Exploitation

SAMARENDRANATH B

Vulnerability

A vulnerability in cyber security refers to any weakness in an organization's information system, system processes, or internal controls.

These vulnerabilities are targets for lurking cybercrimes and are open to exploitation through the points of vulnerability.

Examples of Vulnerabilities

- A weakness in a firewall that can lead to malicious hackers getting into a computer network
- Lack of security cameras
- Unlocked doors at businesses

How is vulnerability different from a cyber security threat and risk?

Vulnerabilities are not introduced to a system but are there from the beginning.

There are not many cases involving cybercrime activities that lead to vulnerabilities.

They are typically a result of operating system flaws or network misconfigurations.

Cyber security threats, on the other hand, are introduced to a system like a virus download or a social engineering attack.

How is vulnerability different from a cyber security threat and risk?

Cyber security risks are generally classified as vulnerabilities, which can lead to confusion as they are not the same.

Risks are actually the probability and impact of a vulnerability being exploited. If these two factors are low, then the risk is low.

It is directly proportional, in which case, the inverse is also true; high probability and impact of vulnerabilities lead to high risks.

When does a vulnerability become exploitable?

A vulnerability, which has at least one definite attack vector is an exploitable vulnerability.

Attackers will, for obvious reasons, want to target weaknesses in the system or network that are exploitable.

Of course, vulnerability is not something that anyone will want to have, but you should be more worried about it being exploitable.

When does a vulnerability become exploitable?

There are cases when something that is vulnerable is not really exploitable. The reasons could be:

Insufficient public information for exploitation by attackers.

Prior authentication or local system access that the attacker may not have

Existing security controls

Strong security practices can prevent many vulnerabilities from becoming exploitable.

What causes the vulnerability?

Complex Systems

Complex systems increase the probability of misconfigurations, flaws, or unintended access.

Familiarity

Attackers may be familiar with common code, operating systems, hardware, and software, leading to known vulnerabilities.

Connectivity

Connected devices are more prone to have vulnerabilities.

Poor Password Management

Weak and reused passwords can lead from one data breach to several.

Causes

Unchecked user input

If software or a website assumes all input is safe, it may run unintended SQL injection.

People

Social engineering is the biggest threat to the majority of organizations. So, humans can be one of the biggest causes of vulnerability

Causes

OS Flaws

Operating systems can have flaws too. Unsecured operating systems by default can give users full access and become a target for viruses and malware.

Internet

The internet is full of spyware and adware that can be installed automatically on computers.

Software Bugs

Programmers can sometimes accidentally leave an exploitable bug in the software.

Types of Vulnerabilities

System Misconfigurations

Network assets with disparate security controls or vulnerable settings can result in system misconfigurations.

Cybercriminals commonly probe networks for system misconfigurations and gaps that look exploitable.

Due to the rapid digital transformation, network misconfigurations are on the rise.

Therefore, it is important to work with experienced security experts during the implementation of new technologies

Types of Vulnerabilities

Out-of-date or Unpatched Software

Similar to system misconfigurations, hackers tend to probe networks for unpatched systems that are easy targets.

Attackers can exploit these unpatched vulnerabilities to steal sensitive information.

To minimize these risks, it is essential to establish a patch management schedule so that all the latest system patches are implemented as soon as they are released.

Types of Vulnerabilities

Missing or Weak Authorization Credentials

A common tactic that attackers use is to gain access to systems and networks through brute force, like guessing employee credentials.

That is why employees must be educated on the best practices of cybersecurity so that their login credentials are not easily exploited.

Types of Vulnerabilities

Malicious Insider Threats

Whether it's with malicious intent or unintentionally, employees with access to critical systems sometimes end up sharing information that helps cyber criminals breach the network.

Insider threats can be really difficult to trace as all actions will appear legitimate.

To help fight against these types of threats, one should invest in network access control solutions and segment the network according to employee seniority and expertise.

Types of Vulnerabilities

Missing or Poor Data Encryption

It’s easier for attackers to intercept communication between systems and breach a network if it has poor or missing encryption.

Cyber adversaries can extract critical information and inject false information onto a server when there is poor or unencrypted information.

This can seriously undermine an organization’s efforts toward cyber security compliance and lead to fines from regulatory bodies.

Types of Vulnerabilities

Zero-day Vulnerabilities

Zero-day vulnerabilities are specific software vulnerabilities that the attackers have caught wind of but have not yet been discovered by an organization or user.

There are no available fixes or solutions in these cases since the vulnerability is not yet detected or notified by the system vendor.

These are especially dangerous as there is no defense against such vulnerabilities until after the attack has happened.

Hence, it is important to remain cautious and continuously monitor systems for vulnerabilities to minimize zero-day attacks.

What is Vulnerability Management?

Vulnerability management is the cyclical practice consisting of the identification, classification, remediation, and mitigation of security vulnerabilities.

There are three essential elements of vulnerability management viz. vulnerability detection, vulnerability assessment, and remediation.

