Cyber security long term internship

Smart Internz

Technology stack: cyber security with IBM QRadar

Project title: mastering threat intelligence: strategies for proactive cyber defense

Team ID : LTVIP2024TMID14858

Team size : 5

Team leader : Reddy hema Latha

Team member : shaik sulthana begum

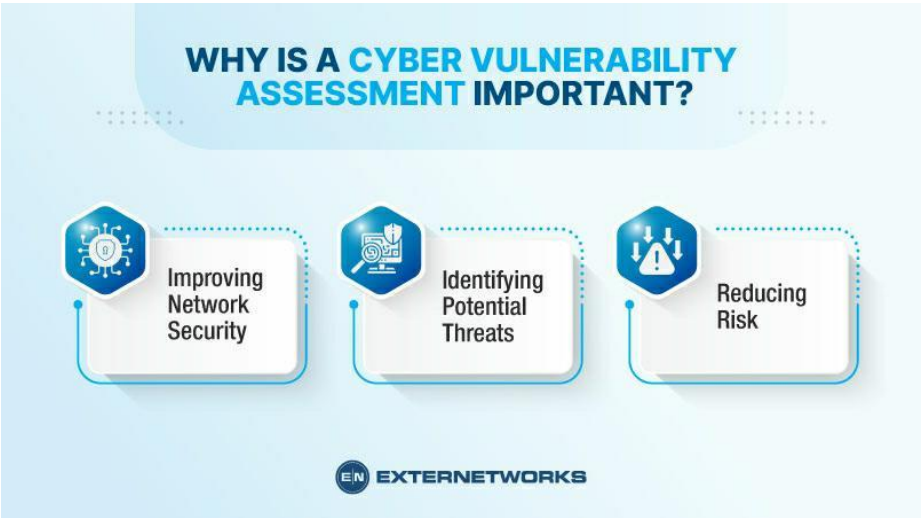
Register number:SBAP0014858

My Task

Vulnerabilities analysis and assessment

A vulnerability assessment is a component of a security assessment. A security assessment requires manual investigation and testing, but a vulnerability scan is automated. A security assessment looks for current and future vulnerabilities, and a vulnerability scan is only a point-in-time snapshot.

Definition:A vulnerability assessment is the testing process used to identify and assign severity levels to as many security defects as possible in a given timeframe. This process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage.



What is a vulnerability assessment?

A vulnerability assessment is the testing process used to identify and assign severity levels to as many security defects as possible in a given timeframe. This process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage. Using a risk-based approach, vulnerability assessments may target different layers of technology, the most common being host-, network-, and application-layer assessments.

Vulnerability testing helps organizations identify vulnerabilities in their software and supporting infrastructure before a compromise can take place. But, what exactly is a software vulnerability?

A vulnerability can be defined in two ways:

- A bug in code or a flaw in software design that can be exploited to cause harm. Exploitation may occur via an authenticated or unauthenticated attacker.
- A gap in security procedures or a weakness in internal controls that when exploited results in a security breach.

How does a vulnerability assessment work?

There are three primary objectives of a vulnerability assessment.

- Identify vulnerabilities ranging from critical design flaws to simple misconfigurations.
- Document the vulnerabilities so that developers can easily identify and reproduce the findings.
- Create guidance to assist developers with remediating the identified vulnerabilities.

Vulnerability testing can take various forms. One method is Dynamic Application Security Testing (DAST). A dynamic analysis testing technique that involves executing an application (most commonly a Web application), DAST is performed specifically to identify security defects by providing inputs or other failure conditions to find defects in real time. Conversely, Static Application Security Testing (SAST) is the analysis of an application's source code or object code in order to identify vulnerabilities without running the program.

The two methodologies approach applications very differently. They are most effective at different phases of the software development life cycle (SDLC) and find different types of vulnerabilities. For example, SAST detects critical vulnerabilities such as cross-site scripting (XSS) and SQL injection earlier in the SDLC. DAST, on the other hand, uses an outside-in penetration testing approach to identify security vulnerabilities while Web applications are running.

