Scansione dei servizi con Nmap – Pratica S5/L2

1. Introduzione

L'esercitazione ha avuto come obiettivo l'analisi dei servizi esposti da sistemi target mediante l'utilizzo dello strumento Nmap, al fine di identificare il sistema operativo, le porte aperte e i servizi in ascolto. L'attività si colloca nella fase di reconnaissance e service enumeration di un penetration test.

2. Ambiente di laboratorio

L'ambiente di laboratorio è stato realizzato su piattaforma **Oracle VirtualBox** e comprende più macchine virtuali configurate all'interno di un contesto di rete controllato.
La macchina **Kali Linux** è utilizzata per l'esecuzione delle attività di scansione, mentre **Metasploitable2** e una macchina virtuale **Windows** rappresentano i sistemi target oggetto dell'esercitazione. È inoltre presente un sistema **pfSense**, mantenuto da un precedente laboratorio e utilizzato esclusivamente come router per consentire alla macchina Kali Linux l'accesso a Internet; tale sistema non è coinvolto nelle attività di scansione previste dall'esercitazione.

Le macchine virtuali risultano configurate all'interno dello stesso segmento di rete locale, consentendo la comunicazione tra Kali Linux e i sistemi target.

Configurazione di rete e indirizzamento IP

Sistema	Indirizzo IP	Subnet
Kali Linux	192.168.50.151	/24
Metasploitable2	192.168.50.101	/24
Windows 10	192.168.50.153	/24
Pfsense	192.168.50.1	/24

3. Attività di scansione

Le attività di scansione sono state effettuate utilizzando lo strumento **Nmap**, applicando differenti tecniche con l'obiettivo di identificare il sistema operativo dei target, le porte aperte e i servizi in ascolto.
Le scansioni sono state eseguite dalla macchina Kali Linux nei confronti dei sistemi target presenti nel segmento di rete locale.

Le tecniche adottate includono:

- OS Fingerprinting
- SYN Scan
- TCP Connect Scan
- Version Detection

Nei paragrafi seguenti vengono descritti i comandi utilizzati e i risultati ottenuti per ciascun target.

