

- Filename: eccouncil-ceh31250-v10-1-2-1-intro_to_ethical_hacking_hacking_concepts.md
- Show Name: CEHv10 (312-50)
- Topic Name: Introduction
- Episode Name: Intro to Ethical Hacking: Hacking Concepts
- Description: In this episode, Daniel and Zach describe and define what a hacker and hacking is in general. They go further down the rabbit-hole by looking into what makes a good hacker and explore the different types of hackers like Script Kiddies, White Hats, and Black Hats. Next they go through the common phases of hacking and finish up with Ethical hacking concepts.

Intro to Ethical Hacking: Hacking Concepts

- Hacking Concepts
 - Hacking defined
 - What makes a good hacker?
 - Highly intelligent
 - Deep understanding of computer systems
 - Someone who enjoys a challenge
 - Hacking can be fun
 - May use their powers for good or evil
 - Hacker Classifications
 - Script Kiddies/Skiddies
 - White Hat
 - Black Hat
 - Grey Hat
 - Hactivist
 - State-sponsored
 - Cyber Terrorist
 - Suicide Hacker
 - Hacking Phases
 - Recon
 - Info gathering
 - Passive
 - No direct interaction with target
 - Public sources of info
 - Active
 - Direct interaction with target
 - Talk, text, email, etc.
 - Scanning
 - Host discovery
 - System enumeration
 - Service discovery
 - Port scanning
 - Service enumeration
 - Vulnerability discovery
 - Access
 - Exploiting vulnerabilities

- OS
 - Application
 - Network
- Priv esc
- Techniques
 - Injection attacks
 - Security misconfiguration exploit
 - Buffer overflow
 - Social Engineering/Phishing/malware
 - Password brute-force
- Maintaining Access
 - Backdoor install
 - User account creation
 - Shell upload
- Covering Tracks
 - Log deletion/modification
 - Malicious file obfuscation
- Ethical Hacking Concepts
 - Who/What
 - Uses their hacking skills to assess system security
 - Helps to reduce attack/threat surface of an organization
 - Vuln discovery and mitigation
 - Have permission to hack
 - When/Where
 - Ongoing Red Team-type assessment
 - Yearly assessments
 - Compliance
 - Why
 - Find the vulnerabilities before the threats do
 - Prevent data breaches
 - Help discover the extent of fallout from a breach
 - How
 - Sweet skillz
 - Technical skills
 - Soft skills
 - EH can quickly adapt to changes
 - Tenacious