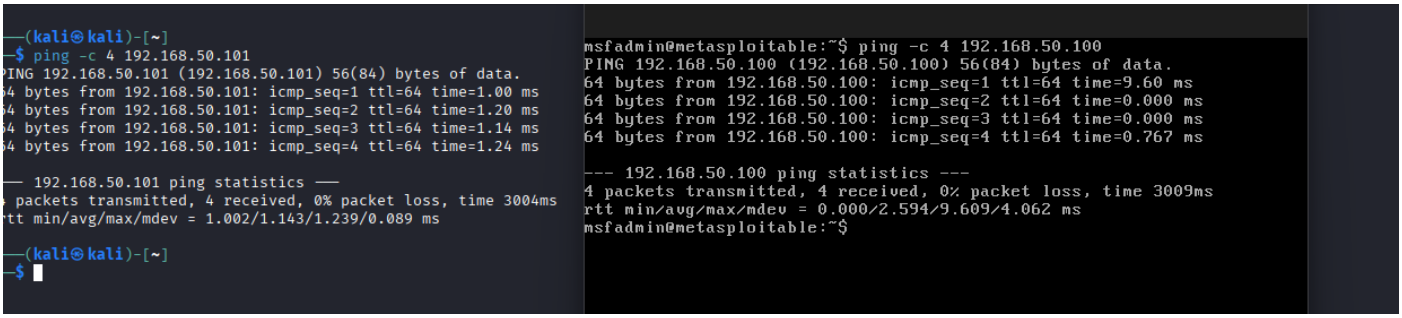
INDICE

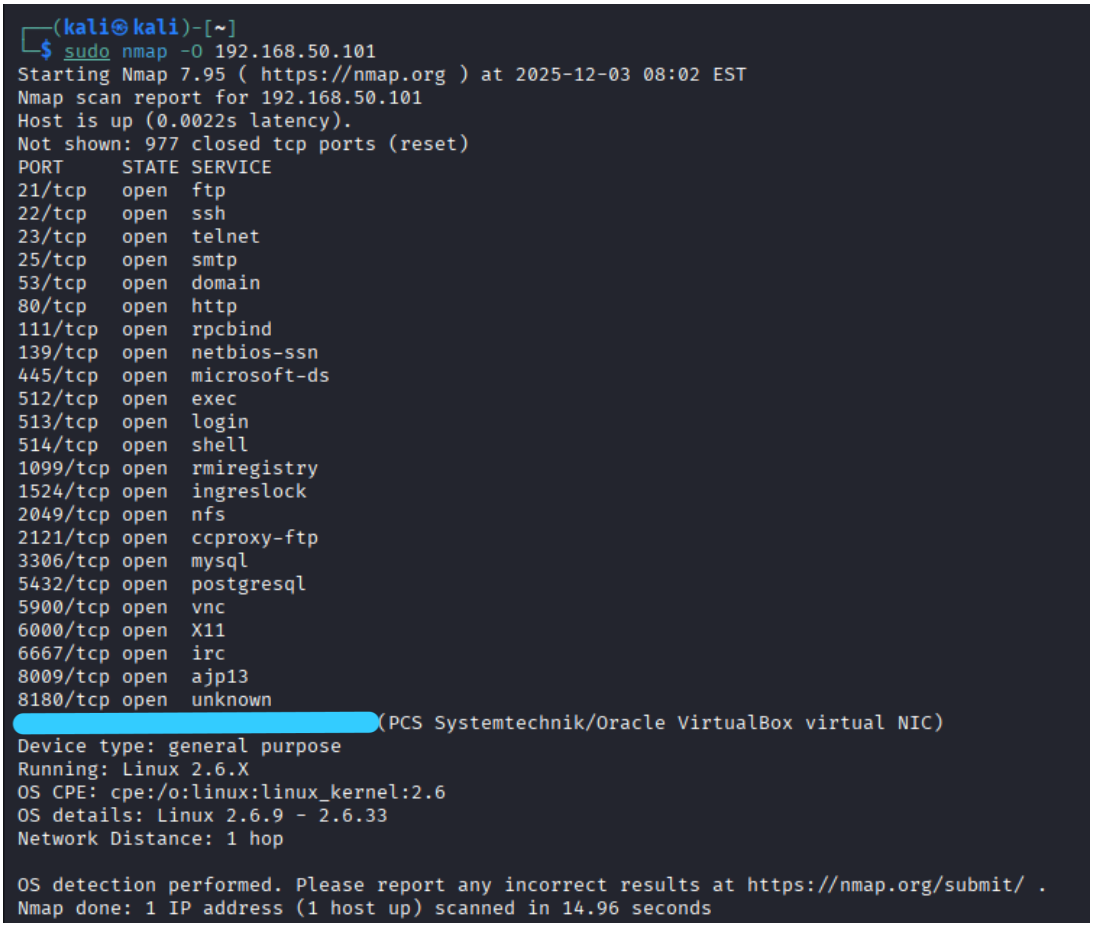
INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: il laboratorio ha previsto l'analisi del comportamento di un host quando è collocato nello stesso segmento di rete del sistema incaricato dell'esecuzione delle verifiche. Operando all'interno di un ambiente condiviso, privo di elementi di instradamento intermedi, è stato possibile osservare in modo diretto la visibilità dei servizi esposti, la rapidità con cui vengono identificati e la naturale riduzione dei tempi di risposta dovuta alla vicinanza logica dei sistemi.

