Agenda

- What Are You Trying to Protect?
- Whom Are You Trying to Catch?
- What Are Common Types of Attacks?
- Attack Tools
In a word, you are trying to protect assets. An organization’s assets can include the following:

- Customer data
- IT assets and network infrastructure
- Intellectual property
- Finances and financial data
- Service availability and productivity
- Reputation
Customer Data

- Customer private data is vulnerable to theft and abuse by another individual.
- When private data is used to impersonate an individual, the outcome is called identity theft.
IT assets and Network Infrastructure

- Hardware, software, and services
- Threats can exist, both internal to the IT infrastructure and external, given that the IT infrastructure is connected to the Internet.
- Damage to data caused by new threats includes armored virus, ransomware, and cryptolocker malware, which can cost corporations time and money to fix or replace.
Armored viruses have hardened code that makes it difficult to reverse-engineer and build an anti-virus for the malware.

Ransomware is a new form of malware linked to a time clock, forcing the victim organization to pay a ransom to prevent its data from being deleted.

Cryptolocker is a specific form of ransomware that encrypts critical files or data until the victim pays a ransom to obtain the decryption keys.
In February 2016, Hollywood Presbyterian Medical Center was a victim of ransomware using a cryptolocker malware application. The cryptolocker malware locks systems by encrypting critical files and demanding a ransom to obtain the decryption key. Hollywood elected to pay the ransom of $17,000 using Bitcoin to obtain the decryption keys. The hospital made the decision to pay the ransom and return to normal operations. In this case, no data breach occurred, but the incident resulted in a complete loss of control of all computer systems, given that critical files were encrypted and thus rendered unusable.

more info here: CBS news
https://www.youtube.com/watch?v=RJhowoj960w
or ABC news: Ransomware a top threat in 2017
https://www.youtube.com/watch?v=vQHp1xWYtf4
Intellectual Property

- **Intellectual property** is the center of many organizations. Intellectual property is an asset of an organization. It can be a unique business process or actual data such as customer data.
- Examples of intellectual property include such things as patents, drug formulas, engineering plans, scientific formulas, and recipes.
- The core issue from an IT security perspective is protecting the theft of intellectual property and preventing its release to competitors or to the public. The theft of intellectual property can nullify an organization’s competitive advantage.
Finances and Financial Data

- Real financial assets, such as bank accounts, trading accounts, purchasing accounts, corporate credit cards, and other direct sources of money or credit.
- Data that allows access to real financial assets, usernames and passwords for banking or investment accounts.
- Loss of financial data due to malicious attacks not only represent significant physical loss, but can also have long-term effects on a company’s reputation and brand images.
Service Availability and Productivity

- Computer applications provide specific services that help organizations conduct business operations. It is important that critical services be available for use when organizations need them.
- When the uber server is not available, customers can’t order uber rides.
- When american airline’s server is not available, customers can’t book flights.
- Imagine when the Pornhub server is not available?
- Imagine when the Ashley Madison (the "Life is short. Have an affair" website) server is not available?
Service Availability and Productivity

- **Downtime** is the time during which a service is not available due to failure or maintenance. Downtime can be intentional or unintentional.

- System administrators often schedule **intentional downtime** in advance, for example, when servers need operating system upgrades or patches.

- **Unintentional downtime** is usually the result of technical failure, human error, or attack.

- **Opportunity cost** is the amount of money a company loses due to downtime. Opportunity cost usually measures the loss of productivity experienced by an organization due downtime. Suppose American Airline’s reservation server fails. While the server is down, no customers can book flights. You can measure the opportunity cost of that downtime in the dollar amount of the unsold tickets.
One of the most important things that information security professionals try to protect is their organization’s reputation and brand image.

Companies that suffer from security breaches and malicious attacks that expose any assets are likely to face serious negative consequences in the public eye.

Among other consequences, this could lead to a decline in the organization’s revenue, net worth, and market capitalization.
Whom Are You Trying to Catch?

- **hacker** in the computing community, the term hacker generally describes a person who enjoys exploring and learning how to modify something, particularly related to computer systems. Hackers, for good or bad, are considered to be experts and tinkerers, but because of the way the media negatively portrays the term, hackers are often the subject of some controversy.

- **cracker** A cracker has a hostile intent, possesses sophisticated skills, and may be interested in financial gain. Crackers represent the greatest threat to networks and information resources.

- **script kiddie** a wannabe hacker, a person of any age with little or no skill. This person simply follows directions or uses a "cookbook" approach to carrying out a cyberattack, without fully understanding the meaning of the steps he or she is performing.
Whom Are You Trying to Catch?

Hackers can be categorized as follows:

- **black-hat hacker** a black-hat hacker tries to break IT security and gain access to systems with no authorization in order to prove technical prowess. Black-hat hackers generally exploit holes in systems, but they generally do not attempt to disclose vulnerabilities they find to the administrators of those systems. They tend to promote the free and open use of computing resources as opposed to the notion of security.

- **white-hat hacker** a white-hat hacker, or ethical hacker is an information systems security professional who has authorization to identify vulnerabilities and perform penetration testing. White-hat hackers will identify weaknesses for the purpose of fixing them, and black-hat hackers find weaknesses just for the fun of it or to exploit them.

- **gray-hat hacker** a gray-hat hacker is a hacker with average abilities who may one day become a black-hat hacker but could also opt to become a white-hat hacker.
Attack Tools

- Protocol analyzers
- Port scanners
- OS fingerprint scanners
- Vulnerability scanners
- Password crackers
- Keystroke loggers
Protocol Analyzers

- **Protocol analyzer** or packet sniffer is a software program that enables a computer to monitor and capture network traffic, whether on a LAN or a wireless network.
- Attackers can capture and compromise passwords and cleartext data.
- Example: **Wireshark**
Port Scanner

- **Port scanner** is a tool used to scan IP host devices for open ports that have been enabled. This provides attackers with valuable information that can be used in the attack.

- Example: **nmap**
Operating system fingerprint scanner is a software program that allows an attacker to send a variety of packets to an IP host device, hoping to determine the target device’s operating system from the response.

Once an attacker knows what OS and version is installed, the better chance he has to use applicable software vulnerabilities and exploits.

Example: nmap
Vulnerability Scanners

- **Vulnerability scanner** is a software program that is used to identify and, when possible, verify vulnerability on an IP host device. From this information, a vulnerability scanner compares known software vulnerabilities in its database with what it has just found.

- Attackers can capture and compromise passwords and cleartext data.

- For a complete and up-to-date list of known software vulnerabilities and exposures, visit [https://cve.mitre.org](https://cve.mitre.org). The **Common Vulnerabilities & Exposure (CVE)** list is maintained and managed by the Mitre Corporation on behalf of the U.S. Department of Homeland Security. This list is now referred to as the **National Vulnerability Database (NVD)**.
Password Crackers

- **Password cracker** is a software program that performs one of two functions: a brute-force password attack to gain unauthorized access to a system or recovery of passwords stored as a cryptographic hash on a computer system.

- **Dictionary password attack**: A subset of brute-force attacks, in which hackers try shorter and simpler combinations, including actual words, because such passwords are so common.
Keystroke Loggers

- **Keystroke logger** is a type of surveillance software or hardware that can record to a log file every keystroke a user makes with a keyboard.

- The keystroke logger might store the log file locally for later retrieval or send it to a specified receiver.

- Employers might use keystroke loggers to ensure that employees use work computers for business purposes only.
Keystroke Loggers Example: Hardware Based

image source: keelog
A large portion of the material is adapted from:

- Fundamentals of Information Systems Security - David Kim, Michael G. Solomon