

- 1) What is Operating System and Network Security
  - a) Reliably
    - i) Store
    - ii) Modify
    - iii) Protect
    - iv) And grant access to
  - b) Information, so that it is available only to
    - i) Authorized users
      - (1) Based on ownership or
      - (2) Role within the organization
- 2) OS
  - a) What is an OS?
    - i) Allows interaction between hardware, software, and the user
    - ii) Provide basic input/output
    - iii) Manages resources
- 3) Computer networks
  - a) What is a network
    - i) Linked devices
  - b) LAN
  - c) MAN
  - d) WAN
- 4) Why is security necessary
  - a) Protection of information and resources
  - b) Privacy
  - c) Facilitate workflow
  - d) Addressing Holes or bugs
  - e) Compensating for human error or neglect
- 5) Cost
  - a) Training
  - b) Adding security to a protect when purchased
  - c) Third party security
  - d) Operations
    - i) Configuration
    - ii) Testing
    - iii) Updating
    - iv) TCO
- 6) Types of Attacks
  - a) Machine targeting
  - b) Password misuse
  - c) Virus, etc
  - d) DOS
  - e) Spoofing
  - f) Port Scanning
- 7) Organizations that help prevent attacks
- 8) Hardening your system
  - a) Taking action block attacks
- 9) Built in OS security
  - a) Logon
  - b) Certificate
  - c) File/folder and resource security
    - i) firewalls
  - d) Policies
  - e) Remote access tools
  - f) Disaster recovery
- 10) Built in NOS security
  - a) Authentication/encryption
  - b) Firewalls
  - c) Topology provided enhancements
    - i) Wired more secure than wireless, VPN more secure than standard dial up
  - d) Monitoring
    - i) benchmark
    - ii) Look for opportunities