- Filename: eccouncil-ceh31250-v11-1-14-1-threat-modeling.md
- Show Name: CEHv11 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Threat Modeling

==

Threat Modeling

Objectives:

- Define Threat Modeling
- List and describe the 5 steps in the Threat Modeling process

---

- I know we've talked a bit about Threat Modeling in other episodes, but can you just give us a quick reminder of what Threat Modeling is?
    - A systematized approach to assess the risk/security of an organization
        - Know thy enemy
            - What are the common/most likely attack methods
            - The more detail the better
        - Know thyself
            - Where are we vulnerable
- What are the steps in the Threat Modeling process?
    1. Identify security objectives
    - What needs to be secured?
    - Any regulatory or policy compliance requirements?
    2. Application overview
    - Identify:
        - Roles
            - Who will be using this?
        - Usage scenarios
            - How will this be used normally?
            - How could this be misused?
        - Technologies
            - OS
            - Supporting Apps and services
            - Network technologies
        - Security mechanisms
            - Authentication
            - Authorization
            - Input validation
            - Encryption
    3. Decompose the application
    - Diagrams help here

    - Identify
        - Trust boundaries
        - Data flows
        - Entry points
        - Exit points
  4. Identify threats
  5. Identify Vulnerabilities

- This sounds like a lot of work to develop. Are there any standard models for us to use as a guide?
    - STRIDE
        - https://blog.eccouncil.org/what-is-stride-methodology-in-threat-modeling/
    - PASTA (Process for Attack Simulation and Threat Analysis)
        - https://blog.eccouncil.org/what-is-pasta-threat-modeling/
    - DREAD
        - https://blog.eccouncil.org/dread-threat-modeling-an-introduction-to-qualitative-and-quantitative-risk-analysis/