CompTIA Security + 1.0 Threats,Attacks and Vulnerabilities

Filename: comptia-secplussy0501-1-3-threat_vector_types_and_attributes
Title: Threat Vector Types and Attributes
Subtitle: CompTIA Security+ (SY0-501)

1.3 Threat Vector Types and Attributes

- 1.3 Explain threat actor types and attributes.
  - Types of actors
    - Script kiddies
      - Lacking expertise in hacking
      - Use existing technologies
        - Scripts (automated approach)
        - Software Programs
        - Considered by the hacking culture to be immature, lazy and a lack of discipline(for not learning the knowledge needed to hack)
    - Hacktivist
      - Undermining a companies reputation
      - Destabilization of and organization
      - Social Change
      - Using computers and networks to promote a political stance
      - Examples
        - Anonymous
        - Lulz Security or LulzSec
      - Scenarios
        - Publishing Emails
        - Publishing SMS records
        - Publishing passwords
        - Sources handing over infomation to WikiLeaks
    - Organized crime
      - Massive attacks that are commonly profit drive
      - Ransomware publishers, black market data thieves selling medical records
    - Nation states/APT
      - They may be directly sponsered by government
      - These threat actors have access to complex systems with financial support of a government unlike smaller goups
      - APT - These attacks can remain undetected for a long time
      - APT - High value targets - Major banks, insurance companies, national defense systems
    - Insiders
      - Countermeasure are in place to stop outsiders like firewalls, antimalware, intrusion detection and prevention.
      - How much does a company invest in preventing the attack from with in the company
        - Can lead to:
          - Fraud
          - Sabotoge of systems or data
          - Theft of Data
          - Destruction of Data
          - Encryption of data
          - Complete Data Loos
          - Unauthorized access to or discloser of data
    - Competitors
  - Attributes of actors
    - Internal/external
      - Insiders vs. everyone else
    - Level of sophistication
      - Organized Crime
      - Nation-state/APT
      - Script-kiddies (not to sophisticated)
    - Resources/funding
      - Organized Crime
      - Nation-state/APT
    - Intent/motivation
      - Hacktivist
      - Insiders
  - Use of open-source intelligence (OSINT)
    - Overt or undesguised
    - Examples
      - Today the media is a HUGH source of open-source intelligence
      - Governments Reports, press conference
      - Social Media
      - Academic publications

- Deep Web