CompTIA Security + 2.0 Technologies and Tools

Filename: comptia-secplussy0501-2-3-troubleshoot_common_security_issues
Title: Troubleshoot Common Security Issues
Subtitle: CompTIA Security+ (SY0-501)

2.3 Troubleshoot Common Security Issues

- 2.3 Given a scenario, troubleshoot common security issues.
  - Unencrypted credentials/clear text
    - FTP, Telnet, PAP, HTTP
  - Logs and events anomalies
    - Clear log Audit Logs in Windows
  - Permission issues
    - Win10-2 Shared Folder (wbryan)
    - Connect from Win01
  - Access violations
  - Certificate issues
    - Show Local Cert Store Intermediate CA\CRLs
    - http://www.badssl.com
  - Data exfiltration
    - FTP
  - Misconfigured devices
    - Firewall
      - Disabled/Enabled
      - Authentication Mismatchs in wf.msc
      - Rule miconfiguration
    - Content filter
      - Show Filtering in MSAs
    - Access points
      - Show http://ui.linksys.com
      - Weak Cipher(WPS)(WEP)
      - Unencrypted Remote Management
  - Weak security configurations
    - Show TLS1.0 Connection on http://www.badssl.com
    - Mentioned throughout
  - Personnel issues
    - Policy violation
    - Insider threat
    - Social engineering
    - Social media
    - Personal email
  - Unauthorized software
    - Remove the root Certificate for notepad++
    - Applocker
  - Baseline deviation
    - SCW
  - License compliance violation (availability/integrity)
  - Asset management
  - Authentication issues
    - Domain Issues
      - Missing Domain Trust
      - Unavailable Logon Server
      - Extrememly strict policies
      - Anonymous login (missing non-repudiation)
    - User
      - Incorrect password
      - User lockout