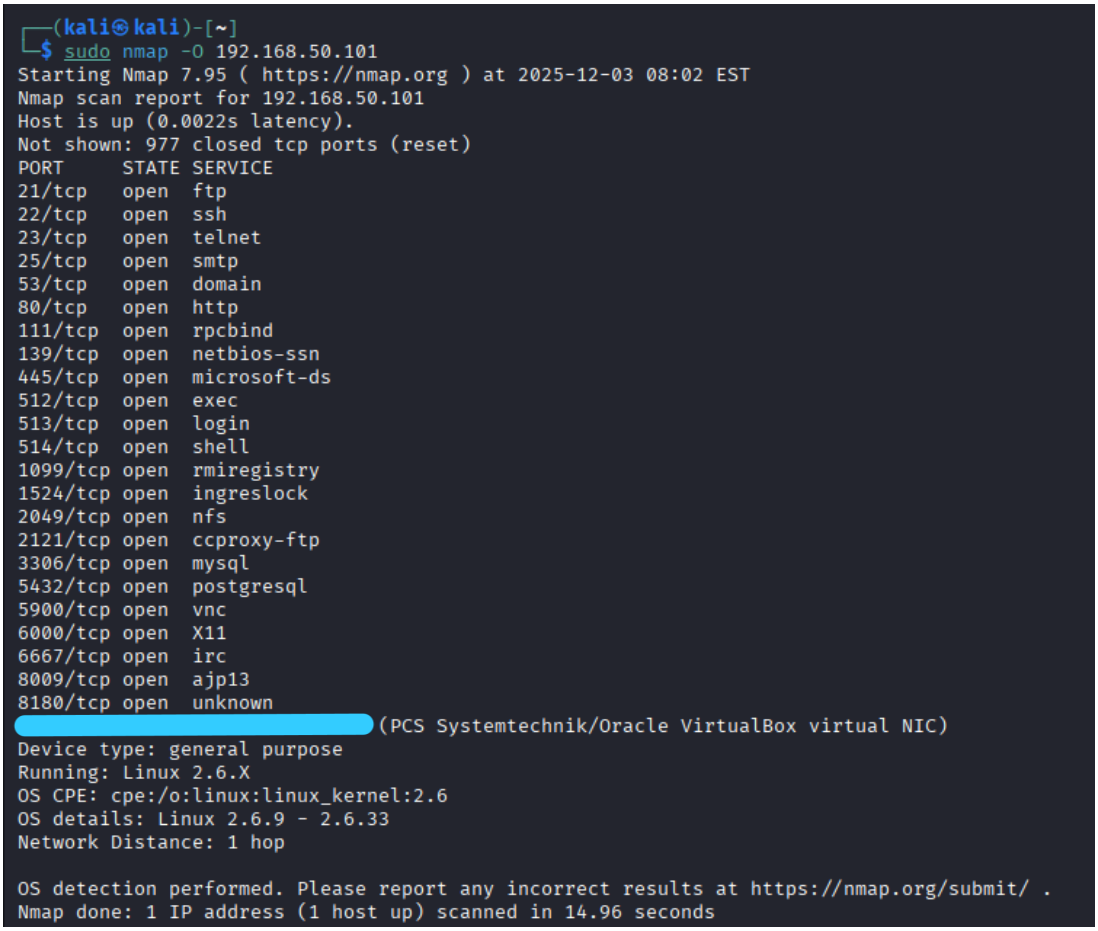
OBIETTIVO: esaminare il profilo operativo dell'host quando opera nella stessa rete del sistema di controllo, verificando la disponibilità dei servizi, la loro esposizione e il comportamento complessivo in un contesto privo di barriere o salti di rete.



