Vulnerability Concepts

Reading

45m

Status | Incomplete

Introduction

During a vulnerability assessment, a number of distinct types of vulnerabilities must be considered, and these types fall into four key categories: software, network, hardware, and people. In this reading, you will dig into some key aspects of each category. You will also explore some additional resources where you can learn about vulnerabilities and vulnerability types in greater depth.

Reading

> **Policy Matters**
>
> A robust and well-written Cyber Security policy that addresses each of these types of vulnerabilities can provide key actions to help address the vulnerabilities.
>
> As you examine each type, you will see how a well-written policy can often mitigate, at least in part, many of the typical vulnerabilities found.

Software Vulnerabilities

Description

These are vulnerabilities that impact the software used by a company or organization, including coding issues that may provide unauthorized access or data leaking.

Cause

The two primary causes of software vulnerabilities that make systems susceptible to network-based attacks are typically:

- Software or hardware misconfiguration
- Poor development methods

Potential Result

Utilizing these weaknesses, attackers conduct a variety of attacks on corporate resources.

How Policy Helps

Policies can reduce the risk of software vulnerabilities by mandating software use life cycles, as well as retirement for software that is out of its support cycle.

Network Vulnerabilities

Description

Network vulnerabilities include vulnerabilities in network protocols such as HTTP that may provide unauthorized access or data loss.

Cause

Common areas of network vulnerabilities are:

- Network misconfigurations
- Old, out of date, or unsupported network hardware and OSs

How Policy Helps

Policies can reduce network vulnerabilities by mandating network hardware life cycles and retirement for network hardware that is out of its support cycle. In addition, policies can also mandate that any network hardware or software patches are applied and tested before new network hardware is put into the production environment.

Hardware Vulnerabilities

Description

This type of vulnerability includes problems with physical devices, such as printers, computer hardware, and specialty hardware like automation systems, that may provide illegal access or data loss.

Cause

As with the network area, hardware vulnerabilities are often caused by:

- Continued use of unsupported items (as with the network area)
- Use of items that are inherently insecure (e.g., IoT devices) or not updated regularly

How Policy Helps

Due to the general insecurity of a lot of IoT devices and the software that is used to access or use them, policies may impose stringent security requirements and special permissions for the use of these types of devices, or even prohibit their use outright.

Policies may also require hardware to be updated and patched regularly within its support cycle or be replaced at a set maximum age. These update requirements are usually implemented for security reasons as well as failure avoidance reasons.

People

No matter how secure your hardware and software may be, there is always a vulnerability involved with people. This includes problems caused by human error, such as misconfigured websites that allow unwanted access or data leaks.

Cause

In this area, there are also vulnerabilities that arise from poor training, social engineering, and any number of human failings.

How Policy Helps

This is an excellent example of where policies can assist with vulnerabilities. Policies can include mandatory training and guidance on behaviour that can deter social engineering attacks and strengthen an organization's overall security posture.

Additional Vulnerabilities

There are other common vulnerabilities unique to specific environments or functions. Take web servers, for example. Because they are public facing and allow connections in order to fulfill their purpose, they have a host of specific vulnerabilities that need to be checked and kept up with.

Featured Resources

CWE

The MITRE Corporation's Common Weakness Enumeration (CWE) is a comprehensive list of software and hardware weaknesses that has been developed and maintained by a community of specialists since 2006.

This list will be a useful reference to have handy in your future Cyber Security studies and work.

> Take some time to peruse the CWE site and become familiar with its organization and content. The About section will give you useful insights on how the list is organized and used, and how to get involved in the community.

NVD

NIST maintains the National Vulnerability Database (NVD), where vulnerabilities are analyzed and categorized. While you may already have some familiarity with this database, take a few minutes to refresh your memory of the purpose and content of the database.

> ? **Reflection**
>
> As you review and recall the NVD resource above, consider how it compares and contrasts with the CWE.
>
> How might a Cyber Security professional make use of these resources together?

Further Reading

There's more than one way to categorize and organize vulnerability types. The following readings will give you a better feel for the breadth of areas and types of vulnerabilities you need to be aware of and able to help secure.

Crowdstrike: 7 Most Common Types Of Cyber Vulnerabilities

Intellipaat: What is Vulnerability in Cyber Security? Types and Definition

> Read the articles above and compile a complete list of vulnerability types that you can refer back to in future coursework, and in your Cyber Security career.
>
> Reach out to a colleague or two to compare your list and see if you have missed anything.

Summary of Key Takeaways

While exploring some of the types of vulnerabilities Cyber Security professionals are responsible for protecting and where they can be found, you have seen the following:

- Vulnerabilities are found in all categories of hardware and software.
- Vulnerabilities can stem from a wide range of causes, including but not limited to, poor development process and practice, poor configuration, poor maintenance and updating practices, human failings like social engineering, and use of out of date technologies and tools.
- Policy is one commonly used tool to assist in reinforcing and supporting good procedures to help minimize or mitigate some causes of vulnerabilities being present.

Conclusion

Vulnerabilities come in all shapes, sizes, and sources, and as Cyber Security professionals, it is your job to protect organizations from threats that would seek to take advantage of those vulnerabilities. Bad actors will not be picky, choosy, or selective on where they look other than to look for whatever vulnerabilities they feel that they can successfully take advantage of. As a result, you need to be as thorough and broad as you can with looking for, being aware of, and actively working to mitigate as many types and areas of vulnerability as you can.

✓ Mark Completed

← Previous
Overview - Vulnerability Assessment

Next
Common Vulnerabilities and Exploits (CVE) List →

How well did this activity help you to understand the content?

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W05D2

Tue Jul 23

› Outline & Notes (1)

› Lectures (1)

⌄ Work (10)

10 hrs

Project: Risk Management Case Study

Risk Management Case Study Presentation ✓

Regulatory Drivers & Cyber Security Compliance

Cyber Security Regulations Presentation

Course Reflection ✓

Overview - Vulnerability Assessment

Vulnerability Concepts

Common Vulnerabilities and Exploits (CVE) List

- Vulnerability Severity
- Security Vulnerabilities Scenarios with AI

› Other (1)

W05D2 Schedule »

Powered by Lighthouse Labs.