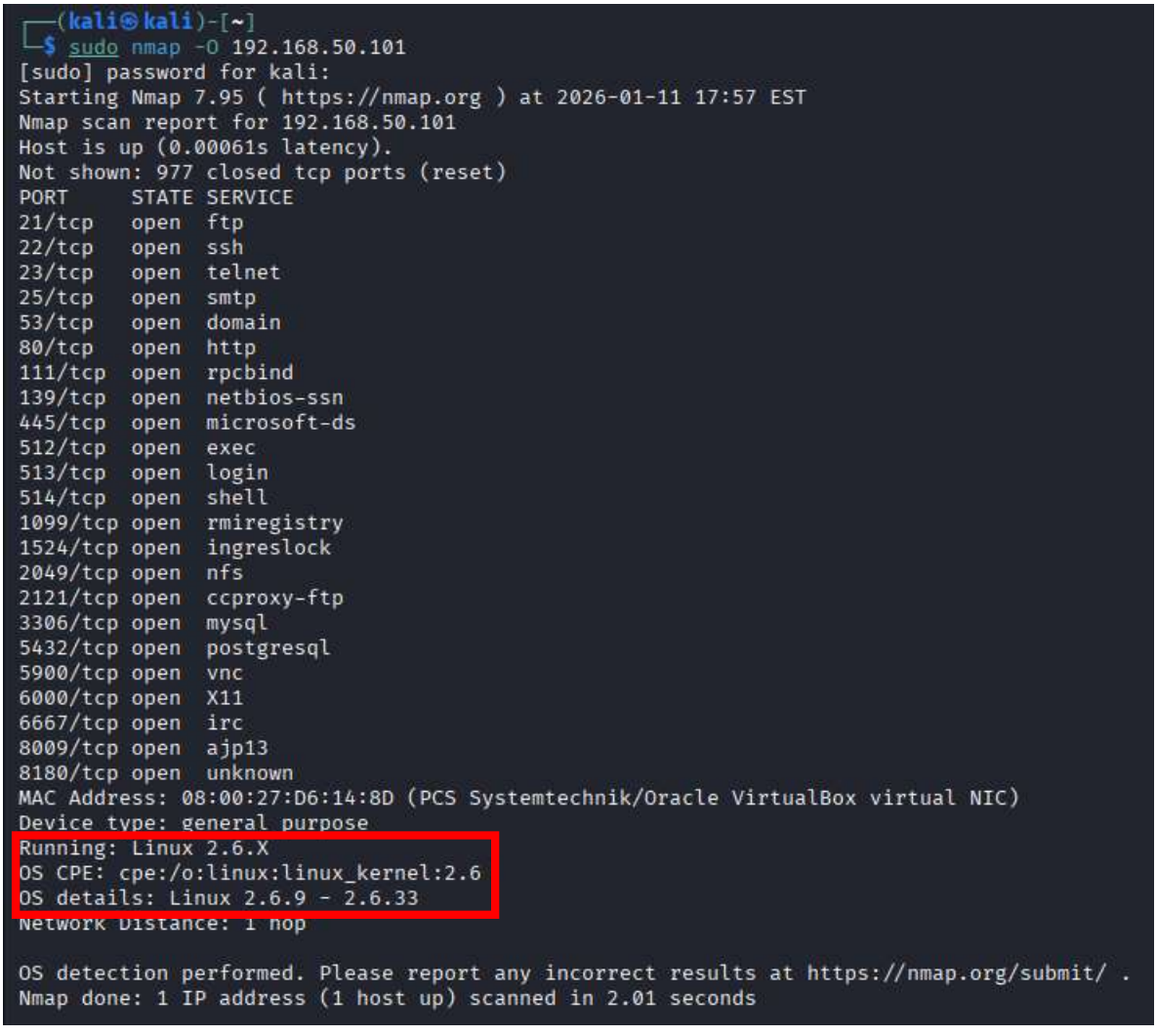
3.1 OS Fingerprinting – Target Metasploitable2

Per l'identificazione del sistema operativo del target Metasploitable2 è stata utilizzata la funzionalità di **OS fingerprinting** di Nmap, che consente di stimare il sistema operativo analizzando il comportamento dello stack TCP/IP del target.

Il comando utilizzato è il seguente:

sudo nmap -O 192.168.50.101

Di seguito è riportato l'output ottenuto dall'esecuzione del comando sulla macchina Kali Linux:

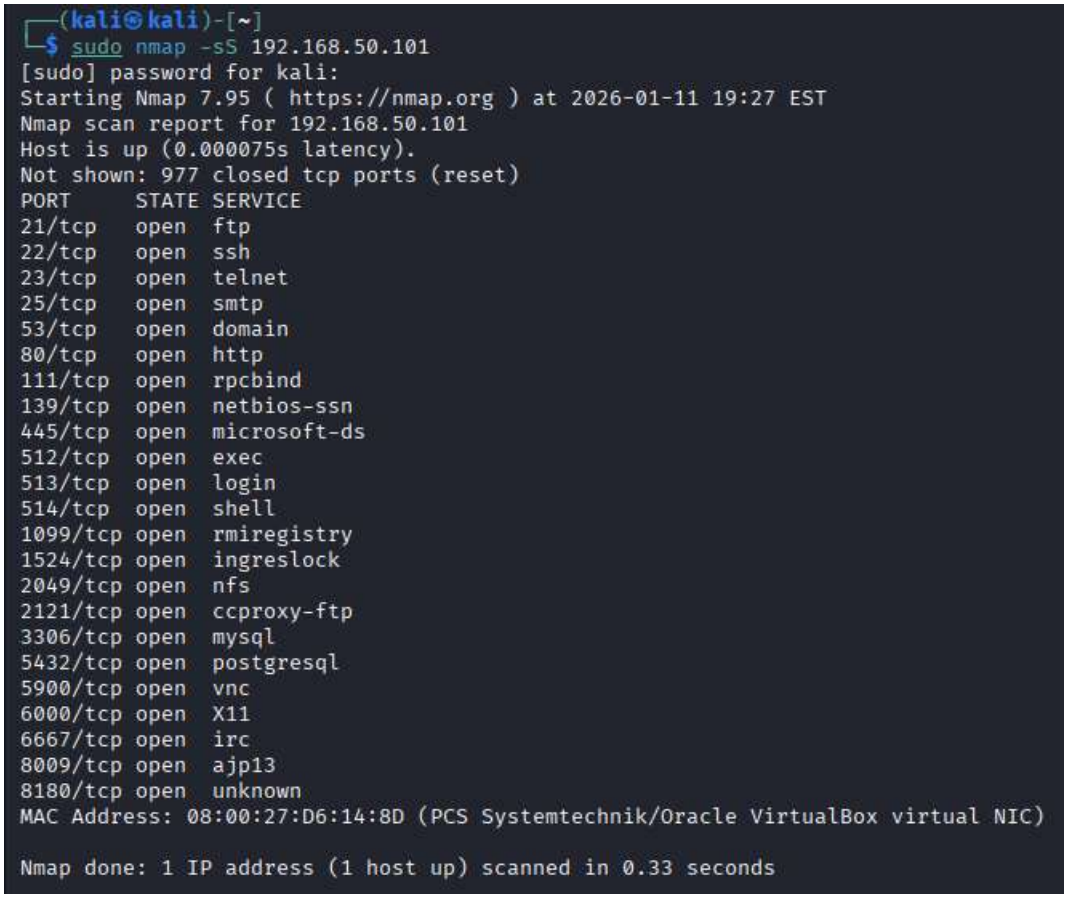


Dall'analisi dell'output è possibile stimare che il sistema operativo del target sia un **Linux con kernel 2.6.x**, con un intervallo di versione compreso tra **2.6.9 e 2.6.33**. L'identificazione è basata su tecniche di fingerprinting attivo e deve essere considerata una stima probabilistica.

Il comando utilizzato è il seguente:

sudo nmap -sS 192.168.50.101

Di seguito è riportato l'output ottenuto dall'esecuzione del comando sulla macchina Kali Linux:



La scansione ha evidenziato la presenza di numerose porte TCP aperte e relativi servizi in ascolto, confermando l'ampia superficie di attacco del sistema Metasploitable2.
L'utilizzo della SYN scan consente di ottenere tali informazioni senza completare il three-way handshake TCP, rendendo la tecnica meno invasiva e più discreta rispetto a una TCP Connect scan.

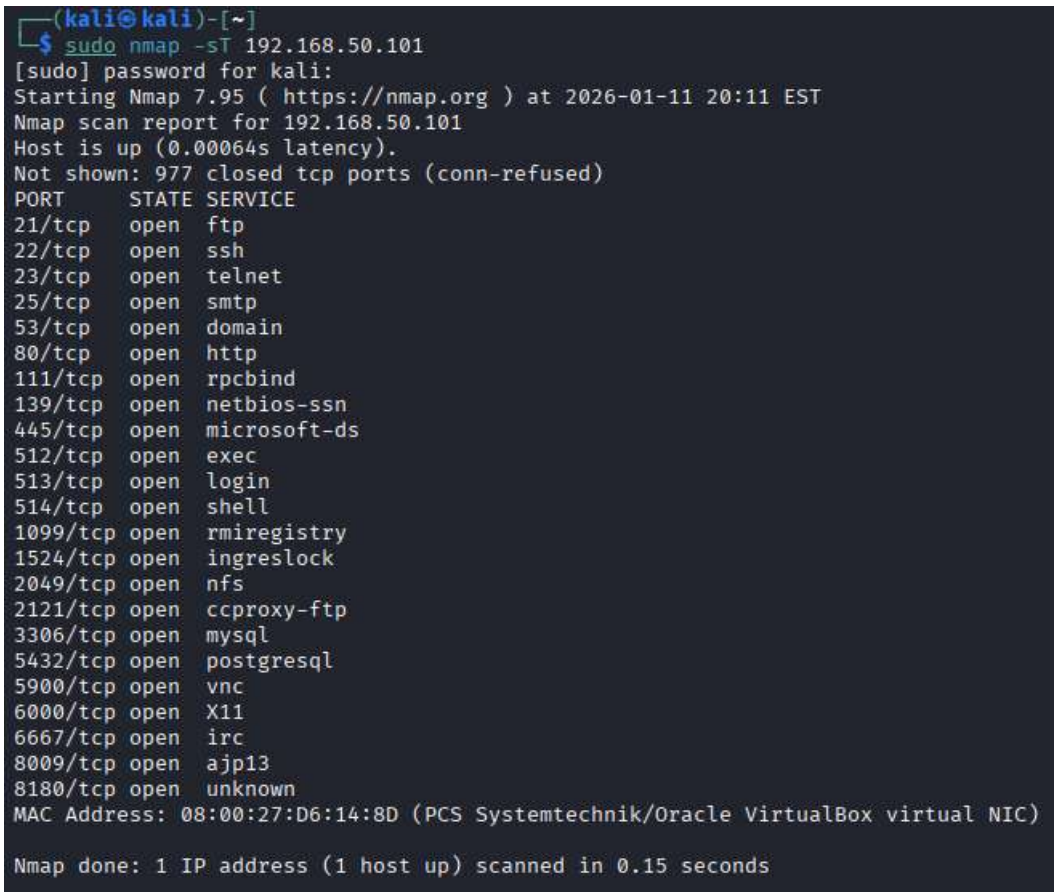
3.3 TCP Connect Scan – Target Metasploitable2