Per iniziare l'analisi nella nuova configurazione di rete, è stata verificata la capacità dei due sistemi di comunicare direttamente all'interno della medesima subnet.
A tal fine è stato utilizzato un semplice test di connettività, basato sull'invio di una serie di richieste ICMP tra le due macchine; l'operazione ha confermato una comunicazione pienamente stabile: ciascun sistema ha risposto alle richieste provenienti dall'altro con tempi di latenza coerenti con un ambiente locale e senza alcuna perdita di pacchetti.

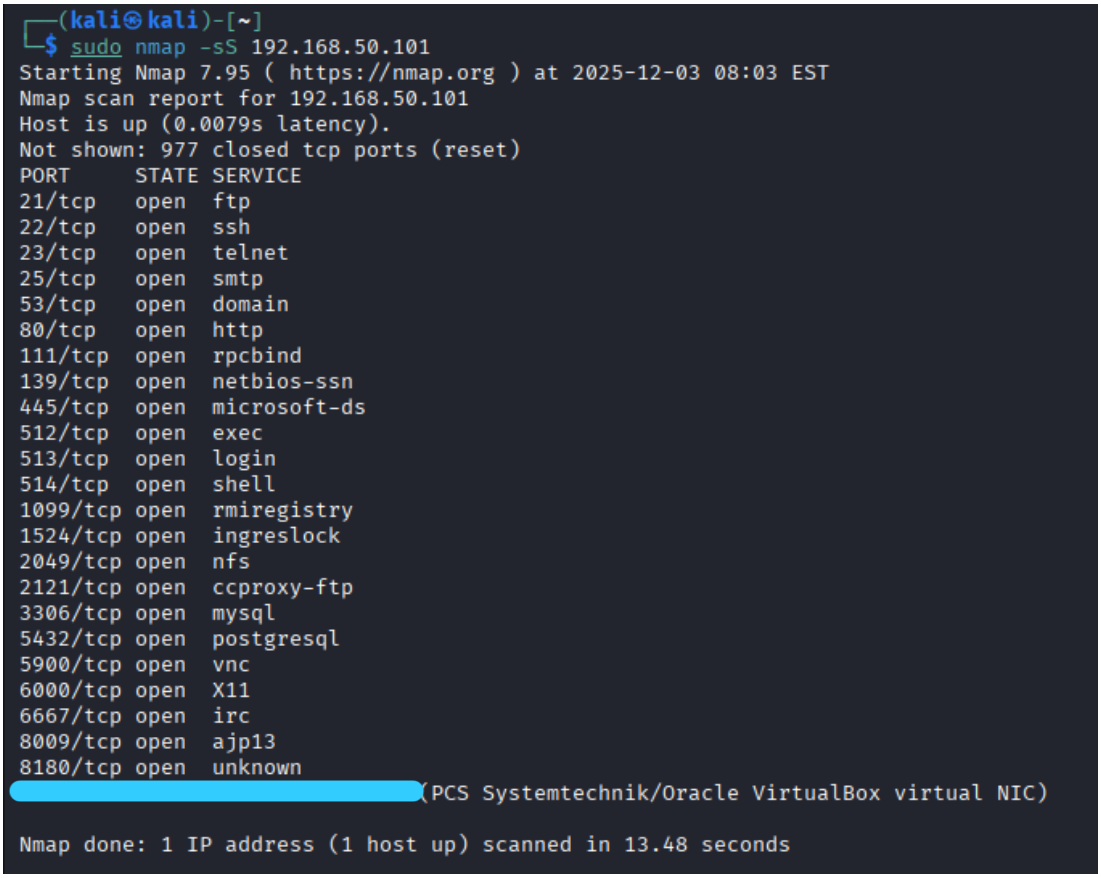


L'analisi ha previsto l'esecuzione di una scansione completa dell'host, utilizzando un approccio orientato all'identificazione del sistema operativo e alla rilevazione dell'intera superficie di servizi esposti.
L'operazione ha restituito un quadro dettagliato delle porte in ascolto e delle applicazioni attive sull'indirizzo di destinazione, evidenziando una struttura caratterizzata da servizi di rete, componenti applicativi e funzionalità tipiche di un ambiente server articolato.
L'indagine ha inoltre permesso di determinare con precisione la tipologia di sistema in uso ed ulteriori informazioni strutturali che contribuiscono a delineare il profilo operativo della macchina.
L'esito conferma un comportamento coerente con quello di un host raggiungibile direttamente nella stessa rete locale, in cui la comunicazione avviene senza passaggi intermedi.
DIFFERENZE RISCONTRATE: il risultato ottenuto si distingue nettamente da quello osservabile quando le due macchine risiedono su reti separate.
Nel caso precedente, la comunicazione prevedeva il transito attraverso un dispositivo di instradamento, circostanza che introduceva una latenza più elevata ed un comportamento più selettivo nella risposta ai tentativi di rilevazione.
Nella configurazione attuale, invece, la non necessità di attraversare gateway o router, riduce sensibilmente la distanza di rete e consente una visibilità diretta dei servizi esposti. Ne deriva una risposta più immediata, completa e priva delle limitazioni che normalmente emergono quando il traffico deve attraversare segmenti di rete differenti.



