Threat modeling

Introduction

This page will consist of a number of checklists that help in threat modeling an application.

General high level overview

1. Gather relevant documentation
2. Identify and categorize primary and secondary assets
3. Identify and categorize threats and threat communities
4. Map threat communities against primary and secondary assets

Business Asset Analysis

Organizational Data

- Policies, Plans, and Procedures
- Product Information (e.g. trade secrets, R&D data)
- Marketing Information (plans, roadmaps, etc.)
- Financial Information (e.g. bank, credit, equity accounts)
- Technical Information
    - Infrastructure Design Information
    - System Configuration Information
    - User Account Credentials
    - Privileged User Account Credentials
- Employee Data
    - National Identification Numbers (SSNs, etc.)
    - Personally Identifiable Information (PII)
    - Protected Health Information (PHI)
    - Financial Information (e.g. bank, credit accounts)
- Customer Data
    - National Identification Numbers (SSN's, etc.)
    - Personally Identifiable Information (PII)
    - Protected Health Information (PHI)
    - Financial Accounts (e.g. bank, credit, equity accounts)
    - Supplier Data
- Human Assets
    - Executive Management
    - Executive Assistants
    - Middle Management
    - Administrative Assistants
    - Technical/Team Leads
    - Engineers
    - Technicians
    - Human Resources

Business Process Analysis

- Technical infrastructure supporting process
- Information assets supporting process
- Human assets supporting process
- 3rd party integration and/or usage of/by process

Threat Agents/Community Analysis

Internal	External
Employees	Business Partners
Management (executive, middle)	Competitors
Administrators (network, system, server)	Contractors
Developers	Suppliers
Engineers	Nation States
Technicians	Organized Crime
Contractors (with their external users)	Hacktivists
General user community	Script Kiddies (recreational/random hacking)
Remote Support	

Threat Capability Analysis

- Analysis of tools in use
- Availability to relevant exploits/payloads
- Communication mechanisms
- Accesibility

Motivation Modeling

Why would an attacker want to exploit?

- Profit (direct or indirect)
- Hacktivism
- Direct grudge
- Fun / Reputation
- Further access to partner/connected systems

Finding relevant news of comparable Organizations being compromised

- Google news for articles where target-like has been hacked