REPORT : Scansione dei servizi con NMAP
Introduzione e Scopo

Il report in questione ha lo scopo di presentare in modo strutturato i risultati delle attività di scansione di rete condotte con lo strumento Nmap. L'analisi si concentra su due sistemi target distinti, identificati come "**Metasploitable**" e "**Windows**", sui quali sono state eseguite diverse tipologie di scansione per la raccolta di informazioni. L'obiettivo principale è fornire una mappatura chiara e dettagliata della configurazione di rete dei sistemi, delle porte aperte e dei servizi esposti.

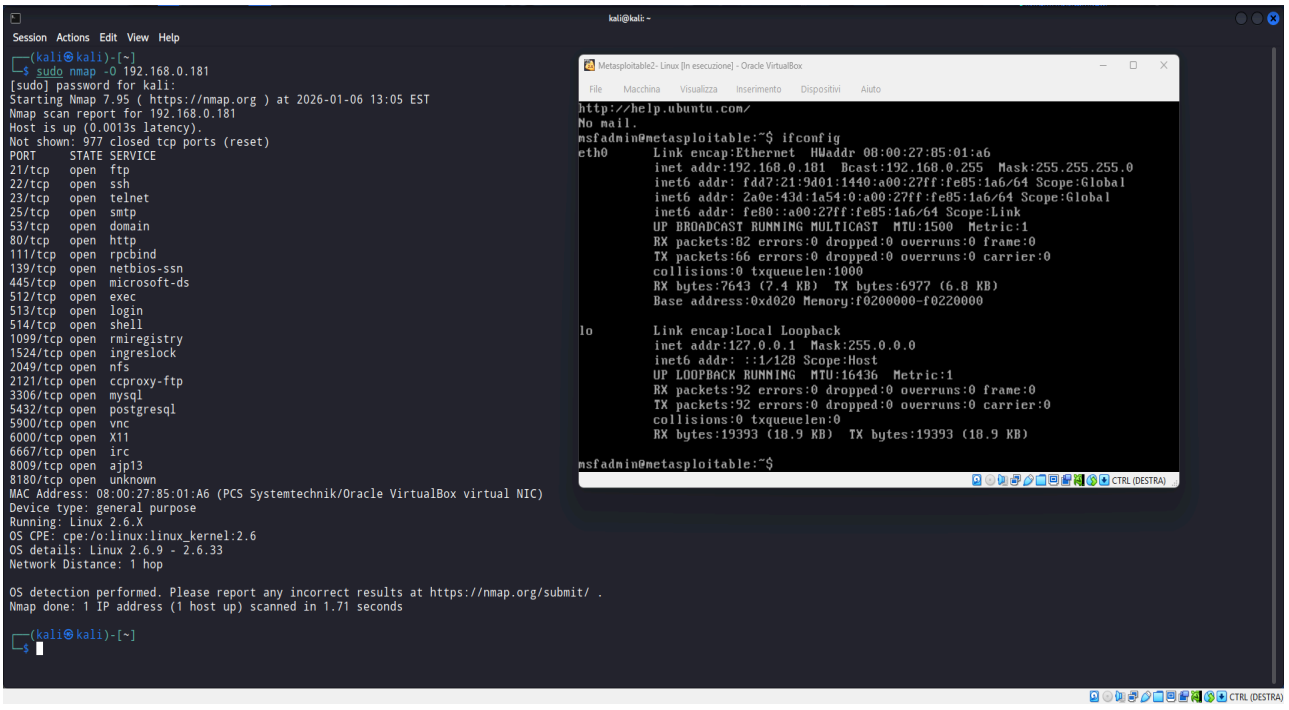
L'analisi procederà esaminando singolarmente ciascun target, iniziando con il sistema Metasploitable.

Analisi del Target 1: Metasploitable (192.168.0.181)

L'analisi del primo target si concentra sulla macchina virtuale **Metasploitable**, un sistema deliberatamente configurato con vulnerabilità note . L'importanza strategica di questa analisi risiede nell'identificare quella che è la sua configurazione di rete e la superficie d'attacco esposta, elementi fondamentali per comprendere le potenziali vie di accesso per un utente.

