Vulnerability Assessments and Tools

Reading

45m

Status | Incomplete

Introduction

You've spent time looking into what exactly a vulnerability is and what it means to security professionals charged with protecting an organization and its assets. Now you'll learn about the assessments and tools that you can use to discover vulnerabilities and work to prioritize and mitigate them.

Searching for vulnerabilities in networks and setups can be a long and involved process. It takes time to thoroughly check every device and every configuration for weaknesses that can be exploited. Fortunately, there are tools out there that are purpose-built to assist you with this search.

Categorizing Tools

There are many different ways to categorize the different types of vulnerability assessments and scanning tools that are out there.

Here are some examples:

- Purpose for the vulnerability assessment - compliance vs regular monitoring or spot checks
- Type of target device(s) - servers vs web applications vs mobile devices/apps
- Network vs. device vs. cloud - environment and types of devices scanned, routers and switches vs. servers vs. cloud services
- Internal vs. external start point - scanner positioned inside the company network or starting from the internet to work its way in
- Depth of information collection - surface scan vs. penetration testing, authenticated vs. unauthenticated scanning (whether or not the scanner is giving authentication credentials to use during the scan)
- Method used to collect information
- And the list goes on

Three Main Purposes

When choosing an assessment tool, it can help to determine which of the three main purposes or major goals your organization has for completing a vulnerability assessment or scan.

Discovery

In this case, the point behind completing the scan is to find out (or, discover, if you will) what devices you have connected to your network. This could be simply for documentation purposes, or as part of an initial planning step within a more complete vulnerability assessment.

> ⚠ It’s important to remember that this assessment type is not thorough and is not actually intended to bring visibility to all the vulnerabilities in an environment.

Full

If you opt to complete a full vulnerability assessment, you are looking to get a complete picture of the vulnerabilities in the environment you are investigating. The scope of the investigation can vary. You may be doing a scan on a single server, a full network segment, a set of cloud resources, an organization’s public facing services, or a full scan of an organization's entire IT infrastructure. The distinguishing factor in this case is that whatever the targets are, you are trying to find any and all vulnerabilities that can be exploited, in order to rate the potential severity of each and prioritize how to tackle them.

> ⚠ It should be noted that this type of scan is not intended to be quiet or stealthy. It is specifically intended to be thorough.

Compliance

You may need to perform a vulnerability assessment specifically for compliance purposes. In this case, the target will be restricted to the parameters of the compliance requirements, and most likely, nothing outside of that. The key here is to be thorough around the purpose of the compliance vulnerability assessment to ensure and prove that you have met the requirements and spirit of the framework or regulations. You will not want to muddy the waters or get distracted from the purpose at hand.

Additional Categories of Vulnerability Assessments

Other ways that vulnerability assessments can be categorized are the methods and targets of the assessment.

Methods:

- Internal scanning
- External scanning
- Authenticated scanning
- Unauthenticated scanning

Targets:

- Host-based scan
- Network scan
- Web application scan
- Port scan
- Database scan
- Source code vulnerability scan
- Cloud vulnerability scan

Choosing the Right Tool

Vulnerability scanning tools range widely, from large, well-established, industry-accepted tools to open-source free tools. Tools can be online or downloadable, and can have a wide variety of different ranges and sets of features available in them.

> ℹ The key isn’t to know every vulnerability scanning tool in existence; instead, you want to develop the skills to find the tool that will suit your purpose in a given situation.

Here are some guiding questions to determine if a tool suits your particular needs:

- Is it compatible with the systems and items you need to scan?
- Is it capable of scanning and assessing the target items/devices/systems that you specifically need to focus on?
- Can it find vulnerabilities in the most critical and sensitive assets of your organization and/or the areas of compliance your organization needs to verify?
- Does it have a dashboard that shows you the most important and useful information?
- Do you want or need a tool that simply identifies the vulnerabilities, or will you also want explanations about the vulnerability and/or recommendations for mitigation?
- Does the cost fit into your budget constraints? This may actually be an important consideration for your organization.

Outsourcing Options

An important consideration in choosing an assessment tool is the capabilities and skills of your team. What if you don't have the time or expertise to complete the vulnerability assessment or scan yourself or within your own team? Nowadays, there are all kinds of organizations out there that specialize in performing and reporting on vulnerability assessments and compliance reporting. You can still use the guiding questions above to find one within your price range and that offers a service within the range of outputs you are looking for.

Further Reading

The following readings will give you additional information on what a vulnerability assessment is and various ways to categorize or look at them.

> Read the three articles and summarize any points into your PKM that you think might be useful in future coursework, and in your Cyber Security career.

TechTarget: Types Of Vulnerability Scanning And When To Use Each

Infosec Institute: Common Vulnerability Assessment Types

CBT Nuggets: 3 Types of Vulnerability Scans: Discovery, Full, Compliance

> **Tap into your Community of Practice to expand your ideas** Reach out to a colleague or two to compare your reflections and see if you have noticed different things.
>
> Update your PKM with any additional ideas from your peers that you find valuable.

Summary of Key Takeaways

In examining types of vulnerability assessments, you have seen:

- There are many ways to evaluate and categorize the various types of assessments that can be done.
- When choosing a tool and assessment to complete, the key points to consider are the purpose of the assessment, the devices that will be scanned, and the scope or depth required for the scan.
- The importance of the output of the chosen tool, especially in relation to the capability and knowledge levels of the team that will be required to interpret and act on the results of the assessment.
- The availability of organizations and services to perform vulnerability assessments as an outsourced service.

Conclusion

There are many facets to consider when we look at performing a vulnerability assessment. Some of the areas to consider include why we are performing the assessment, what the desired target is, the depth of scan required, and the amount and depth of output included in the results.

Review Questions

Answer all of the questions below to review your understanding. Try to answer them in your own words.

? After conducting a full vulnerability assessment, what are the next steps a cybersecurity team should take based on the findings?

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

? How does the choice between authenticated and unauthenticated scanning impact the results of a vulnerability assessment?

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

✓ Mark Completed

Previous
Vulnerabilities Knowledge Check

Next
Vulnerability Assessment Tools

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

Let us know how we're doing

W05D3

Wed Jul 24

Outline & Notes (1)

Lectures (1)

Work (8)

6 hrs

- Case Study: Class Network Vulnerabilities
- Peer Review: Class Network Vulnerabilities
- Vulnerabilities Knowledge Check
- Vulnerability Assessments and Tools
- Vulnerability Assessment Tools
- What is OpenVAS?
- Accessing OpenVAS
- Using OpenVAS/GVM

W05D3 Schedule »