- Filename: eccouncil-ceh31250-v10-1-1-2-intro_to_ethical_hacking_threats_pt2.md
- Show Name: CEHv10 (312-50)
- Topic Name: Introduction
- Episode Name: Intro to Ethical Hacking: Threats Pt.2
- Description: In this episode, Daniel and Zach explain a few foundational concepts with regards to Ethical Hacking. Here they continue to look specifically at threats. They pick back up by discussing a few motivations common to the threat actor. They also define threat categories, attack vectors, and types of defenses against threats.

==========

## Intro to Ethical Hacking: Threats Pt.2

- Information Security Threats and Attack Vectors
    - Security Threats
        - Anyone motivated to attempt to exploit system vulnerabilities to attain a specific goal
            - Goals
                - Monetary/Economic
                    - Theft/Ransom
                        - Money/IP/Both
                    - Hacking for hire
                    - Target's loss of revenue/savings/both
                - Revenge
                    - Slander
                - Ideology
                - Political/State-sponsored
                - Cause disruption
                    - Anarchists
                    - Business continuity
                - Data Manipulation
                - Bragging Rights
        - Categories
            - Network
                - MITM
                - DoS/DDoS
                - DNS/ARP Poisoning
            - Host
                - Password cracking
                - Malware
                - Priv Esc
                - Code Execution
            - Application
                - Injection attacks
                - Buffer Overflow
                - Security misconfigurations
    - Attack Vectors
        - Web Apps
        - Phishing

        - Malware
            - Ransomware
        - Mobile
- Insider
- Cloud
- APT
- Botnet
        - IoT
- Types of System Attacks
    - Application Attacks
    - OS Attacks
    - Security misconfiguration attacks
- Types of Attack Defenses
    - Defensive Security
        - Building walls/gates/guards
    - Offensive Security
        - Annoyance
            - Deploying systems meant to frustrate attackers
                - Waste their time and effort
        - Attribution
            - Identify the attackers
                - WebBug
                    - A file that, when accessed, gathers info about the person that accessed it
        - Attack
            - No illegal activities
            - Further annoyance
                - Use BeEF to send constant pop-ups