

- Filename: eccouncil-ceh31250-v11-1-6-1-tactics-techniques-and-procedures.md
- Show Name: CEHV11 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Tactics, Techniques, and Procedures

Tactics, Techniques, and Procedures

Objectives:

- Define Tactics, Techniques, and Procedures as they pertain to threat modeling
-
- What do we mean when we use the term 'TTP'?
 - The behavior of a threat actor
 - Why are we concerned with the behavior of an attacker?
 - Profiling
 - Threat modeling
 - Explain the concept of Tactics.
 - Tactics are initial objectives
 - I want to gather networking information about my target
 - I want to find out what services my target is running
 - I want to get all the email addresses I can
 - What vulnerabilities does my target have
 - So how does Techniques differ from Tactics?
 - Techniques are the ways I achieve my objective and tools used
 - Perform DNS queries using dig
 - Perform network scans and banner grabbing
 - Scrape the internet for email addresses with the target domain
 - Perform vulnerability scanning against my target
 - Where do Procedures fit into the equation?
 - Advanced action taken to achieve objectives
 - Threat actor profiles users on social media
 - Performs advanced application testing to discover zero-day exploits
 - Does advanced obfuscation techniques in malware payloads