CompTIA Security + 2.0 Technologies and Tools

Filename: comptia-secplussy0501-2-2-software_based_security_posture_assessment
Title: Software-based Security Posture Assessment
Subtitle: CompTIA Security+ (SY0-501)

2.2 Software-based Security Posture Assessment

- 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.
  - Protocol analyzer
    - Wireshark, Message Analyzer
  - Network scanners
    - Rogue system detection
    - Network mapping
  - Wireless scanners/cracker
    - Show WiFi Explorer
    - Show Details in lower pane
  - Password cracker
    - Cain and Abel
  - Vulnerability scanner
    - Common Vulnerability Scoring System (CVSS)
    - Common Vulnerabilities and Exposures(CVEs)
    - CVE-IDs
    - Rapid7
      - Create Site
      - Add Assests
      - Choose *Audit* Template
      - LocalHost Scanning Engine
      - Save and Scan
      - Load previous results
    - Examples
      - Rapid7
      - nmap
      - nessus
      - OpenVAS
      - Burp Suite(Web Application vulenabilities)
  - Configuration compliance scanner
    - MS Security Configuration Wizard
      - C:\Windows\security\msscw\Policies\
  - Exploitation frameworks
  - Data sanitization tools
    - Overwriting 1's and 0's
    - DoD 5220.22-M Standard
      - Pass 1: Writes a zero and verifies the write
      - Pass 2: Writes a one and verifies the write
      - Pass 3: Writes a random character and verifies the write
    - Examples
      - scrub, Show in CentOS 7
      - DBAN (Darik's Nuke and Boot) Show Boot Disk
      - Active KillDisk
  - Steganography tools
    - iSteg
    - Xiao
    - Image Steganography
    - Stegahide
    - Crypture
    - SteganographX Plus
  - Honeypot
  - Backup utilities
    - On Premise
      - Baracuda
      - Acronic
      - Symantec
      - Windows Server Backup
      - RSync
    - Cloud-Based
      - Carbonite
      - Amazon S3
      - Microsoft Azure
      - OneDrive for Business

        - Dropbox for Business
    - Mention Windows Server Backup is a feature
    - Show features including optimization
- Banner grabbing
    - Telnet Port 25, 21, 80
- Passive vs. active
- Command line tools
    - ping
        - testing reachability
    - netstat
        - viewing connections
        - use telnet port 21, 25
    - tracert
        - mapping connection paths
    - nslookup/dig
        - dig from Mac terminal (*dig {hostname}*)
        - dig from Mac for a record type (*dig @8.8.8.8 www.google.com -t*)
    - arp
        - Controling/Modifying/Viewing ARP table and cache
    - ipconfig/ip/ifconfig
        - ipconfig from Windows Machine
        - ip from CentOS
        - ifconfig from CentOS and Mac
        - Mention grep capabilities
    - tcpdump
        - Mention and show tcpdump options
    - nmap
        - run basic nmap scan (*nmap -v 10.10.10.100*)
    - netcat
        - mention