Al fine di confrontare i risultati ottenuti con la SYN scan, è stata eseguita una **TCP Connect Scan**, tecnica che utilizza la chiamata di sistema connect() per stabilire una connessione TCP completa con il target.

Il comando utilizzato è il seguente:

sudo nmap -sT 192.168.50.101

Di seguito è riportato l'output ottenuto dall'esecuzione del comando sulla macchina Kali Linux:



La TCP Connect scan ha restituito un elenco di porte aperte e servizi in ascolto sovrapponibile a quanto rilevato tramite SYN scan. La differenza principale risiede nel comportamento della scansione, che in questo caso completa il **three-way handshake TCP**, risultando più invasiva e maggiormente rilevabile dal sistema target.

Confronto tra SYN Scan e TCP Connect Scan

I risultati ottenuti tramite TCP Connect scan risultano **coerenti e sovrapponibili** a quelli emersi dalla precedente SYN scan in termini di porte aperte e servizi individuati. Tuttavia, le due tecniche presentano differenze significative dal punto di vista operativo: mentre la **SYN scan non completa il three-way handshake TCP** e risulta quindi più discreta e meno facilmente rilevabile, la **TCP Connect scan stabilisce una connessione completa con il target**, rendendola più invasiva e maggiormente soggetta a logging.
La scelta tra le due tecniche dipende dal contesto operativo e dal livello di privilegio disponibile sul sistema di scansione.