Identificazione dell'Host e del Sistema Operativo

La scansione iniziale di tipo ***OS fingerprinting*** ha permesso di raccogliere le informazioni fondamentali per l'identificazione univoca dell'host e del suo sistema operativo. I dati chiave emersi sono i seguenti:



Confronto tra Scansioni Porte: SYN Scan vs. TCP Connect

Per l'analisi approfondita della superficie di attacco esposta dal sistema, sono state impiegate due metodologie distinte e complementari di **port scanning**, finalizzate all'identificazione delle porte **TCP** (Transmission Control Protocol) attive e in ascolto. Nello specifico, la ricognizione è stata eseguita tramite una **SYN Scan** (nota anche come half-open scanning) e una **TCP Connect Scan** (o full-open scanning).

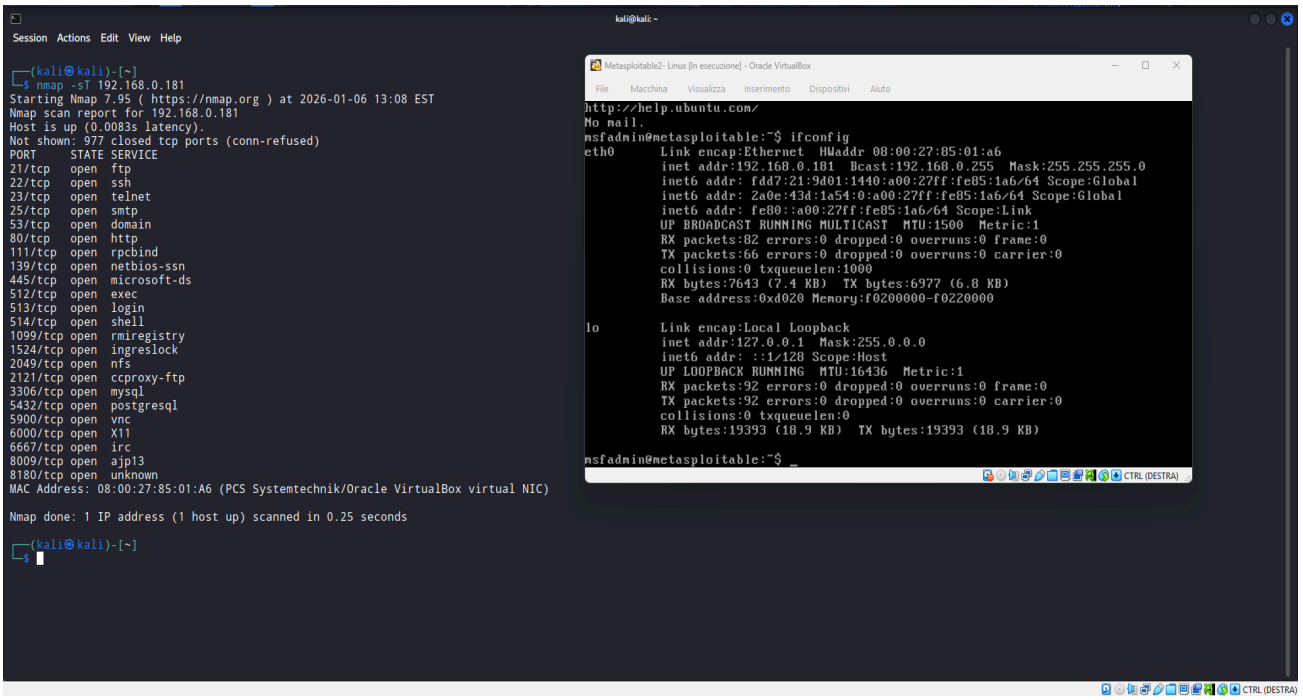
La **SYN Scan** sfrutta l'invio di pacchetti **SYN** (Synchronize) per avviare l'handshake TCP, ma, in caso di risposta **SYN/ACK** (indizio di porta aperta), interrompe immediatamente la procedura inviando un pacchetto **RST** (Reset) anziché completare l'handshake con l'ACK finale. Questo approccio è spesso preferito per la sua rapidità e per la minore "rumorosità" sui *log* di sistema, agendo in modo più furtivo.

La **TCP Connect Scan** è invece un metodo più diretto che tenta di stabilire una connessione TCP completa e tridirezionale (**SYN -> SYN/ACK -> ACK**). Questo tipo di scansione, pur essendo meno discreta e più facilmente rilevabile da sistemi di sicurezza, è considerato il più affidabile in termini di verifica dello stato di una porta, poiché simula esattamente il comportamento di un'applicazione client legittima.

