Intro to Computer Security

Agenda

- Overview of Key Ideas in Computer Security
  - Confidentiality, Integrity, Availability
  - Protecting Data
  - Threats, Vulnerabilities, and Risks
  - Defense in Depth

Exercise - 5 Minutes

- In groups of 2-4, answer the following:
  - What is information security?
  - What things does it include?

Exercise - 5 Minutes

- In groups of 2-4, answer the following:
    - What does it mean to have a secure computer?
    - Can you have a completely secure computer?

> ““The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards—and even then, I have my doubts.””

–Eugene Spafford

Computer Security

- We can see only what we should be able to see
- We can't modify what we should not be able to modify
- We can verify that what we are seeing is from the entity we expect
- We can access the things that should be available
- We are protected: Hackers, failures, negligence, misuse

Confidentiality, Integrity, Availability - CIA Triad

- Confidentiality
  - Only those authorized to view data can view it
  - Might involve proving you have access to data and you are who you say you are
- Integrity
  - Data is not modified from an unauthorized source
  - You can ensure the data is from the source/sender
- Availability
  - Systems and services are available
  - Resilience against attacks, failures, compromise

Exercise - 5 Minutes

- In groups of 2-4, imagine the following:
  - You receive an email from a person you know, how would CIA be applied to that email?
  - You want to check a balance of an account through a web page, how would CIA be applied to that account?

Computer Security - Data

- Applying security to data involves to primary categories:
- Data at Rest
  - Stored files on a filesystem
  - Records in a database
  - Physical folders (physical security)
- Data in Motion
  - Data communicated through a web page
  - Data sent via network
  - Radio data via WiFi, Bluetooth, NFC, LoRa, etc

Exercise - 5 Minutes

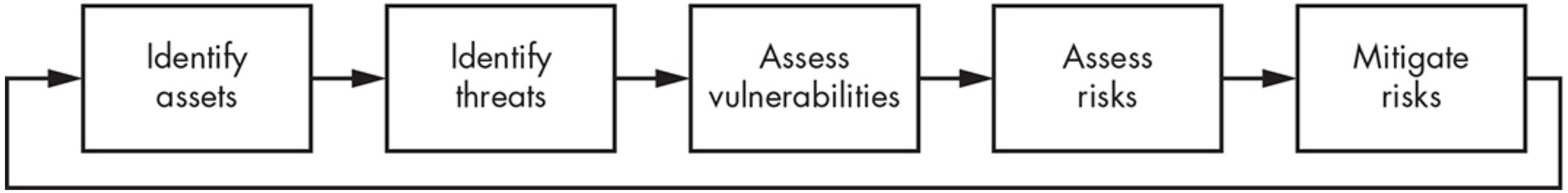
- In groups of 2-4, answer the following:
  - How does confidentially apply to data at rest?
  - What about data in motion?
  - How does integrity apply to data at rest?
  - What about data in motion?
  - How does availability apply to data at rest?
  - What about data in motion?

Threats, Vulnerabilities, and Risks

- Threats
  - Something (person, software, etc) that can cause harm
  - Could be a natural disaster, power outage, etc
- Vulnerabilities
  - Where a system or computer is vulnerable to harm
  - Insecure code, physical security to data center, no backup disk
- Risks
  - The possibility of a threat happening
  - Well known vulnerability in a very popular library → Higher Risk
  - Less known vulnerability on a server that is not connected to a network → Less Risk

How Do We Manage Risks?

- Identify Assets - What do we need to protect?
- Identify Threats - What can harm the things we want to protect?
- Assess Vulnerabilities - What vulnerabilities could have a high impact?
- Assess Risks - What would the impact be of the vulnerability? What are we willing to accept?
- Mitigate Risks - How can we reduce the risk?