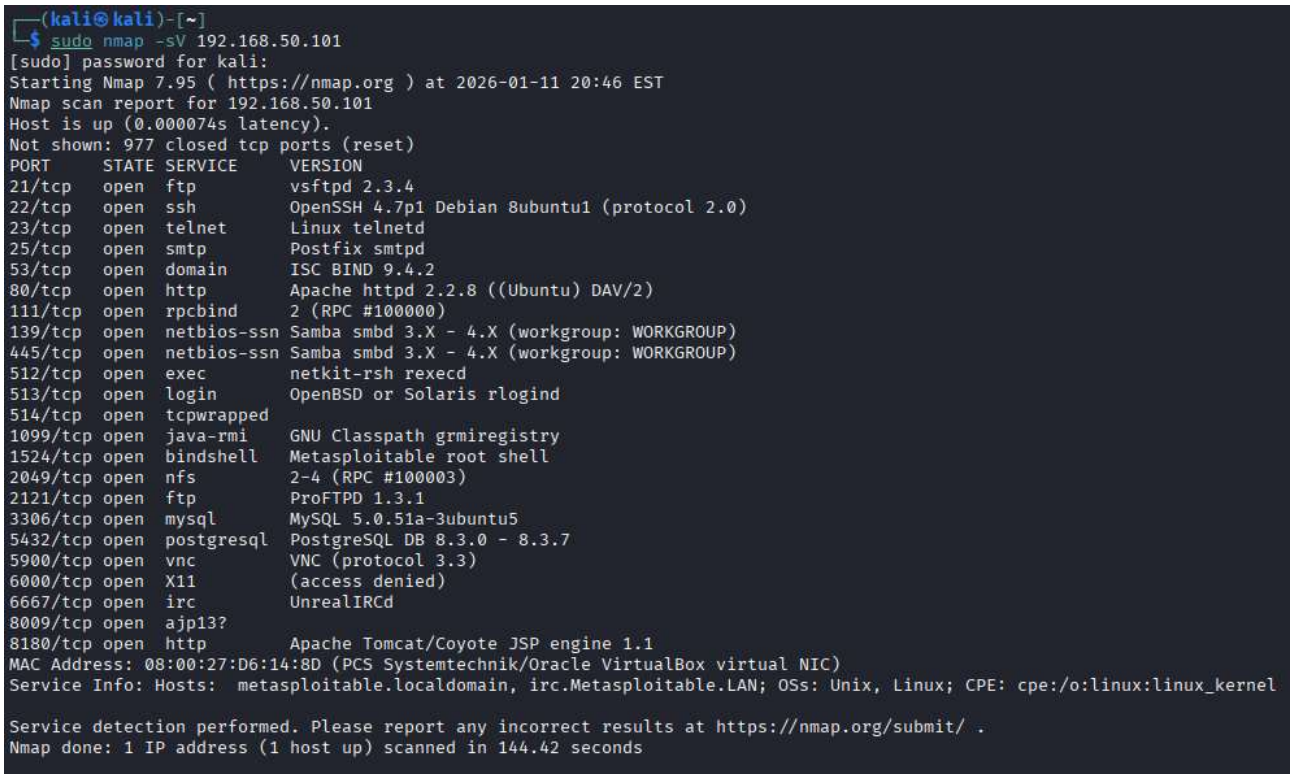
3.4 Version Detection – Target Metasploitable2

Per identificare i servizi in ascolto e le relative versioni applicative sul target Metasploitable2 è stata eseguita una **Version Detection**, tecnica che consente a Nmap di interrogare attivamente i servizi individuati sulle porte aperte e di analizzarne i banner di risposta.

Il comando utilizzato è il seguente:

sudo nmap -sV 192.168.50.101

Di seguito è riportato l'output ottenuto dall'esecuzione del comando sulla macchina Kali Linux:



La Version Detection ha consentito di identificare in modo dettagliato i servizi in esecuzione e le relative versioni software, evidenziando la presenza di numerosi servizi obsoleti e intenzionalmente vulnerabili. Le informazioni ottenute risultano particolarmente rilevanti in quanto permettono di correlare i servizi individuati a potenziali vulnerabilità note, rappresentando un passaggio fondamentale per le successive fasi di vulnerability assessment.

