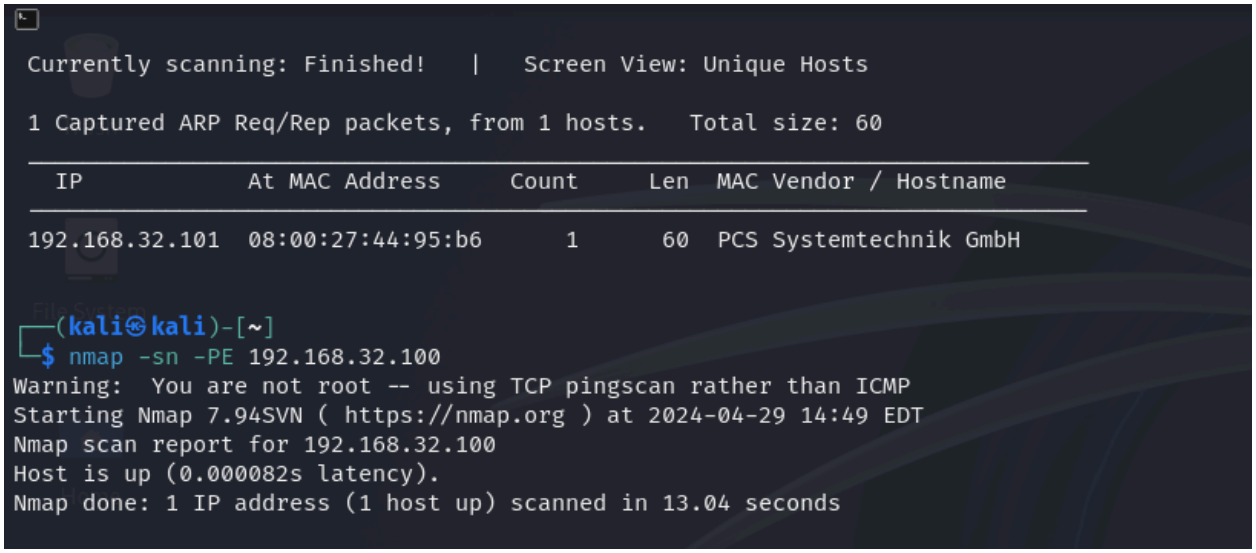
REPORT W10-D5

Traccia

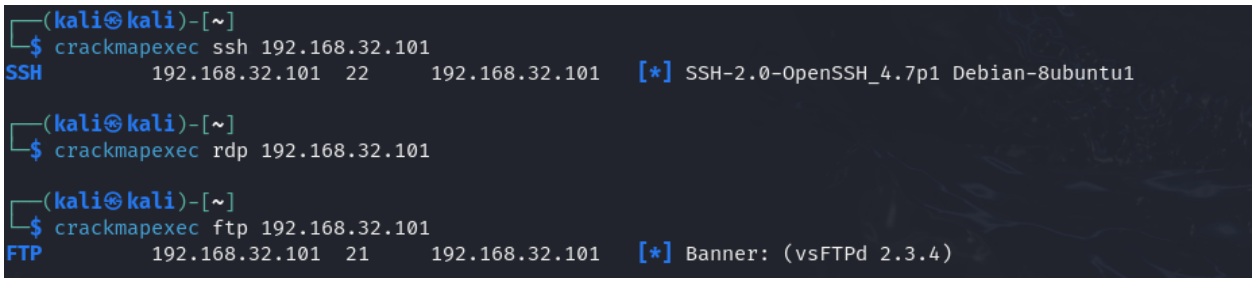
https://www.yeahhub.com/15-most-useful-host-scanning-commands-kalilinux/

Utilizzare alcuni di questi strumenti per raccogliere informazioni sulla macchina metasploitable e produrre un report. Nel report indicare sopra l'esecuzione degli strumenti e nella parte finale un riepilogo delle informazioni trovate.