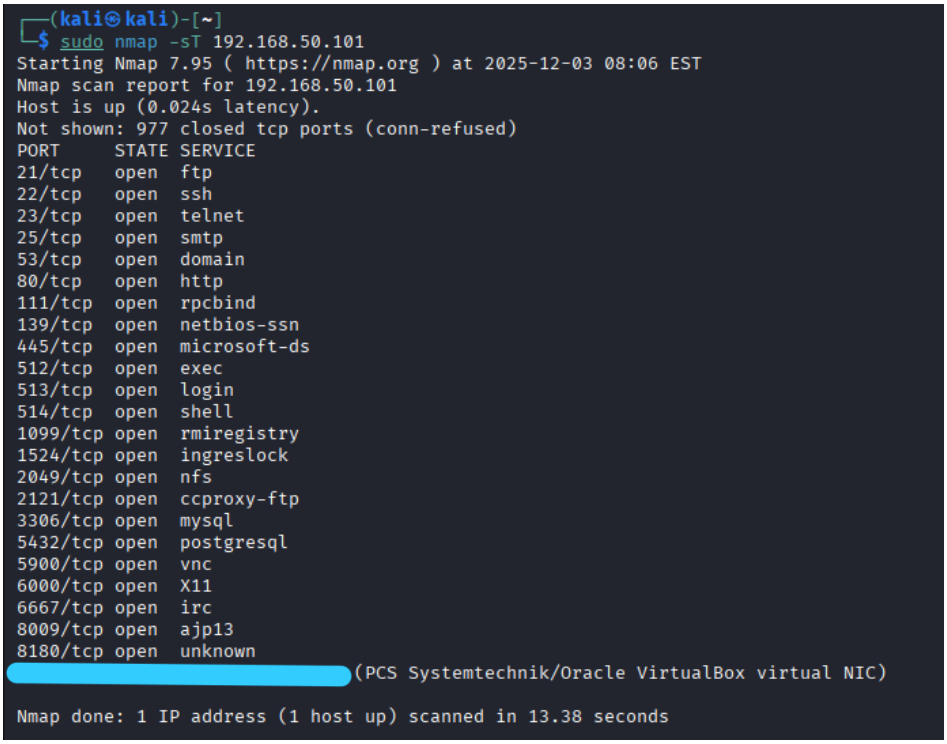
L'analisi effettuata consentito di ottenere una visione completa dei servizi attivi sull'host e delle sue caratteristiche operative. La scansione ha evidenziato porte TCP in stato "open", associate a funzionalità di servizi di gestione remota, componenti applicativi, protocolli di rete ecc.
L'host ha risposto in modo diretto alle richieste, mostrando piena raggiungibilità e una distanza di rete pari a un solo hop, elemento che conferma la presenza delle due macchine all'interno della stessa rete locale.
La rilevazione del sistema operativo ha restituito un profilo coerente con un ambiente Linux basato su kernel della serie 2.6, mentre l'indicazione dell'indirizzo MAC ha confermato la natura virtualizzata dell'interfaccia

DIFFERENZE RISCONTRATE: Quando le macchine risiedono su reti diverse, la visibilità dei servizi diminuisce sensibilmente e il tracciato delle risposte risulta filtrato dal sistema di routing o dal firewall intermedio.
Il rilevamento dell'OS diventa meno preciso, alcune porte non rispondono o risultano "filtered", e la latenza cresce per via dell'hop aggiuntivo.