Threats, Vulnerabilities, and Risks

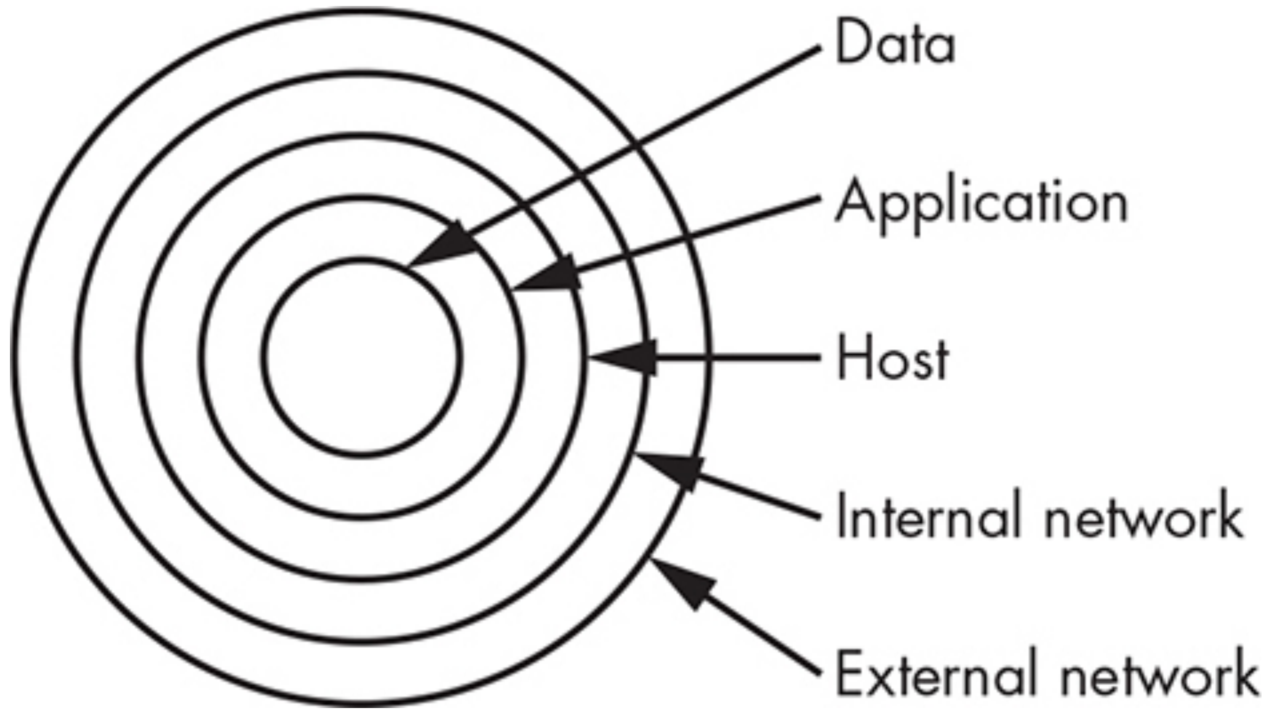
- Personal Photos
- What are the threats?
- What are the vulnerabilities?
- What are the risks?
- How do we manage these risks?

Incident Response

- Usually a separate team within an organization
- Several steps:
  - Preparation - How should we respond to the incident?
  - Detection and Analysis - How can we detect if an incident occurred and understand it?
  - Containment - How do we ensure the damage from the incident does not spread?
  - Eradication - How do we remove the cause of the incident?
  - Recovery - How do we recover from the incident?

Defense in Depth

- When implementing computer security, we want layers
- Don't rely on one single defense (e.g. password to a system)
- Possible layers:
  - External Network - VPN, DMZ, logging, pen testing, etc
  - Network Perimeter - Firewalls, proxies, logging, pen testing, etc
  - Internal Network - IDS, IPS, logging, pen testing, etc
  - Host - Auth, hardening, IDS, IPS, firewall, antivirus, scanning, pen testing, logging, etc
  - Application - Patching, pen testing, auditing, logging, etc
  - Data - Encryption, backups, authorization, etc



Key Takeaways

- CIA - This is our compass
- Data at rest and in transit - Need to protect both
- Threats, vulnerabilities, and risks - Need to identify
- Risks - Sometimes the business will dictate what is acceptable, we need to make our case as professionals
- Incidents will happen - Have a plan
- Defense in depth - Layers!

Intro to Linux and CLI

- Open your VM!