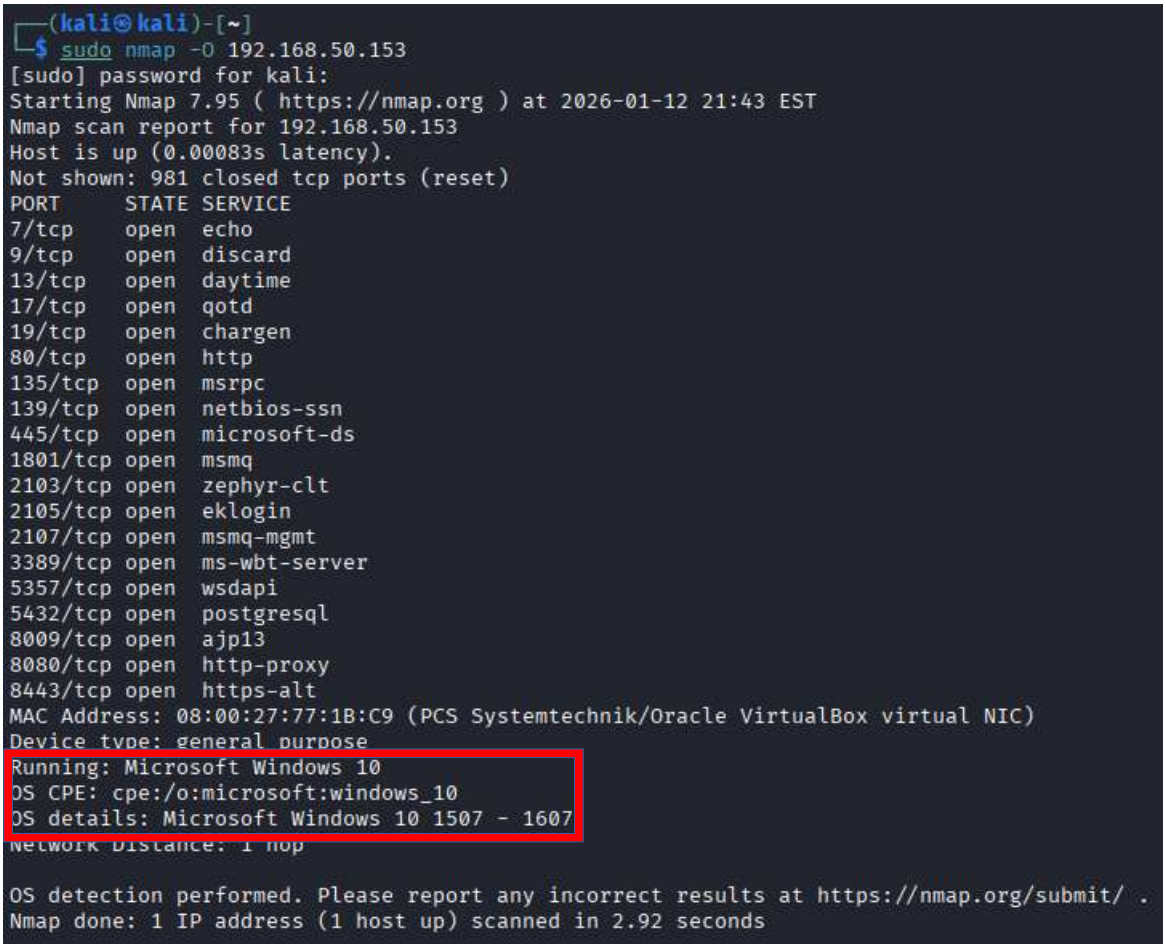
3.5 OS Fingerprinting – Target Windows

Per l'identificazione del sistema operativo del target Windows è stata eseguita una scansione di **OS fingerprinting** tramite Nmap, al fine di stimare il sistema operativo in esecuzione analizzando il comportamento dello stack TCP/IP.

Il comando utilizzato è il seguente:

sudo nmap -O 192.168.50.153

Di seguito è riportato l'output ottenuto dall'esecuzione del comando sulla macchina Kali Linux:



L'OS fingerprinting ha consentito di identificare il sistema target come **Microsoft Windows 10**, con una stima di versione compresa tra **1507 e 1607**.

Come per le precedenti scansioni, il risultato deve essere interpretato come una stima basata su tecniche di fingerprinting attivo, la cui accuratezza dipende dai servizi esposti e dalla configurazione del sistema.

4. Conclusioni

L’attività di laboratorio ha permesso di applicare le principali tecniche di scansione offerte da Nmap, consentendo l’identificazione dei sistemi operativi, delle porte aperte e dei servizi in ascolto sui target analizzati.
Le scansioni SYN e TCP Connect hanno prodotto risultati equivalenti in termini di porte rilevate, evidenziando come le differenze tra le tecniche siano principalmente di natura operativa.
La Version Detection ha fornito informazioni dettagliate sui servizi e sulle versioni applicative, risultando fondamentale per una corretta valutazione della superficie di attacco.