Task-3:

1.What is vulnerability scanning?

→ Vulnerability scanning is an automated process of identifying security weakness in system,networks or applications. It checks for outdated software,misconfiguration ,or missing patches that attackers could exploit.

2. What is the difference between vulnerability scanning and penetration testing?

→ Vulnerability scanning:

1. Automated and broad scanning of systems for known vulnerabilities.

2.Identify possible risks.

3.Example nessus scan .

→ Penteration testing :

1.Manual and targeted testing to exploit vulnerabilities.

2.Confirm how those risks can be exploited

3.Example:metasploit

3. What are some common vulnerabilities in personal computers?

→ Outdated operating systems,Weak or reused passwords,Missing antivirus or firewall,Unpatched software (like browsers, Java, etc.),Open ports (e.g:Telnet or RDP)

4. How do scanners detect vulnerabilities?

→ Scanners use databases of known CVEs (Common Vulnerabilities and Exposures) and test our system against them. They check for version numbers, configurations, and responses to network probes.

5. What is CVSS?
→ CVSS (Common Vulnerability Scoring System) is a standardized way to rate the severity of vulnerabilities from **0 to 10**, where:

- 0–3.9 → Low
- 4.0–6.9 → Medium
- 7.0–8.9 → High
- 9.0–10 → Critical

6. How often should vulnerability scans be performed?
→ Ideally:

- Weekly or monthly for organizations.
- After major software updates or configuration changes.

Regular scans ensure new vulnerabilities are detected quickly.

7. What is a false positive in vulnerability scanning?

→ A false positive is when a scanner reports a vulnerability that doesn’t actually exist.

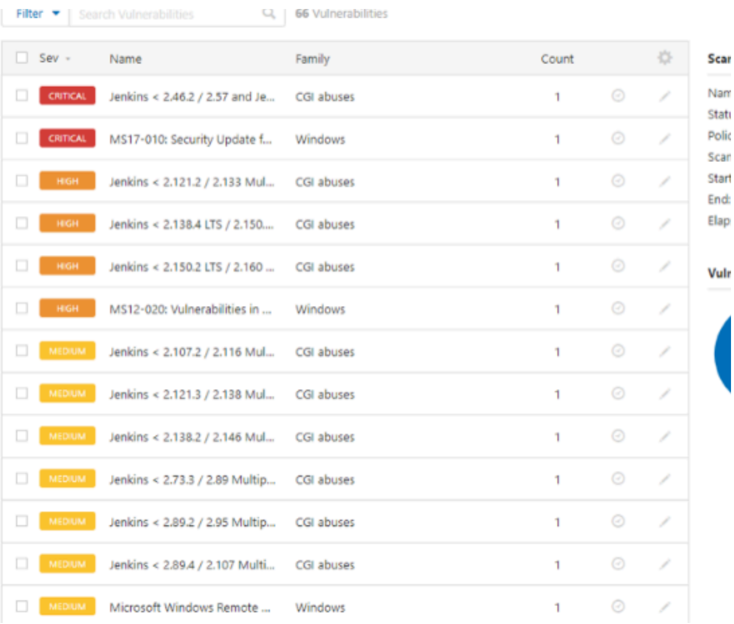
8. How do you prioritize vulnerabilities?

→Based on CVSS score (critical > high > medium > low).

Based on asset importance (server > personal system).

Based on exploit availability (if public exploit exists → fix faster).

*Resuts of nessus:



□	Sev	Name	Family	Count
□	CRITICAL	Jenkins < 2.46.2 / 2.57 and Je...	CGI abuses	1
□	CRITICAL	MS17-010: Security Update f...	Windows	1
□	HIGH	Jenkins < 2.121.2 / 2.133 Mul...	CGI abuses	1
□	HIGH	Jenkins < 2.138.4 LTS / 2.150...	CGI abuses	1
□	HIGH	Jenkins < 2.150.2 LTS / 2.160 ...	CGI abuses	1
□	HIGH	MS12-020: Vulnerabilities in ...	Windows	1
□	MEDIUM	Jenkins < 2.107.2 / 2.116 Mul...	CGI abuses	1
□	MEDIUM	Jenkins < 2.121.3 / 2.138 Mul...	CGI abuses	1
□	MEDIUM	Jenkins < 2.138.2 / 2.146 Mul...	CGI abuses	1
□	MEDIUM	Jenkins < 2.73.3 / 2.89 Multip...	CGI abuses	1
□	MEDIUM	Jenkins < 2.89.2 / 2.95 Multip...	CGI abuses	1
□	MEDIUM	Jenkins < 2.89.4 / 2.107 Multi...	CGI abuses	1
□	MEDIUM	Microsoft Windows Remote ...	Windows	1