Advanced Threat Analysis

1. Introduction

Advanced Threat Analysis focuses on identifying, modeling, and understanding sophisticated cyber threats to proactively defend systems and networks.

2. STRIDE Threat Modeling

STRIDE is a threat modeling framework used to identify security threats.

- **Spoofing** – Impersonating a legitimate user
- **Tampering** – Modifying data or code
- **Repudiation** – Denying performed actions
- **Information Disclosure** – Unauthorized data exposure
- **Denial of Service** – Making services unavailable
- **Elevation of Privilege** – Gaining higher access rights

Example:
In a web application, weak authentication can lead to spoofing, while missing authorization checks can cause privilege escalation.

3. MITRE ATT&CK Framework

MITRE ATT&CK is a globally recognized knowledge base of adversary tactics and techniques.

Common Tactics:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Lateral Movement
- Command and Control

Example:
Phishing emails map to **T1566 – Phishing**, while PowerShell abuse maps to **T1059 – Command and Scripting Interpreter**.

4. Advanced Persistent Threats (APT)

APTs are long-term, targeted cyberattacks typically conducted by nation-state actors.

Characteristics:

- Stealthy
- Persistent access

- Targeted data exfiltration

5. Zero-Day Exploits

A zero-day exploit targets vulnerabilities unknown to vendors and without patches, making them highly dangerous.

6. SolarWinds Supply Chain Attack

In 2020, attackers compromised SolarWinds Orion updates, distributing malware to thousands of organizations.

Impact:

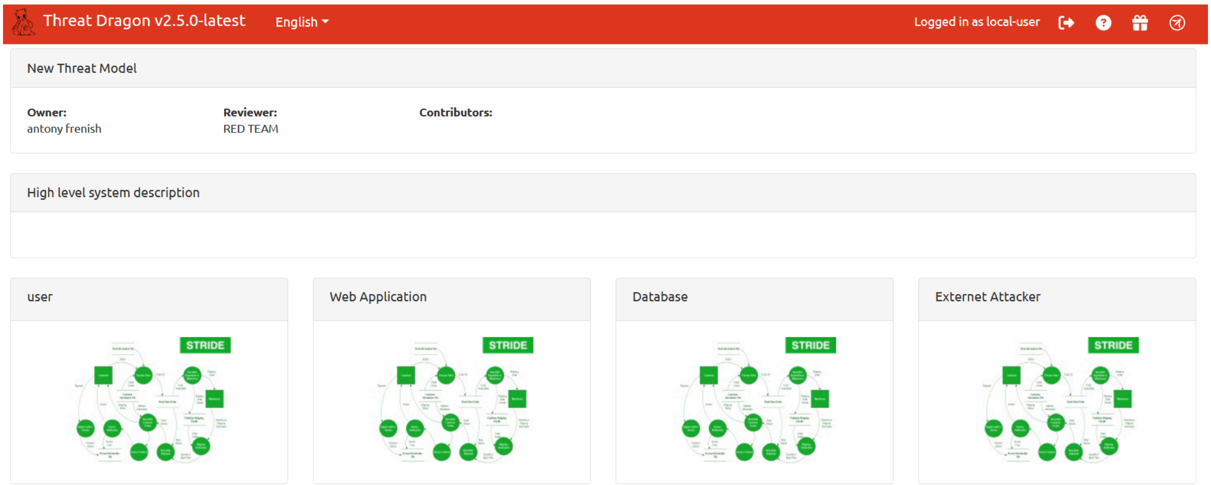
- Government agencies compromised
- Long-term stealth access

MITRE Mapping:

- Initial Access – Supply Chain Compromise
- Execution – PowerShell
- Persistence – Scheduled Tasks

7. Threat Modeling Diagram

A basic threat model was created using OWASP Threat Dragon showing:
 User → Web Application → Database → External Attacker



New Threat Model

Owner: antony frenish

Reviewer: RED TEAM

Contributors:

High level system description

user

Web Application

Database

Externet Attacker