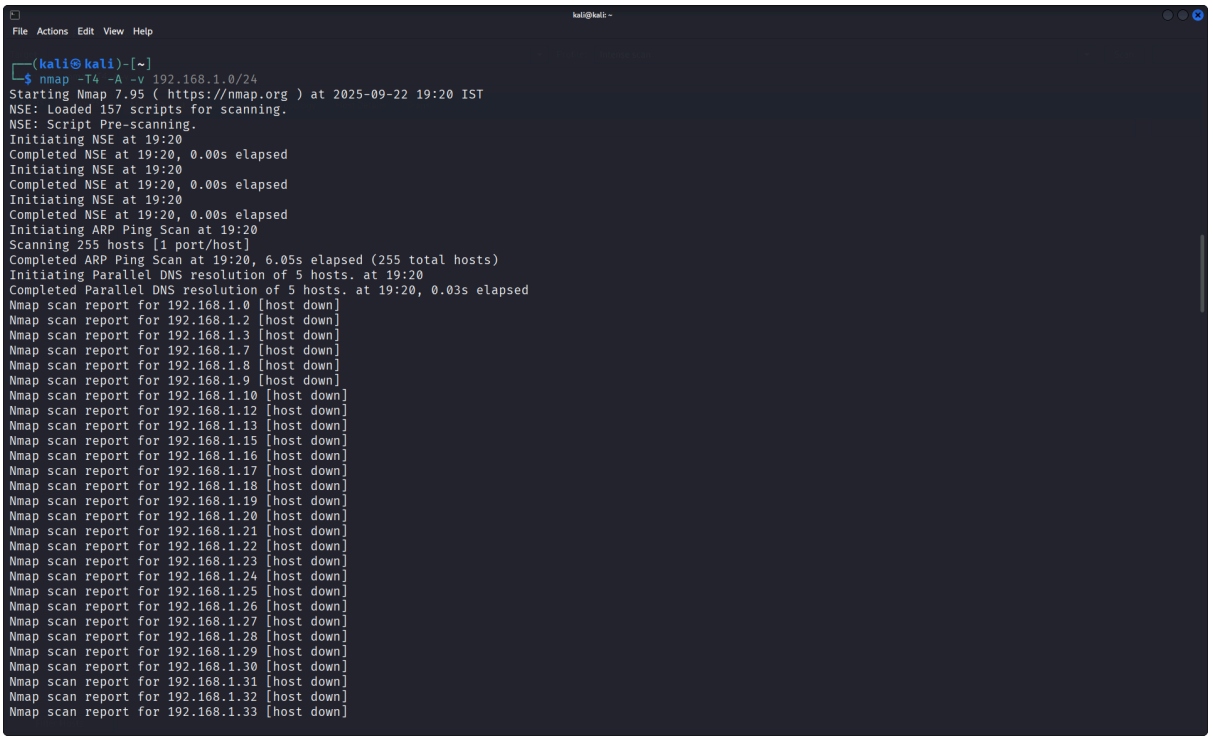
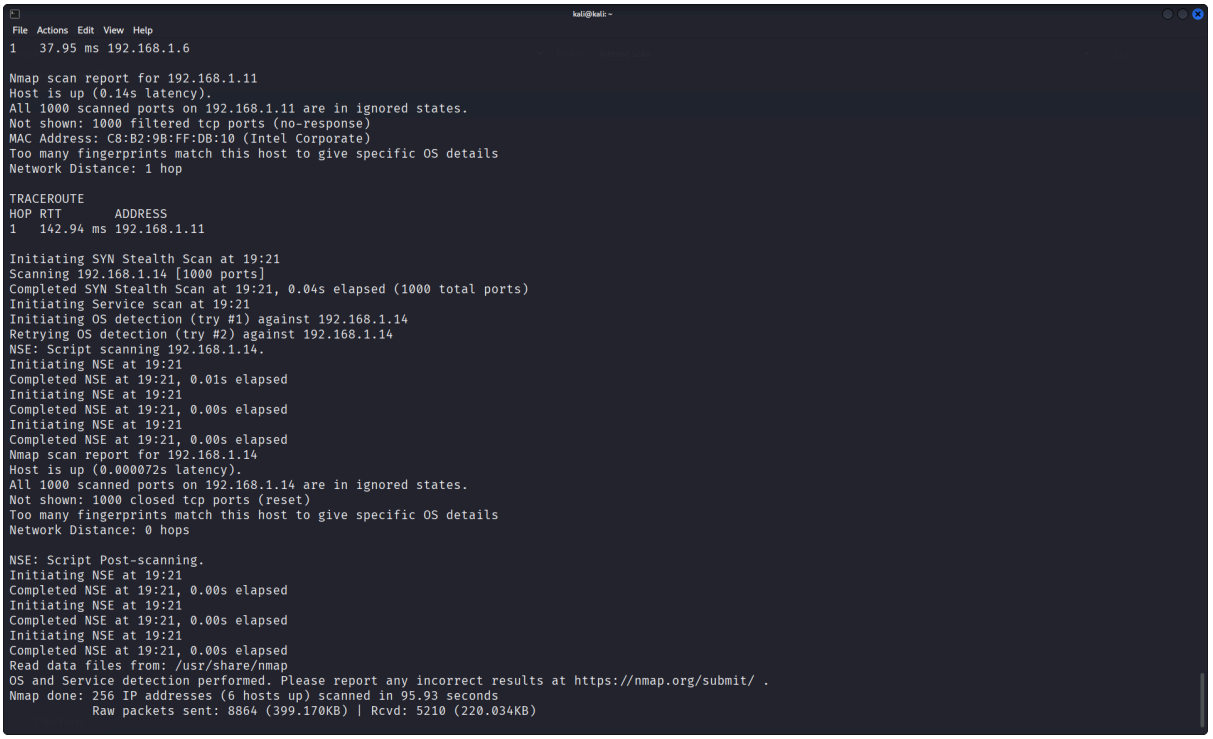
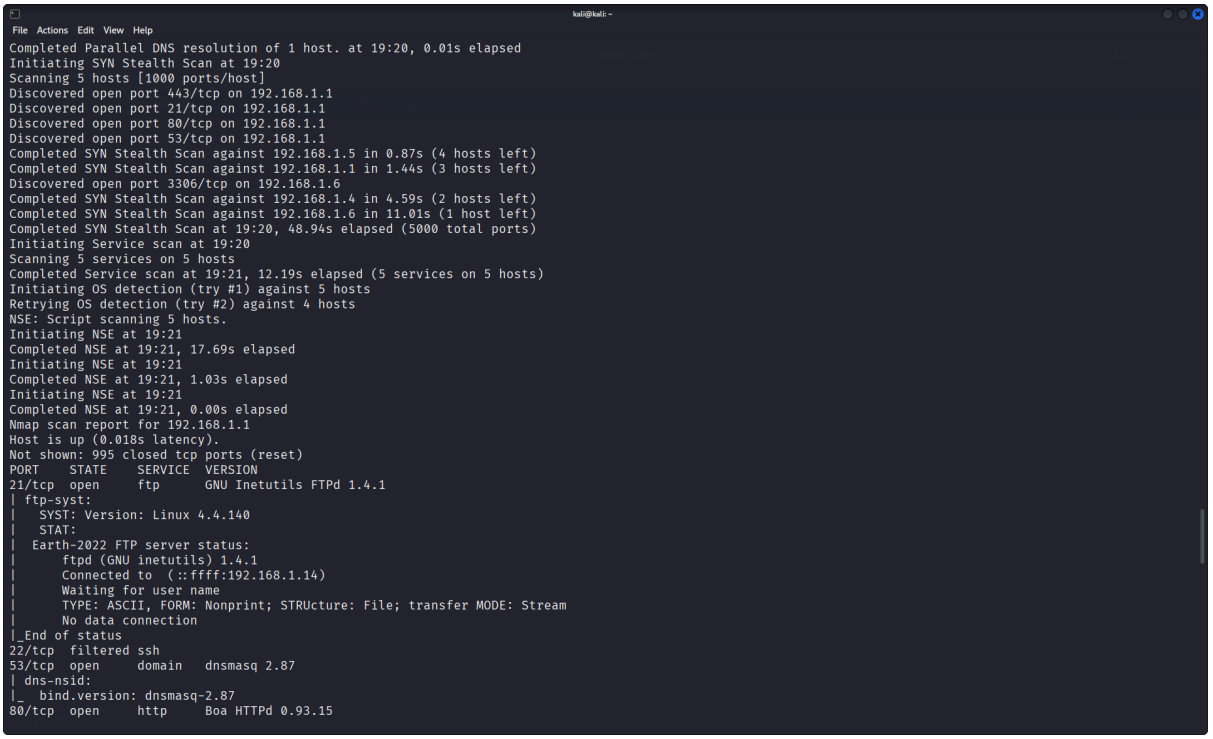
ELEVATE LABS

TASK - 1

Nmap Scan = nmap -T4 -A -v IP.address




kali@kali: ~
File Actions Edit View Help
1 37.95 ms 192.168.1.6
Nmap scan report for 192.168.1.11
Host is up (0.14s latency).
