M3 D4

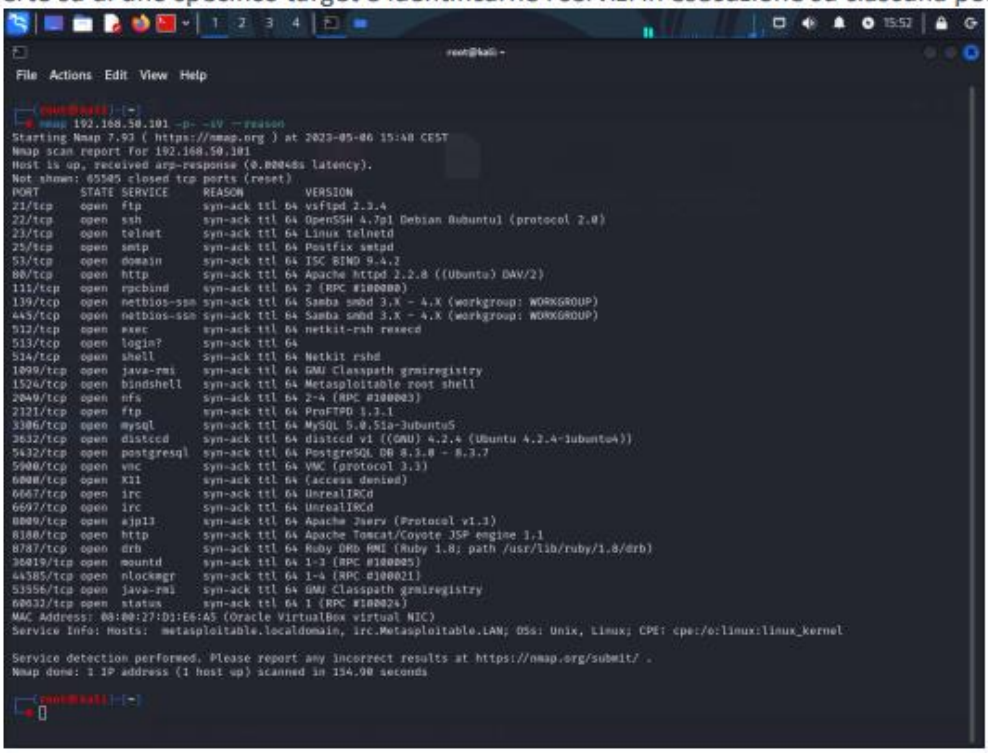
GIORNO 5 – ESERCIZIO

FASE DI RACCOLTA INFORMAZIONI

nmap -sn -PE (nostro IP) ci permettere di scansionare una rete e scoprirne gli host attivi.

nmap (nostro IP) --top-ports 10 --open viene utilizzato per eseguire una scansione di un singolo target e identificare le 10 porte più frequentemente utilizzate e aperte su tale target.

nmap (nostro IP) -p- -sV --reason è un comando utilizzato per eseguire una scansione di tutte le porte aperte su di uno specifico target e identificarne i servizi in esecuzione su ciascuna porta.



nmap -sS -sV -T4 (nostro IP) questa scansione utilizza una combinazione di tecniche di scansione per determinare quali porte sono aperte sul target e identificare i servizi specifici che vengono eseguiti su tali porte. La scansione viene eseguita utilizzando una tecnica di scansione SYN, che riduce il rischio di essere rilevati, e viene eseguita con un livello di intensità moderato per ridurre il tempo di scansione.