Threat and Vulnerability Test

By: Mishelly Sandoval, Lucas Higgs, and Tianna Green

Contributors: Frederick Asante, Shemar Brown, Jane Pierre, Elizabeth Bond, Jonathan Henao, and Aaron Kaah

What is a Threat Assessment?

- Threat assessment is a process of evaluating and identifying potential security risks or threats to an individual, organization, or community. It involves the identification of potential threats, assessment of their credibility, and the development of strategies to mitigate or manage those threats. (Department of Homeland Security, n.d.)

Threat Assessment

Key Components:

- Identifying the potential threat
  - The first step in a threat assessment is to identify the potential threat, which could be anything from an individual to a natural disaster.

- Assessing the credibility of the threat
  - Once a potential threat has been identified, it is important to assess its credibility. This involves gathering information and evaluating the likelihood and potential impact of the threat.

- Developing a threat management plan
  - Based on the assessment of the threat, a threat management plan is developed to mitigate or manage the risk. This plan may involve strategies such as increased security measures, evacuation procedures, or communication protocols.

- Ongoing monitoring and review
  - Threat assessments should be an ongoing process, with regular monitoring and review to ensure that the threat management plan remains effective and up-to-date.

What is a Vulnerability Assessment?

- A vulnerability assessment is a systematic process of identifying and evaluating security weaknesses in an organization's infrastructure, systems, and operations. It is an important step in developing effective security measures to protect against potential threats (Meadows, 2020).

Vulnerability Assessment

- Key Points
  - Vulnerability assessment is a proactive approach to managing security risks by identifying weaknesses before they can be exploited by attackers.
  - It involves a comprehensive evaluation of an organization's security posture, including its physical security, network security, and operational security.
  - The process typically involves several steps, such as identifying assets to be protected, assessing the vulnerabilities of those assets, prioritizing vulnerabilities based on risk, and developing a remediation plan.
  - Vulnerability assessment can be performed by internal or external security professionals, or a combination of both.
  - The goal of vulnerability assessment is to identify and address potential security weaknesses before they can be exploited by attackers.

Risk Assessment

- What is it?
  - Risk assessment is the process of identifying and analyzing potential risks to determine the likelihood and impact of harm to people, property, or the environment. It is an essential component of risk management and can be used to inform decisions about how to allocate resources and implement mitigation strategies (ISO, 2018).

- Includes
  - It involves identifying hazards, assessing the likelihood and consequences of those hazards, and evaluating existing risk mitigation measures.
  - The process can be qualitative, quantitative, or a combination of both, depending on the complexity and scope of the risk.
  - Risk assessment can be used in various contexts, such as occupational health and safety, environmental management, and security risk management.
  - The goal of risk assessment is to identify potential risks and implement effective risk management strategies to reduce the likelihood and impact of harm.

Differences between the 3?

Threat Assessment:

- Focuses on identifying potential threats to individuals, organizations, or communities.
- Evaluates the likelihood and potential impact of harm from specific threats.
- Involves analyzing the motives, capabilities, and behaviors of potential threats.

Vulnerability:

- Focuses on identifying weaknesses in an organization's infrastructure, systems, and operations.
- Evaluates the likelihood and potential impact of harm resulting from those vulnerabilities.
- Involves analyzing the organization's physical security, network security, and operational security.

Risk:

- Focuses on identifying potential risks to people, property, or the environment.
- Evaluates the likelihood and potential impact of harm resulting from those risks.
- Involves analyzing hazards, vulnerabilities, and existing risk mitigation measures.

Threat and Vulnerability Assessment

1. Define the scope
2. Identify potential threats
3. Assess vulnerabilities
4. Analyze risks
5. Prioritize risks
6. Develop a risk management plan
7. Monitor and update

Threat and Vulnerability tools

- Types
  - NMAP
  - Burp Suite
  - Openvas
  - Metasploit
  - Wireshark

NMAP

- Nmap (Network Mapper) is a free and open-source network exploration and security auditing tool that can be used in threat and vulnerability assessments of non-profit organizations. It is designed to identify hosts and services on a network, as well as potential security vulnerabilities that can be exploited by attackers
- Includes
  - Nmap can be used to scan a network for open ports, running services, and potential vulnerabilities.
  - It can be used to identify potential misconfigurations or weaknesses in network devices, such as firewalls or routers (Lyon, 2019).
  - Nmap can also be used to identify potential vulnerabilities in web applications or other software running on the network (Lyon, 2019).
  - Nmap offers various scanning techniques and customization options, allowing security professionals to tailor the tool to the specific needs of the assessment (Lyon, 2019).
  - Nmap can be run from a command-line interface or a graphical user interface, depending on the user's preference and experience level (Nmap, n.d.).

