B.Tech, 6^{th} Sem., Computer Networking: Security(CLASS NOTE)

Dr. Laxmidhar Biswal

April 10, 2025

Compare and contrast various types of security controls

Dr. Laxmidhar Biswal

Chapter 05

Introduction

1 Chapter 05

- Introduction

Introduction/Motivation

Explain common threat vectors and attack surfaces

Objectives of this chapter

To understand various common threat vectors—such as message-based, image-based, file-based, voice calls, removable devices, vulnerable software, unsecure networks, open service ports, default credentials, supply chain attacks, and human/social engineering tactics—and how to secure systems against them effectively for cybersecurity readiness and certification preparedness.

Explain common threat vectors and attack surfaces

Message-Based Threats

- Email Phishing: Disguised as legitimate emails, trick users into clicking links or attachments.
- SMS (Smishing): Fake texts deceive users into revealing data or installing malware.
- Instant Messaging (IM): Exploits messaging apps to spread malware or malicious links.

Image-Based Threats

- Malicious Code in Images: Images embedded with harmful code can compromise systems.

Explain common threat vectors and attack surfaces

File-Based Threats

- Malware via Files: Infected files exploit software flaws to execute harmful code.

Voice Call Threats

- Vishing: Voice scams trick victims into revealing sensitive info.
- Caller ID Spoofing: Attackers mask their identity to gain trust.

Removable Devices

- USB Attacks: Malware-loaded drives infect systems upon connection.

Explain common threat vectors and attack surfaces

Vulnerable Software

- Outdated/Flawed Software: Exploitable weaknesses from bugs or poor design.
- Scanning Methods:
  - Client-based: Agent installed for regular checks.
  - Agentless: Remote scanning (e.g., Nmap, Wireshark).

Unsupported Systems

- Legacy Software: Unpatched, outdated apps targeted for known vulnerabilities.

Explain common threat vectors and attack surfaces

Unsecure Networks

- Wireless: No encryption allows easy data interception.
- Wired: Unprotected ports open to unauthorized access.
- Bluetooth: Poor pairing protection can allow data leaks.

Open Service Ports

- Exposed Ports: Attackers scan and exploit unsecured open ports.

Supply Chain Attacks

- MSPs/Vendors/Suppliers: Weak links in the chain can be exploited to breach larger networks.

Explain common threat vectors and attack surfaces

Human Vectors / Social Engineering

- Phishing/Spear Phishing: Deceptive emails for mass or targeted victims.
- Smishing: Fraudulent SMS texts.
- Misinformation: Spread of false info to manipulate public or create chaos.
- Impersonation: Fake identities to trick users.
- BEC (Business Email Compromise): Hacked email accounts used for fraud.
- Pretexting: Made-up scenarios to extract info.
- Watering Hole Attacks: Trusted websites infected to target regular visitors.
- Brand Impersonation: Fake emails/sites of trusted brands.
- Typosquatting: Misspelled domain names lead to

References

https://www.ebooks.com/en-ag/book/210192090/comptia-security-sy0-601-certification-guide/ian-neil/

Question
??

The End