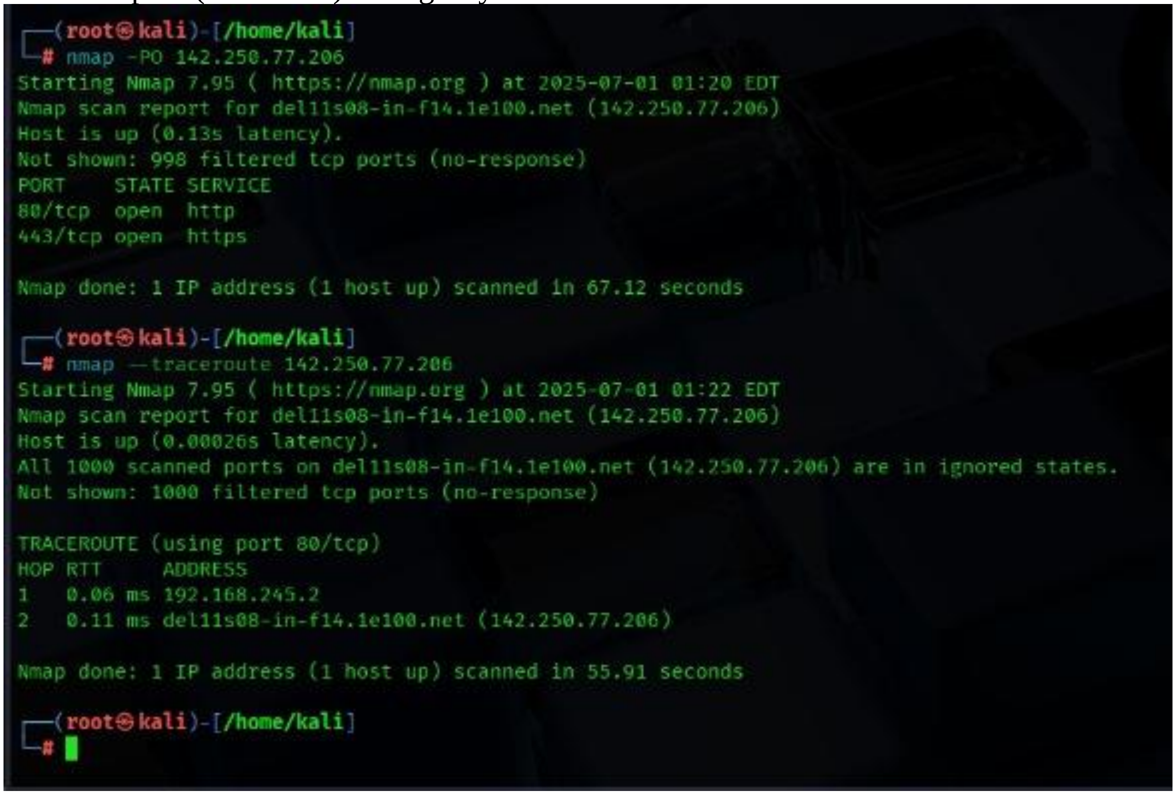
Reconnaissance & Scanning Report

Date: July 1, 2025
Target IPs: Includes 142.250.77.206 (Google server)
Tools Used: Nmap on Kali Linux

1. Objectives

- Identify live hosts on the network
- Discover open ports and running services
- Perform OS and service fingerprinting