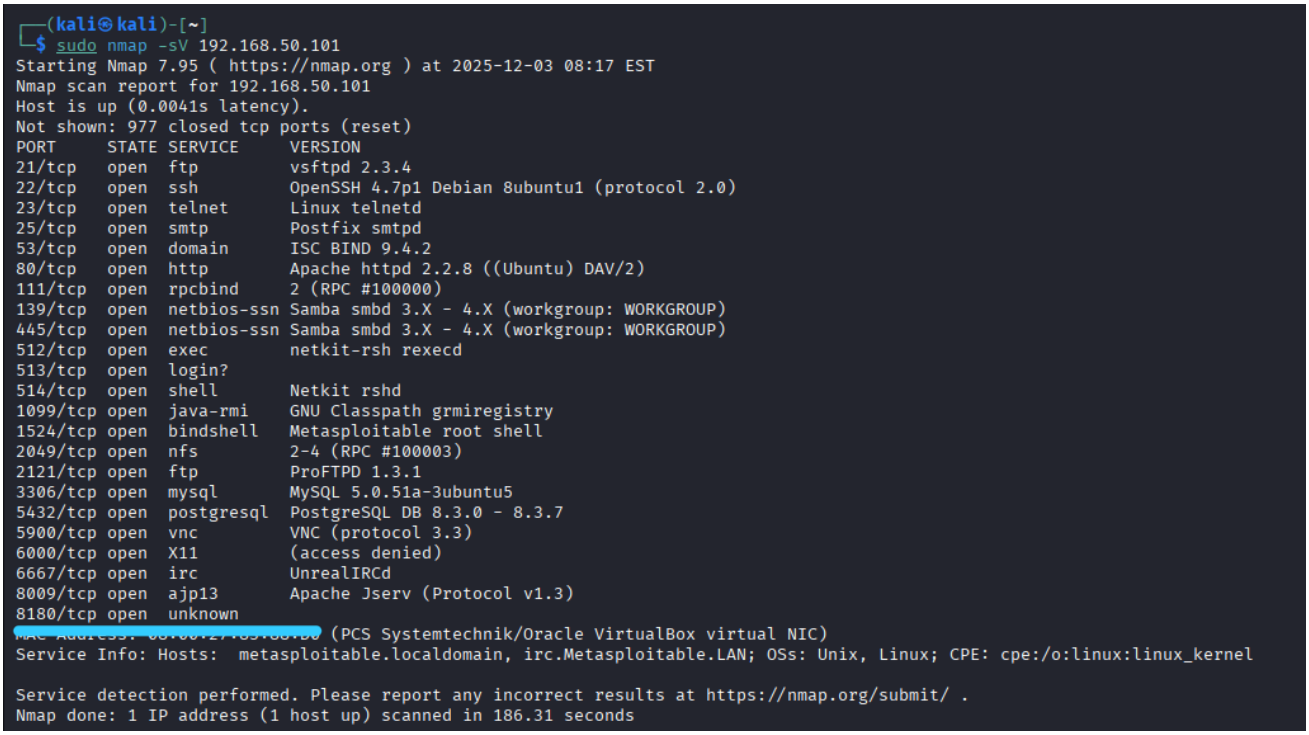
È stata eseguita un'analisi di identificazione del sistema operativo sull'host tramite una scansione avanzata, finalizzata a rilevare sia i servizi effettivamente in ascolto sia le caratteristiche strutturali dell'ambiente.
La procedura ha individuato un numero elevato di porte TCP in stato *open*, confermando la presenza di servizi applicativi e e funzionalità tipiche di un sistema progettato per essere raggiungibile nella sua interezza all'interno della stessa rete.
L'analisi ha inoltre restituito informazioni dettagliate sul sistema operativo rilevato, sull'indirizzo MAC associato all'interfaccia e sulle specifiche della piattaforma, delineando così un quadro completo e coerente del comportamento dell'host quando collocato nello stesso segmento di rete del sistema che esegue la scansione.

DIFFERENZE RISCONTRATE : quando due macchine risiedono sulla stessa rete, l'host risulta integralmente raggiungibile e tutte le porte aperte vengono enumerate senza limitazioni. La distanza di rete si riduce a un singolo hop e l'identificazione del sistema operativo produce un risultato completo e accurato; le risposte sono più rapide e non si osservano filtraggi intermedi.
Al contrario, nello scenario su reti diverse alcune informazioni vengono parzialmente mascherate, il percorso di rete introduce latenza aggiuntiva e la visibilità dei servizi si riduce in funzione del routing e delle regole intermedie.
L'analisi complessiva risulta quindi più ricca e immediata solo quando i sistemi si trovano nello stesso segmento.