Burp Suite

- Burp Suite is a popular web application security testing tool that can be used in threat and vulnerability assessments of non-profit organizations. It is designed to identify potential security vulnerabilities in web applications by simulating attacks and providing detailed feedback on application behavior.
- Includes
  - Burp Suite can be used to scan web applications for common vulnerabilities, such as SQL injection, cross-site scripting (XSS), and broken authentication (PortSwigger, n.d.).
  - It can also be used to perform more advanced attacks, such as session hijacking, CSRF, and command injection (PortSwigger, n.d.).
  - Burp Suite offers a range of features, including a proxy server, spider, and scanner, that can be used to customize the testing process and generate detailed reports on vulnerabilities (PortSwigger, n.d.).
  - It can be integrated with other tools, such as Nmap or Metasploit, to provide a comprehensive assessment of an organization's security posture (PortSwigger, n.d.).
  - Burp Suite can be run on a local machine or deployed in the cloud, depending on the needs of the assessment (PortSwigger, n.d.).

Openvas

- OpenVAS (Open Vulnerability Assessment System) is a free and open-source vulnerability scanner that can be used in threat and vulnerability assessments of non-profit organizations. It is designed to identify potential security vulnerabilities in network infrastructure and web applications by conducting comprehensive scans and generating detailed reports on identified vulnerabilities.
- Includes
  - OpenVAS can be used to scan network infrastructure, including servers, routers, and firewalls, for potential vulnerabilities (OpenVAS, n.d.).
  - It can also be used to scan web applications for common vulnerabilities, such as SQL injection, cross-site scripting (XSS), and directory traversal (OpenVAS, n.d.).
  - OpenVAS offers a range of features, including customized scan configurations, reporting options, and integration with other tools, such as Nmap and Metasploit (OpenVAS, n.d.).
  - It can be run on a local machine or deployed in the cloud, depending on the needs of the assessment (OpenVAS, n.d.).
  - OpenVAS can be used to evaluate compliance with industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS), or regulatory requirements, such as the General Data Protection Regulation (GDPR) (OpenVAS, n.d.).

Metasploit

- Metasploit is a powerful penetration testing and exploitation framework that can be used in threat and vulnerability assessments of non-profit organizations. It is designed to simulate real-world attacks and identify potential security vulnerabilities in network infrastructure and web applications.
- Includes
  - Metasploit can be used to identify potential vulnerabilities in network infrastructure, including servers, routers, and firewalls, and web applications (Rapid7, n.d.).
  - It can also be used to simulate real-world attacks, such as brute-force attacks, SQL injection, and cross-site scripting (XSS), to identify potential vulnerabilities and recommend remediation strategies (Rapid7, n.d.).
  - Metasploit offers a range of features, including custom payloads, automatic exploitation, and reporting, that can be used to customize the testing process and generate detailed reports on identified vulnerabilities (Rapid7, n.d.).
  - It can be integrated with other tools, such as Nmap or Burp Suite, to provide a comprehensive assessment of an organization's security posture (Rapid7, n.d.).
  - Metasploit can be run on a local machine or deployed in the cloud, depending on the needs of the assessment (Rapid7, n.d.).

Wireshark

- Wireshark is a free and open-source network protocol analyzer that can be used in threat and vulnerability assessments of non-profit organizations. It is designed to capture and analyze network traffic in real-time to identify potential security vulnerabilities and diagnose network problems.
- Includes
  - Wireshark can be used to capture and analyze network traffic, including packets sent and received by network infrastructure and web applications (Wireshark, n.d.).
  - It can be used to identify potential security vulnerabilities, such as unauthorized access, data breaches, and denial-of-service attacks, by analyzing network traffic patterns and identifying anomalies (Wireshark, n.d.).
  - Wireshark offers a range of features, including packet filtering, real-time traffic analysis, and customized reporting, that can be used to customize the testing process and generate detailed reports on identified vulnerabilities (Wireshark, n.d.).
  - It can be integrated with other tools, such as Nmap or Metasploit, to provide a comprehensive assessment of an organization's security posture (Wireshark, n.d.).
  - Wireshark can be run on a local machine or deployed in the cloud, depending on the needs of the assessment (Wireshark, n.d.).