Pentesting Fundamentals

1. What is Penetration Testing:

- There are over 2,200 cyber-attacks every day - 1 attack every 39 seconds.

2. Penetration Testing Ethics:

- White VS Grey VS Black Hat Hackers
- Rules of Engagement

3. Penetration Testing Methodologies:

- Pentesting Stages:
  - Information Gathering
  - Enumeration/Scanning
  - Exploitation
  - Privilege Escalation
  - Post-exploitation
    - 1. What other hosts can be targeted (pivoting)
    - 2. What additional information can we gather
    - 3. Covering your tracks
    - 4. Reporting
- OSSTMM (The Open-Source Security Testing Methodology Manual)
- OWASP (Open Web Application Security Project)
- NIST Cybersecurity Framework 1.1 (National Institute of Standards & Technology)
- NCSC CAF (National Cyber Security Center Cyber Assessment Framework)

4. Black, White & Grey box Penetration Testing

5. Practical: ACME Penetration Test