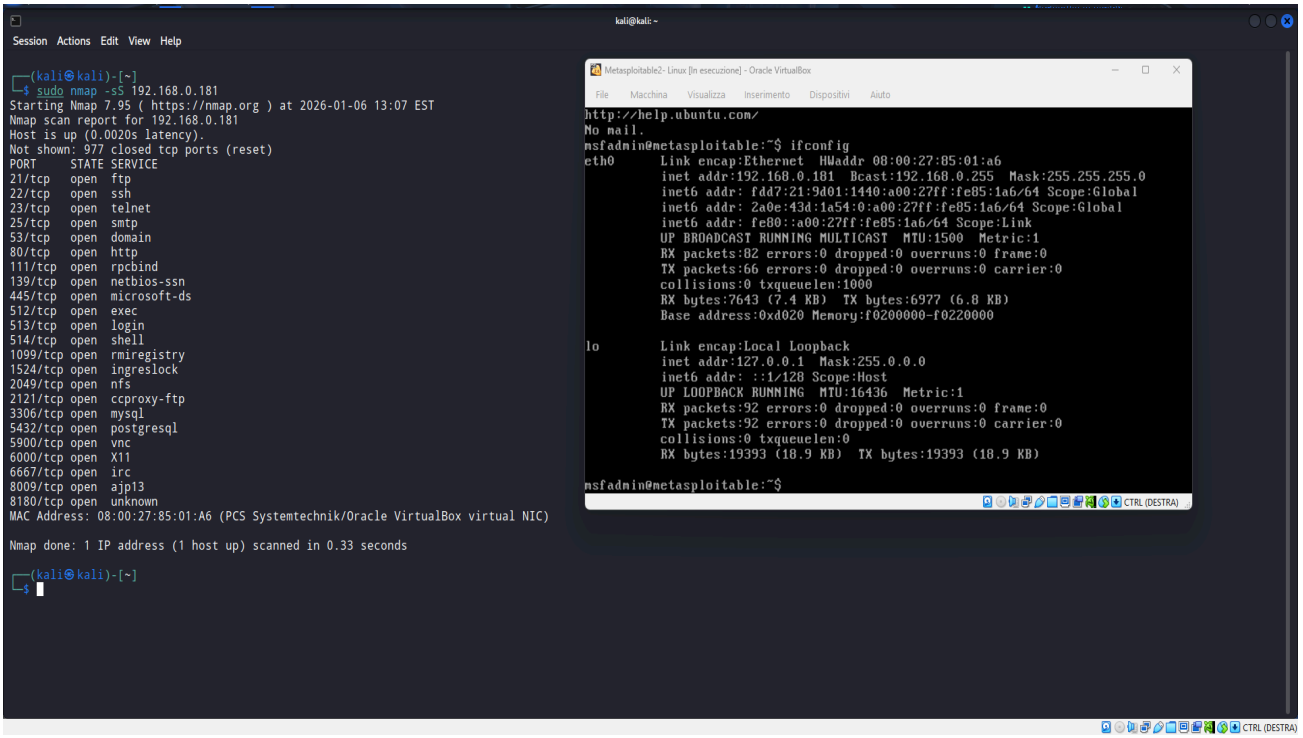
Il confronto dei risultati ottenuti da queste due diverse tecniche di scansione ha prodotto un dato significativo: **entrambe le tecniche hanno identificato lo stesso identico set di porte aperte**. Non si è riscontrata alcuna differenza, nemmeno minima, tra l'elenco delle porte individuate dalla **SYNScan** e quello prodotto dalla **TCP Connect Scan**.

In altre parole, se fossero presenti meccanismi di sicurezza attivi in grado di monitorare lo stato delle connessioni (come un firewall stateful), ci si aspetterebbe che la **SYN Scan**, data la sua natura incompleta, venisse trattata in modo differente (ad esempio bloccata o ignorata) rispetto alla **TCP Connect Scan,** alterando potenzialmente i risultati. La perfetta sovrapposizione dei set di porte conferma, pertanto, che il traffico di scansione è stato trattato in modo indifferenziato dal sistema bersaglio o dai dispositivi di sicurezza di rete intermedi.