Another method of vulnerability assessment in and of itself, penetration testing entails goal-oriented security testing. Emphasizing an adversarial approach (simulating an attacker's methods), penetration testing pursues one or more specific objectives

10 common web application Vulnerabilities

- Security misconfiguration :Security misconfiguration is a very common type of web application vulnerability. It is used to describe insecure default configurations, incomplete ...
- Broken access control : Broken Access Control is a type of application security vulnerability that enables users to access data and functionalities that they should not have access to ...
- Cryptographic failures :Cryptographic failures. Previously known as 'Sensitive Data Exposure', the focus in this issue is on failures related to cryptography. These often lead to ...
- Injection : Injection attacks exploit vulnerabilities in input validation and inadequate data handling. Attackers inject data such as SQL queries, code snippets.

SYNOPSYS®

Web apps are the most widely used attack vector

64% of companies globally have experienced a cyberattack in the past year

Web application attacks accounted for **70%** of cyberattacks

Web attacks are a growing risk

Attacks starting in web apps increased from **32%** in 2020 to **54%** in 2021

Operational limitations increase your risk

Security programs require planning and resources to be successful

Meanwhile, new web attacks happen every **39 seconds**

30,000 websites are hacked every day

In-house security expertise is rare and expensive

3.5 million unfilled cybersecurity jobs by 2025

33% increase in demand for infosec analysts through 2030

False positives from AST scans cause more problems

How can I tell if my organization requires a vulnerability assessment?

conduct a vulnerability assessment to verify that security initiatives performed earlier in the SDLC are effective. For example, an organization that properly trains developers in secure coding and performs reviews of security architecture and source code will most likely have fewer vulnerabilities than an organization that does not conduct those activities.

Whether your organization develops applications or uses third-party applications, vulnerability testing annually, or after significant changes to the applications or application environments are implemented, is critical to ensure a rock-solid security initiative.

The Importance of Vulnerability Assessment

The most common security vulnerabilities are rooted either in technology issues or user behavior:

- Breaches can occur if insiders accidentally expose information to an external source or leak information intentionally (i.e., malicious insiders).
- Lost and stolen devices that contain unencrypted data are also a major vector for infiltration into a company's network.

- Cybercriminals can install malware on target systems to exfiltrate data or gain control over computing systems.

Vulnerability management helps companies prevent data breaches and leaks, but it requires continuous vigilance. The process is ongoing and involves conducting periodic vulnerability assessments – when one assessment completes, another must begin.

Vulnerability assessments allow security teams to identify, analyze, categorize, report, and remediate security vulnerabilities in operating systems, business applications, endpoint devices, and browsers.

Organizations discover thousands of new vulnerabilities each year, requiring constant patching and reconfiguration to protect their networks, applications, and operating systems. However, many companies lack an effective patch management strategy and don't apply the necessary patches in time to prevent a breach.

It is impractical to patch all vulnerabilities immediately. A vulnerability management system helps prioritize vulnerabilities and ensure the security team addresses high-risk vulnerabilities first. Vulnerability management encompasses

the tooling and processes needed to find and remediate the most critical vulnerabilities regularly.

Types of Vulnerability Assessment Tools

Modern vulnerability assessments rely on automated scanning tools. Here are the main categories of tools used to scan an environment for vulnerabilities:

- Network-based scanning—used to identify potential network security attacks. This type of scan can also detect vulnerable systems on wired or wireless networks.
- Host-based scanning—used to identify vulnerabilities on servers, workstations, or other network hosts. This type of scan looks for vulnerable open ports and services, providing insights about the configuration settings and patch history of scanned systems.

