- Filename: eccouncil-ceh31250-v12-1-17-1-diamond-model-of-intrusion-analysis.md
- Show Name: CEHv12 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Basic Cybersecurity Concepts

==========

Diamond Model of Intrusion Analysis

Objectives:

- Be sure to make diamond.pdf available as Learner Resources

---

1. What is the Diamond Model?
2. Explain the Core Features

- **Adversary**
    - The threat actor and/or group that is responsible for utilizing a Capability against the Victim to achieve their goals and intents.
    - Little to no knowledge about the Adversary usually
        - Empty for most events
    - <u>Adversary Operator</u>
        - Actual threat actor performing attacks
    - <u>Adversary Customer</u>
        - Person(s) that stand to gain from attack
            - Might be the same as Adversary Operator, but not necessarily
- **Capability**
    - TTPs of the Adversary
        - <u>Capability Capacity</u>
        - <u>Adversary Arsenal</u>
- **Victim**
    - The target of the Adversary
        - <u>Victim Persona</u>
            - The people and organizations
        - <u>Victim Asset</u>
            - The Victim's attack surface
        - Networks, servers, email, hosts, etc
- **Infrastructure**
    - Any physical and/or logical communication structures used to attack the Victim and effect the Victim
    - <u>Type 1</u>
        - Fully owned and controlled by the Adversary and used to carry out attack
    - <u>Type 2</u>
        - Infrastructure owned by a 3rd-party, but used by Adversary to attack
    - Bots, Zombies, compromised accounts, etc
    - <u>Service Providers</u>
        - Any organization that provides the Attacker with services
    - Wittingly or Unwittingly
        - ISPs, Email providers, DNS, Cloud, etc

3. Explain the Meta-Features

- Timestamp
    - Date/Time an event occurred
- Phase
    - Which step, or "Phase" of hacking
        - Think Cyber Kill-Chain or CEH Hacking Methodology
- Result
    - What did the Adversary accomplish and how does it affect the Victim
        - Which of the CIA were compromised?
        - "Post-Conditions"
- Direction
    - Check the PDF p.17 for details
- Methodology
    - Labling of the general "class of activity"
        - e.g. Phishing Attack
- Resources
    - The resrouces required for the event to occur
        - Software
        - Hardware
        - Funds
        - Access (how does the Adversary make actual contact with Victim?)