TCP SCAN:

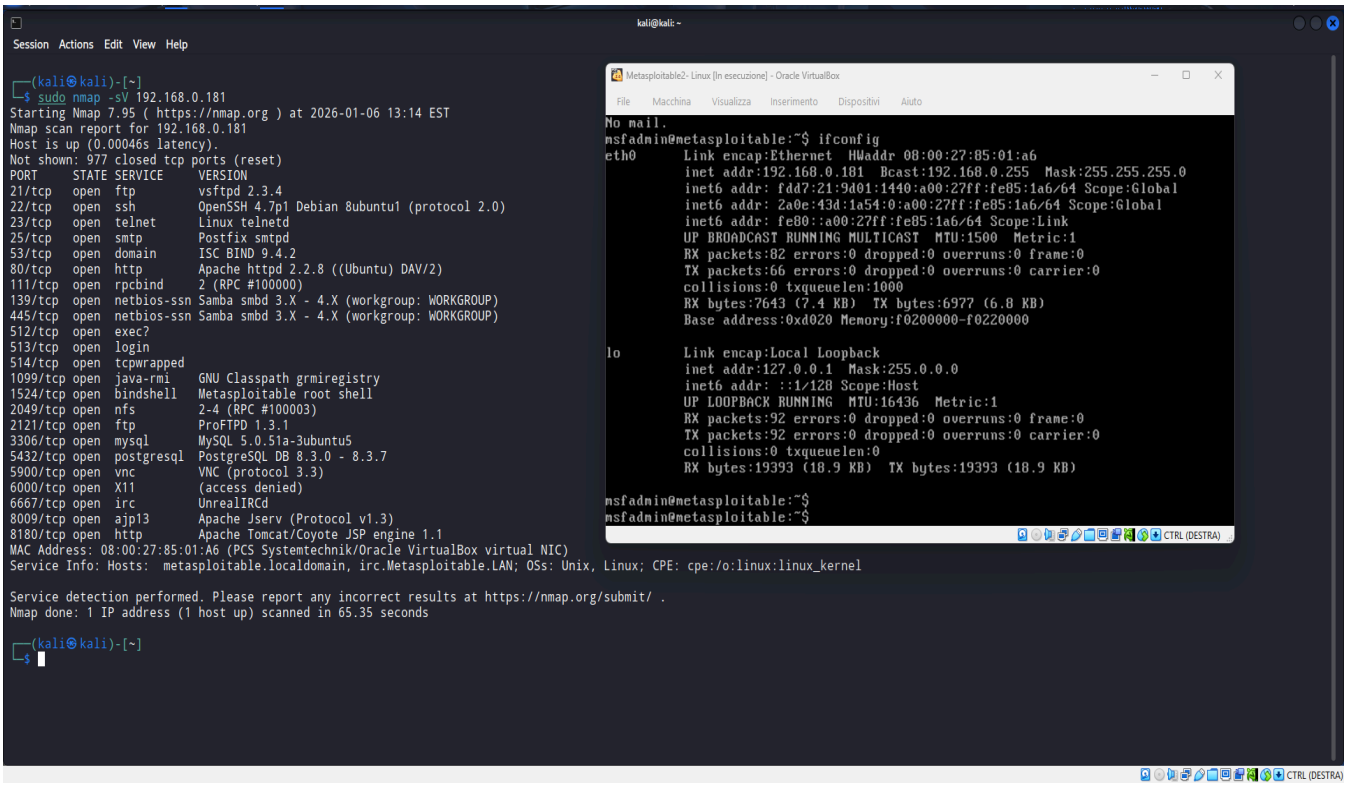


SYN SCAN:



Analisi dei Servizi e delle Versioni

La scansione di rilevamento delle versioni (`Version detection`) fornisce le informazioni più significative, associando a ogni porta aperta uno specifico servizio software e, dove possibile, la sua esatta versione. Questa informazione è cruciale per la successiva fase di ricerca di vulnerabilità note. I risultati di tale scansione sono catalogati nella tabella sottostante.



Dall'analisi emergono diverse criticità di sicurezza che richiedono attenzione immediata. La presenza di un servizio di `Metasploitable root shell` sulla porta 1524 rappresenta un'esposizione diretta e non autenticata al sistema con i massimi privilegi. Inoltre, il servizio `vsftpd 2.3.4` è una versione notoriamente vulnerabile a un backdoor, che consente l'esecuzione di comandi remoti. Infine, la presenza di software datati come `OpenSSH 4.7p1` e `Apache httpd 2.2.8` introduce ulteriori rischi, poiché queste versioni sono affette da multiple vulnerabilità pubblicamente note.