Trace the path (traceroute) to target systems



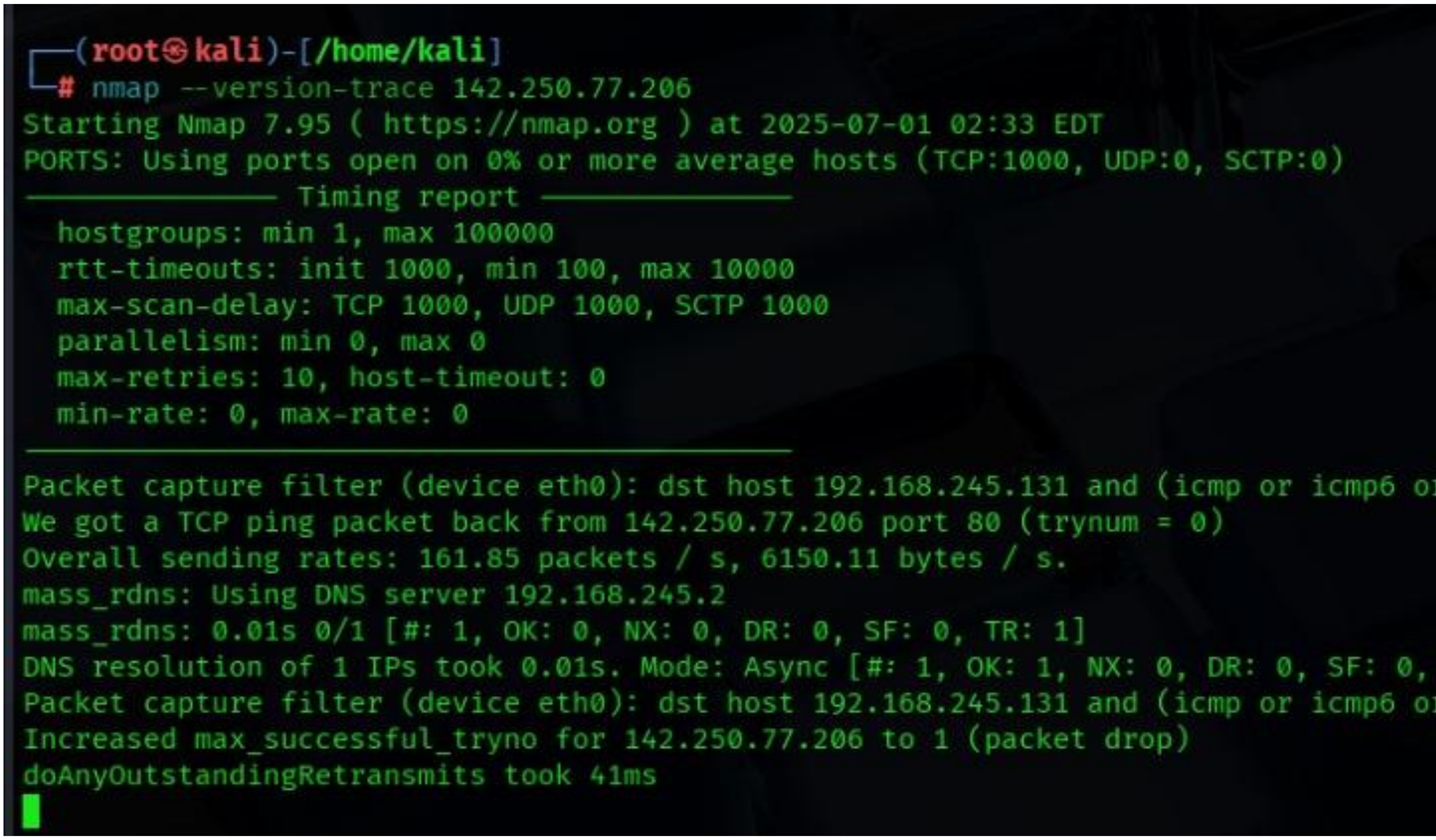
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PO 142.250.77.206
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 01:20 EDT
Nmap scan report for del11s08-in-f14.1e100.net (142.250.77.206)
Host is up (0.13s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 67.12 seconds

┌──(root㉿kali)-[/home/kali]
└─# nmap --traceroute 142.250.77.206
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 01:22 EDT
Nmap scan report for del11s08-in-f14.1e100.net (142.250.77.206)
Host is up (0.00026s latency).
All 1000 scanned ports on del11s08-in-f14.1e100.net (142.250.77.206) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.06 ms 192.168.245.2
2   0.11 ms del11s08-in-f14.1e100.net (142.250.77.206)