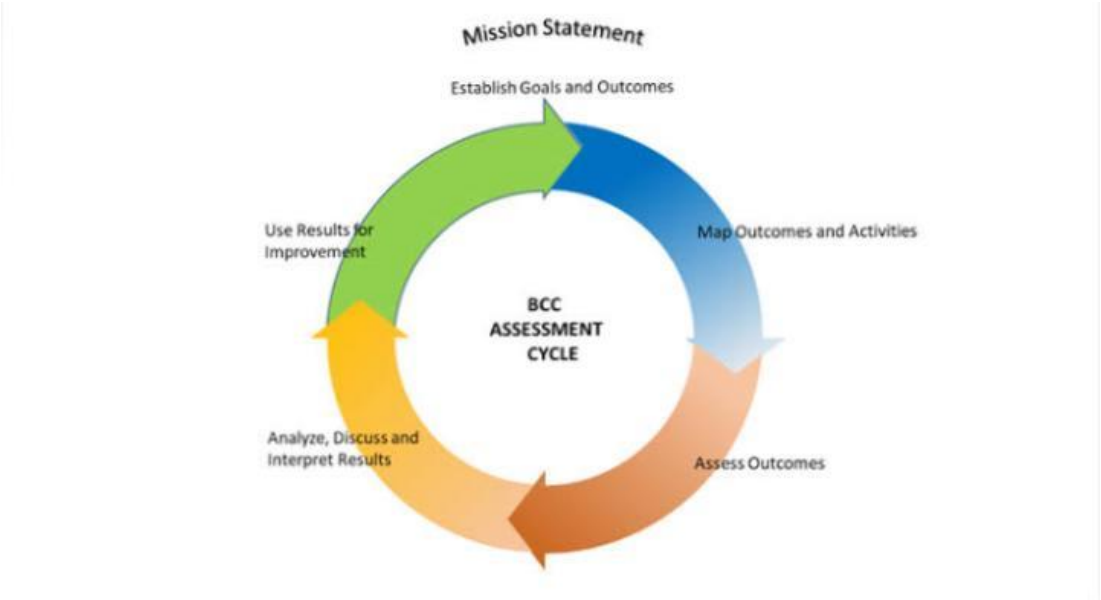
- Wireless network scans—used to scan an organization's Wi-Fi network to identify security weaknesses. These scans can identify malicious access points and ensure that wireless networks are configured securely.
- Application scans—used to test websites and mobile applications for known software vulnerabilities and misconfigurations.
- Database scans—used to identify vulnerabilities that might allow database-specific attacks like SQL and NoSQL injection, as well as general vulnerabilities and misconfigurations in a database server

5-Step Vulnerability Assessment Process:

1. . Initial preparation:In this stage, the team decides the scope and goals of vulnerability testing. This involves:
    - Identifying protected assets and equipment and mapping out all endpoints.
    - Determining the business value of each asset and the impact if it is attacked.
    - Identifying access controls and other security requirements of each system.

- Determining if systems hold sensitive data, and how sensitive data is transferred between systems.
- Recording a baseline of services, processes, and open ports on protected assets.
- Determining operating systems and software deployed on assets.

This information can help security teams understand the attack surfaces and the most severe threat scenarios, and develop a remediation strategy.



2. Vulnerability Assessment Testing:In this stage, the team runs automated vulnerability scans on target devices and environments. If necessary, they use

manual tools to investigate the security posture of a system. In order to automate this stage and make it more efficient, teams will typically rely on one or more vulnerability databases, vendor security advisories, and threat Intelligence feeds. A single test can take anywhere from a minute to several hours, depending on the size of the target system and the type of scan.

3. Prioritize Vulnerabilities:At this stage, the team removes false positives from vulnerability scanning results and prioritize vulnerabilities according to several factors. These can include:
    - score provided by a vulnerability database
    - The business impact if a vulnerability is exploited
    - Sensitive data that might be at risk
    - The ease of exploiting the vulnerability
    - How long the vulnerability has been in place
    - The ability to perform lateral movement from this system to other sensitive systems
    - The availability of a patch and the effort needed to deploy it.