All 1000 scanned ports on 192.168.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: C8:B2:9B:FF:DB:10 (Intel Corporate)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
TRACEROUTE
HOP RTT ADDRESS
1 142.94 ms 192.168.1.11
Initiating SYN Stealth Scan at 19:21
Scanning 192.168.1.14 [1000 ports]
Completed SYN Stealth Scan at 19:21, 0.04s elapsed (1000 total ports)
Initiating Service scan at 19:21
Initiating OS detection (try #1) against 192.168.1.14
Retrying OS detection (try #2) against 192.168.1.14
NSE: Script scanning 192.168.1.14.
Initiating NSE at 19:21
Completed NSE at 19:21, 0.01s elapsed
Initiating NSE at 19:21
Completed NSE at 19:21, 0.00s elapsed
Initiating NSE at 19:21
Completed NSE at 19:21, 0.00s elapsed
Nmap scan report for 192.168.1.14
Host is up (0.000072s latency).
All 1000 scanned ports on 192.168.1.14 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
NSE: Script Post-scanning.
Initiating NSE at 19:21
Completed NSE at 19:21, 0.00s elapsed
Initiating NSE at 19:21
Completed NSE at 19:21, 0.00s elapsed
Initiating NSE at 19:21
Completed NSE at 19:21, 0.00s elapsed
Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 95.93 seconds
Raw packets sent: 8864 (399.170KB) | Rcvd: 5210 (220.034KB)


kali@kali: ~
File Actions Edit View Help
Completed Parallel DNS resolution of 1 host. at 19:20, 0.01s elapsed
Initiating SYN Stealth Scan at 19:20
Scanning 5 hosts [1000 ports/host]
Discovered open port 443/tcp on 192.168.1.1
Discovered open port 21/tcp on 192.168.1.1
Discovered open port 80/tcp on 192.168.1.1
Discovered open port 53/tcp on 192.168.1.1
Completed SYN Stealth Scan against 192.168.1.5 in 0.87s (4 hosts left)
Completed SYN Stealth Scan against 192.168.1.1 in 1.44s (3 hosts left)
Discovered open port 3306/tcp on 192.168.1.6
Completed SYN Stealth Scan against 192.168.1.4 in 4.59s (2 hosts left)
Completed SYN Stealth Scan against 192.168.1.6 in 11.01s (1 host left)
Completed SYN Stealth Scan at 19:20, 48.94s elapsed (5000 total ports)
Initiating Service scan at 19:20
Scanning 5 services on 5 hosts
Completed Service scan at 19:21, 12.19s elapsed (5 services on 5 hosts)
Initiating OS detection (try #1) against 5 hosts
Retrying OS detection (try #2) against 4 hosts
NSE: Script scanning 5 hosts.
Initiating NSE at 19:21
Completed NSE at 19:21, 17.69s elapsed
Initiating NSE at 19:21
Completed NSE at 19:21, 1.03s elapsed
Initiating NSE at 19:21
Completed NSE at 19:21, 0.00s elapsed
Nmap scan report for 192.168.1.1
Host is up (0.018s latency).
Not shown: 995 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp GNU Inetutils FTPd 1.4.1
| ftp-syst:
| SYST: Version: Linux 4.4.140
| STAT:
| Earth-2022 FTP server status:
| ftpd (GNU inetutils) 1.4.1
| Connected to (::ffff:192.168.1.14)
| Waiting for user name
| TYPE: ASCII, FORM: Nonprint; STRUcture: File; transfer MODE: Stream
| No data connection
|_End of status
22/tcp filtered ssh
53/tcp open domain dnsmasq 2.87
| dns-nsid:
|_ bind.version: dnsmasq-2.87
80/tcp open http Boa HTTPd 0.93.15