Task 4 Cheat Sheet — Network Security & Vulnerability Assessment

Quick reference guide for scanning, enumeration, vulnerability analysis, and verification.

Overview

Goal: discover hosts, enumerate ports/services, run vulnerability scans, verify findings, capture traffic, and produce prioritized remediation steps.
Core tools: nmap, netdiscover, OpenVAS/Nessus, Wireshark, xsltproc, git (+ Git LFS for large files).

Quick Lab Checks

```
# verify network interfaces & IP (Kali)
ip a
# verify target IP (on target VM)
ip a # or ifconfig
```

Why: confirm both VMs are on same Host-Only network.

Host Discovery

```
# ARP-based discovery
sudo netdiscover -r 192.168.56.0/24 -P -o scans/host_discovery.txt
# ICMP ping sweep
sudo nmap -sn 192.168.56.0/24 -oN scans/host_discovery_nmap.txt
```

Save output: scans/host_discovery.txt / scans/host_discovery_nmap.txt

Nmap Scanning Progression

1. Top ports

```
sudo nmap --top-ports 100 -T4 192.168.56.102 -oN scans/top100.txt
```

2. Full TCP + service/version + OS

```
sudo nmap -sS -sV -O -p- -T4 192.168.56.102 -oA scans/full_combo
```

3. NSE vulnerability scripts

```
sudo nmap --script vuln 192.168.56.102 -oN scans/vuln_check.txt
```

4. HTTP vuln scripts

```
sudo nmap -sV --script http-vuln* 192.168.56.102 -oN scans/http_vulns.txt
```

Convert & Present Results

```
# convert XML to HTML
xsltproc scans/full_combo.xml -o scans/full_combo.html
```

Open scans/full_combo.html in browser for report view.

Vulnerability Scanning (OpenVAS / Nessus)

```
# OpenVAS setup
sudo gvm-setup
sudo gvm-start
```

Access via https://127.0.0.1:9392/
Create target -> Create task -> Run scan -> Export HTML/PDF
For Nessus:
Install, access https://localhost:8834, create scan, run, export report.
Save reports in vuln_reports/openvas_report.html or .pdf.
Note: scanners give prioritized lists — verify top issues manually.

Manual Verification

```
# banner grab
nc -v 192.168.56.102 21
# http header check
curl -I http://192.168.56.102/
# test service
curl http://192.168.56.102:8080/some-path
```

Purpose: verify findings and avoid false positives.

Packet Capture (Wireshark)

1. Start Wireshark on host-only interface (e.g., enp0s8).
2. Generate traffic (curl, nmap, browse target).
3. Stop & save as pcaps/task4_capture.pcap.

Useful filters:

```
ip.addr == 192.168.56.102
http
tcp.flags.syn==1
```

Quick iptables Checks (Hardening Demo)

```
# List rules
sudo iptables -L -n -v
# Block port example
sudo iptables -A INPUT -p tcp --dport 21 -j DROP
# Save rules
sudo sh -c "iptables-save > /etc/iptables.rules"
```

CVSS & Prioritization

Exploitability + Impact => Priority.
Critical/High: RCE, auth bypass
Medium: config leaks
Low: informational
Remediate high first, then medium, then low.

Deliverable Filenames

scans/full_combo.nmap, scans/full_combo.xml, scans/full_combo.html
scans/vuln_check.txt
vuln_reports/openvas_report.html
pcaps/task4_capture.pcap (use Git LFS if large)
notes/task4_analysis.md (findings table + mitigation)
scripts/helpers.sh

Quick Report Template

Port/Service — Evidence — Risk — Recommendation
Example:
21/tcp vsftpd 2.3.4 — scans/full_combo.nmap — HIGH — Update/disable FTP, use SFTP, firewall off.

Useful One-liners

```
# Save top 10 ports
sudo nmap --top-ports 10 192.168.56.102 -oN scans/top10.txt
# Append vuln scripts output
sudo nmap --script vuln 192.168.56.102 -oN - >> scans/vuln_check.txt
```

```
# Fast masscan (noisy)
sudo masscan 192.168.56.102 -p1-65535 --rate=1000 -oG scans/masscan_grep.txt
```

Troubleshooting

- Nmap reports all ports filtered: check network adapter & target VM status.
- gvm-start fails: sudo gvm-check-setup or rerun gvm-setup.
- Large PCAPs: use Git LFS or external cloud link.

Prepared for ApexPlanet Cybersecurity Internship — Task 4