Vulnerability Detection

Vulnerability detection includes the following three methods:

Vulnerability scanning

Penetration testing

Google hacking

Cyber Security Vulnerability Scan

As the name suggests, the scan is done to find vulnerabilities in computers, applications, or networks.

For this purpose, a scanner (software) is used to discover and identify vulnerabilities that arise from misconfiguration and flawed programming within a network.

Some popular vulnerability scanning tools are

SolarWinds Network Configuration Manager (NCM),

ManageEngine Vulnerability Manager Plus,

Rapid7 Nexpose,

Acunetix,

Probely,

TripWire IP 360, etc.

Penetration Testing

Penetration testing or pen testing is the practice of testing an IT asset for security vulnerabilities that an attacker could potentially exploit.

Penetration testing can be automated or manual.

It can also test security policies and employee security awareness, identifying and responding to security incidents, and adherence to compliance requirements.

Google Hacking

Google hacking is the use of a search engine to locate security vulnerabilities.

This is achieved through advanced search operators in queries that can locate hard-to-find information or data that has been accidentally exposed due to the misconfiguration of cloud services.

These targeted queries are mostly used to locate sensitive information not intended for public exposure.

Cyber Security Vulnerability Assessment

Once a vulnerability is detected, it goes through the vulnerability assessment process.

What is a vulnerability assessment?

It is a process of systematically reviewing security weaknesses in an information system. It highlights whenever a system is prone to known vulnerabilities, classifies the severity levels, and recommends appropriate remediation or mitigation if required.

The assessment process includes:

Identify vulnerabilities: Analyzing network scans, firewall logs, pen test results, and vulnerability scan results to find anomalies that might highlight vulnerabilities prone to cyber-attacks.

Verify vulnerabilities: Decide whether an identified vulnerability could be exploited and classify its severity to understand the level of risk.

Mitigate vulnerabilities: Identify appropriate countermeasures and measure their effectiveness if a patch is unavailable.

Remediate vulnerabilities: Update affected software or hardware wherever possible.

Types of vulnerability assessments

Network-based assessment

This type of assessment is used to identify potential issues in network security and detect systems that are vulnerable on both wired and wireless networks.

Host-based assessment

Host-based assessment can help locate and identify vulnerabilities in servers, workstations, and other network hosts.

It generally assesses open ports and services and makes the configuration settings and patch management of scanned systems more visible.

Types of vulnerability assessments

Wireless network assessment

It involves scanning Wi-Fi networks and attack vectors in the infrastructure of a wireless network.

It helps validate that a network is securely configured to avoid unauthorized access and can also detect rogue access points.

Application assessment

It is the identification of security vulnerabilities in web applications and their source code.

This is achieved by implementing automated vulnerability scanning tools on the front end or analyzing the source code statically or dynamically.

Types of vulnerability assessments

Database assessment

The assessment of databases or big data systems for vulnerabilities and misconfiguration, identifying rogue databases or insecure dev/test environments, and classifying sensitive data to improve data security.

Vulnerability management becomes a continuous and repetitive practice because cyber attacks constantly evolve.

Vulnerability Remediation

To always be one step ahead of malicious attacks, security professionals must have a process for monitoring and managing known vulnerabilities.

Once a time-consuming and tedious manual job, it is now possible to continuously keep track of an organization’s software inventory with the help of automated tools and match them against the various security advisories, issue trackers, or databases.

If the tracking results show that the services and products are relying on risky code, the vulnerable component needs to be located and mitigated effectively and efficiently.

Steps

Step 1: Know Your Code

Knowing what you're working with is crucial and the first step of vulnerability remediation.

Monitoring software inventory to determine which software components are being used and what needs immediate attention will significantly prevent malicious attacks.

Step 2: Prioritize Your Vulnerabilities

Organizations need to have prioritization policies in place. The risk of the vulnerabilities needs to be evaluated first by going through the system configuration, the likelihood of an occurrence, its impact, and the security measures in place.

Step 3: Fix

Once the security vulnerabilities that require immediate attention are known, it is time to map out a timeline and work plan for the fix.

Summary

With networks becoming more and more complex, it has become critical to actively manage cyber security vulnerabilities.

To actively manage cyber security vulnerabilities, it is essential to have visibility of internal and third-party network ecosystems.

Risk Assessment and Vulnerability Assessment

For securing IT assets, the assessment of risks and vulnerabilities is essential.

A comprehensive vulnerability assessment should be done to understand and mitigate the threats in an IT environment.

Risk assessment and vulnerability assessment are the two most popular and widely accepted ways to spot threats and analyze them.

What is a Vulnerability Assessment?

Vulnerability assessment examines systems to spot gaps that could result in exploitation, while risk assessment identifies these recognized threats and evaluates likelihood and impact.

With the help of vulnerability assessment, companies can define and prioritize vulnerabilities that exist in the company's current network infrastructure, computer systems, and resources.