COMANDO 1/2

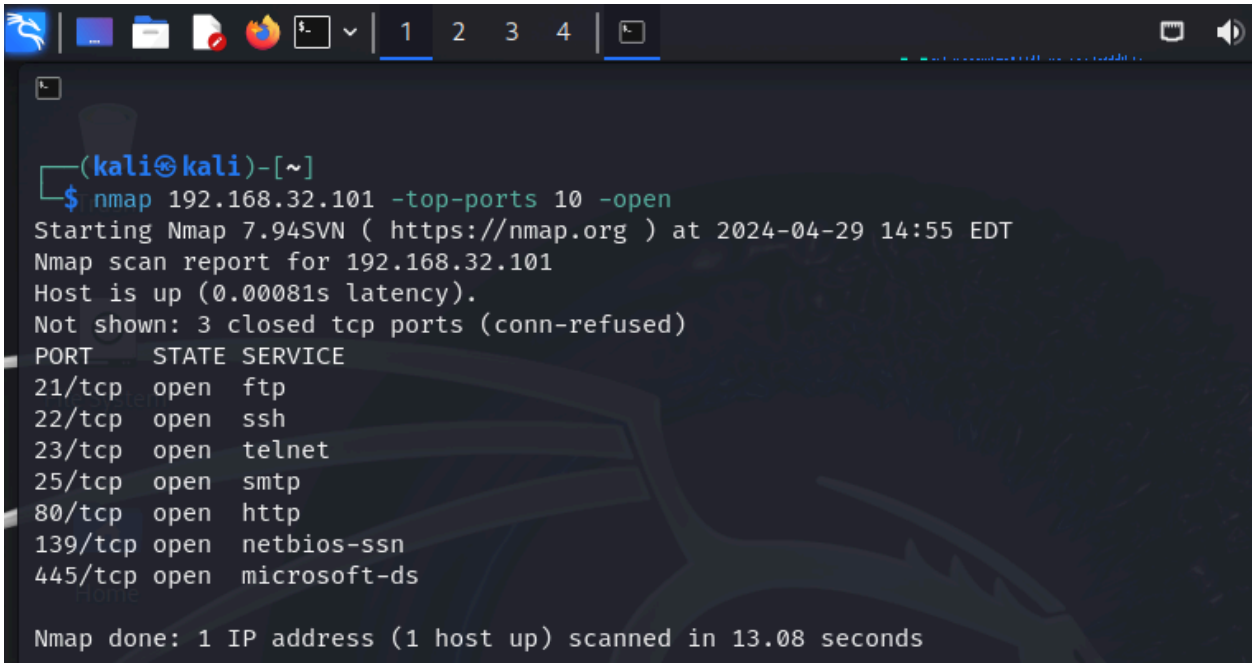


COMANDO 3

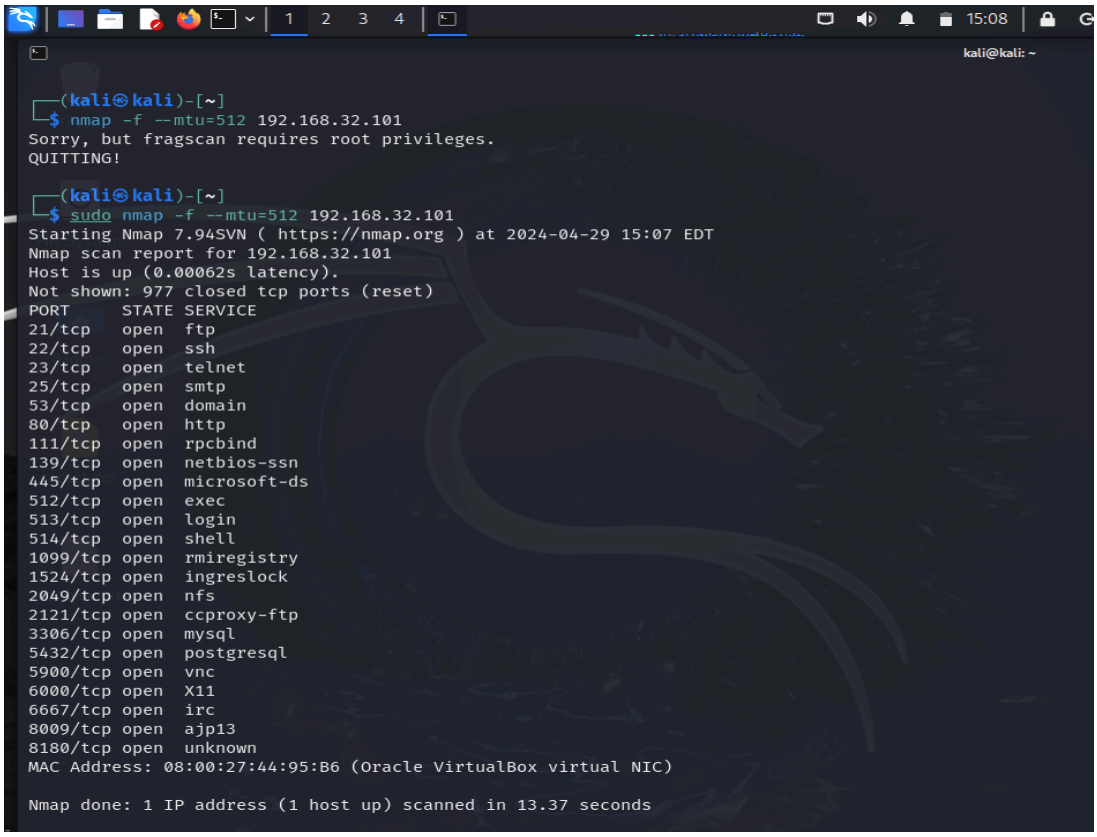


REPORT W10-D5

COMANDO 4

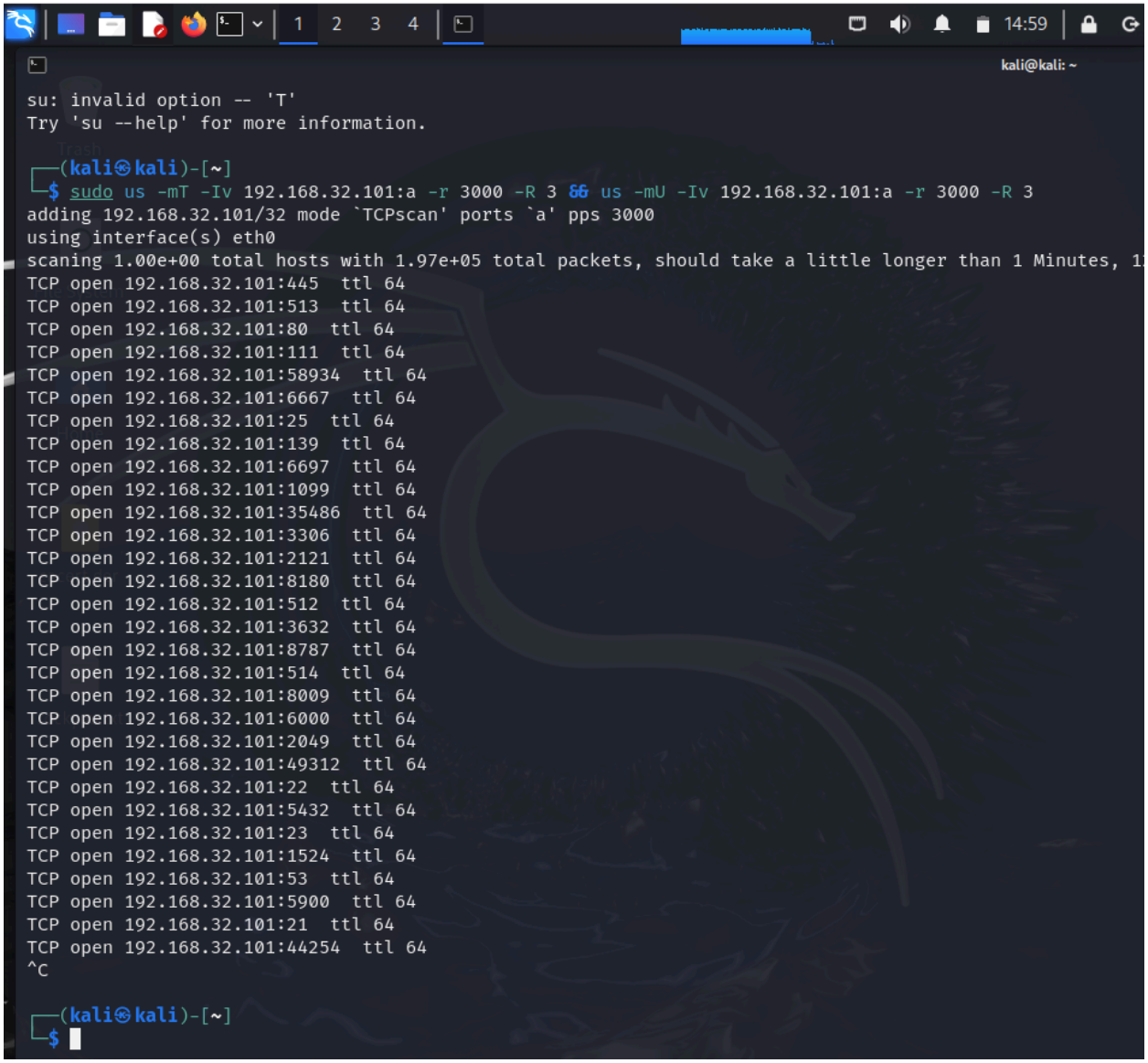


COMANDO 5



REPORT W10-D5

COMANDO 6



RIEPILOGO FINALE

Per riassumere le informazioni acquisite tramite tutti questi comandi, elenchiamo tutte le info ricavate:

- Tramite il **COMANDO 1** *(nmap -sn -PE “TARGET”)* viene eseguita una scansione di tipo ping dal tool. Lo switch “-sn” va ad indicare ad Nmap di eseguire una scansione tramite ping ai target selezionati disabilitando lo

scan delle ports, mentre -PE indica il tipo di ping in questo caso ICMP ECHO. Il risultato dello scan indica il target attivo.

