filename:comptia-secplussy0601-9-5-1-pentesting-techniques
Showname: Security+ (SY0-601)
Topic: Operational Security and Incident Response
Episode: Pentesting Techniques
Learner Objectives:

Explain the techniques used in penetration testing

Description:In this episode, the viewer will identify the techniques used in penetration testing such as white and black box testing, rules of engagement, persistence, pivoting, lateral movement, privilege escalation , cleanup and bug bounties

---

- 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