4.Create a Vulnerability Assessment Report:At this stage, the team creates a unified report showing vulnerabilities

found in all protected assets, with a plan for remediating them. For medium to high risk vulnerabilities, the report should provide information about the vulnerability, when it was discovered, which systems it affects, the potential damage if attackers exploit it, and the plan and effort required to remediate it. Where possible, the team should also provide a proof of concept (PoC) demonstrating how each critical vulnerability could

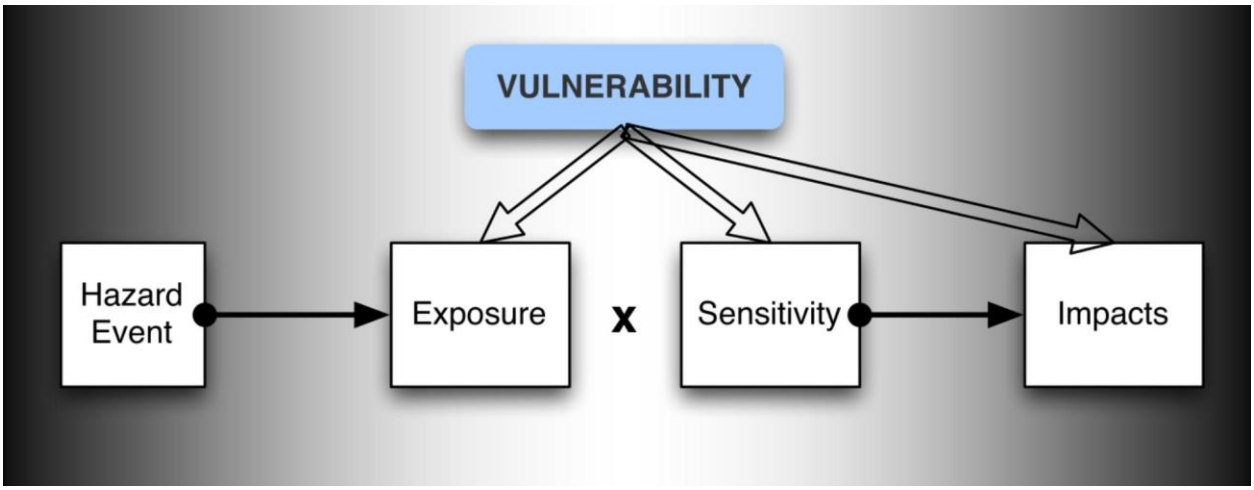
5. Continuous Vulnerability Assessment:

Vulnerability scans provide a point-in-time snapshot of vulnerabilities that exist in an organization's digital infrastructure. However, new deployments, configuration changes, newly discovered vulnerabilities, and other factors can result in new vulnerabilities. Because vulnerabilities are not static, vulnerability management should also be a continuous process.

Software development teams should incorporate automated vulnerability assessment into their continuous integration and deployment (CI/CD) pipeline. This allows vulnerabilities to be identified and fixed as early as possible in the software development

lifecycle (SDLC), eliminating the need to develop and release patches for vulnerable code.

However, because this process cannot catch all vulnerabilities, and many vulnerabilities occur in legacy or third-party systems, it must be complemented by continuous vulnerability scans of production systems.



Conclusion

In this article, we explained the basics of vulnerability assessment, covered the main tools that can be used to identify vulnerabilities, including network scanning, host scanning, and application scanning, and presented a 5-step

process for managing vulnerability assessments in your organization:

Initial preparation – defining scope and goals of vulnerability testing.

Vulnerability testing – running automated tests to identify vulnerabilities in systems included in the scope.

Prioritize vulnerabilities – identify which vulnerabilities are important and require attention, and their possible business impact.

Create vulnerability assessment report – produce a plan detailing the medium and high priority vulnerabilities found and recommended remediations.

Continuous vulnerability assessment – scanning for vulnerabilities on a continuous basis to see if previous vulnerabilities were remediated and discover new ones.

Reference :

http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf


Thank you!