati

TCP SYN Scan

Comando: nmap -sS 192.168.50.101

Descrizione: Scansione TCP SYN senza completare il 3-way handshake.

Risultati:

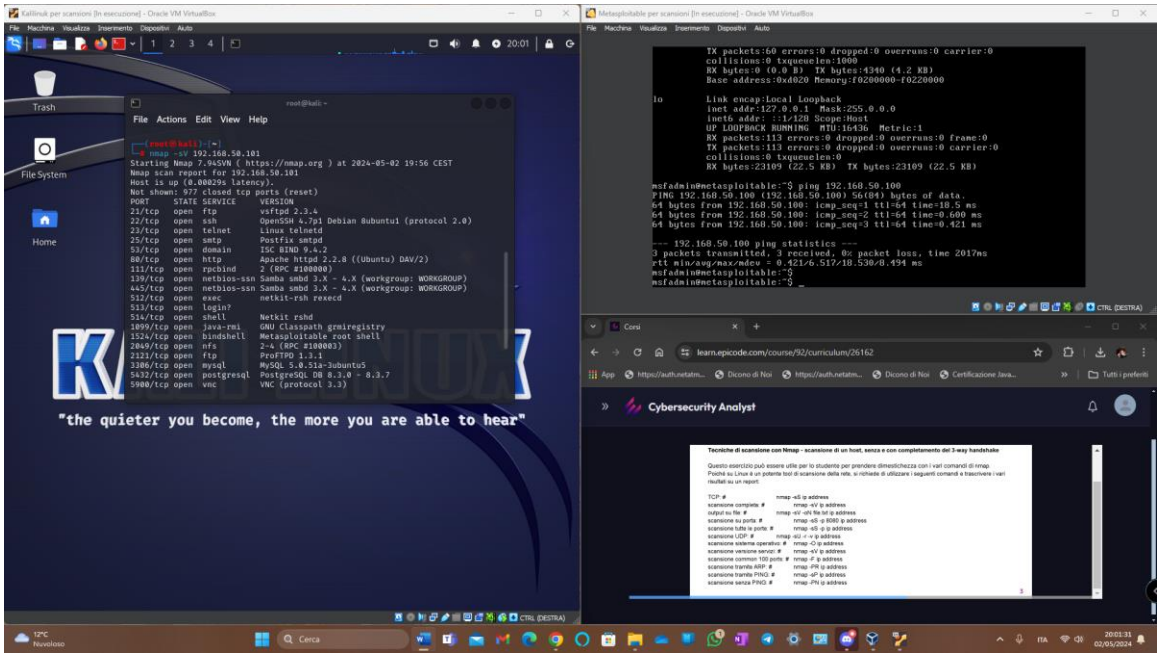


Complete Scan

Comando: nmap -sV 192.168.50.101

Descrizione: Identifica servizi e versioni aperte.

Risultati:

