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

---

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 infrastructure node

---

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	Hostname	Open Ports	Services	Remarks
200.44.199.112	mil-06-p65.cantv.net	None (filtered)	-	Host reachable; possibly filtered

---

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 **QoS-based 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.