Nmap done: 1 IP address (1 host up) scanned in 55.91 seconds

┌──(root㉿kali)-[/home/kali]
└─# 
```

2. Techniques / Commands Used

Command	Description	Notes
nmap --script=ipidseq -v -iR 10 -p 80	Randomized scan on 10 IPs	Detected

		filtered port 80 (firewalled)
nmap --version-trace 142.250.77.206	Version detection + trace	Packet drops observed
nmap -A -p 80 142.250.77.206	Aggressive scan	Detailed fingerprinting; Google HTTP headers
nmap 142.250.77.206	Default port scan	Discovered ports 80 (HTTP), 443 (HTTPS)
nmap -sV 142.250.77.206	Service version detection	Identified as GWS (Google Web Server)
nmap --traceroute 142.250.77.206	Network tracing	Final hop: Google infrast

ructur
e node

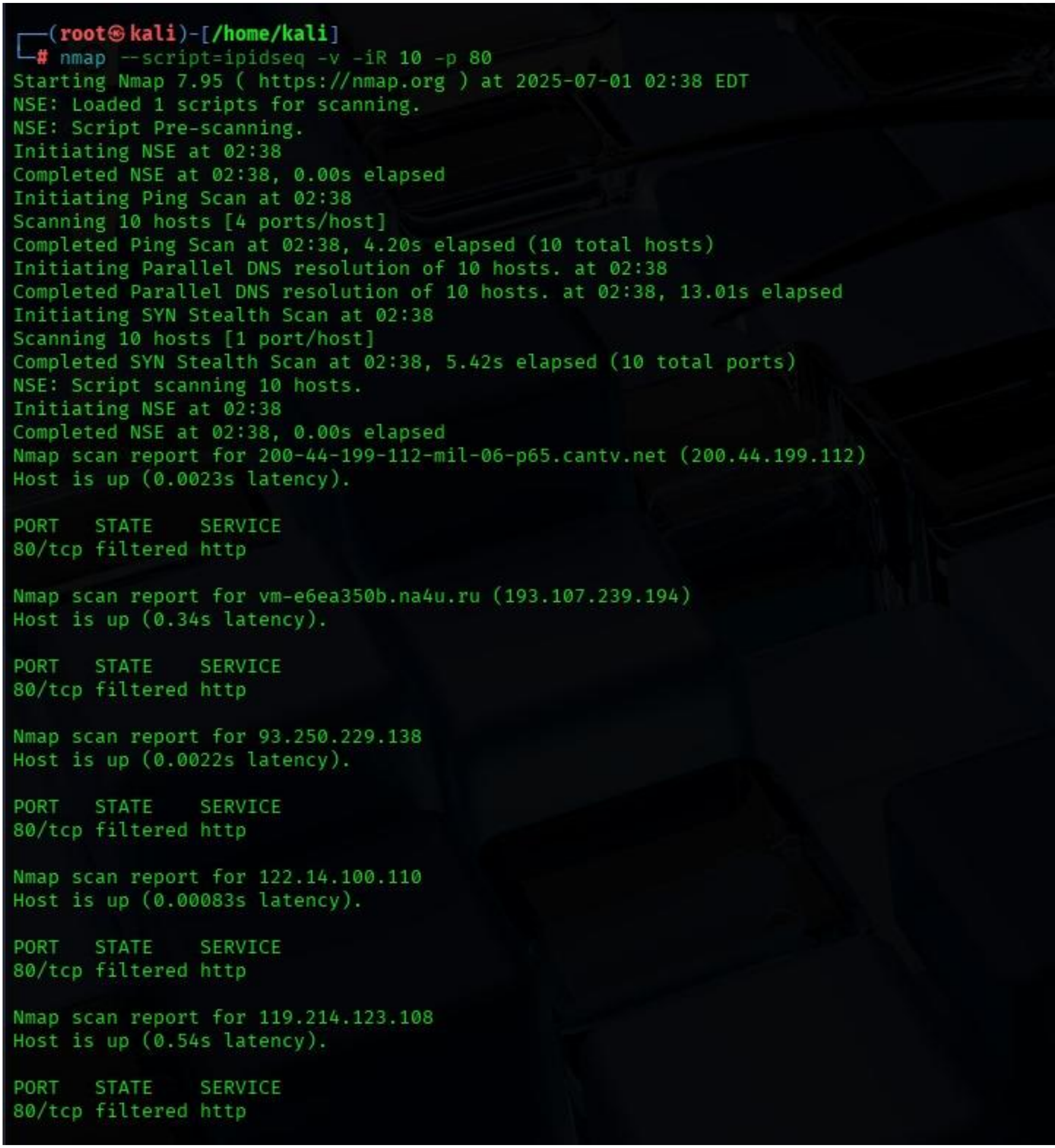


