filename:comptia-secplussy0601-9-6-1-pentesting-exercise-types
Showname: Security+ (SY0-601)
Topic: Operational Security and Incident Response
Episode: Pentesting Exercise Types
Learner Objectives:

Identify the techniques used in penetration testing

Description:In this episode, the viewer will identify the techniques used in penetration exercise types commonly known and red, blue, purple and white team exercises.

- Exercise types
    - Red-team
        - Offensive Security
        - Testing defense mechanism and resiliency to external attacks
        - Test/improves the capabilities of the defense mechanisms
        - Identify and exploit vulnerabilities
        - Physical, hardware, software and human vulnerabilities
        - Help address and fix identified security vulnerabilities
        - Typically not part of the company
        - Skill examples
            - computer systems and protocols
            - software development skills
            - penetration testing
            - Communication interception
            - Social engineering skills
            - Attack frameworks (MITRE ATT&CK)
    - Blue-team
        - Defensive security

    - Identify potential vulnerabilities
    - But instead of exploiting the vulnerabilities, they seek to avoid, deter, resist an respond to threats
    - Think of it a monitoring, detection and reaction (what countermeasure need to be in place or upgrade, reconfigured)
    - Detect block mitigate
    - Usually part of the company
    - IDS, IPS, packet analysis, log/packet aggregation
    - EDR (endpoint detection and response)
    - Honey-pots
    - Skill examples
      - Security strategy
      - Analysis skills
      - Hardening techniques
      - System detection tools
  - Red-team/blue-team discussions
    - Red-team discusses the attack methods used, actions take
    - Blue-team can use this information to evalute and prioritize changes to prevent another similiar attack from being successful.
    - Lack of sharing information of attack techniques and tools gave rise to the “purple team”
  - Purple-team
    - Red and blue teams working in unison
    - Both teams fully debrief each other
    - Both teams sharing information like
      - Attack techniques
      - Attack tools
      - Finding and outcomes
  - White-team
    - Responsible for refereeing the red team/blue team engagement
    - Observes the excerise
    - Scores the exercise

- Resolve disputes between the red/blue team
- The judges of that enforce the RoE
- Derive the lessons-learned
- Accurate post-exercise/engagement assessment