Co-funded by
the European Union

Course: Security Analysis and Risk Management

Project: Cyber Security 4 ALL(CS4ALL)

Chapter 2

Threat Modeling and Vulnerability Assessment

Overview

- Introduction to threat modeling
- Threat Modeling Methodologies
  - STRIDE Model: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service & Elevation of Privilege
  - PASTA Methodology: Process for Attack Simulation And Threat Analysis
- Techniques for vulnerability identification and assessment
- Tools and practices for vulnerability scanning

Introduction to Threat Modeling

- **Definition:**
  - Threat Modeling is a structured approach used in cybersecurity to identify, evaluate, and prioritize potential threats to a system or application.
- **Goal:**
  - To understand and mitigate security risks by analyzing how malicious entities could attack a system and what defenses can be put in place to prevent or reduce the damage from these attacks.

Co-funded by
the European Union

Introduction to Threat Modeling

- **Purpose:**
  - Helps anticipate potential threats, understand security requirements, and design defenses.
- **Importance:**
  - Proactive Security
  - Efficient Resource Allocation
  - Improve Communication

Co-funded by the European Union

Steps in Threat Modeling

- **Asset Identification**
  - Identify critical components of the system (Asset may be Personally Identifiable Information (PII), Passwords, Secrets, Session IDs,) and understand their importance in the overall system functionality.
- **Threat Identification**
  - Identify potential threats using models like STRIDE, PASTA, VAST or OCTAVE.

Co-funded by the European Union

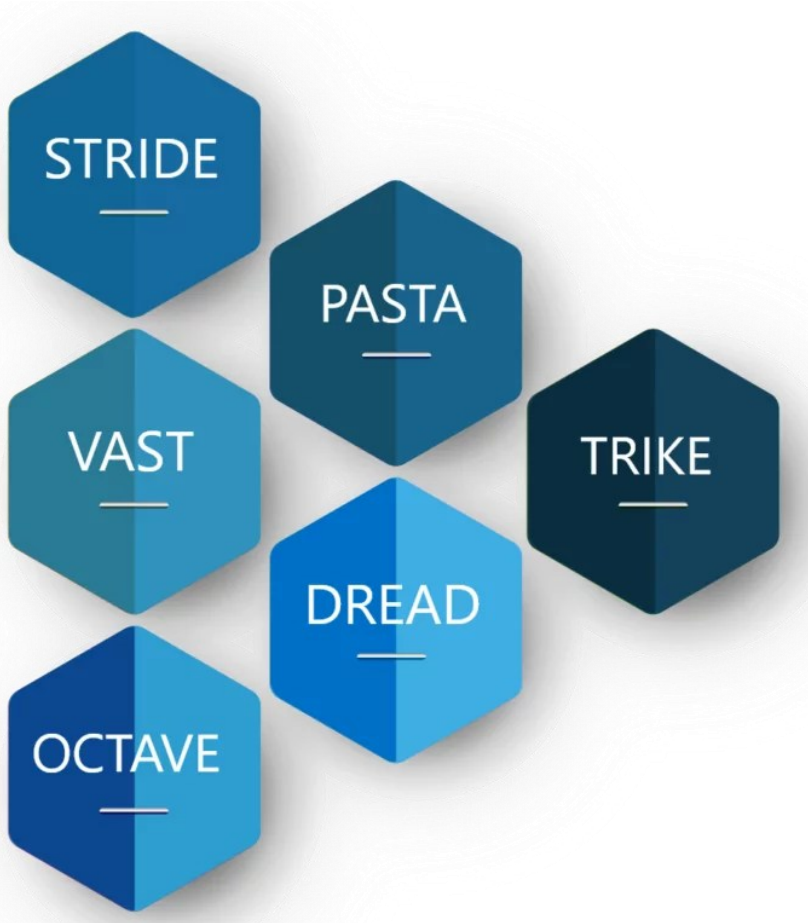
Steps in Threat Modeling

- **Vulnerability Identification**
  - Examine the system for possible weaknesses that could be exploited by threats.
- **Risk Assessment**
  - Evaluate the impact and likelihood of identified threats and vulnerabilities to prioritize remediation efforts.
- **Mitigation Strategy**
  - Design and implement security controls and countermeasures to reduce the risk from the identified threats.

Co-funded by
the European Union

Threat Modeling Methodologies

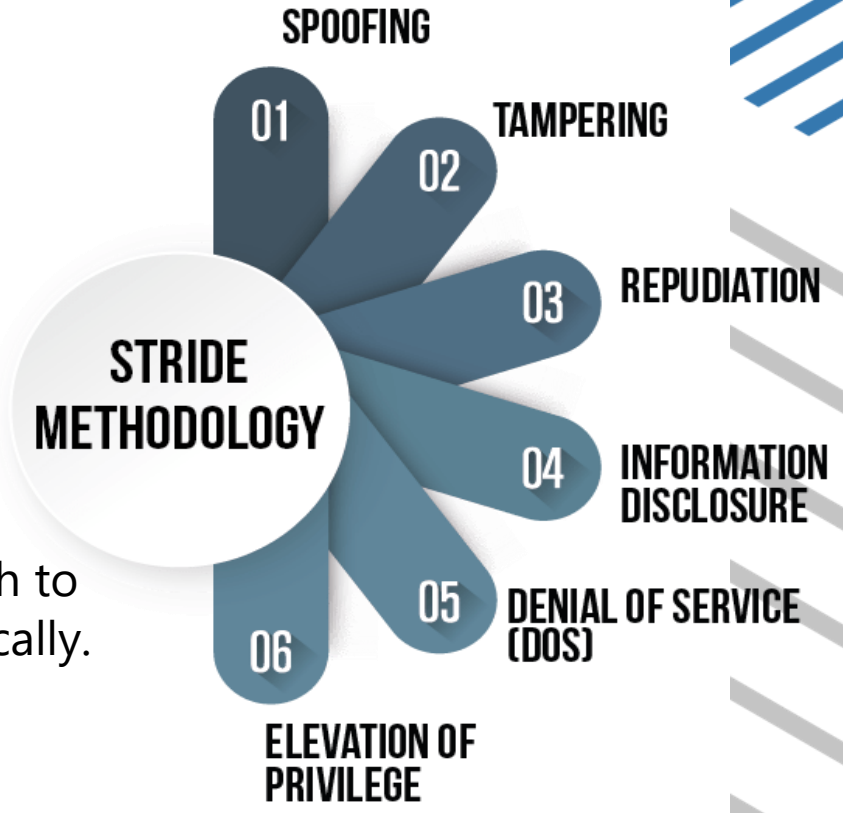
- **STRIDE**
- **PASTA**
- VAST
- OCTAVE
- DREAD
- TRIKE



Co-funded by the European Union

STRIDE

- It is an approach to threat modeling developed by Loren Kohnfelder and Praerit Garg at Microsoft in 1999.
  - S: Spoofing
  - T: Tampering
  - R: Repudiation
  - I: Information Disclosure
  - D: Denial of Service
  - E: Elevation of Privilege



- **Benefit:** Organized approach to categorize threats systematically.

Co-funded by the European Union

STRIDE

- **Spoofing:**
  - Impersonating another identity to access data or resources.
- **Tampering:**
  - Unauthorized alteration of data.
- **Repudiation:**
  - Denying an action, leading to lack of accountability.

Co-funded by the European Union

STRIDE

- **Information Disclosure:**
  - Unauthorized access to confidential information.
- **Denial of Service:**
  - Disrupting service availability.
- **Elevation of Privilege:**
  - Gaining higher access levels than authorized.

Co-funded by
the European Union

STRIDE

	Type of Threat	What Was Violated	How Was It Violated?
S	Spoofing	Authentication	Impersonating something or someone known and trusted.
T	Tampering	Integrity	Modifying data on disk, memory, network, etc.,
R	Repudiation	Non-repudiation	Claim to not be responsible for an action
I	Information Disclosure	Confidentiality	Providing information to someone who is not authorized
D	Denial of Service (DoS)	Availability	Denying or obstructing access to resources required to provide service
E	Elevation of Privilege	Authorization	Allowing access to someone without proper authorization

Co-funded by the European Union

PASTA

- **Definition:**
    - **Process for Attack Simulation and Threat Analysis (PASTA)**
    - is a seven step methodology to create a process for simulating attacks to IT applications, analyzing the threats, their origin, the risks they pose to an organization and how to emigrate them.
- **Objective**:
    - to identify the threat, enumerate them and assign a score.

Co-funded by the European Union

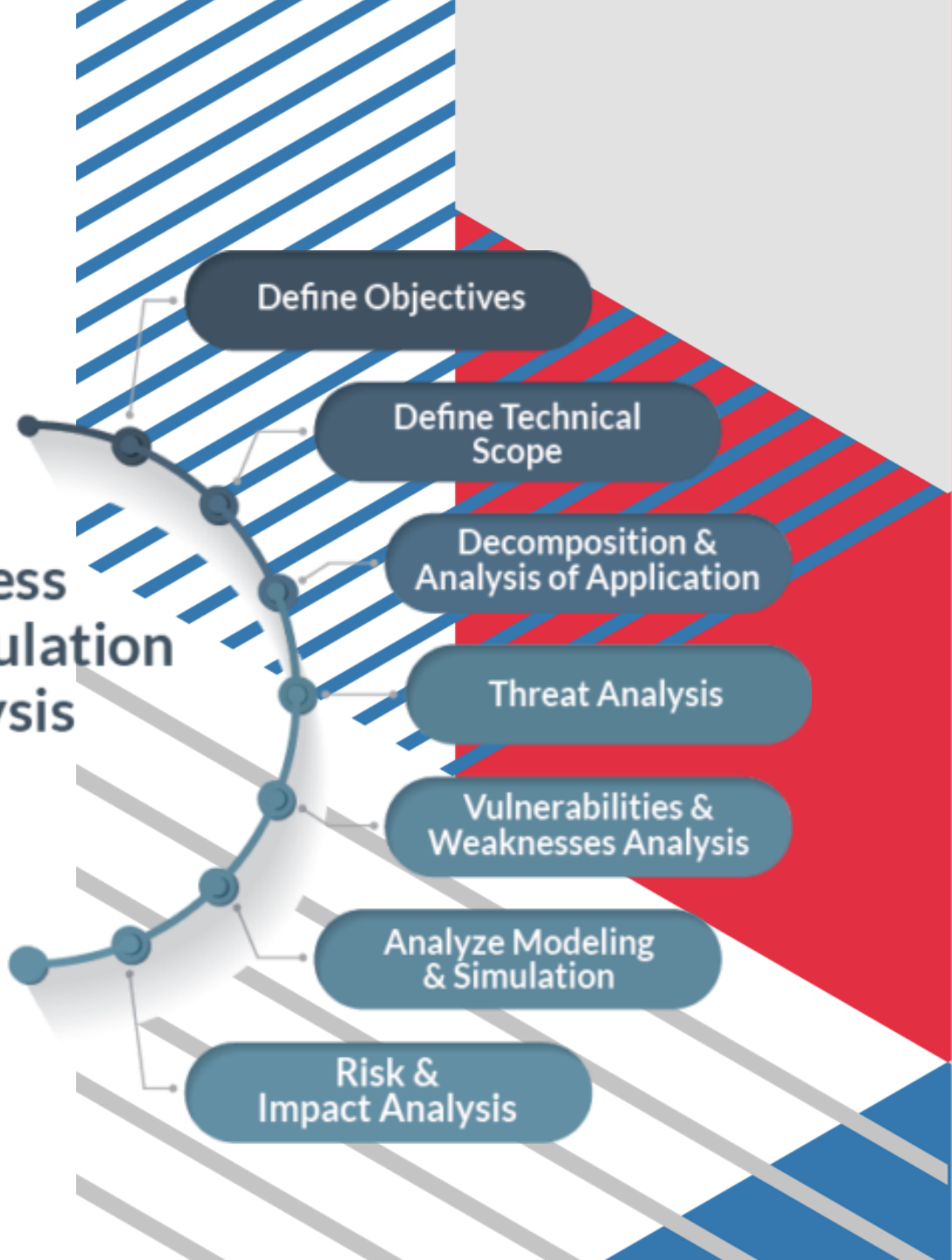
PASTA

- **PASTA:**
  - **Focus:**
    - Attack simulation to identify possible attack paths.
  - **Phases:**
    - Seven phases, from defining objectives to modeling and risk analysis.
  - **Use Case:**
    - Ideal for complex systems needing detailed threat scenarios.

Co-funded by the European Union

PASTA Phases

1. Define Business Objectives
2. Define Technical Scope
3. Decompose Application and Infrastructure
4. Analyze Threats
5. Enumerate Vulnerabilities
6. Analyze Exploits
7. Develop Mitigation Strategies



CS4ALL
CYBERSECURITY FOR ALL
Co-funded by the European Union

Vulnerability Identification and Assessment

- **Vulnerability assessment** is the process of identifying, quantifying and prioritizing security vulnerabilities in an organization's IT infrastructure.

- It involves scanning systems, networks, and applications for known vulnerabilities, misconfigurations, and weaknesses that could be exploited by attackers to gain unauthorized access, steal data, or disrupt operations.

Co-funded by the European Union

Importance of Vulnerability Identification and Assessment

- **Proactive Risk Management**
  - helps organizations identify and mitigate security risks before they can be exploited by malicious actors.

- **Compliance Requirements**
  - Many regulatory frameworks and industry standards, such as PCI DSS, HIPAA, and GDPR, require regular vulnerability assessments to ensure compliance with security requirements.

Co-funded by the European Union

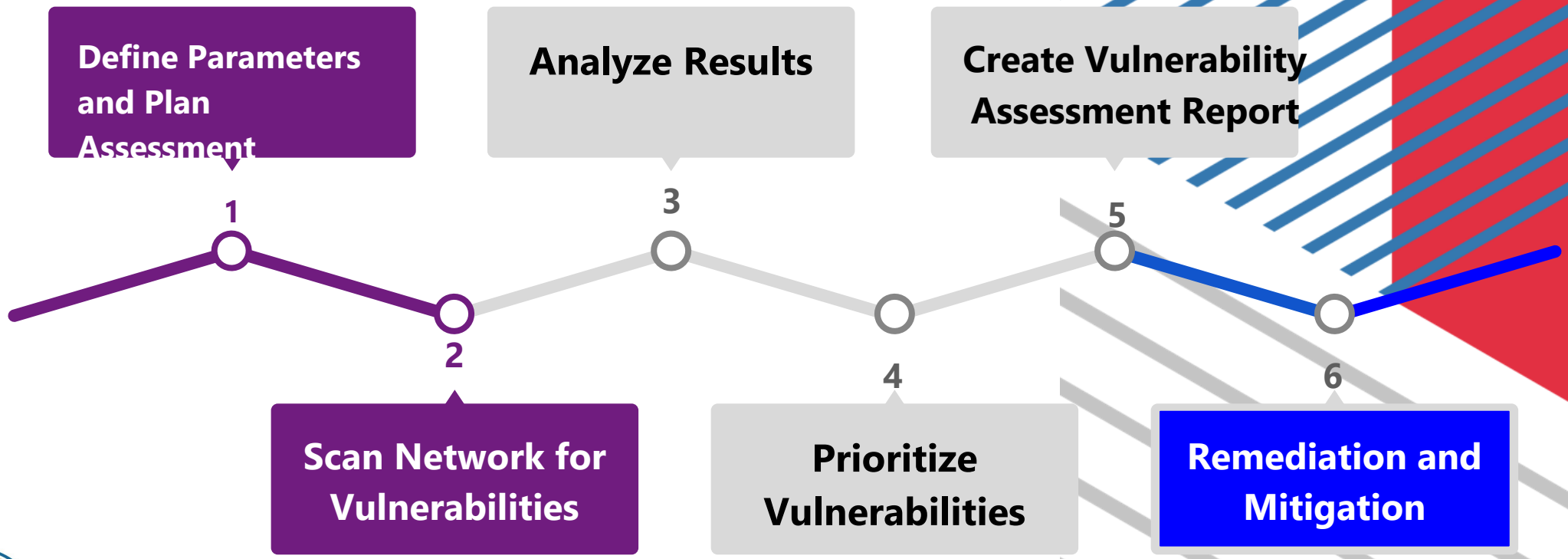
Importance of Vulnerability Assessment

- **Enhanced Security Posture**
  - By addressing vulnerabilities promptly, organizations can strengthen their overall security posture and reduce the likelihood of successful cyber attacks.

- **Cost Savings**
  - Identifying and remedying vulnerabilities early can help organizations avoid the financial costs associated with data breaches, regulatory fines, and reputational damage.

Co-funded by the European Union

Vulnerability Assessment Process



Co-funded by the European Union

Techniques for Vulnerability Identification and Assessment

- Manual Code Review:
  - Reviewing code for common flaws and vulnerabilities.
- Automated Scanning:
  - Using tools to detect vulnerabilities automatically.

Co-funded by the European Union

Techniques for Vulnerability Identification and Assessment

- Penetration Testing:
  - Ethical hacking to exploit system weaknesses.
- Configuration Review:
  - Ensuring configurations meet security standards.

Co-funded by the European Union

Tools and Practices for Vulnerability Scanning

- **Tools:**
  - **Nessus**: Comprehensive vulnerability scanner for networks.
  - **OpenVAS**: Open-source tool for scanning network vulnerabilities.
  - **Burp Suite:** Web application scanner focusing on OWASP vulnerabilities.

Co-funded by the European Union

Tools and Practices for Vulnerability Scanning

- **Tools:**
  - **Nmap:** is used for host discovery, port scanning, service enumeration, and vulnerability detection.
  - **QualysGuard:** provides comprehensive scanning, reporting, and remediation capabilities for networks, hosts, and web applications.
  - **OWASP ZAP**: helps to identify security vulnerabilities in web applications, APIs, and websites.

Tools and Practices for Vulnerability Scanning

- **Best Practices:**
  - Regular scanning schedules.
  - Reviewing and validating scan results.
  - Prioritizing fixes based on risk assessment.

Co-funded by the European Union

Conclusion

- **Threat Modeling:** Helps preemptively identify threats.
- **Methodologies:** STRIDE and PASTA offer structured ways to categorize and assess threats.
- **Vulnerability Identification and Assessment:**
  - Techniques and tools are essential for discovering and managing risks.
  - helps organizations identify and mitigate security risks before they can be exploited by malicious actors.

Thank You

Co-funded by
the European Union

References

1. https://www.eccouncil.org/threat-modeling/
2. Shostack, Adam. *Threat Modeling: Designing for Security*. Wiley, 2014.
3. Microsoft, "Threat Modeling," Microsoft Learn, accessed November 2024, https://learn.microsoft.com/en-us/security/engineering/threat-modeling
4. https://www.imperva.com/learn/application-security/vulnerability-assessment/
5. https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis
6. https://www.esecurityplanet.com/networks/vulnerability-assessment-process/

Questions & answers

Invite questions from the audience.

Co-funded by
the European Union