Lecture 1: Introduction to Information Security

BKACAD's Security Training

Table of Content

Information Security Overview

Hacking Concepts, Types & Phases

Ethical Hacking / Penetration Testing

Information Security Control

Laws & Standards

Information Security Overview

Information Security is the practice of preventing unauthorized access, use, disclosure, modification, disruption or destruction of information.

Information Security Overview

Elements of Information Security

- CIA
- AAA
- Non-Repudiation

Hacking Concepts, Types & Phases

Hacking: Exploiting system vulnerabilities and compromising security controls to gain unauthorized access to system resources

Hacking Concepts, Types & Phases

Hacker Classes:

- Black Hats
- White Hats
- Gray Hats
- Suicide Hackers
- Script Kiddies
- Cyber Terrorists
- State Sponsored Hackers
- Hacktivist

Hacking Concepts, Types & Phases

Five Phases of Hacking:

1. Reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Clearing Tracks

Ethical Hacking

Ethical Hacking: Using tools and techniques to identify vulnerabilities w/ permission

Pentest Phases = Planning + Hacking Phases + Reporting

Penetration Testing

Planning Phase

ROE (Rules of Engagement)

- Formal permissions to conduct a penetration test
- Acts as a guideline for penetration testers & clearly explain the allowed and restricted activities during the test

Penetration Testing

ROE Includes

- Specific IP addresses/ranges to be tested
- Restricted hosts
- List of acceptable testing techniques
- Times when testing is to be conducted
- Points of contact for the penetration test team
- Handling of information collected by the penetration test team

Penetration Testing

Understand Customer Requirements

- Identify what needs to be tested
- Creating checklist of testing & testing requirement
- Identify time frame & testing hours
- Develop an emergency plan

Penetration Testing

Sign Penetration Testing Contract

- Non-Disclosure Clause
- Objective of Penetration test
- Fees and Project schedule
- Sensitive Information

Sign Confidentiality Agreement

Sign Non-Disclosure Agreement

Penetration Testing

Open Source Penetration Testing Methodology

- OWASP
- OSSTMM
- ISSAF
- NIST

Information Security Control

Information Assurance

Network Security Zoning

Defense in Depth

Security Policies

Physical Security

Risk Management

Laws & Standards

Payment card Industry Data Security Standard (PCI DSS)

ISO/IEC 27001:2013

Health Insurance Portability and Accountability Act (HIPAA)

Vietnam’s Cyber Security Law