1. Network Discovery (The "Ping Sweep")

First, identify which devices are alive on your subnet without scanning every port yet.

```
# -sn: Ping scan (no port scan)

# -oG: Output in grepable format to easily pull IP addresses

sudo nmap -sn 192.168.1.0/24 -oG live_hosts.txt
```

---

2. Comprehensive Port & Service Scan

Once you have your target IP (e.g., 192.168.1.50), run a deep scan to identify the OS and service versions.

```
# -p-: Scan all 65,535 ports

# -sV: Service version detection

# -O: Operating System detection

# -T4: Faster execution (aggressive timing)

sudo nmap -p- -sV -O -T4 192.168.1.50
```

---

3. Vulnerability Scripting (The "Analysis" Phase)

This is where Nmap checks the discovered services against known exploit databases.

```
# --script vuln: Runs a large category of vulnerability detection scripts

sudo nmap -sV --script vuln 192.168.1.50
```

---

4. The "All-in-One" Professional Command

If you want to generate your **Deliverable (Network Scan Report)** in one go, use this combined string. This covers steps 2 through 7 of your guide.

```
sudo nmap -p- -sV -sC -O --script vuln -oA final_report 192.168.1.50
```

Breakdown of this command:

- -sC: Runs default "safe" scripts (identifies common misconfigurations).
- -oA final_report: Saves the results in three formats (.nmap, .xml, and .gnmap). This satisfies the "Save scan results" and "Document findings" steps.

---

5. Documenting Findings (Interpreting Results)

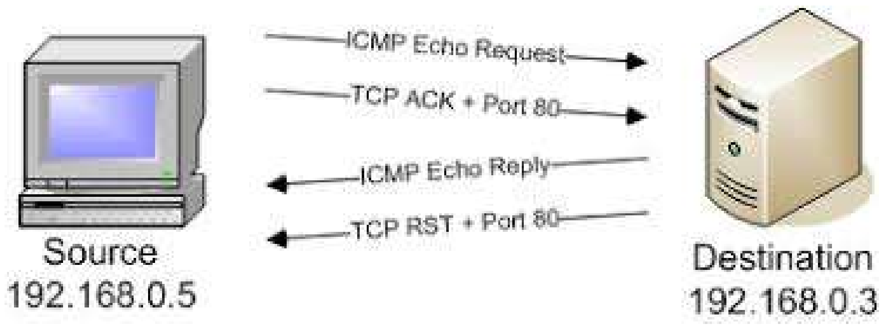
After the scan, you can manually inspect the report for risks:

```
# Search for "VULNERABLE" keywords in your saved report

grep -i "VULNERABLE" final_report.nmap
```

Final Outcome Checklist:

Step	**Nmap Code Snippet**
Local Network Scan	-sn [network/prefix]
Open Ports	-p- --open
Service/OS Detection	-sV -O
Analyze Vulnerabilities	--script vuln
Save Results	-oA [filename]


ICMP Echo Request
TCP ACK + Port 80
ICMP Echo Reply
TCP RST + Port 80
Source
192.168.0.5
Destination
192.168.0.3