VULNERABILITY ASSESSMENT CHECKLIST

A vulnerability assessment checklist, including guiding questions, should cover areas like network configuration, system patching, user access controls, application security, data protection, and physical security, with key questions focusing on identifying potential weaknesses and assessing their impact:

Network Assessment:

Firewall configuration:

- Are all necessary ports properly filtered and secured?
- Are default firewall rules reviewed and updated regularly?
- Are firewall logs monitored for suspicious activity?

Network segmentation:

- Are sensitive network segments isolated from public networks?
- Are network access controls implemented based on user roles?

Wireless security:

- Is WPA2 or WPA3 encryption used on wireless networks?
- Are strong passwords enforced for wireless network access?
- Are rogue access points regularly detected and removed?

System Assessment:

Operating System patching:

- Are all systems updated with the latest security patches?
- Is a patch management system in place to automate updates?

Account management:

- Are strong password policies enforced for all user accounts?
- Are privileged accounts properly managed and monitored?

System hardening:

- Are unnecessary services disabled on servers?
- Are default configurations reviewed and modified to enhance security?

Application Assessment:

Input validation:

- Are user inputs properly sanitized to prevent injection attacks (SQL, XSS)?
- Authentication/Authorization:
- Are strong authentication mechanisms (multi-factor) implemented?
- Are user permissions properly assigned based on their roles?

Session management:

- Are session timeouts set appropriately?
- Is session hijacking prevented through proper cookie management?

Data Protection:

Data encryption:

- Is sensitive data encrypted at rest and in transit?
- Are encryption keys properly managed and secured?

Data backups:

- Are regular backups performed and tested for data recovery?
- Are backup systems protected from unauthorized access?

Access Control:

- User access management:
- Are user accounts reviewed regularly for appropriate access levels?
- Is the principle of least privilege followed?

Remote access:

- Are secure protocols (VPN) used for remote access?
- Are strong authentication methods required for remote logins?

Physical Security:

Data center access:

- Are physical access controls implemented for data center entry?

Device security:

- Are physical devices (servers, laptops) secured with locks or cable ties?

General Questions:

Vulnerability scanning process:

- How frequently are vulnerability scans performed?
- What tools are used to conduct vulnerability scans?

Remediation plan:

- Is there a documented process for addressing identified vulnerabilities?
- How are vulnerabilities prioritized based on risk level?

Compliance requirements:

- Does the organization comply with relevant security standards (e.g., PCI DSS, HIPAA)?