filename:comptia-secplussy0601-9-3-1-vulnerability-scans
Showname: Security+ (SY0-601)
Topic: Operational Security and Incident Response
Episode: Vulnerability
Learner Objectives:

Summarize the techniques used in security assessments.

Description:In this episode, the viewer will identify the types of vulnerability scans suchs as credentialed vs. non-credentialed, intrusive vs. non-intrusive as well as scan results type like false positives and negatives as well as true positives and negatives

---

- Why would we want to perform penetration testing?
    - Detail examination of an organization's security posture
    - Using an attacker mindset and techniques to exploit an organizations vulnerabilities
- Penetration testing
    - White-box
        - Full knowledge of the environment
    - Black-box
        - Completely unknown environment
    - Gray-box
        - Partial knowledge of the environment
    - Rules of engagement
        - RoE
        - Timeline for the test
        - When the test can happen
        - What can be tested
        - What data can be gathered

        - Legal concerns
        - Third-party concern
        - Communication
    - Recon, inital access, priviledge escalation, pivoting, lateral movement, persistence
    - Cleanup
    - Bug bounty