Cisco CCNA (200-301)

Defining Key Security Concepts

Learning Objective: Define threats vulnerabilities, exploits and mitigation techniques

Description: A CCNA Professional should be familiar with key security concepts. You will learn how to define the following terms in the context of security: threats, vulnerabilities, exploirts and mitigation techniques.

Q: Why is security terminology so important?

Q: Is important to memorize definitions of these terms?

Q: So how are we going to address these key concepts?

- Asset (a located item that is assessed as valuable to an entity)
- Threats (Potential danger or weakness to assets)
    - Attackers
    - Unrealized Exploit
    - Default settings (unhardened system)
- Vulnerabilities (True danger or weakness to assets)
- Exploits (attack against a weakness)
    - taking advantage of existing weakness in software coding or firmware
- Mitigation Techniques (countermeasures)
    - Administrative (Policy)
    - Technical (Implementation)
    - Physical (Control)

Endnotes, External and Etc.

5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)