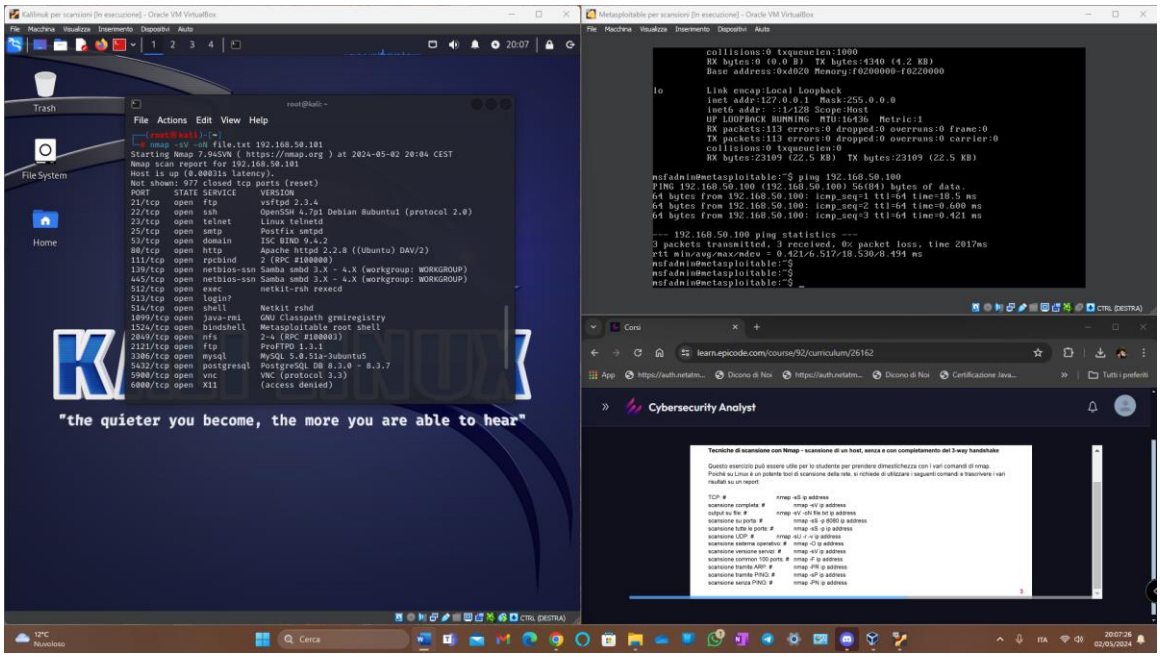


Output to File

Comando: nmap -oN file.txt 192.168.50.101

Descrizione: Salva l'output delle scansioni in un file di testo.

Risultati:

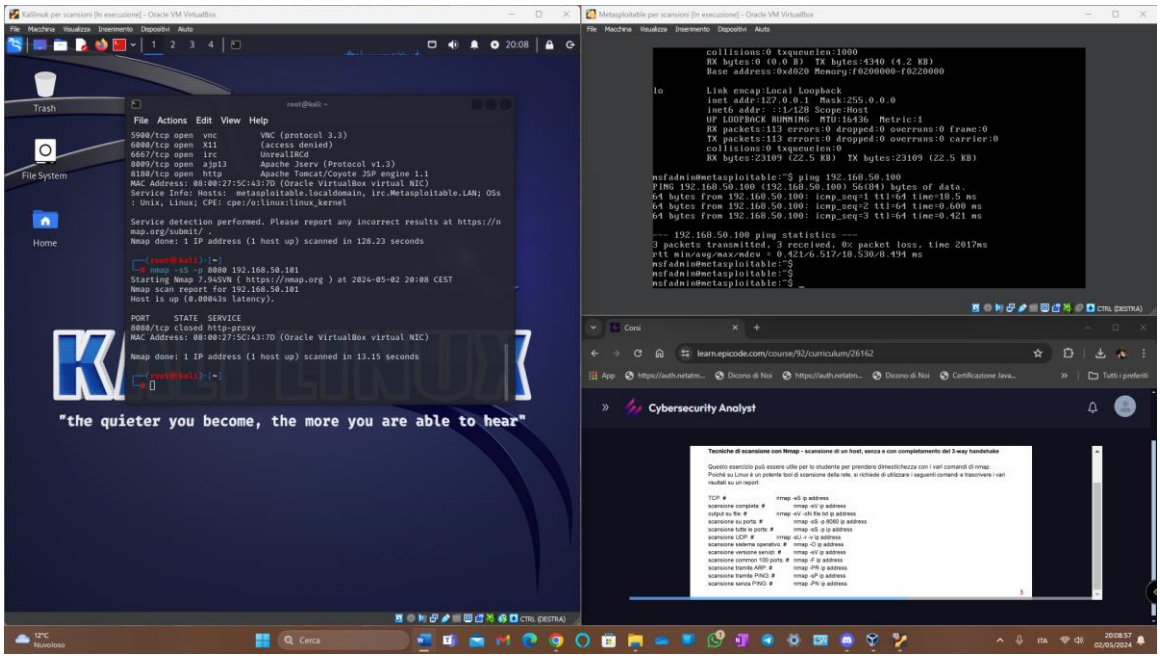


Specific Ports Scan

Comando: nmap -p 8080 192.168.50.101

Descrizione: Scansiona porte specifiche.

