AP Cybersecurity

Syllabus Checklist · 大纲自查表

Tick one box per statement: ☐ not yet ☐ nearly ☐ confident. 每条打一个勾：尚未掌握 / 快会了 / 有把握。

1. Introduction to Security 安全导论

1.1 Understanding Social Engineering 理解社会工程学

- ☐☐☐ Identify common indicators of social engineering tactics.
- ☐☐☐ Explain how social engineering tactics influence victims to perform a desired action.
- ☐☐☐ Describe possible impacts for victims of social engineering attacks.

1.2 Suspicious Website Logins 可疑的网站登录

- ☐☐☐ Identify common signs of a password attack.
- ☐☐☐ Explain how adversaries take advantage of weak authentication.
- ☐☐☐ Explain how to make authentication stronger.

1.3 Best Practices for Public Networks 公共网络的最佳实践

- ☐☐☐ Identify the type of adversary conducting a cyberattack.
- ☐☐☐ Identify types of wireless cyberattacks.
- ☐☐☐ Describe actions individuals can take to increase protection of sensitive data when using the internet and Wi-Fi.

1.4 AI-Based Cybersecurity Attacks 基于 AI 的网络安全攻击

- ☐☐☐ Explain how adversaries use AI-powered tools to augment cyberattacks.
- ☐☐☐ Explain how to protect against some AI-augmented cyberattacks.

1.5 Leveraging AI in Cyber Defense 在网络防御中运用 AI

- ☐☐☐ Explain how cyber defenders can leverage AI-powered tools to protect networks, applications, and data.
- ☐☐☐ Explain how AI-powered tools are enabling faster and more accurate threat detection and response.

2. Securing Spaces 保护物理空间

2.1 Cyber Foundations 网络安全基础

- ☐☐☐ Identify social engineering attacks.
- ☐☐☐ Identify types of adversaries.
- ☐☐☐ Describe the phases of a cyberattack.
- ☐☐☐ Describe the risk assessment process.
- ☐☐☐ Identify strategies for managing risk.
- ☐☐☐ Identify types of security controls.
- ☐☐☐ Explain why a defense-in-depth security strategy is necessary to optimally protect an organization.

2.2 Physical Vulnerabilities and Attacks 物理漏洞与攻击

- ☐☐☐ Identify common physical attacks.
- ☐☐☐ Explain how threats can exploit common physical vulnerabilities to cause loss, damage, disruption, or destruction to assets.
- ☐☐☐ Assess and document risks from physical vulnerabilities.

2.3 Protecting Physical Spaces 保护物理场所

- ☐☐☐ Identify managerial controls related to physical security.
- ☐☐☐ Determine mitigation strategies for risks from physical vulnerabilities.

2.4 Detecting Physical Attacks 检测物理攻击

- ☐☐☐ Identify ways security controls can detect physical attacks.
- ☐☐☐ Determine effective placement of security controls for detecting physical attacks.
- ☐☐☐ Apply detection techniques to identify physical attacks.

3. Securing Networks 保护网络

3.1 Network Vulnerabilities and Attacks 网络漏洞与攻击

- ☐☐☐ Identify common network attacks.
- ☐☐☐ Explain how adversaries can exploit network vulnerabilities to steal, disrupt, or destroy network communication.
- ☐☐☐ Assess and document risks from network vulnerabilities.

3.2 Protecting Networks: Managerial Controls and Wireless Security 保护网络：管理性控制与无线安全

- ☐☐☐ Identify managerial controls related to network security.
- ☐☐☐ Configure wireless network security features.

3.3 Protecting Networks: Segmentation 保护网络：网络分段

- ☐☐☐ Identify techniques for segmenting a network.
- ☐☐☐ Explain why network segmentation can increase network security.

3.4 Protecting Networks: Firewalls 保护网络：防火墙

- ☐☐☐ Identify types of network-based firewalls.
- ☐☐☐ Explain how a firewall uses an access control list to allow or deny traffic entering or leaving a network.
- ☐☐☐ Determine the effective placement of firewalls in a network.
- ☐☐☐ Configure a firewall to manage the flow of network traffic.

