LO#10: Explain Different Types of Penetration Testing and its Phases

Penetration Testing

- Penetration testing is a method of evaluating the security of an information system or network by simulating an attack to find out vulnerabilities that an attacker could exploit
- Security measures are actively analyzed for design weaknesses, technical flaws, and vulnerabilities
- It not only points out vulnerabilities but also documents how the weaknesses can be exploited
- The results are delivered to executive management and technical audiences in a comprehensive report

Notes:

Why do Penetration Testing?

- Identify the threats facing an **organization's information assets**
- Test and validate the efficacy of **security protections and controls**
- Reduce an organization's expenditure on IT security and enhance **Return On Security Investment (ROSI)** by identifying and remediating vulnerabilities or weaknesses
- Change or upgrade **existing infrastructure** of software, hardware, or network design
- Provide assurance with a comprehensive **assessment of organization's security** including policy, procedure, design, and implementation
- Focus on **high-severity vulnerabilities** and emphasize **application-level security issues** to development teams and management
- Gain and maintain **industry regulated** certification (BS7799, HIPAA, or other regulations)
- Provide a comprehensive approach of **preparation steps** that can be taken to prevent future exploitation
- Adopt **best practices** in compliance with legal and industry regulations
- Evaluate the efficacy of **network security devices** such as firewalls, routers, and web servers

Comparing Security Audit, Vulnerability Assessment, and Penetration Testing

Security Audit

- Checks whether the organization is following a set of standard **security policies and procedures**

Vulnerability Assessment

- Focuses on **discovering the vulnerabilities in the information system** but provides no indication of whether the vulnerabilities can be exploited or the amount of damage that may result from their successful exploitation

Penetration Testing

- A methodological approach to security assessment that **encompasses the security audit** and vulnerability assessment and demonstrates if the vulnerabilities in the system can be successfully exploited by attackers

Notes: