Vulnerability Assessment

What is vulnerability assessment

A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

Examples of threats that can be prevented by vulnerability assessment include:

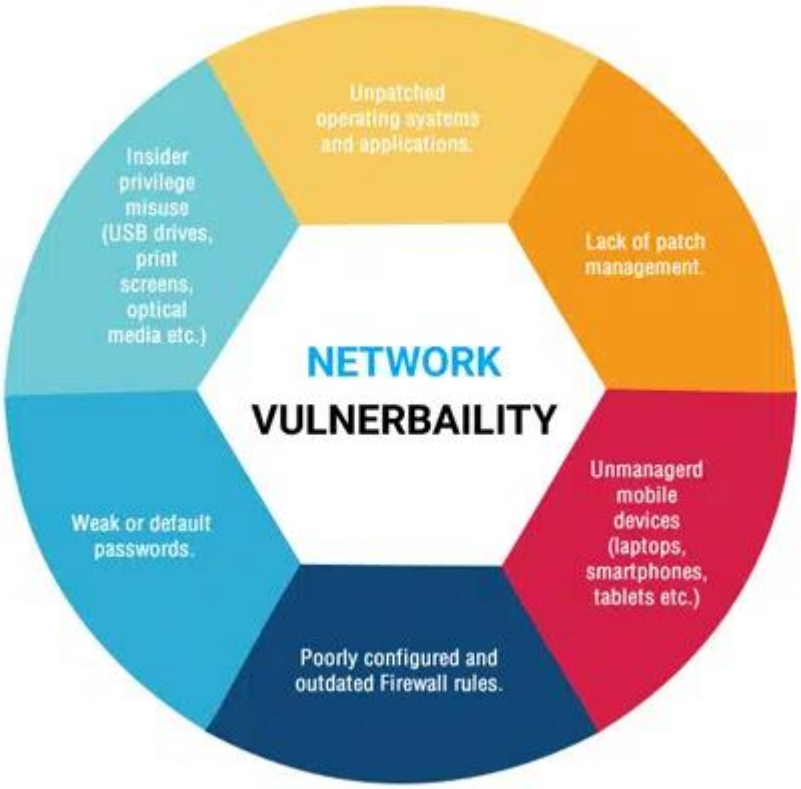
1. SQL injection, XSS and other code injection attacks.
2. Escalation of privileges due to faulty authentication mechanisms.
3. Insecure defaults – software that ships with insecure settings, such as a guessable admin passwords.

There are several types of vulnerability assessments. These include:

1. **Host assessment** – The assessment of critical servers, which may be vulnerable to attacks if not adequately tested or not generated from a tested machine image.
2. **Network and wireless assessment** – The assessment of policies and practices to prevent unauthorized access to private or public networks and network-accessible resources.
3. **Database assessment** – The assessment of databases or big data systems for vulnerabilities and misconfigurations, identifying rogue databases or insecure dev/test environments, and classifying sensitive data across an organization's infrastructure.
4. **Application scans** – The identifying of security vulnerabilities in web applications and their source code by automated scans on the front-end or static/dynamic analysis of source code.

Vulnerability assessment: Security scanning process

The security scanning process consists of four steps: testing, analysis, assessment and remediation.



How to Perform a Comprehensive Network Vulnerability Assessment

Now that we've analyzed the importance of performing regular network analyses, let's look at the steps that ensure every analysis is thorough and productive:

1. Risk Identification and Analysis

Network vulnerability assessments begin with the complex process of **identifying the potential risks and threats** facing each of the organization's assets. Your team can streamline this process by carefully structuring a list of those threats and ensuring that nothing slips through the cracks. Make sure none of the information you gather is wasted and that you **don't overlook any assets by creating one centralized document** with all of the necessary information pertaining to threats and vulnerabilities. Once your team has cataloged all this information on your organization's assets, you can begin analyzing and assigning risks to assets. **Risks are**

assigned to assets based on their potential impact and likelihood of the threat becoming a reality. When you have completed this process, your security team can **prioritize assets that are most at risk or which would be most critically affected by having their vulnerabilities exploited.**

