CompTIA Security + 1.0 Threats,Attacks and Vulnerabilities

Filename: comptia-secplussy0501-1-5-vulnerability_scanning_concepts
Title: Vulnerability scanning concepts
Subtitle: CompTIA Security+ (SY0-501)

1.5 Vulnerability Scanning Concepts

- 1.5 Explain vulnerability scanning concepts
  - Vulnerability scanners give the ability to identify a variety of systems across the network including:
    - Laptops
    - Desktops
    - Client and Servers
      - Client-side vulnerabilties
      - Server-side vulnerabilities
  - Passively test security controls
    - Can be performed by PVSs or Passive Vulnerabilty Scanner
    - Passive scan does not locate wireless SSIDs that have be hidden
    - Active scan emit probes to the APs to locate them
  - Identify vulnerabilities
    - Classify
      - Low Importance
      - Medium Importance
      - High Importance
    - Types
      - SMB Detection
      - DCE Enumeration Detection
      - OS Identification
      - Open Ports
      - Open Systems
  - Identify lack of security controls
    - Types(Lack of)
      - Physical Controls
        - Locks
        - Fences
        - Man-traps
      - Access Controls
        - Data
        - Programs
        - Systems
        - Equipment
    - Potential Outcome
      - Intercepting Data
      - Accessing a remote host to steal, modifying data
      - Impersonation of a user/employee/contractor
      - Inserting communications
      - replaying communications
  - Identify common misconfigurations
    - Password Management
      - Weak passwords
      - Password reuse
      - Password Sharing
      - Shared Accounts
    - Unecessary Services
    - Disablng Firewall
    - *Use Windows Server 2016 with MBSA*
    - *Use scan results talking about best practices*
  - Intrusive vs. non-intrusive
    - Intrusive
      - Remember that not all companies can afford downtime while a thorough vulernability scan is performed
      - Intrusive scans could introduce the possibility of downtime
      - destructive security auditing or intrusive scanning can yield more accurate results as the intent is to use the exact same methods an attack would use
      - Intrus
    - Non-intrusive
      - This technique usually employs simple scans such aa file systems, missing updates
  - Credentialed vs. non-credentialed
    - Credentialed scans can give acccess to more information
    - Non-credentialed scans give limited information
  - False positive

- False negative = Incorrectly identified
  - Malicious traffic identified as legitimate
- False positive = Incorrectly identified
  - Legitimate traffic identified as malicious
  - An IDS/IPS learning process will start with a lot of false positives intially then over time will be reduced as the process continues
- True negative = Correctly identified
- True positive = Correctly identified