Computer Security Key Definitions

Objectives

- Understand what the key terms are for computer security
- Discuss the how each of the key terms are used
- Discuss some examples of each

Asset

- An asset is anything that needs to be protected
- This could be:
    - Information – Examples: medical records, social security numbers, banking data
    - Computer System – Examples: defense systems, critical infrastructure
    - Service – Examples: Websites, life/safety systems
    - Facilities that house any of the 3 above

Threat/Threat Agent

- A threat is any potential violation of security that could cause harm to the asset.
- This could be:
    - Someone wanting to do harm
    - An insecure service
    - Unacknowledged system, service, information
- A threat agent is anyone or anything that wants to do harm or harms an asset
    - Hackers
    - Hacktivists
    - Not malicious entity – Example: someone that accidentally runs into a power pole and knocks out power to a facility

Vulnerability

- A vulnerability is a flaw or weakness in the design or implementation of an asset that could be used by a threat or threat agent to undermine security
- The could be:
  - Incorrect configurations of a system
  - An open port on a networked computer
  - Poor backup strategy
  - Poor coding

Exploit

- An exploit is any software or tools that are intentionally used to take advantage of a vulnerability on an asset.
- This could be:
  - Hacking tools such as: Metasploit, Ophcrack
  - A crowbar that is used on a cracked door – think of physical security here

Risk

- A risk is the probability that a threat will take advantage of a vulnerability on an asset and cause harm.
- Think about risk of losing data. For example: If I only have 1 backup copy of data from my main computer. If I lose that backup, the risk is higher that my data may be lost.
- How about risk of a personal photo collection vs a banking system. The risk that an threat agent wants to get the data is much higher on the banking system.

Attack

- An attack is any intentional or unintentional event that harms or intends to harm an asset.
- Examples:
  - Denial of Service attack
  - Data breach
  - Physical destruction of equipment

Mitigation/Compensating Control

- Mitigation is any tool, service or system that lessens the risk of attack.
- Compensating control is any tool, service or system that takes lowers the risk of attack on an asset by intentionally getting in the way of the threat.
    - For example: A firewall in between a vulnerable system and the internet

An example where all definitions are used

- Back in 2010, the university suffered from a 2 day complete internet outage due to a denial of service attack
- The assets that were impacted were the internet, the firewalls, the computer systems that were unable to get to the internet, the people trying to do their jobs but couldn’t, etc.
- The vulnerability was the recursive DNS servers that are used to translate IP addresses into names.
- The exploit was the sending massive amounts of traffic to the DNS servers
- The threat agent was someone or something sending us massive amount of traffic. We still aren’t sure who it was.
- The mitigation was determining what the attack structure looked like and placed code on the DNS servers to drop the packets.
- The compensating control was putting the recursive servers behind a firewall that could handle the traffic appropriately.