CompTIA Security + 2.0 Technologies and Tools

Filename: comptia-secplussy0501-2-4-analyze_and_interpret_output_from_security_technologies
Title: Analyze and Interpret Output from Security Technologies
Subtitle: CompTIA Security+ (SY0-501)

2.4 Analyze and Interpret Output from Security Technologies

- 2.4 Given a scenario, analyze and interpret output from security technologies.
  - HIDS/HIPS
    - Snort
    - Mention complexities of setting up snort
    - Sophos takes that burden away
  - Antivirus
    - Eicar File
    - CryptoLocker
  - File integrity check
    - Example 1.
      - Show QuickHash file on desktop
      - Copy to SHA folder
      - Compare message digest
    - Example 2
      - On CentOS run touch file01.txt
      - vi file01.txt
      - a, type "This is my important text", ESC, : , wq
      - sha256sum file01.txt = screenshot value
      - vi file01.txt
      - a, type "This is evil text", ESC, : , wq
      - sha256sum file01.txt = screenshot value
      - Compare the screenshots
  - Host-based firewall
    - Show Firewall Logs
    - C:\Windows\System32\LogFiles\Firewall\pfirewall.txt
  - Application whitelisting
  - Removable media control
    - Educate users and maintain awareness
    - Limit the use of removable media
    - Implement removable media policies
    - Encrypt all removable media
    - Bitlocker to Go
  - Advanced malware tools
    - The "why"
      - Attacks are sophisticated
      - Code Morphing, Obfuscation, Polymorphic
      - Dynamic
      - Databases rely on known threats
      - Zero Days/New Threat Risk
    - Threat Intelligence
      - Global reach
      - Malware Databases
      - Reports (common threats)
      - Research
      - Helps to remain ahead of the curve
    - Heuristics
      - Best guess effort
      - False Positives
  - Patch management tools
    - Windows Update
    - WSUS
    - System Center Configuration Manager
    - yum, apt-get
  - UTM
  - DLP
  - Data execution prevention
    - Advanced System Properties
    - No Execute
  - Web application firewall