SEC520

Internet Security

Course Introduction

Today's Content

- Instructor , SEC520 WIKI, *Purpose of Course*
- *Course Outline / Evaluation / Policies*
- Course Readings / Resources
- Supplies Check-list (Required for next class)
- Lesson:
  - Basic Security Issues
  - “Inside the Security Mind”
    - Security Plans vs. Security Applications
    - Virtues of Security / Professionalism
- Preparing for Lab1

Basic Security Issues

From textbook “Computer Security Basics”
(*Lehtinen, Russell & Gangemi Sr., Chapter 1*)

- Computer security has gained wider recognition as a result of recent events (911, world-wide terrorism, hacking incidents, WikiLeaks, Edward Snowden, etc).

- “Computer security has different interpretations based on what era the term describes”

  - For example: physical protection (locked rooms), protection of home computer systems, business (and home) continuity (backups), data protection (online database management systems).

Basic Security Issues

From textbook “Computer Security Basics”
(*Lehtinen, Russell & Gangemi Sr., Chapter 1*)

- Basic principals of computer security encapsulated in CIA model (goals / objectives) of computer security: **CIA**:
  - ***C****onfidentiality*
  - ***I****ntegrity*
  - ***A****vailability*
- *Within the CIA model, the AAA protocol is widely used and recognized:*
  - ***A****uthentication (prove who you say you are)*
  - ***A****uthorization (who can do what task)*
  - ***A****ccountability (leave an audity trail)*

Basic Security Issues

From textbook "Computer Security Basics"
(*Lehtinen, Russell & Gangemi Sr., Chapter 1*)

- Threats to computer security come in many forms:
  - Physical (breakins)
  - Natural (disasters)
  - Hardware (failure, surges, etc)
  - Software (bugs, vulnerabilities)
  - Media (stolen data)
  - Emination (electromagnetic radiation)
  - Communication (via network)
  - Human (mistakes, not following policies, etc)
  - Malicious Hackers (inside and outside)

Inside The Security Mind

- The following concepts are contained in the textbook: “Inside the Security Mind, Making the Tough Decisions”, Kevin Day

- A security countermeasure (Wikipedia) is a “measure or action taken to counter or offset an undesirable action”.

- “If a security effort is to be successful and durable without draining vast recources from our organization, it has to be addressed not only in technology, but within the mind” (or an appropriate security plan).

- There is a tendency for people to rely on technology and “gimiks” as opposed to consistently **following a set of essential practices or “guidelines”**. In other words, effective information security professions adopt a “Security Mind”, and religiously follow a simple set of virtues and rules (i.e. guidelines and principles).

Inside The Security Mind

- Although the profession of Information Security is relatively new, certain “age-old” principles can be used to protect (or harden) an organizations IT system.

- Like security guidelines, accounting guidelines have been in place for centuries to prevent fraud including:
  - Policies & Procedures
  - Training & Communication Procedures
  - Generally Accepted Accounting Principles
  - Control Methods
  - Verification (Audits)

Four Virtues of Security

In the above mention text book, **“Good security is all about <u>focus</u>” and consistently “following the guidelines”**. The following general guidelines should be considered involving Information security:

- Daily Consideration
  - Security must be considered for every decision that the organization makes (eg. Install new program, adding or changing procedures).
- Community Effort
  - Community extends within the outside the organization. Keep informed within the community to “stay ahead” of the security threats”. Orgnaziations such as the Government (CIA, NSA) as well as private industry (SANS Institute) provide information, resources and “best practices”.

Four Virtues of Security

- Higher Focus
  - Following the rule of Least privilege where it is safer to deny all access, then allow access when required. This is not an easy task, especially if tasks that were normally granted are “taken away” (for example Seneca IT and computing professors).

- Education
  - Consistently following policies and Procedures, and providing training / communication to employees (users). You will learn one of the biggest threats to computer security is human vulnerability.

Professionalism

Q: Why should I consistently following guidelines when security threats change constantly?

A: To be a IT Security professional (or any professional in a particular field), you need to consistently follow a set of proven (and possibility) established guidelines.

According to WIKIPedia:

To profess is "to claim to have knowledge or understanding of (a given area of interest, subject matter)."

Professionalism

WIKIPedia indicates the term **Professionalism** has the following attributes:

"a high degree of systematic knowledge; strong community orientation and loyalty; self-regulation; and a system of rewards and diciplinary measures defined and administered by the community of workers"

Professionalism

In order to maintain professionalism, there exists a mechanism of "checks and balances":

- Systematic Knowlege (set of **guidelines**)
- Strong Community (**support** and **resources**)
- Self Regulation (**compliance** of guidelines)

Without this mechanism, IT security professionals will NOT face security challenges (recognized or new) in a time-tested framework, which will lead to negative outcomes. This is why good IT security experts make the big bucks! They earn it! They don't panic! They follow guidelines!

Performing Lab1

Perform the Following Lab:

Lab 1: Setup Hard Disk Pack for labs

It is extremely important to “hit the ground running” prior to next week! It will be assumed that you have completed lab1 before the start of week 2…