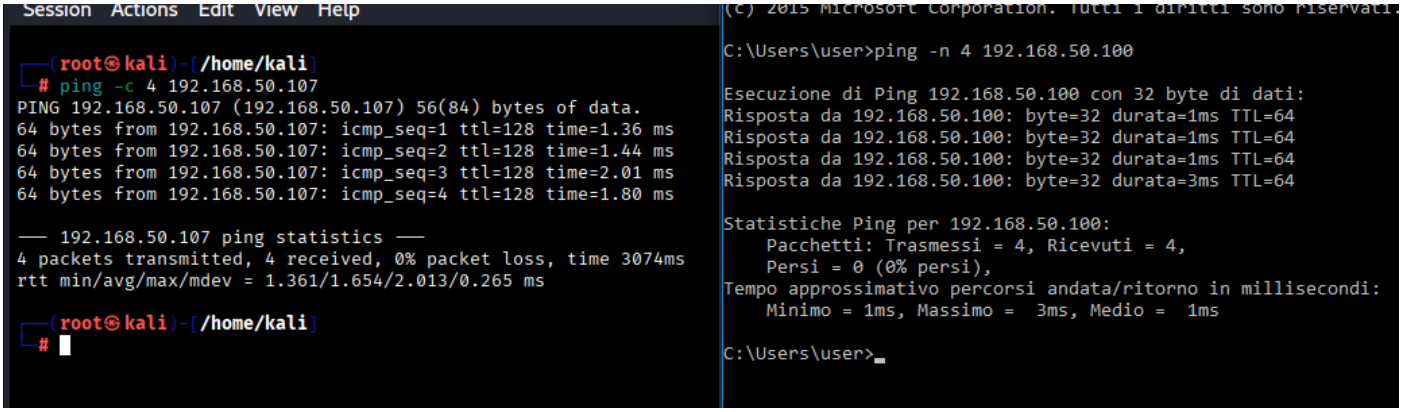
INDICE

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: il presente laboratorio analizza l'impatto del **Windows Defender Firewall** sull'esposizione dei servizi di rete di una macchina Windows raggiungibile dall'esterno. L'attività è stata svolta in un ambiente controllato composto da una macchina **Kali Linux**, utilizzata per effettuare le scansioni di rete, e una macchina **Windows 10**, configurata come sistema target.
Attraverso l'osservazione dei risultati delle scansioni prima e dopo l'attivazione del firewall, è stato possibile valutare come le politiche di filtraggio influenzino la visibilità delle porte e dei servizi esposti, nonché il processo di rilevamento dell'host da parte degli strumenti di analisi.

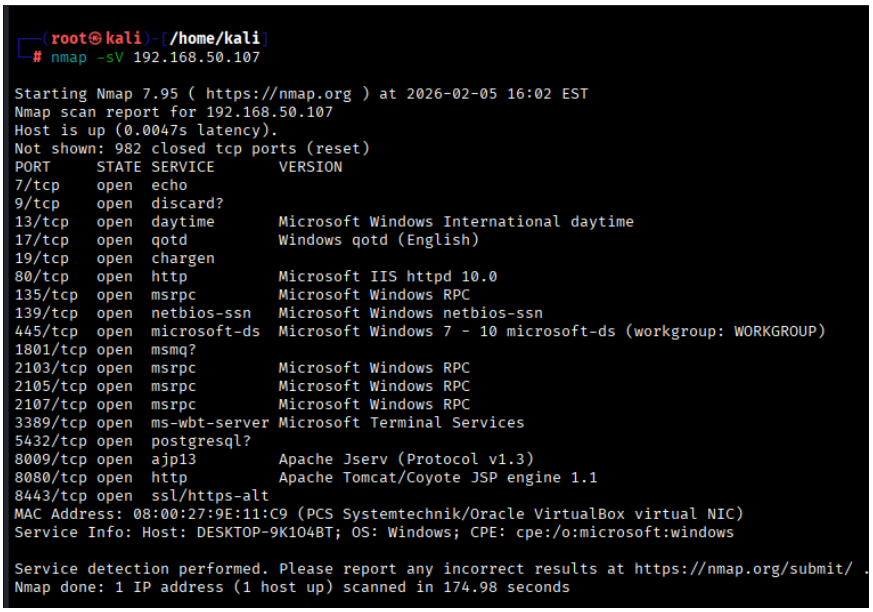
OBIETTIVO: verificare come l'attivazione del Windows Defender Firewall e il blocco del traffico ICMP incidano sui risultati di una scansione dei servizi di rete, evidenziando la riduzione della superficie d'attacco e la necessità di tecniche alternative di rilevamento quando l'host non risponde alle richieste di discovery.



