CEN429 Secure Programming Week-11

Security Certificates and Penetration Testing Plans

Author: Dr. UÄŸur CORUH

Contents

1 CEN429 Secure Programming **1**
1.1 Week-11 . . . 1
1.1.1 Outline . . . 1
1.1.2 **Week-11: Security Certificates and Penetration Testing Plans** . . . 1
1.1.3 **Conclusion** . . . 3

List of Figures

List of Tables

1 CEN429 Secure Programming

1.1 Week-11

1.1.0.1 Security Certificates and Penetration Testing Plans Download

- PDF[1]
- DOC[2]
- SLIDE[3]
- PPTX[4]

1.1.1 Outline

- Importance of Security Certificates
- Penetration Testing Plans and Tools
- Certification Processes and Relationships

1.1.2 Week-11: Security Certificates and Penetration Testing Plans

The goal of this week is to learn the importance of security certifications, the standards used, and how penetration testing (PenTest) processes are planned. Security certificates demonstrate the compliance of software and hardware with international security standards, while penetration tests help identify security vulnerabilities and analyze potential threats.

1.1.2.1 1. Importance of Security Certificates Theoretical Explanation: Security certificates indicate that a system or product meets certain security standards. Certificates usually provide assurance to users that a product has undergone specific security testing.

- **Why Important?**

[1] pandoc_cen429-week-11.pdf
[2] pandoc_cen429-week-11.docx
[3] cen429-week-11.pdf
[4] cen429-week-11.pptx

- Provides reliability.
- Shows compliance with international standards.
- Meets regulatory and legal requirements.
- Increases product security level.
- Instills confidence in users and customers.

Application Examples:

1. Analyzing why a system requires a security certificate.
2. Examining the effects of security certificates on commercial products.

1.1.2.2 2. Common Security Certificates and Standards

Theoretical Explanation: Many security standards and certifications are used to ensure the security of hardware and software products. These standards guide how products should be tested and certified.

- **ETSI (European Telecommunications Standards Institute):** Establishes standards for telecommunications and network security.
- **EMV (Europay, MasterCard, Visa):** A standard used to secure card-based payment systems.
- **GSMA:** Security standards for mobile devices and networks.
- **ISO/IEC 27001:** Information security management systems standard.
- **PCI DSS (Payment Card Industry Data Security Standard):** A standard used to secure payment card information.

Application Examples:

1. Creating a network security plan based on ETSI standards.
2. Exploring how PCI DSS compliance is ensured for a payment system.

1.1.2.3 3. EAL (Evaluation Assurance Level) Certification

Theoretical Explanation: EAL (Evaluation Assurance Level) indicates the degree to which a product meets certain security requirements. It provides security assurance at various levels (from EAL1 to EAL7).

- **EAL Levels:**
  - **EAL1:** Functionally tested.
  - **EAL2:** Structurally tested.
  - **EAL3:** Methodically tested and checked.
  - **EAL4:** Design reviewed and methodically tested.
  - **EAL5:** High assurance, semantically analyzed.
  - **EAL6 and EAL7:** Extremely high security level, mathematically proven.

Application Examples:

1. Investigating how the EAL certification process works.
2. Assessing the security of a system based on EAL levels.

1.1.2.4 4. Penetration Testing (PenTest) Plans

Theoretical Explanation: Penetration testing simulates attacks to identify vulnerabilities and security weaknesses in a system. Penetration testing plans include the areas to be tested, methodology, objectives, and process.

- **Why Conduct Penetration Testing?**
  - To identify security vulnerabilities.
  - To test the system against real-world attacks.
  - To strengthen defense mechanisms by identifying weaknesses.
  - To proactively improve system security.

PenTest Process Steps:

1. **Reconnaissance:** Gathering information about the system.
2. **Scanning:** Identifying open ports, services, and vulnerabilities.
3. **Exploitation:** Exploiting identified vulnerabilities to gain access.
4. **Privilege Escalation:** Gaining administrative privileges within the system.
5. **Maintaining Access:** Making the access permanent.

6. **Evidence Collection:** Documenting the discovered vulnerabilities.

Application Examples:

1. Creating a penetration testing plan for a web application.
2. Simulating real-world attacks to analyze the security weaknesses of a system.

1.1.2.5 5. Penetration Testing Methods Theoretical Explanation: Penetration testing methods vary depending on the type of system and attack objectives. Common testing methods include:

- **Whitebox Testing:** The tester has knowledge of the system's internal structure and source code.
- **Blackbox Testing:** The tester has no prior knowledge of the system. Attacks are carried out from the outside.
- **Graybox Testing:** The tester has partial knowledge of the system. For example, they may have information about the application structure or user roles.

Application Examples:

1. Analyzing the differences between whitebox and blackbox testing.
2. Conducting graybox testing on a system and reporting the results.

1.1.2.6 6. Penetration Testing Tools Theoretical Explanation: Various tools are used during penetration testing to analyze system vulnerabilities. These tools are chosen based on the scope and objectives of the test.

- **Nessus:** A popular tool used for vulnerability scanning.
- **Metasploit:** A framework used for exploiting vulnerabilities and testing weaknesses.
- **Wireshark:** A tool used to monitor and analyze network traffic.
- **Burp Suite:** A tool used for security testing of web applications.
- **OWASP ZAP:** An open-source tool used to detect security vulnerabilities in web applications.

Application Examples:

1. Scanning a system for security vulnerabilities using **Nessus**.
2. Exploiting a security vulnerability using **Metasploit** and analyzing the results.

1.1.2.7 7. The Relationship Between Penetration Testing and Certification Theoretical Explanation: Penetration testing results play a crucial role in the security certification process of a system. Certification bodies often consider penetration test results to verify the security of a system.

- **How Are They Related?**
  - PenTest results are included in the certification process, proving the security level.
  - Specific tests must be passed successfully to obtain a security certificate.
  - Regular penetration tests are conducted to ensure certification compliance.

Application Examples:

1. Analyzing how penetration test results can be integrated into the certification process.
2. Preparing a security testing plan in line with certification requirements.

1.1.3 Conclusion

This week, we examined the impact of security certifications and penetration testing on system security. Security certificates demonstrate compliance with international standards, while penetration tests uncover vulnerabilities and improve the security of a system. These two processes work together to enhance the security level of software and hardware products.

$$End - Of - Week - 11$$