Capstone Project: Full VAPT Engagement

VAPT Engagement – Safety & Execution Checklist

Lab Setup & Safety

- Work in isolated lab (Host-only, NAT, or dedicated VLAN)
- Snapshot both VMs before testing
- Keep logs of all actions (timestamps, commands, screenshots)
- Don't run exploits on production systems
- Note attacker and target IPs

Attacker Machine (Kali) Setup

- Start & update Kali: `sudo apt update && sudo apt -y upgrade`
- Create lab directories: `mkdir -p ~/vapt/lab/{scans,evidence,notes}`
- Set permissions: `chmod 700 evidence`
- Confirm networking: `ip a`, `route -n`
- Log session info: `echo "<ATTACKER-IP> - $(date --iso-8601=seconds)" >> notes/session_info.txt`

Reconnaissance & Banner Grabbing

- Nmap top-ports scan: `sudo nmap -sS -Pn -T4 --top-ports 100 <TARGET-IP> -oA scans/initial_top100`
- Service/version scan: `sudo nmap -sS -sV -Pn -T4 <TARGET-IP> -oA scans/initial_svc`
- Save outputs: `.nmap, .xml, .gnmap`
- FTP banner grab:
  - `echo | nc -w 3 <TARGET-IP> 21 > evidence/ftp_banner.txt`
  - `curl -v ftp://<TARGET-IP>/ 2>&1 | tee evidence/ftp_curl_banner.txt`
- Passive capture: `sudo tcpdump -n -i any host <TARGET-IP> and port 21 -w evidence/ftp_banner_capture.pcap`

Target Machine Setup & Hardening

- Snapshot / backup VM
- Confirm IP & services: `ip a`, `ss -tuln`, `ps aux | egrep 'vsftpd|ftp'`
- Capture local banners: `dpkg -l | grep vsftpd`
- Enable logging & save logs: `mkdir -p ~/vapt_logs`
- Create admin user: `sudo adduser labadmin && sudo usermod -aG sudo labadmin`
- Stop & disable service if needed: `sudo systemctl stop vsftpd && sudo systemctl disable vsftpd`
- Apply safe upgrades: `sudo apt update && sudo apt install --only-upgrade vsftpd`
- Firewall restriction (example):
    - `sudo ufw default deny incoming`
    - `sudo ufw allow from 10.0.0.0/24 to any port 22 proto tcp`

Verification & Evidence

- Re-scan with Nmap: `sudo nmap -sS -sV -Pn -T4 <TARGET-IP> -oA scans/post_remediation`
- Compare pre/post scans: `diff -u scans/initial_svc.nmap scans/post_remediation.nmap | tee evidence/scan_diff.txt`
- Re-run OpenVAS/GVM scan and export results
- Preserve logs, PCAPs, banner files, and OpenVAS reports

Reporting (PTES)

- Include snapshots & timestamps
- Commands run & outputs
- Raw banners & PCAP screenshots
- Remediation steps (service stopped, upgraded, firewall applied)
- Rescan evidence demonstrating mitigation