Principles of Cyber Security_ Lecture 02- Requirements for computer protection

Contents

Lecture 02: Describe how to defend against attacks

Outline

- Overview
- Objectives
- Tips
- Quick Quizzes
- Class Discussion Topics
- Additional Projects
- Additional Resources
- Key Terms

Principles of Cyber Security_ Lecture 02- Requirements for computer protection

Lecture Notes

Overview

Lecture 2 will look at who is responsible for different types of attacks and what the ***fundamental defenses*** against attackers are.

Lecture Objectives

2.1 Identify the types of attackers that are common today

2.2 Describe the five basic principles of defense

OB.2.1: Identify the Types of Attackers That are Common Today

2.1.1 Types of Attackers:

Within the realm of computer security, various threat actors manifest, each with distinctive objectives and methodologies. Let's delve into a few archetypes:

- **Malicious Hackers:**
  - Within the cybersecurity landscape, individuals commonly referred to as "malicious hackers" leverage their technical prowess for illicit activities. Their endeavors may involve unauthorized access to computer systems, exfiltration of sensitive data, or intentional disruption of computational processes.

- **Cybercriminal Syndicates:**
  - Syndicated groups within the cybercrime sphere orchestrate activities with the primary motive of financial gain. Their sophisticated tactics encompass deploying malicious software to compromise systems, subsequently demanding ransom payments—a contemporary manifestation of digital extortion.

- **Nation-State Operatives:**
  - State-sponsored actors, emblematic of cyber-espionage, pursue intelligence objectives on behalf of their respective nations. Such operatives engage in sophisticated cyber activities, including infiltrating systems and conducting covert operations to obtain sensitive information.

- **Insider Threats:**
  - The insider threat paradigm underscores the risk posed by individuals within an organization with authorized access. These individuals may intentionally compromise security protocols, perpetrate data breaches, or inadvertently facilitate external attacks through compromised access privileges.

- **Hacktivism:**
  - Cyber activists, colloquially known as hacktivists, employ their computational prowess as a means of advancing ideological or political causes. Tactics employed include website defacements, distributed denial of service (DDoS) attacks, or the exposure of sensitive information to garner attention for their socio-political agendas.

Principles of Cyber Security_Lecture 02- Requirements for computer protection

OB.2.2: Describe the Five Basic Principles of Defense

In computer security, there is no simple solution to securing information. This can be seen through the different types of attacks that users face today, as well as the difficulties in defending against these attacks.

2.2 Defending Against Attacks

1. Through multiple defenses may be necessary to withstand an attack, these defenses should be based on five fundamental security principles: layering, limiting, diversity, obscurity, and simplicity.

2.2.1 Five Fundamental Security Principles

- **Layering**

1. That information security must be created in layers.
2. One defense mechanism may be relatively easy for an attacker to circumvent. Instead, a security system must have layers, making it unlikely that an attacker has the tools and skills to break through all the layers of defenses.
3. Layered approach (also called defense-in-depth) can also be useful in resisting a variety of attacks. Layered security provides the most comprehensive protection.

- **Limiting**

1. Limiting access to information reduces the threat against it.
2. Only those who must use data should have access to it. In addition, the amount of access granted to someone should be limited to what that person needs to know.
3. Some ways to limit access are technology-based, while others are procedural.

Tip	What level of access should users have? The best answer is the least amount necessary to do their jobs, and no more.

- **Diversity**

1. Explain that layers must be different (diverse) so that if attackers penetrate one layer, they cannot use the same techniques to break through all other layers.
2. Using diverse layers of defense means that breaching one security layer does not compromise the whole system.

Principles of Cyber Security_ Lecture 02- Requirements for computer protection

- **Obscurity**

1. An example of obscurity is not revealing the type of computer, operating system, software, and network connection that a computer uses. An attacker who knows that information can more easily determine the weaknesses of the system.
2. Obscuring information can be an important way to protect information.

- **Simplicity**

1. Explain that information security is by its very nature complex. Complex security systems can be hard to understand, troubleshoot, and feel secure about.
2. Mention that as much as possible, a secure system should be simple for those on the inside to understand and use. Complex security schemes are often compromised to make them easier for trusted users to work with. Keeping a system simple from the inside but complex on the outside can sometimes be difficult but reaps a major benefit.

2.2.2 Frameworks and Reference Architectures

1. The industry-standard frameworks and reference architectures provide a resource of how to create a secure IT environment.
2. Various frameworks/architectures are specific to a particular sector (industry-specific frameworks) such as the financial industry.
3. Discuss how some of the framework/architectures are domestic while others are worldwide (national vs. international).

Quick Quiz 2

1. _______ is a generic term used to describe individuals who launch attacks against other users and their computers.
2. The motivation of which type of threat actor may be defined as ideology, or attacking for the sake of their principles or beliefs?
   a. script kiddies
   b. hactivists
   c. nation state actors
   d. insiders
3. Attackers who do their work by downloading automated attack software from websites and use it to perform malicious acts are known as which of the following?
   a. script kiddies
   b. hactivists
   c. nation state actors
   d. insiders
4. In which fundamental security principle would only those personnel who must use data have access to it?
   a. layering
   b. limiting
   c. diversity

d. obscurity

5. Which fundamental security principle involves not revealing the type of computer, version of operating system, or brand of software that is used?

e. layering

f. limiting

g. diversity

h. obscurity

2.2.3 Class Discussion Topics

1. What are the differences between hactivists and state-sponsored attackers?
2. Ask students to explain why creating a defense-in-depth is a good strategy when creating a secure IT environment.

2.2.4 Additional Projects

1. Read more about phishing scams and write a report with a series of guidelines to recognize them and other fraudulent e-mails.
2. Nessus is a widely used free vulnerability scanner tool used by many security experts.

   Try to read more about Nessus and write a report summarizing its more important features.

2.2.5 Additional Resources

1. FTC – Computer Security

   http://www.consumer.ftc.gov/topics/computer-security
2. How to recognize phishing e-mail messages, links, or phone calls

   http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx
3. Anti-Phishing Working Group

   http://www.antiphishing.org/
4. SANS' Information Security Reading Room

   http://www.sans.org/reading_room/
5. Zero day initiative

   http://www.zerodayinitiative.com/