- Tramite il **COMANDO 2** *(netdiscover -r "TARGET")* andiamo ad eseguire il tool netdiscover è uno strumento di discovery di rete utilizzato per identificare dispositivi sulla stessa rete locale. Inserendo lo switch "-r" andiamo a specificare il range di indirizzo da scannerizzare (si potrebbe inserire anche la notazione in CIDR /24).

- Tramite il **COMANDO 3** *(crackmapexec "TARGET")* utilizzeremo crackmapexec, uno strumento utilizzato per l'automazione e l'esecuzione di attacchi di penetration testing, che utilizzeremo per controllare le ports aperte. Tramite "SSH" e "FTP" abbiamo effettuato banner grabbing alle porte 21-22.

- Tramite il **COMANDO 4** *(nmap "TARGET" –top-ports 10 –open)* in cui lo switch "-top-ports 10" indica 10 delle well known port e "-open" indica di mostrare a schermo solo quelle che risultano aperte.

- Tramite il **COMANDO 5** *(sudo nmap -MTU=512 "TARGET")* si va a selezionare la dei Maximum Transmission Unit (MTU) a 512 byte tramite lo switch "-MTU".

- Tramite il **COMANDO 6** *(us -mT -lv "TARGET":a -r 3000 -R 3 && us -mU -lv "TARGET":a -r 3000 -R 3*), suddiviso in 2 comandi dal "&" in cui si richiede una TCP scan dallo switch "-mT" e un UDP scan dal "-mU", mentre "-r" indica 3000 pacchetti al secondo e "-R" imposta a 3 il numero dei tentativi falliti.