Analisi del Target 2: Windows (192.168.0.230)

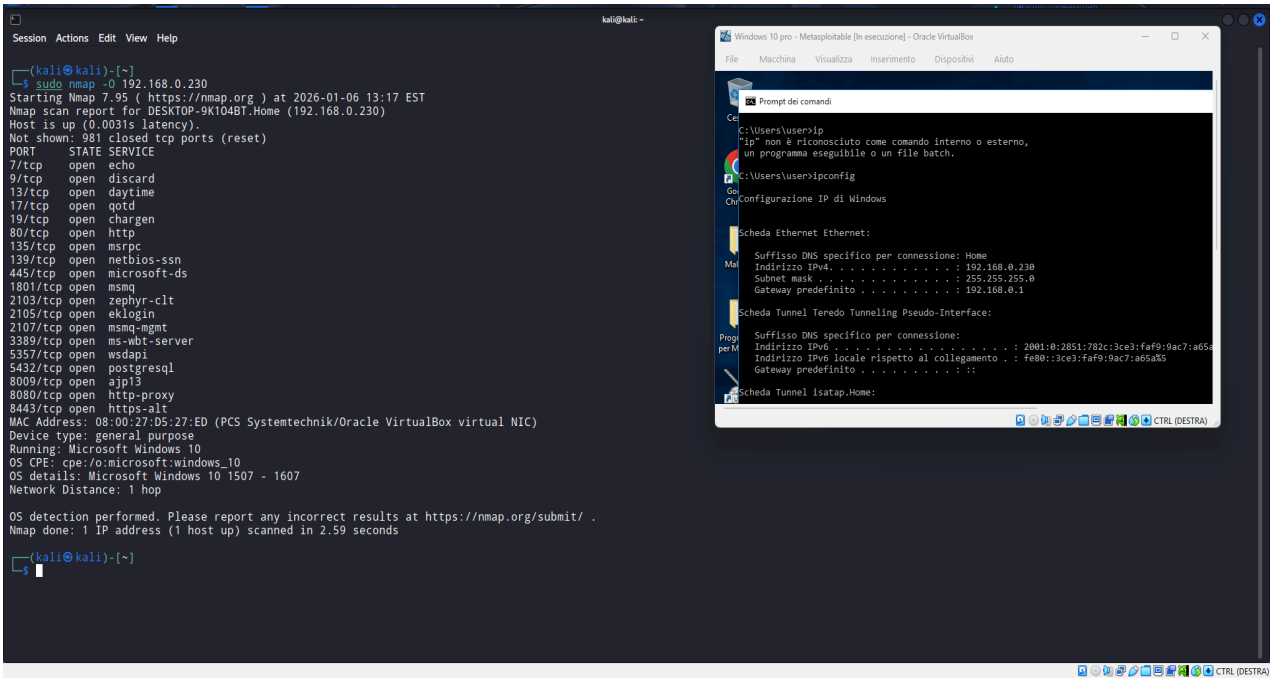
L'analisi si sposta ora sul secondo target identificato nella rete, una macchina con indirizzo IP **`192.168.0.230`**. Per questo host, l'obiettivo dell'attività era l'identificazione del sistema operativo e la mappatura delle porte aperte.

3.1 Identificazione dell'Host e del Sistema Operativo

La scansione **OS fingerprinting** ha fornito le seguenti informazioni identificative per l'host:

- **Indirizzo IP:** `192.168.0.230`
- **Hostname:** `DESKTOP-9K1048T.Home`
- **Indirizzo MAC:** `08:00:27:DE:27:ED`
- **Produttore Scheda di Rete:** PCS Systemtechnik/Oracle VirtualBox virtual NIC
- **Sistema Operativo Rilevato:** Microsoft Windows 10 (versione stimata `1507 - 1607`).

OS fingerprinting



La scansione ha identificato il tipo di sistema operativo e un set di porte TCP aperte sull'host Windows.

Conclusioni

La scansione di rete ha delineato chiaramente la situazione della sicurezza dei sistemi esaminati. I principali riscontri sono:

1. È stata ottenuta una corretta identificazione di entrambi i sistemi target: una macchina **Linux (Metasploitable)** e una macchina **Microsoft Windows 10**.
2. Per il sistema Metasploitable, la mappatura dei servizi ha rivelato una postura di sicurezza estremamente critica. La presenza di servizi critici come una **root shell remota** (porta 1524), versioni di software **notoriamente vulnerabili** (es. vsftpd 2.3.4) e protocolli di gestione **non cifrati** (Telnet) contribuisce a una superficie d'attacco eccezionalmente ampia e a rischio elevato.
3. Il confronto tra le scansioni di tipo **SYN e TCP Connect** sul target ha confermato che entrambe le metodologie hanno prodotto **risultati identici**, suggerendo l'assenza di meccanismi di filtraggio di base sulla rete.