- Filename: comptia-pentestplus-pt0001-3-4-2-exploitation_preparation_pt2.md
- Show Name: PenTest+ (PT0-001)
- Topic Name: Information Gathering and Vulnerability Identification
- Episode Name: Exploitation Preparation Pt.2
- Description: In this episode, Daniel and Zach explain the process of leveraging information to prepare for exploitation of a given system. Here they discuss the idea of exploit chaining, Proof-of-Concept(PoC) exploit development, Social Engineering, credential brute-forcing, dictionary attacks, and rainbow tables.

==========

Exploitation Preparation Pt.2

Key Concept: Explain the process of leveraging information to prepare for exploitation

- Exploit chaining
    - Utilizing multiple exploits that build upon each other leading to root shell
        - EXAMPLE:
            1. SQL Injection authentication bypass
            2. File upload
            3. Command injection
            4. Reverse shell
            5. Priv Esc attack to root
        - EXAMPLE:
            1. Access sensitive area with SE attack
            2. Drop network sniffer/keylogger/rubberducky
            3. Harvest creds
            4. Gain access
- Proof-of-concept development (exploit development)
    - Exploit Vulnserver
    - Exploit Unreal IRCd
- Social engineering
    - Deception
- Credential brute forcing
    - Hydra, Medusa, Ncrack
- Dictionary attacks
    - Hashcat, John-the-Ripper, Cain&Abel
- Rainbow tables
    - OphCrack