Introduction to Practical Computer Security

Objectives

- Discuss what is practical computer security
- Explain why there is a need for security
- Discuss some of the key terms used throughout the course

Practical Computer Security

- My definition of practical computer security – the means in which computer security is applied in an every day setting
- Many certifications focus on theory and understanding how to implement security controls
- Bottom line is that if you end up putting all the controls you can in place, you will:
    - End up forcing people to find another solution that actually allows them to do their work, which leads to insecurity
    - Managing too much which may lead to too much management in the end

Brief Case Study - 1

- UCCS deployed NAC (Network Access Control) back in 2007.
- Network Access Control:
  - Forces the user to identify who they are via network protocols or logins
  - Can employ other techniques to control how the user behaviors or how their computer behaves
- Our solution back in 2007 was very black and white
  - Antivirus/Antispyware must be running and up to date
  - Windows must be FULLY up to date
  - It would kick you off the network if those weren’t met

Brief Case Study - 2

- Users would be placed into a quarantined vlan until they complied
- Even if users complied it still took around 15 minutes to get everything up to date and back on the network
- This created a situation that instead of securing users, they went around security and used VPN on the open network to access all resources
- We switched vendors and the secured network went from 45% adoption to 95% adoption because we gave the users a 3 day grace period.

The Burden of Computer Security

- Securing computers is tough!
- Many things have to be taken into account when applying computer security
- Example – The user who needs to share files with another user
  - You have a corporate solution
  - Your users don't know how to use it
  - Your users think they know better
  - What is the risk of not knowing

The Need for Security

- There are a 2 reasons why we need to have security in my opinion.
    - Information
        - Intellectual Property
        - Personal information
    - Safety
        - Safety of people
        - Safety of systems
- How we protect information reduces to 3 key points:
    - Confidentiality
    - Integrity
    - Availability