3.5 Detecting Network Attacks 检测网络攻击

- ☐☐☐ Identify types of automated security tools used to detect network attacks.
- ☐☐☐ Explain how organizations can leverage artificial intelligence (AI) to enhance threat detection and response.
- ☐☐☐ Determine a network detection method.

- ☐☐☐ Evaluate the impact of a network detection method.
- ☐☐☐ Apply detection techniques to identify indicators of network attacks by analyzing log files.

4. Securing Devices 保护设备

4.1 Device Vulnerabilities and Attacks 设备漏洞与攻击

- ☐☐☐ Identify types of computing devices.
- ☐☐☐ Identify the type of malware used in a cyberattack.
- ☐☐☐ Explain how adversaries can exploit common device vulnerabilities to cause loss, damage, disruption, or destruction.
- ☐☐☐ Assess and document risks from device vulnerabilities.

4.2 Authentication 身份验证

- ☐☐☐ Explain why hashes (also called hash outputs, checksums, message digests, or digests) are used to store passwords.
- ☐☐☐ Explain how password attacks exploit vulnerabilities.
- ☐☐☐ Determine the type of authentication used to verify the identity of a user.
- ☐☐☐ Configure login settings to make a device more secure.

4.3 Protecting Devices 设备防护

- ☐☐☐ Identify managerial controls related to device security.
- ☐☐☐ Explain how anti-malware software can make a device more secure.
- ☐☐☐ Explain why keeping a device's operating system and software updated makes it more secure.
- ☐☐☐ Configure a host-based firewall.

4.4 Detecting Attacks on Devices 检测设备攻击

- ☐☐☐ Explain how to detect attacks against devices.
- ☐☐☐ Determine controls for detecting attacks against a device.
- ☐☐☐ Evaluate the impact of a device detection method.
- ☐☐☐ Apply detection techniques to identify indicators of password attacks by analyzing log files.

5. Securing Applications and Data 保护应用与数据

5.1 Application and Data Vulnerabilities and Attacks 应用与数据的漏洞与攻击

- ☐☐☐ Explain how adversaries can exploit application and file vulnerabilities to cause loss, damage, disruption, or destruction.
- ☐☐☐ Explain how application attacks exploit vulnerabilities.
- ☐☐☐ Assess and document risks from application and data vulnerabilities.

5.2 Protecting Applications and Data: Managerial Controls and Access Controls 保护应用与数据：管理性控制与访问控制

- ☐☐☐ Explain how the state or classification of data impacts the type and degree of security applied to that data.
- ☐☐☐ Identify managerial controls related to application and data security.
- ☐☐☐ Determine an appropriate access control model to protect applications and data.

☐☐☐ Configure access control settings on a Linux-based system.

5.3 Protecting Stored Data with Cryptography 用密码学保护存储的数据

☐☐☐ Explain how encryption can be used to protect files.

☐☐☐ Apply symmetric encryption algorithms to encrypt and decrypt data.

5.4 Asymmetric Cryptography 非对称密码学

☐☐☐ Determine the appropriate asymmetric key to use when sending or receiving encrypted data.

☐☐☐ Explain why the length of a key impacts the security of encrypted data.

☐☐☐ Apply asymmetric encryption algorithms to encrypt and decrypt data.

5.5 Protecting Applications 保护应用

☐☐☐ Identify the application security principles of secure by design and security by default.

☐☐☐ Explain how user input sanitization protects applications.

5.6 Detecting Attacks on Data and Applications 检测应用与数据攻击

☐☐☐ Explain how to detect attacks on data.

☐☐☐ Determine controls for detecting attacks against applications or data.

☐☐☐ Evaluate the impact of a method for detecting attacks against an application or data.

☐☐☐ Identify whether a file has been altered by verifying its hash.

☐☐☐ Apply detection techniques to identify and report indicators of application attacks by analyzing log files.