Risultati:

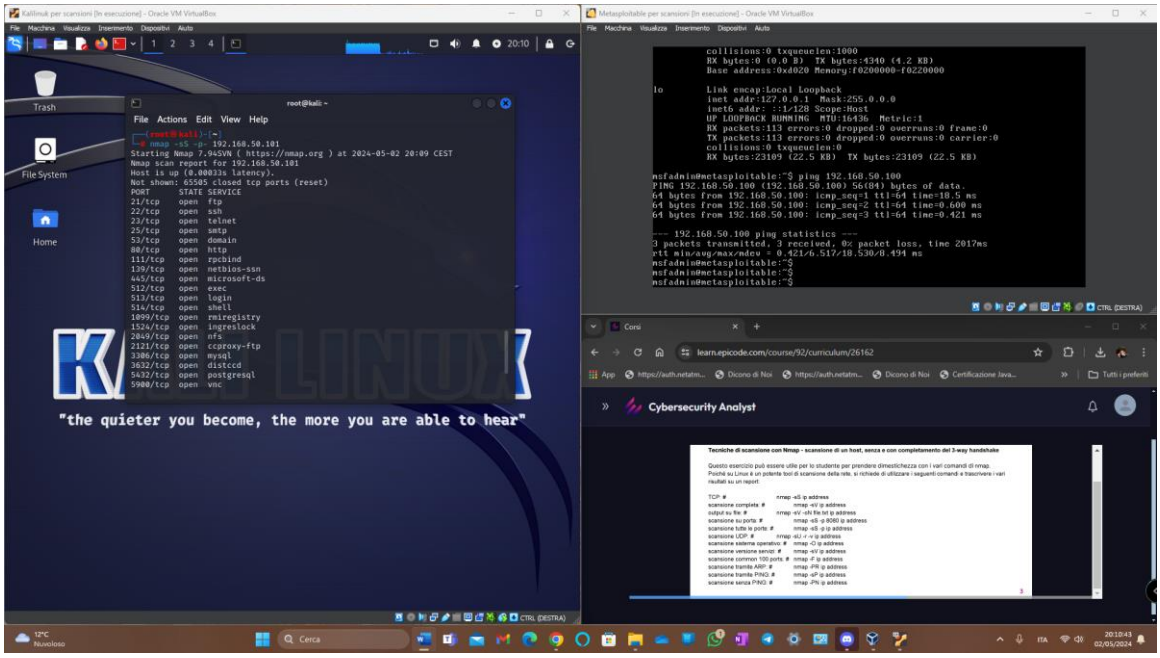


All Ports Scan

Comando: nmap -p- 192.168.50.101

Descrizione: Scansiona tutte le porte da 1 a 65535.

Risultati:

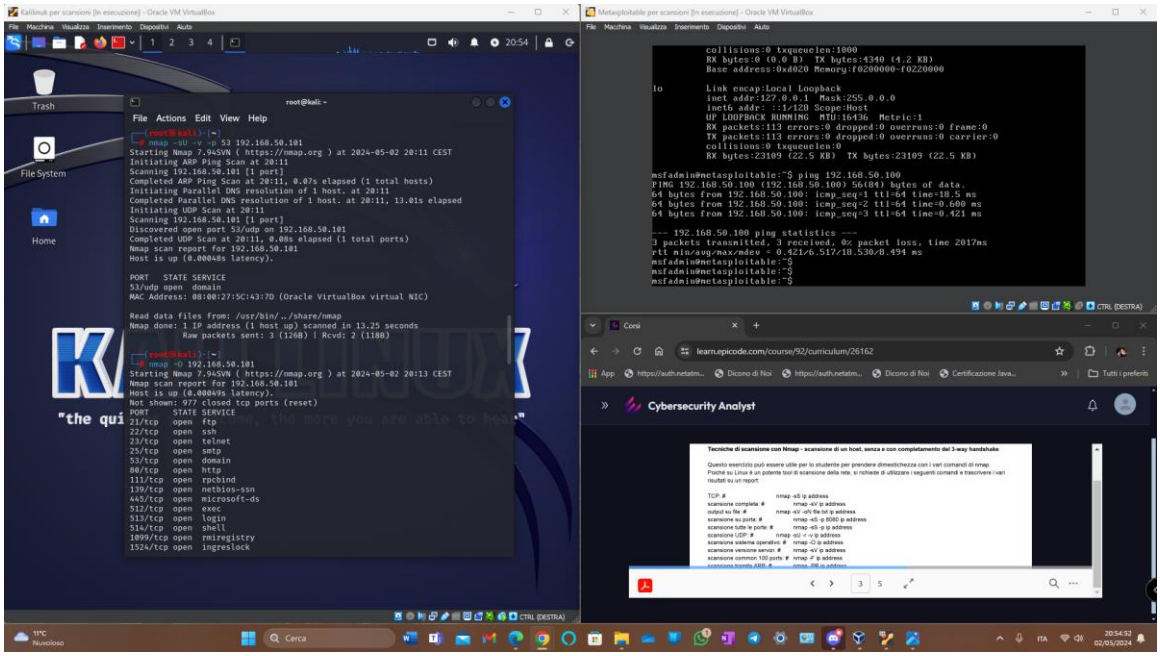


UDP Scan

Comando: nmap -sU 53 192.168.50.101

Descrizione: Scansione delle porte UDP.

Risultati:

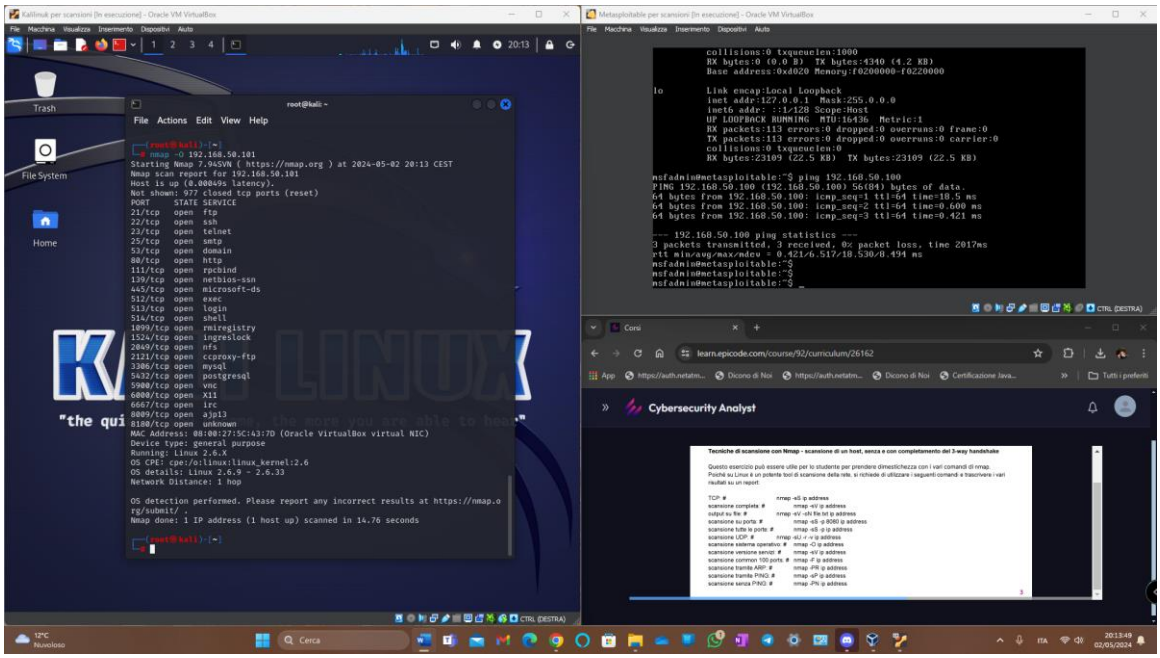


OS Detection

Comando: nmap -O 192.168.50.101

Descrizione: Identifica il sistema operativo della macchina target.

Risultati:

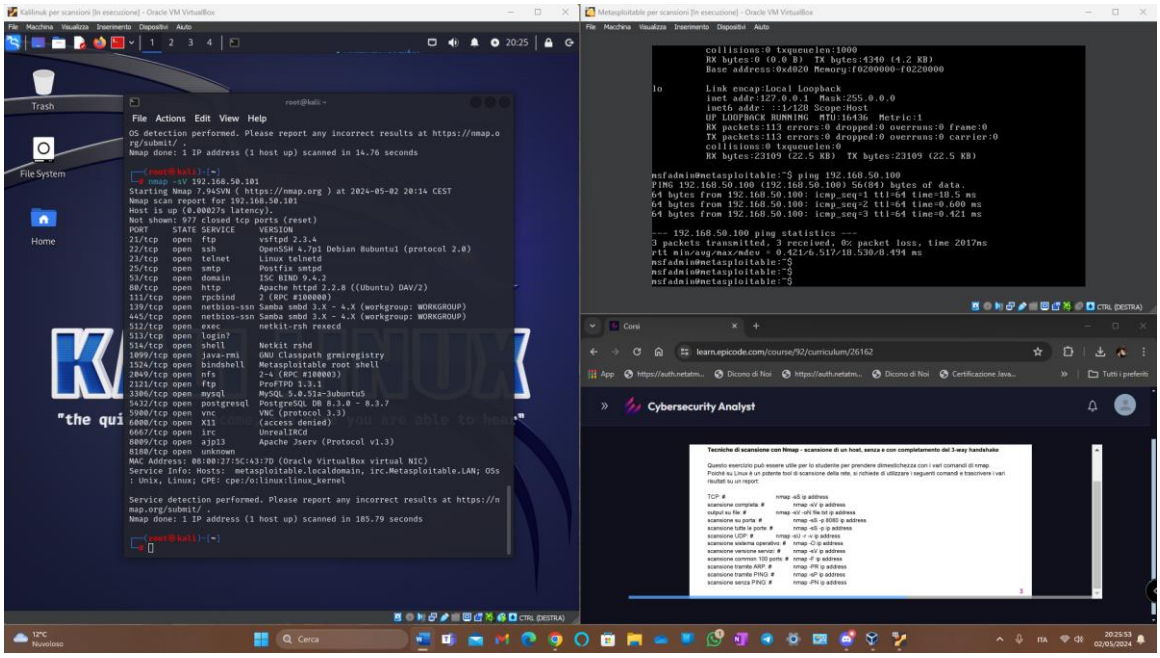


Service Version Detection

Comando: nmap -sV 192.168.50.101

Descrizione: Rileva la versione dei servizi in esecuzione.

Risultati:

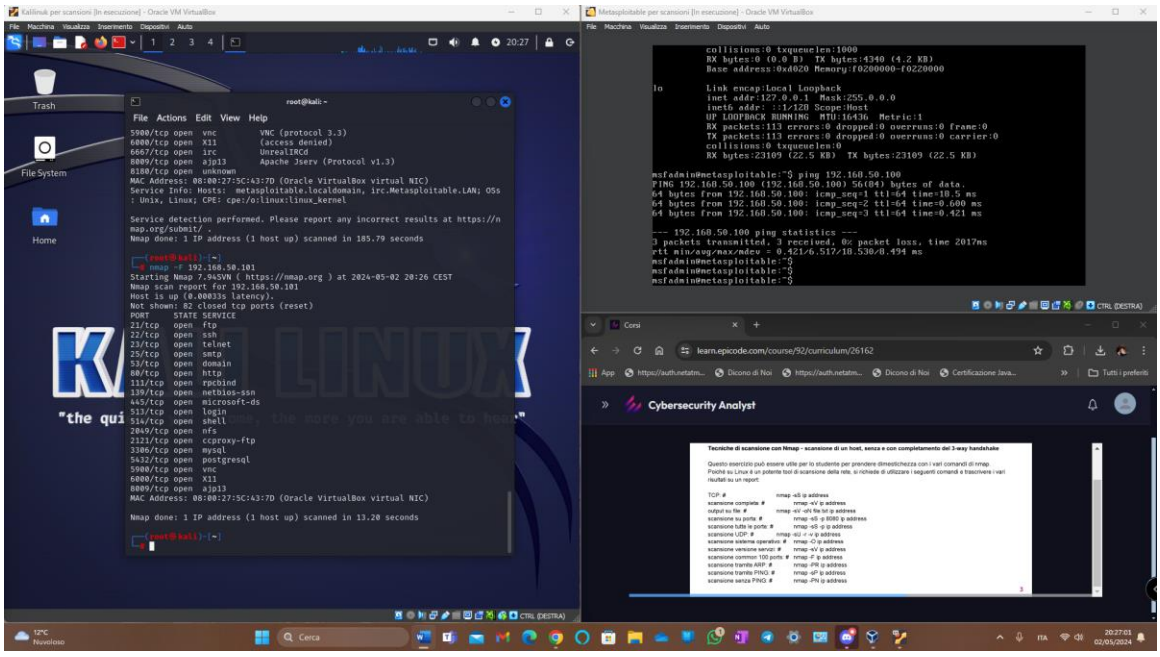


Top 100 Common Ports Scan

Comando: nmap -F 192.168.50.101

Descrizione: Scansiona le 100 porte più comuni molto velocemente.