Prima di procedere con l'analisi dei servizi di rete, è stata verificata la corretta connettività tra le due macchine.

La verifica ha confermato che risultano correttamente raggiungibili reciprocamente, senza perdita di pacchetti e con tempi di risposta stabili.

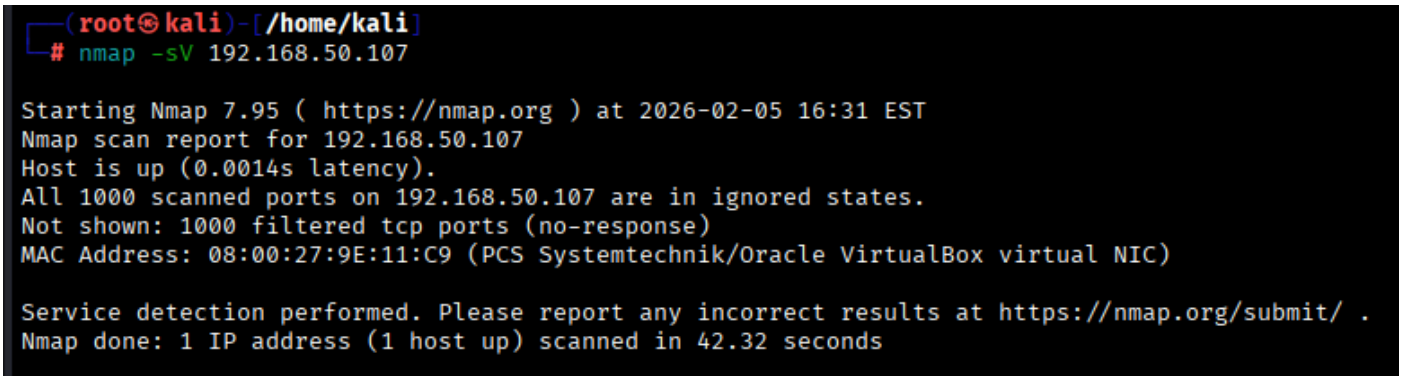
Questo passaggio è risultato fondamentale per assicurare che i risultati delle successive scansioni fossero influenzati esclusivamente dalla configurazione del firewall e non da problemi di rete o di instradamento.



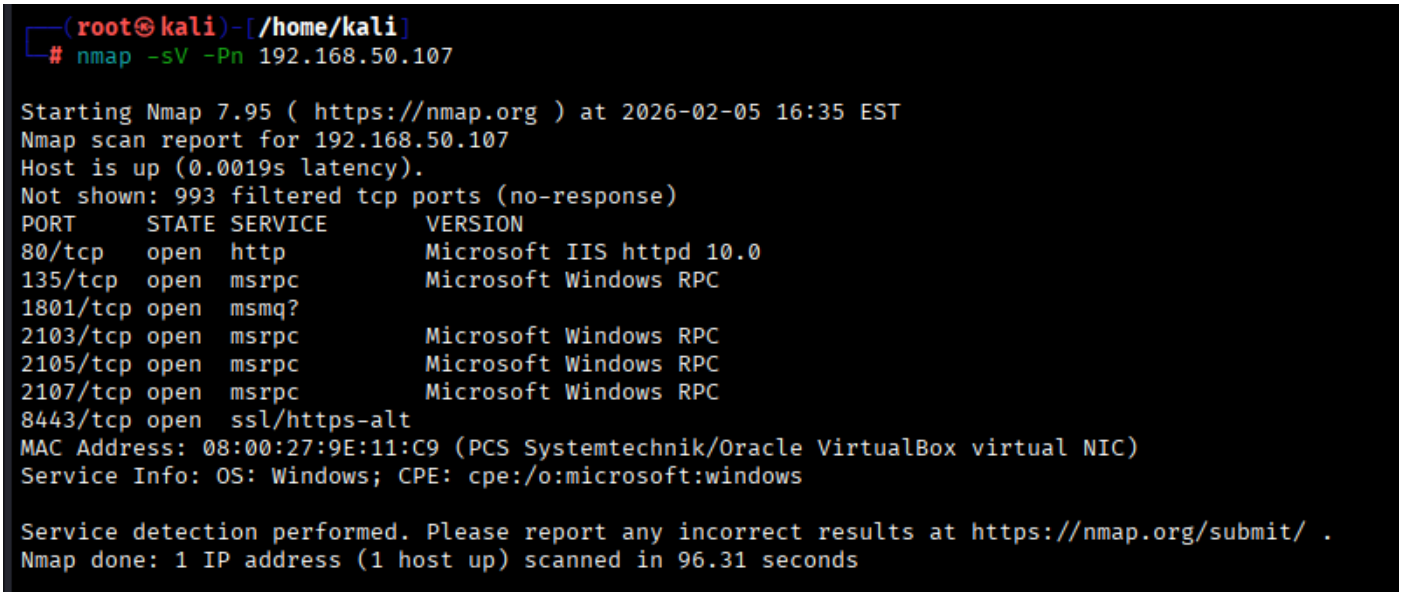
Con il Windows Defender Firewall disattivato, è stata effettuata una scansione dei servizi di rete della macchina Windows al fine di identificare le porte aperte e i servizi esposti. L'analisi ha evidenziato la presenza di numerosi servizi attivi, distribuiti su più porte TCP, inclusi servizi di rete di base, servizi di comunicazione remota e servizi web.

