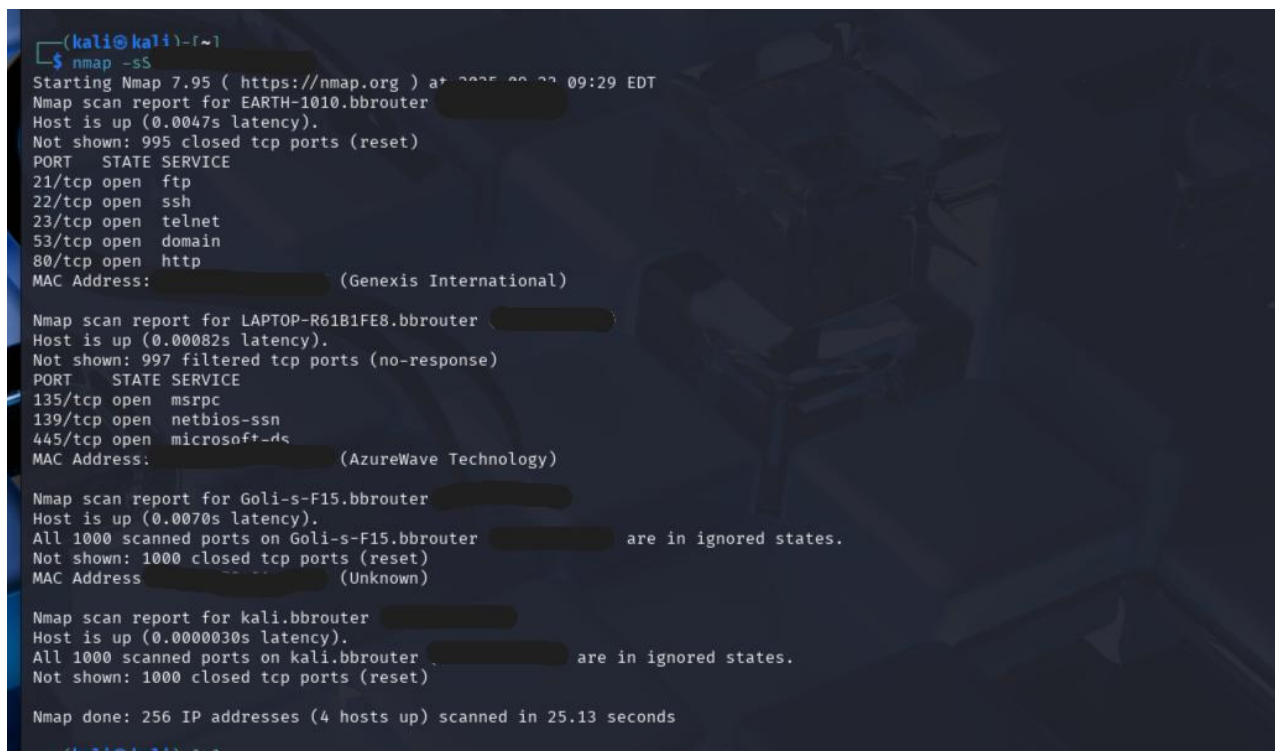


Elevate labs – Task 1



```
(kali@kali) ~  
$ nmap -sS  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-22 09:29 EDT  
Nmap scan report for EARTH-1010.bbrouter  
Host is up (0.0047s latency).  
Not shown: 995 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
53/tcp    open  domain  
80/tcp    open  http  
MAC Address: (Genexis International)  
  
Nmap scan report for LAPTOP-R61B1FE8.bbrouter  
Host is up (0.00082s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
MAC Address: (AzureWave Technology)  
  
Nmap scan report for Goli-s-F15.bbrouter  
Host is up (0.0070s latency).  
All 1000 scanned ports on Goli-s-F15.bbrouter are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
MAC Address (Unknown)  
  
Nmap scan report for kali.bbrouter  
Host is up (0.0000030s latency).  
All 1000 scanned ports on kali.bbrouter are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 25.13 seconds  
(kali@kali) ~
```

Assignment: Nmap Scan Output Analysis

The attached image is a screenshot of a terminal window in Kali Linux, showing the output of an Nmap SYN scan (nmap -sS). This scan was conducted over a local network to enumerate active hosts and identify their open ports and running services.

Key Details:

- Tool Used: Nmap 7.95
- Scan Type: SYN scan (stealth scan), initiated using the -sS option.

Here are the open ports and potential risks

1. FTP (Port 21):

- **Risk:** FTP transmits data, including credentials, in plaintext. Attackers can intercept sensitive information via sniffing. FTP is also commonly targeted for brute-force attacks and buffer overflow exploits.
- **Mitigation:** Use SFTP or FTPS for secure file transfer, disable if not needed.

2. SSH (Port 22):

- **Risk:** While generally secure, exposed SSH ports can be brute-forced if weak passwords are used, or exploited if the service is misconfigured or running outdated versions.
- **Mitigation:** Use key-based authentication, disable root login, change the default port, and enforce strong password policies.

3. Telnet (Port 23):

- **Risk:** Like FTP, Telnet transmits data in plaintext. It is highly insecure and susceptible to sniffing and Man-in-the-Middle (MitM) attacks. Attackers can gain complete shell access if they compromise credentials.
- **Mitigation:** Replace Telnet with SSH, and disable if not absolutely required.

4. DNS (Port 53):

- **Risk:** DNS servers can be abused for DNS amplification attacks, cache poisoning, or as a pivot point for lateral movement if misconfigured.
- **Mitigation:** Restrict access to trusted hosts, keep DNS software updated, and monitor for suspicious queries.

5. HTTP (Port 80):

- **Risk:** Exposed web servers on Port 80 can be attacked through vulnerabilities in web applications (e.g., SQL injection, XSS), brute-force attacks, or exploited if the server software is outdated.

- **Mitigation:** Use HTTPS (port 443) instead, keep web applications and servers patched, and implement Web Application Firewalls (WAF).

6. MSRPC (Port 445):

- **Risk:** Port 445 is heavily exploited in Windows environments for SMB attacks, lateral movement, credential theft, and ransomware (e.g., WannaCry). It may expose sensitive files and allow remote code execution if unpatched.
- **Mitigation:** Block SMB externally, patch systems frequently, and restrict sharing permissions.

7. NetBIOS-SSN (Port 139):

- **Risk:** NetBIOS services can expose system info, facilitate credential brute-forcing, and are commonly targeted for exploitation in Windows networks.
- **Mitigation:** Block or restrict this port, disable NetBIOS over TCP/IP if not required, and ensure strong network segmentation.

Summary Table:

Port	Service	Risk	Mitigation
21	FTP	Plaintext login/data, brute-force, exploits	Use SFTP/FTPS, disable
22	SSH	Brute-force, outdated/config issues	Keys, restrict, update
23	Telnet	Plaintext, sniffing, full shell on compromise	Use SSH, disable
53	DNS	Amplification, cache poisoning, pivoting	Restrict, patch
80	HTTP	App/server vulns, brute-force, outdated software	Use HTTPS, patch, WAF
445	MSRPC/SMB	RCE, ransomware, lateral movement, file abuse	Block extern, patch
139	NetBIOS-SSN	Info leak, brute-force, exploits	Block, segment, restrict

Conclusion:

- The screenshot provides evidence of practical skills in network scanning and assessment using Nmap, supporting the assignment's objective of identifying and analyzing network vulnerabilities.