2. Scope and Scan Frequency Policy

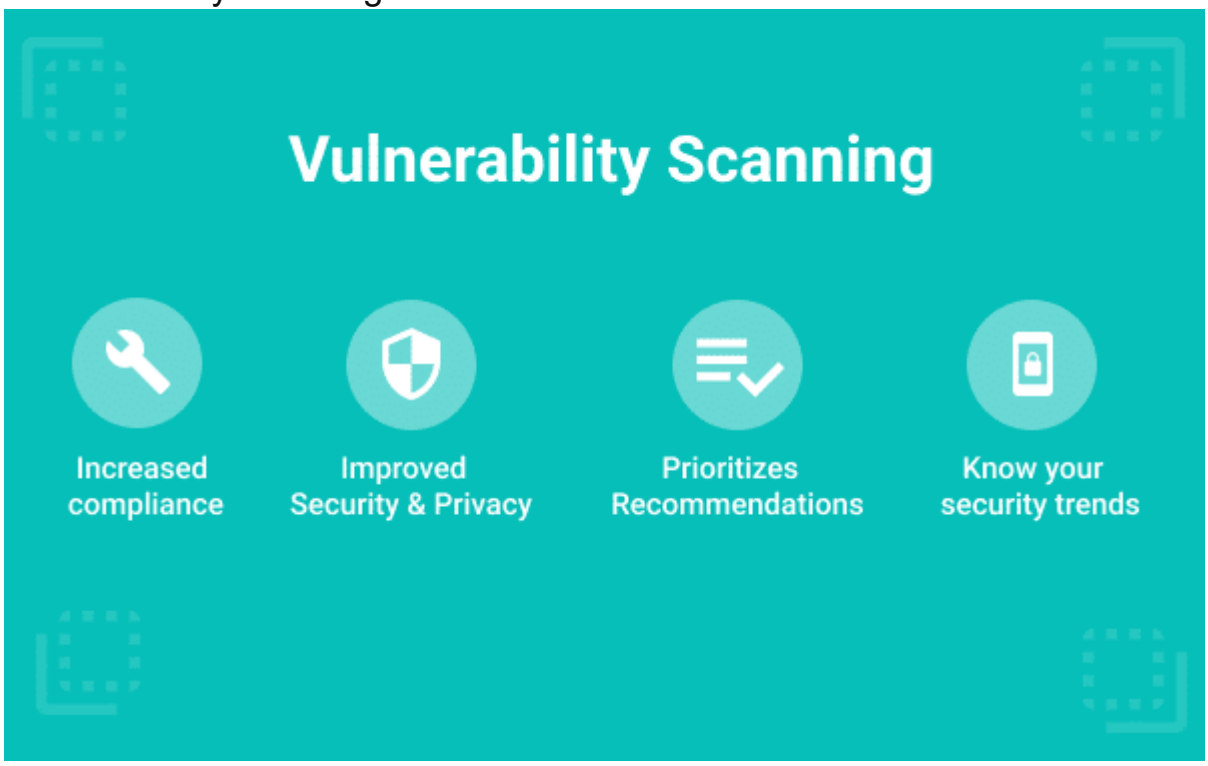
Then it's time to ensure your scanning methodology is thoroughly structured. This involves laying out a predetermined series of **policies and procedures, delineating a straightforward course of action,** and appointing an official owner responsible for what goes into each policy or procedure. Additionally, upper management will need to approve policies before their application.
Part of determining clear scanning policies includes clarifying the **frequency of scanning**. This is a significant step for adhering to many external compliance and security regulations. In addition to laying out the scanning frequency policy, you'll need to document vulnerability scan configuration and functionality and the steps that your team must take once the scan is completed.
The most important information to document is the types of scans that the team will perform, how to implement the scans, the software solutions used, which vulnerabilities should be prioritized, and the actions taken after the scan is completed.

3. Scan Configuration

Configuring scans can be as simple as defining the objectives of the scan and identifying the type of system you want to scan. You can breakdown the process of configuring a network vulnerability scan into four simple steps:

1. **Create a list of target IPs:** Having a list of the IP addresses that host the target system will help you to quickly and easily input them into the vulnerability scanning software to be scanned.
2. **Specify a port range and protocols:** Once the target IPs have been added, you will need to define the port range you want scanned and the protocol you want the software to use.
3. **Define your targets:** In this step, you will need to add specific parameters to your scan by defining if your target's IPs are databases, windows servers, applications, wireless devices, or something else. Narrowing down the breadth of your scan by creating more specific targets for scanning will ensure you receive accurate results.
4. **Define the scan parameters:** You will need to set the scan's aggressiveness, time, and notifications – all of which are parameters that can affect the performance of the scanned devices. For that reason, setting scans for non-business hours is recommended to avoid service interruptions. You can also set up the system to get a notification once the scan is complete.

4. Vulnerability Scanning



Source: https://securetriad.io/vulnerability-scanning-vs-penetration-testing/

Once you have identified the type of scan you want to conduct and set its configurations, you can save the configured settings for future use to save time when running the scan whenever needed. Keep in mind that **scans can range from minutes to hours,** depending on the target size and thoroughness of the scan.
Vulnerability scans can be divided into three phases:

- **Scanning**
- **Enumeration**
- **Vulnerability detection**

During the scanning phase, the software you use will fingerprint the targets specified and gather preliminary information on them. The software will then use this information to enumerate the targets and gain more detailed information, such as which ports and services are in use and running. After determining these specifications, the software will search and identify any existing vulnerabilities in the target IP.

