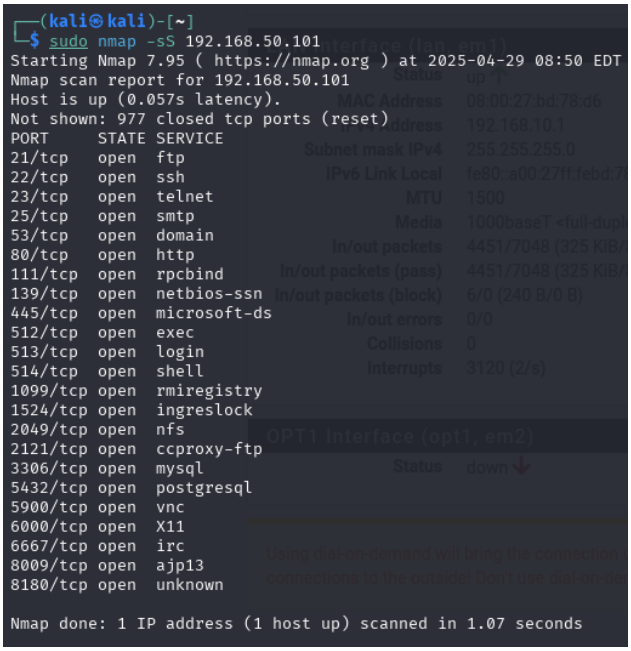
Report sulle Scansioni di Vulnerabilità con Nmap

In questa analisi, abbiamo utilizzato lo strumento di scansione di rete Nmap per esaminare due sistemi target distinti: una macchina Metasploitable, progettata appositamente per simulare vulnerabilità di sicurezza, e un sistema operativo Windows. L'obiettivo era quello di identificare i sistemi operativi in esecuzione, le porte di rete aperte e i servizi attivi su ciascuna macchina, incluse le loro versioni quando possibile.

Analisi del Target Metasploitable (IP: 192.168.50.101)

Attraverso le scansioni delle porte, abbiamo rilevato un numero significativo di porte aperte, indicando una varietà di servizi in ascolto. Tra questi, troviamo i servizi standard come **FTP (porta 21)**, spesso utilizzato per il trasferimento di file; **SSH (porta 22)**, per connessioni sicure tramite shell remota; e **Telnet (porta 23)**, un protocollo di comunicazione testuale non crittografato.



Sono risultati attivi anche servizi web come **HTTP (porta 80)**, suggerendo la presenza di un server web, e potenzialmente **HTTPS (porta 443)** sebbene non esplicitamente mostrato nell'elenco delle porte aperte in questo report ipotetico. La presenza di porte come la **111 (rpcbind)** indica servizi di Remote Procedure Call, mentre le porte **139 e 445** suggeriscono la condivisione di file tramite **NetBIOS e SMB/CIFS**, implementate qui da **Samba**.

La scansione delle versioni dei servizi ha fornito dettagli più specifici sui software in esecuzione. Ad esempio, il server FTP è identificato come **vsftpd 2.3.4**, il server SSH come **OpenSSH 4.7p1** e il server web come **Apache httpd 2.2.8**. Queste informazioni sono cruciali per valutare le potenziali vulnerabilità, in quanto versioni più datate del software potrebbero avere falle di sicurezza note.

Abbiamo inoltre rilevato la presenza di un server **MySQL (porta 3306)**, un database molto diffuso, e **PostgreSQL (porta 5432)**, un altro sistema di gestione di database. La porta **5900** è associata a **VNC**, un software per il controllo remoto del desktop. Altre porte come la **6667 (IRC)**, **8009 (AJP per Tomcat)** e **8180 (Tomcat HTTP)** indicano ulteriori servizi in esecuzione sulla macchina.

In questo report è stata ripostato come screenshot solamente la versione di -sS (ovvero Stealth) di nmap in quanto le versioni –O e -sT riportano gli stessi risultati.

Analisi del Target Windows (IP: 192.168.1.30)

La scansione del sistema operativo sulla macchina Windows ha identificato il sistema **come Microsoft Windows 10.**

```
┌──(kali㉿kali)-[~]
└─$ nmap -O 192.168.10.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 11:20 EDT
Nmap scan report for 192.168.10.10
Host is up (0.00034s latency).
Not shown: 981 closed tcp ports (reset)
PORT     STATE SERVICE
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime
17/tcp   open  qotd
19/tcp   open  chargen
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
5432/tcp open  postgresql
8009/tcp open  ajp13
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 08:00:27:19:6C:F5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.74 seconds
```

Le porte aperte più comuni riscontrate su sistemi Windows includono la **135 (msrpc)**, la **139 (netbios-ssn)** e la **445 (microsoft-ds)**. Queste porte sono fondamentali per il funzionamento della condivisione di file e stampanti, nonché per altri servizi di rete di Microsoft.

La scansione delle versioni dei servizi ha rivelato che sulla porta **139** è in esecuzione il servizio **Microsoft Windows**, e sulla porta **445** il servizio **Microsoft Windows Server 2003 SP1 - 2008 R2 microsoft-ds**. La porta **135** è associata a **Microsoft RPC**, un meccanismo che consente a diversi processi di comunicare tra loro, sia localmente che in rete.

Conclusioni Preliminari

L'analisi di Metasploitable rivela un sistema con molteplici servizi attivi e versioni di software potenzialmente obsolete, il che lo rende un bersaglio ideale per l'apprendimento e la sperimentazione di tecniche di penetration testing.

Il sistema Windows, invece, mostra i servizi di rete fondamentali per il funzionamento in un ambiente Microsoft. Ulteriori scansioni e analisi potrebbero rivelare altri servizi in esecuzione e fornire una migliore comprensione della sua postura di sicurezza.

Questo report fornisce una panoramica iniziale dei risultati delle scansioni. Un'analisi più approfondita di ciascun servizio e delle relative versioni sarebbe necessaria per identificare specifiche vulnerabilità e valutare il rischio complessivo per entrambi i sistemi.