سبر 1213
Network Defense

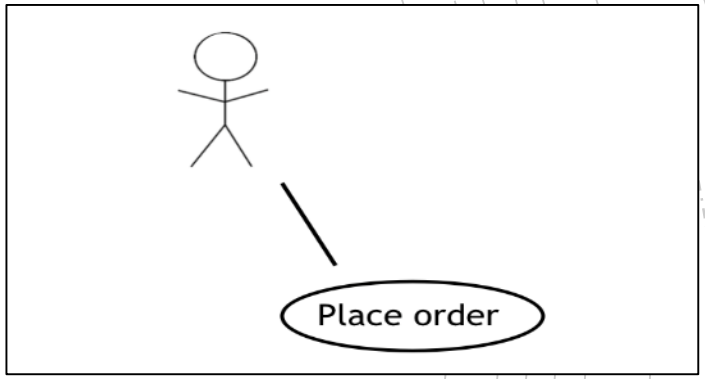
Lecture #1 Part 1
Mastering Security Basics

Topics:

- ✓ Understanding Core Security Goals
- ✓ Introducing Basic Risk Concepts
- ✓ Understanding Security Controls
- ✓ Using Command-Line Tools
- ✓ Understanding Logs

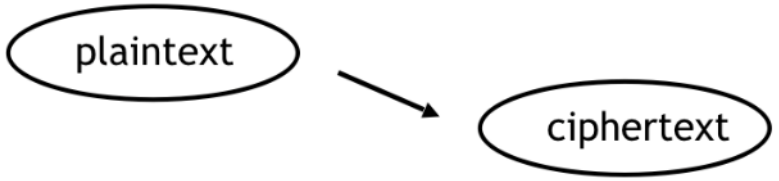
Understanding Core Security Goals

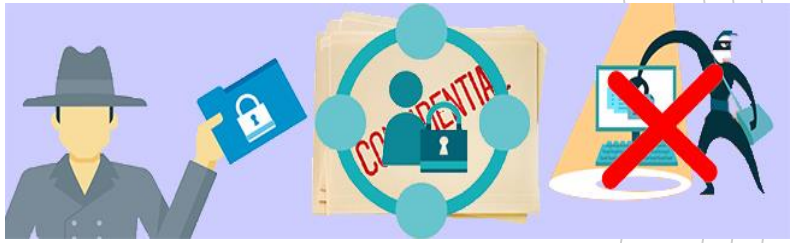
- Use Case – Describes a goal an organization wants to achieve
- Elements
  - Actors
    - Precondition
    - Trigger
    - Postcondition
    - Normal flow
  - Alternate flow



Understanding Core Security Goals

- **Confidentiality**
  - **Encryption**
  - **Access controls**
    - Identification
    - Authentication
    - Authorization





Understanding Core Security Goals

- **Availability**
  - Redundancy & Fault tolerance
  - Scalability and Elasticity
  - Patching
  - Resiliency

Introducing Basic Risk Concepts

- **Threats**
- **Vulnerabilities**
  - Any weakness
- **Risk is**
  - The likelihood that a threat will exploit a vulnerability
- **Risk mitigation**
  - Reduces the chances that a threat will exploit a vulnerability by implementing controls

Understanding Security Controls

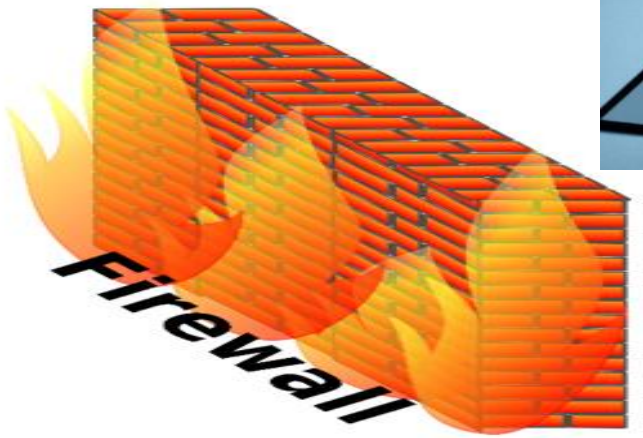
- **Overview**
  - Managerial controls are primarily administrative in function
  - Operational controls help ensure that the day-to-day operations of an organization comply with the security policy
  - Technical controls use technology

Understanding Security Controls

- **Managerial Controls**
  - Risk assessments
  - Vulnerability assessments
- **Operational Controls**
  - Awareness and training
  - Configuration management
  - Media protection
  - Physical and environmental protection

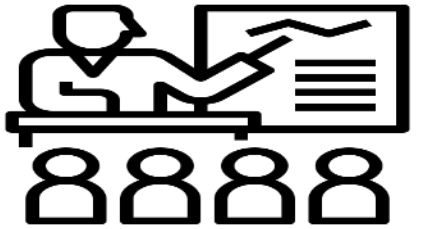
Understanding Security Controls

- **Technical Controls**
  - Encryption
  - Antivirus software
  - IDSs and IPSs
  - Firewalls
  - Least Privilege



Control Types

- **Preventative Controls**
  - Hardening
  - Training
  - Security guards
  - Change management
  - Account disablement policy
  - Intrusion prevention system (IPS)



Control Types

- **Detective Controls**
  - Log monitoring
  - SIEM systems
  - System audit
  - Video surveillance
  - Motion detection
  - Intrusion detection system (IDS)

Control Types

- **Corrective and Recovery Controls**
  - Backups and system recovery
  - Incident handling processes
- **Physical Controls**
- **Compensating Controls**
- **Response Controls**

Control Goals

- **Deterrent**
  - Attempt to discourage individuals from causing an incident
  - Cable locks, hardware locks
- **Compare to prevention**
  - Deterrent encourages people to *decide* not to take an undesirable action
  - Prevention stops them from taking an undesirable action
  - Security guard can be both