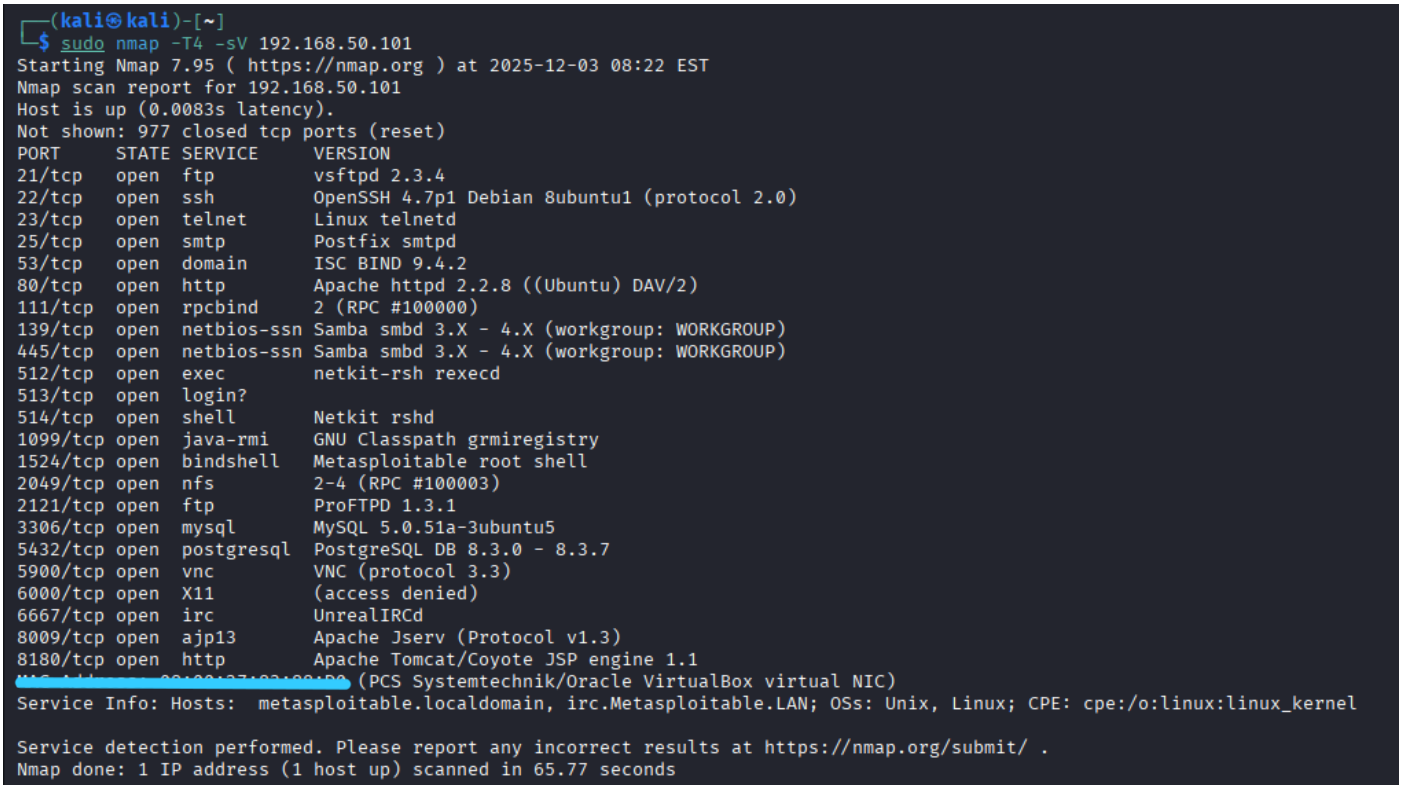
È stata eseguita una scansione mirata utilizzando l'opzione -sT, che effettua una connessione TCP completa verso ogni porta al fine di rilevare in modo affidabile le porte attive sull'host analizzato.
L'operazione ha restituito un elenco esteso di servizi raggiungibili, includendo protocolli applicativi, servizi di rete, database e funzionalità di sistema più specifiche.
Tutte le porte identificate risultano in stato *open*, indicando la piena raggiungibilità dei servizi e confermando la visibilità diretta dell'host all'interno della rete locale.
La procedura si è conclusa con una scansione completa in tempi contenuti, fornendo un quadro chiaro e lineare dell'assetto operativo della macchina analizzata.

DIFFERENZE RISCONTRATE : rispetto allo scenario precedente, in cui le macchine risiedevano su reti distinte, la collocazione nella stessa rete ha prodotto una visibilità molto più diretta dei servizi esposti.
Le scansioni risultano più rapide, prive di salti intermedi e con una rilevazione completa e immediata di tutte le porte aperte. Non si osservano più vincoli legati al routing, né variazioni nella distanza di rete, ora ridotta a un singolo hop; anche la latenza risulta più bassa e stabile, indice di un percorso di comunicazione più lineare.