Risultati:

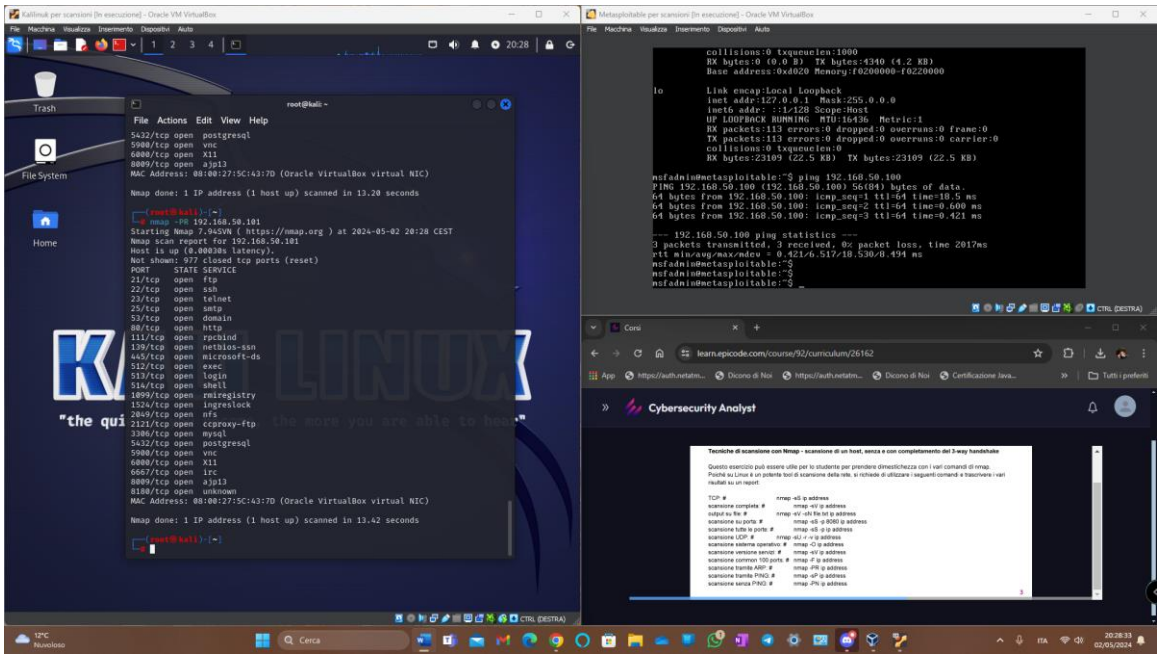


ARP Scan

Comando: nmap -PR 192.168.50.101

Descrizione: Usa l'ARP per trovare host attivi sulla rete locale.

Risultati:

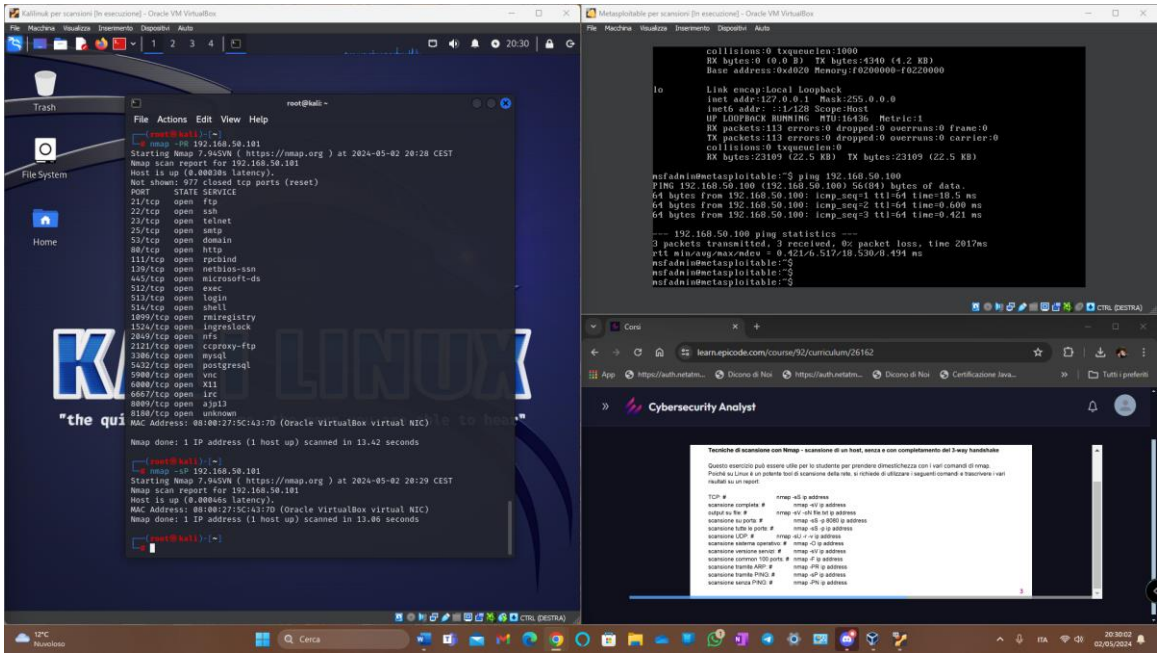


Ping Scan

Comando: nmap -sP 192.168.50.101

Descrizione: Scansiona per verificare se gli host sono attivi usando ICMP.

Risultati:

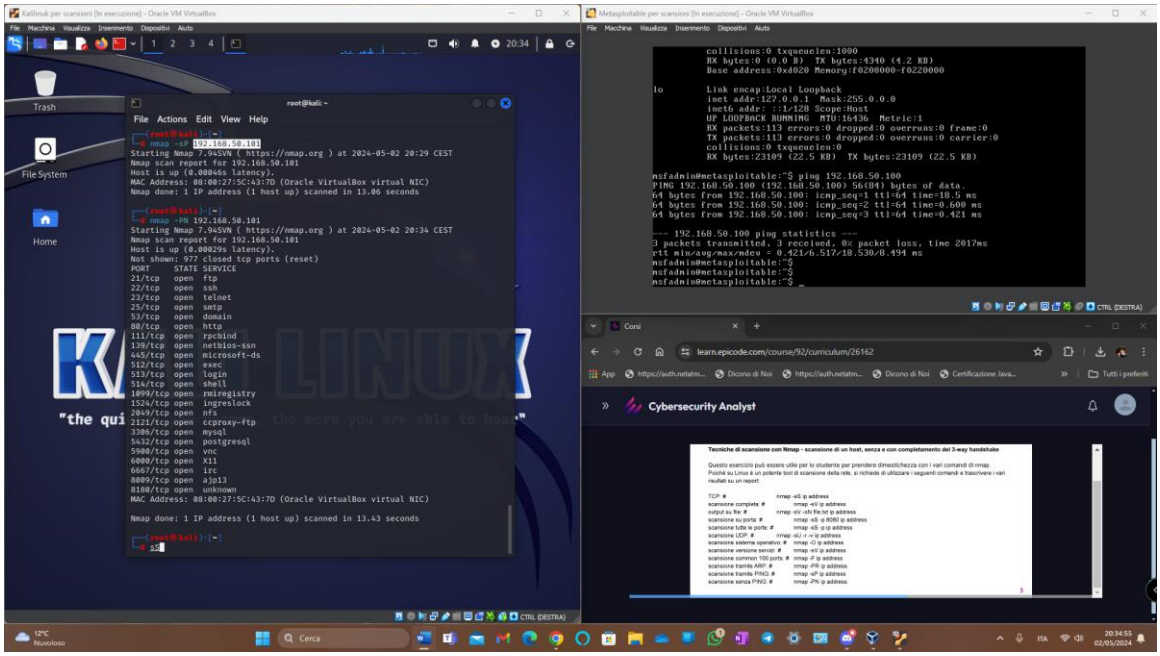


No Ping Scan

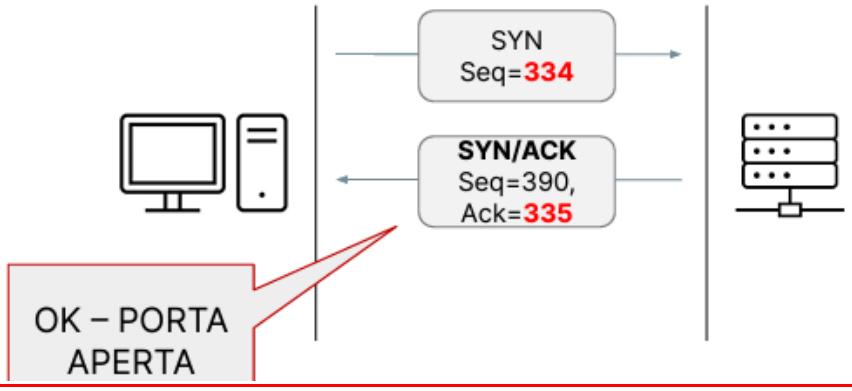
Comando: nmap -PN 192.168.50.101

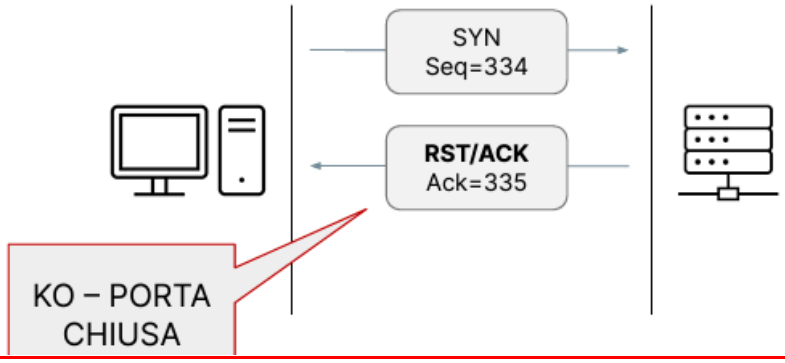
Descrizione: Scansiona senza inviare pacchetti ICMP echo request.

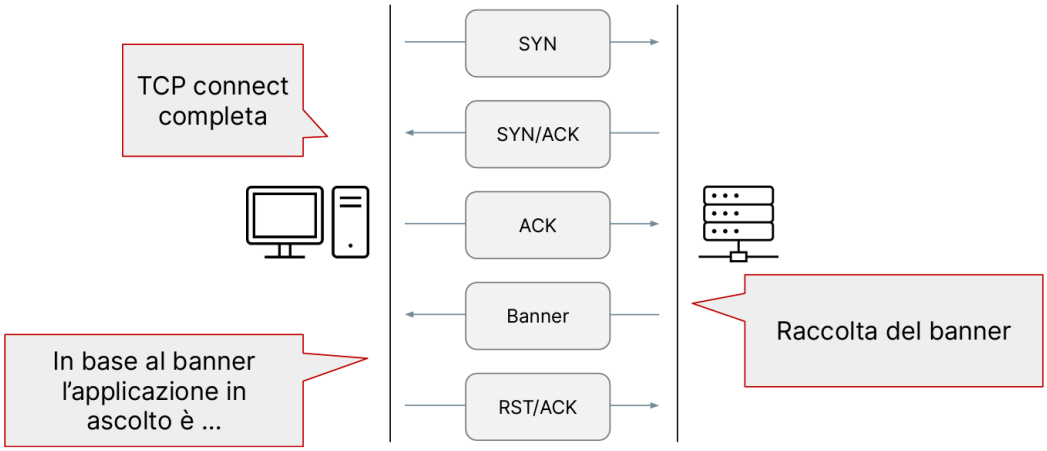
Risultati:



Grafici


SYN
Seq=334
SYN/ACK
Seq=390,
Ack=335
OK – PORTA
APERTA


SYN
Seq=334
RST/ACK
Ack=335
KO – PORTA
CHIUSA


TCP connect
completa
SYN
SYN/ACK
ACK
Banner
RST/ACK
In base al banner
l'applicazione in
ascolto è ...
Raccolta del banner