Il risultato della scansione mostra una superficie d'attacco ampia, caratterizzata da un'elevata visibilità dei servizi disponibili sulla macchina target.

In assenza di meccanismi di filtraggio attivi, il sistema risponde alle richieste di scansione fornendo informazioni dettagliate sui servizi in ascolto, facilitando le attività di enumerazione da parte di un potenziale attaccante.
Questa fase dell'analisi rappresenta lo scenario di riferimento iniziale, utile per confrontare in modo diretto l'efficacia delle misure di protezione introdotte successivamente tramite l'attivazione del firewall.



Dopo l'attivazione del Windows Defender Firewall sulla macchina Windows, è stata ripetuta la scansione dei servizi di rete.
A differenza dello scenario precedente, il sistema target non ha restituito informazioni sui servizi in ascolto, mostrando tutte le porte come filtrate e non rispondenti alle richieste di scansione.
Il risultato evidenzia come l'attivazione del firewall impedisca la rilevazione dei servizi di rete dall'esterno, bloccando il traffico in ingresso e limitando significativamente le informazioni ottenibili tramite attività di enumerazione.
Sebbene l'host risulti raggiungibile a livello di rete, l'assenza di risposte sulle porte scansionate indica l'efficacia delle regole di filtraggio nel mascherare i servizi attivi.
Questo confronto mette in evidenza il ruolo del firewall nella riduzione della superficie d'attacco del sistema, rendendo inaccessibili dall'esterno servizi che risultavano precedentemente visibili in assenza di protezioni attive.



Con il Windows Defender Firewall attivo, il sistema target risulta non rispondere alle richieste di rilevamento iniziale, indicando il blocco del traffico ICMP utilizzato per l'host discovery.
In questa condizione, una scansione standard non consente di individuare servizi esposti, facendo apparire l'host come non raggiungibile o completamente filtrato.
Forzando la scansione dei servizi senza affidarsi alla fase di discovery, è stato comunque possibile rilevare un numero limitato di porte aperte; i servizi individuati risultano significativamente inferiori rispetto allo scenario con firewall disattivato e sono riconducibili a servizi esplicitamente esposti o consentiti dalle regole di filtraggio.
Questa fase evidenzia come il firewall, pur non rendendo il sistema completamente invisibile, sia in grado di ridurre drasticamente le informazioni ottenibili dall'esterno.
Il blocco del traffico ICMP contribuisce a ostacolare le attività di enumerazione, mentre la visibilità residua dei servizi dipende dalle politiche di sicurezza applicate alle singole porte.

CONCLUSIONE

L’attività svolta ha evidenziato in modo chiaro l’impatto del Windows Defender Firewall sulla visibilità dei servizi di rete esposti da un sistema Windows.
Il confronto tra le scansioni effettuate con firewall disattivato e firewall attivato mostra come l’assenza di meccanismi di filtraggio consenta una completa enumerazione dei servizi disponibili, aumentando significativamente la superficie d’attacco del sistema.
L’attivazione del firewall riduce drasticamente le informazioni accessibili dall’esterno, filtrando il traffico in ingresso e mascherando i servizi attivi; ilù blocco del traffico ICMP contribuisce ulteriormente a ostacolare le attività di rilevamento iniziale dell’host, rendendo meno immediata l’individuazione del sistema in rete.
Tuttavia, l’analisi ha mostrato come alcuni servizi possano rimanere accessibili qualora esplicitamente consentiti dalle regole di sicurezza, confermando che il firewall non elimina il rischio ma lo riduce in modo significativo.
Nel complesso, l’esercizio dimostra come una corretta configurazione del firewall rappresenti una misura preventiva efficace per limitare l’esposizione dei servizi e ridurre le possibilità di attacco dall’esterno, evidenziando l’importanza di politiche di sicurezza adeguate anche in contesti di rete locali e controllati.