5. Result Analysis

At this point, your team will need to perform most of the analysis process manually. **Prior knowledge of the scanned system is especially beneficial as your team will know which vulnerabilities will have the most critical impact** and are a high priority. Although scanning tools will often prioritize

vulnerabilities automatically, inside knowledge may mean that your security team will perform this task more effectively.
This stage also involves manual analysis of the automated system's results, including **filtering out false positives and ensuring that the identified vulnerabilities are valid.** Once your team has validated the vulnerabilities, they can start investigating the potential root causes and future impact of each vulnerability to repair existing ones and prevent similar vulnerabilities from appearing in future scans.

6. Remediation and Mitigation
After you have interpreted and validated the results, your team can work on **mitigating each vulnerability.** This requires that the **security team work with IT staff** to ensure all mitigation procedures are carried out. Clear communication and cooperation will streamline and simplify the process while ensuring that successful mitigation procedures are carried out.
At this point, both teams will likely conduct numerous follow-up scans to ensure that they have neutralized the previously discovered vulnerabilities. These scans will continue until the discovered vulnerabilities no longer appear in reports.

Why Network Vulnerability Assessment Is Not Enough
Assessing your network for vulnerabilities prevents cyberattacks from occurring and disrupting your productivity. Unfortunately, while **network vulnerability analysis is a critical aspect of cybersecurity**, it only makes up a fraction of a robust cybersecurity strategy. Maintaining a high standard of security that complies with regulatory requirements and covers your organization's entire attack surface is far from simple, but by **performing routine assessments you will be well on your way towards ensuring that your network is protected**, and that no significant vulnerabilities slip into your blindspot.

1.Vulnerability identification (testing)

2.The objective of this step is to draft a comprehensive list of an application's vulnerabilities. Security analysts test the security health of applications, servers or other systems by scanning them with automated tools, or testing and evaluating them manually. Analysts also rely on vulnerability databases, vendor vulnerability announcements, asset management systems and threat intelligence feeds to identify security weaknesses.

2. Vulnerability analysis

The objective of this step is to identify the source and root cause of the vulnerabilities identified in step one.

It involves the identification of system components responsible for each vulnerability, and the root cause of the vulnerability. For example, the root cause of a vulnerability could be an old version of an open source library. This provides a clear path for remediation – upgrading the library.

3. Risk assessment

The objective of this step is the prioritizing of vulnerabilities. It involves security analysts assigning a rank or severity score to each vulnerability, based on such factors as:

1. Which systems are affected.
2. What data is at risk.
3. Which business functions are at risk.
4. Ease of attack or compromise.
5. Severity of an attack.
6. Potential damage as a result of the vulnerability.

4. Remediation

The objective of this step is the closing of security gaps. It's typically a joint effort by security staff, development and operations teams, who determine the most effective path for remediation or mitigation of each vulnerability.

Specific remediation steps might include:

1. Introduction of new security procedures, measures or tools.
2. The updating of operational or configuration changes.
3. Development and implementation of a vulnerability patch.

Vulnerability assessment cannot be a one-off activity. To be effective, organizations must operationalize this process and repeat it at regular intervals. It is also critical to foster

cooperation between security, operation and development teams – a process known as DevSecOps.

Vulnerability assessment tools

Vulnerability assessment tools are designed to automatically scan for new and existing threats that can target your application. Types of tools include:

1. Web application scanners that test for and simulate known attack patterns.
2. Protocol scanners that search for vulnerable protocols, ports and network services.
3. Network scanners that help visualize networks and discover warning signals like stray IP addresses, spoofed packets and suspicious packet generation from a single IP address.

It is a best practice to schedule regular, automated scans of all critical IT systems. The results of these scans should feed into the organization's ongoing vulnerability assessment process.

Vulnerability assessment and WAF

Imperva's web application firewall helps protect against application vulnerabilities in several ways:

1. As a gateway for all incoming traffic, it can proactively filter out malicious visitors and requests, such as SQL injections and XSS attacks. This eliminates the risk of data exposure to malicious actors.
2. It can perform virtual-patching — the auto-applying of a patch for a newly discovered vulnerability at the network edge, giving developers and IT teams the opportunity to safely deploy a new patch on the application without concern.
3. Our WAF provides a view of security events. Attack Analytics helps contextualize attacks and expose overarching threats, (e.g., showing thousands of seemingly unrelated attacks as part of one big attack campaign).

4. Our WAF integrates with all leading SIEM platforms to provide you with a clear view of the threats you're facing and help you prepare for new attacks.

See Our Additional Guides on Key Data Security Topics

Together with our content partners, we have authored in-depth guides on several other topics that can also be useful as you explore the world of data security.

Cyber Security

- What is a Honeypot | Honeynets, Spam Traps & more
- What is Penetration Testing | Step-By-Step Process & Methods
- What is Information Security | Policy, Principles & Threats

Data Privacy

- What is HIPAA Privacy Rule | HIPPA Security Requirments
- What is Data Governance | Frameworks, Tools & Best Practices
- SOX Compliance | Requirements, Controls & Audits

DLP

Authored by Exabeam

- Data Loss Prevention Tools
- Data Loss Prevention Policy Template
- Understanding Cloud DLP: Key Features and Best Practices