L'operazione ha previsto l'esecuzione di una scansione orientata all'identificazione dettagliata dei servizi direttamente esposti dall'host all'interno della stessa rete.
La procedura ha permesso di rilevare un insieme esteso di porte TCP in stato attivo, associate a componenti applicative, servizi di rete, strumenti di amministrazione remota ecc.
Per ciascun servizio è stata identificata la specifica implementazione software, consentendo di ricostruire un quadro preciso dell'ambiente applicativo presente sull'host.
La risposta ottenuta è stata completa e immediata, con un tempo di rilevazione sensibilmente ridotto grazie alla comunicazione diretta tra macchine appartenenti alla medesima sottorete.

DIFFERENZE RISCONTRATE : quando i sistemi si trovano sulla stessa rete, la rilevazione dei servizi risulta più rapida e lineare, grazie all'assenza di dispositivi intermedi.
Le porte esposte vengono enumerate senza filtri e senza la latenza aggiuntiva tipica di un instradamento multilivello; la visibilità dell'host risulta completa, includendo sia i servizi applicativi sia le informazioni relative alle versioni dei software.
In configurazioni su reti differenti, al contrario, la comunicazione è condizionata dal comportamento del router e da eventuali restrizioni di instradamento, con tempi maggiori, visibilità più limitata e alcune richieste che possono non ricevere risposta.



L'operazione ha previsto l'utilizzo di una scansione avanzata con rilevazione delle versioni dei servizi, combinata con un livello di velocità elevato, al fine di ottenere una panoramica completa e tempestiva delle applicazioni in ascolto sull'host all'interno della stessa rete.
L'analisi ha restituito un quadro molto dettagliato dei servizi presenti, evidenziando comunicazioni di rete, database, servizi web e funzionalità applicative tipiche di un sistema multi-servizio.
Oltre alla disponibilità delle porte, è stata identificata anche la versione dei software in esecuzione, consentendo una visione precisa delle tecnologie operative installate sull'host.
L'esito mostra un sistema pienamente raggiungibile, che risponde senza intermediari, caratteristica tipica di dispositivi che operano sulla medesima subnet.

DIFFERENZE RISCONTRATE : quando le due macchine si trovano sulla stessa rete, la comunicazione avviene direttamente, senza la presenza di nodi intermedi, consentendo una latenza più bassa e una visibilità completa dei servizi disponibili.
Nella configurazione precedente, basata su reti differenti, il traffico era instradato attraverso un gateway, introducendo un hop aggiuntivo e modificando il comportamento della rilevazione. In particolare, l'identificazione del sistema risultava mediata dal router e la distanza di rete appariva maggiore. Inoltre, alcuni tempi di risposta erano inevitabilmente più elevati rispetto a quelli osservati nella stessa subnet. Complessivamente, la scansione nella medesima rete produce un quadro più immediato, completo e diretto dei servizi effettivamente esposti.

CONCLUSIONE

La valutazione effettuata ha messo in evidenza come la collocazione delle due macchine all'interno della stessa rete incida in modo determinante sulla loro visibilità reciproca e sulla completezza dei dati ottenibili.
Quando i sistemi operano sullo stesso segmento di rete, la comunicazione risulta diretta e priva di elementi intermedi: la latenza è ridotta, la risposta ai pacchetti è immediata e le analisi restituiscono un quadro pienamente dettagliato dei servizi disponibili, delle relative porte e delle caratteristiche operative dell'host.
Al contrario, quando le macchine risiedono su reti differenti, la presenza di un instradamento intermedio comporta una perdita di trasparenza: alcuni servizi risultano meno accessibili, la rilevazione è più lenta e le informazioni raccolte appaiono parzialmente filtrate.
Il confronto tra i due scenari dimostra quindi come la prossimità di rete influenzi in modo concreto sia la qualità sia la profondità delle informazioni ottenibili, con ricadute dirette sulla capacità di analizzare il comportamento complessivo dei sistemi coinvolti**.**