Nmap Scan Report

1. Objective

To install and run Nmap on a Kali Linux machine, perform a scan on the local network, identify open ports and services, and document the significance of each.

2. Environment

- Host OS: Kali Linux (VM in VirtualBox)
- Target: Local network hosts in 10.213.17.0/24
- Nmap version: 7.95

3. Commands Used

Basic Service Scan:
nmap -sV 10.213.17.0/24

Advanced Scan:
nmap -A 10.213.17.16

- **-sV:** Detects service/version info.
- **-A:** Enables OS detection, version detection, script scanning, and traceroute.

4. Findings

Target IP	Open Port	Protocol	Service / Version	Notes / Significance
10.213.17.16	-	-	All 1000 filtered TCP ports (no response).	Likely protected by
10.213.17.84	-	-	All 1000 closed TCP ports (reset).	No active services fou

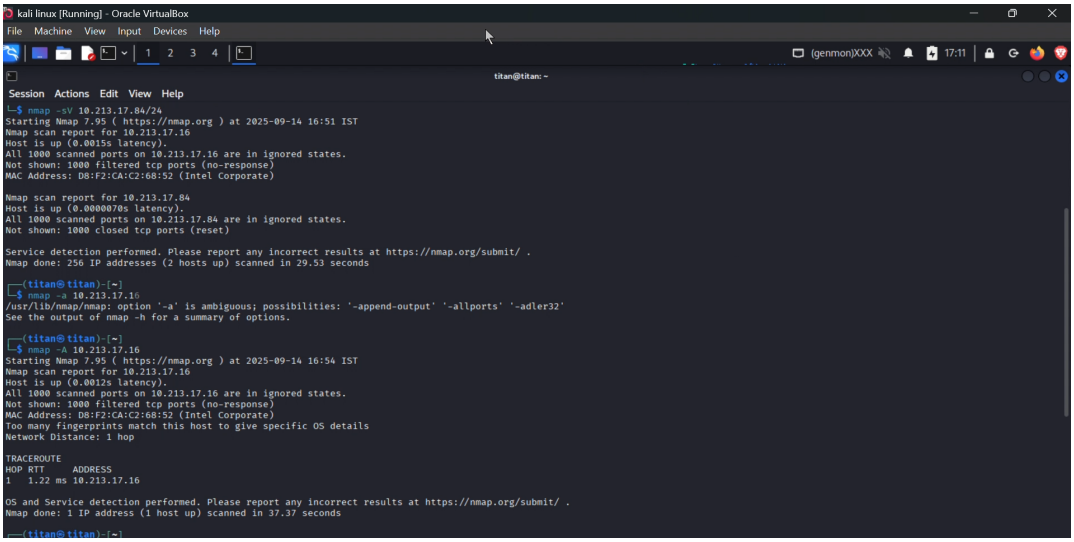
5. Significance of Discovered Ports

No open ports were discovered in this scan. The presence of closed and filtered states indicates that firewall rules or host configurations are restricting access. This is generally good for security but should be monitored to ensure legitimate services are not blocked unintentionally. Routine scans and log monitoring are recommended to detect new changes or vulnerabilities.

6. Conclusion

The scan did not reveal any open ports. The network appears secure, but administrators should continue to maintain security policies, update configurations, and schedule periodic scans.

Appendix: Nmap Scan Screenshot


kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
(genmon)XXX
17:11
titan@titan: ~
Session Actions Edit View Help
└─$ nmap -sV 10.213.17.84/24
Starting Nmap 7.95 (https://nmap.org) at 2025-09-14 16:51 IST
Nmap scan report for 10.213.17.16
Host is up (0.0015s latency).
All 1000 scanned ports on 10.213.17.16 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: D8:F2:CA:C2:68:52 (Intel Corporate)
Nmap scan report for 10.213.17.84
Host is up (0.0000070s latency).
All 1000 scanned ports on 10.213.17.84 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 29.53 seconds
┌──(titan㉿titan)-[~]
└─$ nmap -a 10.213.17.16
/usr/lib/nmap/nmap: option '-a' is ambiguous; possibilities: '--append-output' '--allports' '--adler32'
See the output of nmap -h for a summary of options.
┌──(titan㉿titan)-[~]
└─$ nmap -A 10.213.17.16
Starting Nmap 7.95 (https://nmap.org) at 2025-09-14 16:54 IST
Nmap scan report for 10.213.17.16
Host is up (0.0012s latency).
All 1000 scanned ports on 10.213.17.16 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: D8:F2:CA:C2:68:52 (Intel Corporate)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 1.22 ms 10.213.17.16
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.37 seconds
┌──(titan㉿titan)-[~]