Types

There are different types of vulnerability assessments that

Network-based scans,

Host-based scans,

Wireless network scans,

Web applications scans.

When and Why Companies Use Vulnerability Assessment?

An organization has changed the configuration of a system or its network or has purchased new systems. New systems and changes impact the threat landscape of the organization.

A vulnerability assessment is required to evaluate if threats have changed, existing gaps have been plugged, or if new threats have cropped up.

Vulnerability assessment also improves the operational efficiency of the system and guards against any issues arising out of deploying new software or hardware.

The organization understands if their IT systems are managed optimally and efficiently or not.

What are The Steps of Vulnerability Assessment?

1. ***Identify Assets and Risks***

Identify the crucial IT assets of the organization and their location (on-premise or cloud).

Then make a list of potential threats that should be assessed for those assets; this leads to a security baseline.

This security baseline will help to understand the configuration of the system in terms of security - whether the current system is safe or not.

What are The Steps of Vulnerability Assessment?

2. Create a Detailed Picture

Once the assets and related risks are identified, we move ahead with creating a detailed picture of the current IT structure of the organization considering the software and programs used.

The knowledge of the team that accesses this software and uses other crucial IT assets included in the list should also be considered. It helps spot weaknesses and prioritize the fixes.

What are The Steps of Vulnerability Assessment?

3. Vulnerability Scan

After the system baseline is defined, the next step is to perform a vulnerability scan to detect the existing weaknesses of the current system. It is done using various tools and plug-ins that are designed for vulnerability assessment.

4. Vulnerability Report

The final step is to compile the scan results and summarize each of the vulnerabilities identified during the scan. The report must include the type of vulnerability, potential impact, and the strategy to mitigate each.

Benefits of Vulnerability Assessment

Vulnerability assessment **detects the weaknesses** in the current IT structure before attackers do.

The result is **a complete list of important IT assets** to the organization and the vulnerabilities so that the organization can prioritize fixes thereon.

It is a defined assessment that **provides a complete report of vulnerabilities and coping methods, which helps prepare** for future system upgrades and changes.

The security records developed during the process can be **taken as a reference for later assessment**.

What is Risk Assessment?

Risk assessment is the process of **identifying, analyzing, and evaluating the risks associated** with a specific action or event.

The aim is to prevent application security defects and reduce the likelihood of potential threats within a company’s network and information systems.

A thorough risk assessment allows the organization to view the entire system carefully **from an attacker’s perspective**.

Being an integral part of an organization's information security risk management process, risk assessment helps make informed decisions about resources and tools.

When and Why Companies Use Risk Assessment?

An organization may not be aware of **underlying hazards and risks associated** with the company's networks and systems.

A company must know whether it is lacking in strategic control and which tools are available to reduce the security risks.

Performing a security risk assessment will help you identify loopholes in existing controls, if any, and work on strategies to prevent risks from happening.

When companies are occupied with their day-to-day operations, preventive controls like security assessment often take a back seat, leading to a loss of compliance with regulations and policies.

When and Why Companies Use Risk Assessment?

Running regular risk assessments helps an organization **stay compliant with security standards** and save money, as failing to comply will cost them huge fines and penalties.

Another crucial consideration point is the timing of running a risk assessment. Risk assessments should be conducted at **regular intervals** depending on the size and complexity of a business, for example, once every 6 or 12 months.

Investing in risk assessments before starting new projects or making changes in existing systems and processes for the company to identify and categorize risks beforehand is also important and beneficial**.**

What are The Steps of Risk Assessment?

Risk assessment is a comprehensive activity that begins with documentation review, information gathering, and brainstorming, and continues till the organization creates a risk register.

A risk register lists risks with their root causes, potential responses, and risk categories.

This risk register is updated periodically or otherwise throughout the lifecycle of a project

What are The Steps of Risk Assessment?

1. Identify Risks

Identifying the risks is the foremost and crucial step to get started with risk assessment. If not done correctly, the team can miss out some serious, potential threats.

A list of IT assets and processes should be compiled considering the types of threats that an attack can pose. It will help to monitor and track the potential threats.

What are The Steps of Risk Assessment?

2. Perform Analysis

The next crucial step in risk assessment is analysis, in which the assessing team determines the likelihood of each risk leading to an issue in the system and the potential impact on the company.

This investigation can help comprehend how a successful breach could occur and what should be done to mitigate its associated risks.

What are The Steps of Risk Assessment?

3. Evaluate

Evaluation of risks is the final step that results in prioritizing risks in different categories based on the likelihood of occurrence and the impact each may leave.

Usually, risks are categorized as critical, high, medium, and low, but there can be more categories depending on the complexity of the business.

Benefits of Risk Assessment

Identifying security issues that arise out of various internal and external factors like inefficiencies, non-compliances with set standards etc.

Determining new security requirements to strengthen the company's systems' security.

Creating awareness among employees about the risks and measures to eradicate the issues.

Better planning of the IT structure and resources of the company and developing new security plans and policies.