```
┌──(root㉿kali)-[/home/kali]
└─# nmap --version-trace 142.250.77.206
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 02:33 EDT
PORTS: Using ports open on 0% or more average hosts (TCP:1000, UDP:0, SCTP:0)
────────────── Timing report ──────────────
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
─────────────────────────────────────────────
Packet capture filter (device eth0): dst host 192.168.245.131 and (icmp or icmp6 o
We got a TCP ping packet back from 142.250.77.206 port 80 (trynum = 0)
Overall sending rates: 161.85 packets / s, 6150.11 bytes / s.
mass_rdns: Using DNS server 192.168.245.2
mass_rdns: 0.01s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0,
Packet capture filter (device eth0): dst host 192.168.245.131 and (icmp or icmp6 o
Increased max_successful_tryno for 142.250.77.206 to 1 (packet drop)
doAnyOutstandingRetransmits took 41ms
█
```

3. Key Findings

IP Address	Hostname	Open Ports	Services	Remarks
142.250.77.206	Google server (del11s08-in-f14.1e100.net)	80, 443	HTTP, HTTPS (GWS)	Filtered but accessible; heavy protection
193.107.239.194	vm-e6ea350b.na4u.ru	None (filtered)	-	Likely behind firewall

IP Address		Open Hostname	Services	Remarks Ports
200.44.199.112	mil-06-p65.cantv.net	None	-	Host reachable;



```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script=ipidseq -v -iR 10 -p 80
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-01 02:38 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Initiating Ping Scan at 02:38
Scanning 10 hosts [4 ports/host]
Completed Ping Scan at 02:38, 4.20s elapsed (10 total hosts)
Initiating Parallel DNS resolution of 10 hosts. at 02:38
Completed Parallel DNS resolution of 10 hosts. at 02:38, 13.01s elapsed
Initiating SYN Stealth Scan at 02:38
Scanning 10 hosts [1 port/host]
Completed SYN Stealth Scan at 02:38, 5.42s elapsed (10 total ports)
NSE: Script scanning 10 hosts.
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Nmap scan report for 200-44-199-112-mil-06-p65.cantv.net (200.44.199.112)
Host is up (0.0023s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap scan report for vm-e6ea350b.na4u.ru (193.107.239.194)
Host is up (0.34s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap scan report for 93.250.229.138
Host is up (0.0022s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap scan report for 122.14.100.110
Host is up (0.00083s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap scan report for 119.214.123.108
Host is up (0.54s latency).

PORT   STATE    SERVICE
80/tcp filtered http
```

4. Issues Observed

- Filtered ports: Common in modern networks with IDS/IPS or firewalls.
- Packet loss during version tracing: Suggests rate limiting, packet filtering, or QoSbased drops.

5. Non-Scan Observation

Error Identified: “Your bank is unable to process payments right now.” Diagnosis:

- Could be bank-side server downtime
- Temporary network failure
- API/service limit reached
  Action: Retry later or escalate to bank’s tech support.

6. Conclusion

- Successfully scanned and identified key services on reachable hosts.
- Detected active filtering on several targets — indicating defensive measures.
- Gained partial OS and service fingerprints, especially from the Google IP.
- Traceroute helped validate network paths to target systems.

Suggestions for Future Recon/Reporting:

- Add timestamps or scan duration for time-sensitive engagements.
- Include `-Pn` or `-sS` scans to bypass ping blocks and evade simple IDS detection.
- Log full Nmap outputs (`-oA` or `-oN`) for auditing.
- Consider using tools like Masscan, ZMap, or Amass for broader reconnaissance stages.