- Filename: eccouncil-ceh31250-v10-1-4-1-intro_to_ethical_hacking_pentesting.md
- Show Name: CEHv10 (312-50)
- Topic Name: Introduction
- Episode Name: Intro to Ethical Hacking: Pentesting
- Description: In this episode, Daniel and Zach walk you through the basic terminology and practices of Pentesting. Here you will see pentesting defined, as well as why it's needed and how it differs from other types of security assessments. You'll also be introduced to the different types of security teams, types of pentests, pentesting phases, and pentesting methodologies.

==

Intro to Ethical Hacking: Pentesting

- Penetration Testing Concepts
    - Define Pentesting
        - What is it?
            - Thorough and practical security assessment
            - Done through actual discovery and exploit of found weaknesses
            - Documents the findings in delivered report
            - Suggests mitigation
        - Why engage in it?
            - Find the flaws before the bad guys do
            - Compliance and Regulation
            - Evaluate current security posture and attack surface
        - How does it differ from other types of Security Assessments?
            - Security Audit
                - Verifies that org is security policy compliant
            - Vulnerability Assessment
                - Discovery of actual security vulns
                - Exploitability of found vulns
                - Explore possible fallout from exploitation
            - Pentest
                - Proves the exploitability of vulns
    - Teams defined (DIAGRAM)
        - Blue Team
        - Red Team
            - Little to no external access
            - May or may not give Blue Team a heads-up before conducting tests
    - Types of Pentests
        - Black-box
        - White-box
        - Grey-box
    - Pentesting Phases
        - Pre-Attack
            - Planning and prep
            - Methodology design
            - Info gathering
        - Attack

    - Penetrate perimeter
    - Target Acquisition
    - Priv Esc
    - Execution, implantation, retraction
  - Post-Attack
    - Report delivery/presentation
    - Clean-up
    - Artifact destruction
- Testing Methodologies
  - https://www.owasp.org/index.php/Penetration_testing_methodologies
  - EC-Council LPT Methodology