- Filename: eccouncil-ceh31250-v11-1-9-1-hacking-phases.md
- Show Name: CEHv11 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Hacking Phases

==

Hacking Phases

Objectives:

- Define 'hacking'
- Describe what a 'hacker' is and isn't
- Label hacker 'classes' or 'categories'
- Classify, order, and describe each of the 5 hacking phases

- What is 'hacking'?
    - General term
    - Term as it's applied to computer security
- A hacker is a person in a hoodie, right? Or are there others that would fit the description of a hacker?
    - Threat actor
    - Hobbyist
- What are the categories that hackers may fall under?
    - White Hat
    - Black Hat
    - Grey Hat
    - Suicide Hacker
    - Script Kiddies
    - Cyber Terrorist
    - State-Sponsored
    - Hacktivist
- Let's discuss the 5 hacking phases? Can you list those out for us?
    - 1)Recon, 2)Scanning, 3)Gaining Access, 4)Maintaining Access, 5)Clearing Tracks
- We've touched a bit on Recon in previous episodes, is there anything else we need to be aware of in regards to Recon?
    - Passive Recon
    - Active Recon
- How does the Scanning phase differ from the Recon phase?
    - Pushing Active Recon farther
        - Port and Service scans
        - Host discovery scans
        - OS enumeration
        - Vulnerability Scanning
- Is the 'Gaining Access' phase as simple as the name implies, or is there more to it?
    - Hacker exploits a Vulnerability and gains system access
    - Methods for doing that are as varied as the vulnerabilities, but include
        - Password attacks

        - RCE attacks
        - Injection attacks
        - Session Hijacking

    - Priv Esc and Pivoting

- So the next phase is 'Maintaining Access'? That seems logical.

    - Install malware

        - RATs
        - Rootkits
        - Backdoors

    - Crack user passwords
    - System Hardening

        - Make sure that only they have the ability to control the system

            - No other hackers are invited to the party

- Why are attackers concerned with Covering Tracks? And what tracks are they covering?

    - Hide their identity!!!
    - Maintain access
    - Clearing logs
    - Stenography
    - Tunneling

...