LO#09: Explain Threat Modeling Methodology

Threat Modeling Methodologies

CEH

STRIDE

- STRIDE stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-Service, and Elevation of privilege
- STRIDE is used by analysts to classify threats
- Once a DFD-based threat model is developed, an analyst can check its application against STRIDE methodology

PASTA

- PASTA stands for Process for Attack Simulation and Threat Analysis
- Seven-Stage PASTA Methodology:
  - Definition of Objectives (DO)
  - Definition of Technical Scope (DTS)
  - Application Decomposition and Analysis (ADA)
  - Threat Analysis (TA)
  - Weakness and Vulnerability Analysis (WVA)
  - Attack Modeling and Simulation (AMS)
  - Risk and Analysis Management (RAM)

TRIKE

- An open-source threat modeling methodology that follows the risk management approach
- Models that effectively form the levels of the TRIKE methodology:
  - Requirements Model
  - Implementation Model
  - Threat Model
  - Risk Model

Notes:

Threat Modeling Methodologies (Cont'd)

VAST

- VAST stands for Visual, Agile, and Simple Threat modeling
- The primary objective of developing this methodology is to scale the threat modeling across the infrastructure and entire DevOps portfolio
- Based on the practical approach in the development of the following threat models:
  - Application Threat Model
  - Operational Threat Model

DREAD

- DREAD stands for Damage, Reproducibility, Exploitability, Affected Users, and Discoverability
- A sorting scheme for calculating, comparing, and ranking the possible extent of threat for each assessed risk
- The DREAD formula for calculating the risk value:

  Risk = (Damage + Reproducibility + Exploitability + Affected Users + Discoverability)/5

OCTAVE

- OCTAVE stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation
- Three stages of OCTAVE methodology:
  - Build Asset-Based Threat Profiles
  - Identify Infrastructure Vulnerabilities
  - Develop Security Strategy and Plans

Threat Profiling and Attribution

- Threat Profiling and Attribution involves collecting information about threat actors and **building an analytic profile of the adversary**
- It describes the **adversary's technological details**, goals, and motives which can be resourceful in building a strong countermeasure

The threat profile can be created to include the details of the following attributes:

1. Description
2. Motive
3. Intent
4. Capability
5. Ownership Detail
6. Target Detail
7. Operating Methods
8. Objective

Notes: