Tryhackme: Vulnerability Management

Daniel Schwarzentraub · Follow
4 min read · Sep 26, 2023

Task 1: Introduction

As per NIST, a vulnerability is defined as "*A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source*". In this room, we will learn the process of effectively identifying, detecting, mitigating, and reporting a vulnerability in a system in line with standard frameworks. The room entails a practical example through an open-source tool that will help us understand various vulnerability management lifecycle processes.

Learning Objectives

- Vulnerability management vs vulnerability scanning
- How are vulnerabilities classified?
- Processes of vulnerability management lifecycle
- How can we use a vulnerability management framework in cybersecurity?

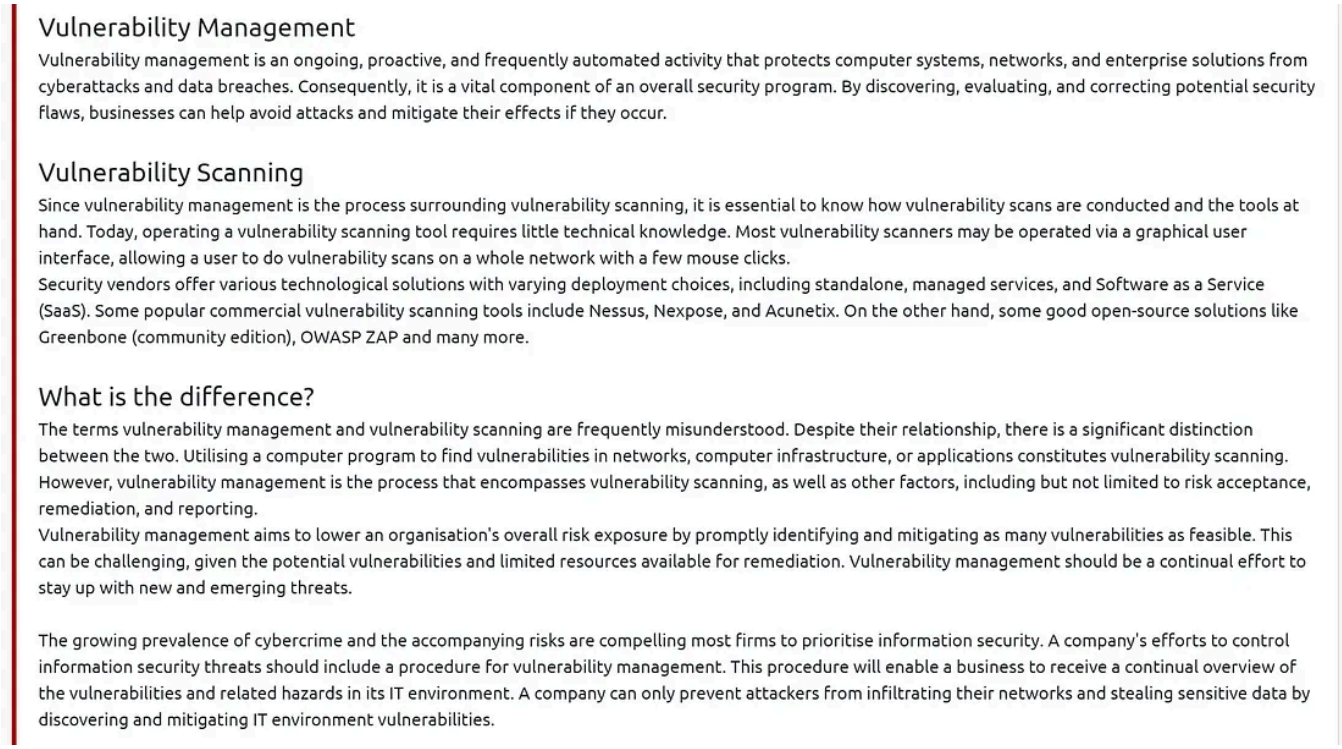
Prerequisites

An understanding of the following topics is recommended before starting the room:

- Security principles
- Understanding vulnerability databases
- How to exploit vulnerabilities

Let's begin!

Task 2: Vulnerability Management vs Vulnerability Scanning



Vulnerability Management

Vulnerability management is an ongoing, proactive, and frequently automated activity that protects computer systems, networks, and enterprise solutions from cyberattacks and data breaches. Consequently, it is a vital component of an overall security program. By discovering, evaluating, and correcting potential security flaws, businesses can help avoid attacks and mitigate their effects if they occur.

Vulnerability Scanning

Since vulnerability management is the process surrounding vulnerability scanning, it is essential to know how vulnerability scans are conducted and the tools at hand. Today, operating a vulnerability scanning tool requires little technical knowledge. Most vulnerability scanners may be operated via a graphical user interface, allowing a user to do vulnerability scans on a whole network with a few mouse clicks.
Security vendors offer various technological solutions with varying deployment choices, including standalone, managed services, and Software as a Service (SaaS). Some popular commercial vulnerability scanning tools include Nessus, Nexpose, and Acunetix. On the other hand, some good open-source solutions like Greenbone (community edition), OWASP ZAP and many more.

What is the difference?

The terms vulnerability management and vulnerability scanning are frequently misunderstood. Despite their relationship, there is a significant distinction between the two. Utilising a computer program to find vulnerabilities in networks, computer infrastructure, or applications constitutes vulnerability scanning. However, vulnerability management is the process that encompasses vulnerability scanning, as well as other factors, including but not limited to risk acceptance, remediation, and reporting.
Vulnerability management aims to lower an organisation's overall risk exposure by promptly identifying and mitigating as many vulnerabilities as feasible. This can be challenging, given the potential vulnerabilities and limited resources available for remediation. Vulnerability management should be a continual effort to stay up with new and emerging threats.

The growing prevalence of cybercrime and the accompanying risks are compelling most firms to prioritise information security. A company's efforts to control information security threats should include a procedure for vulnerability management. This procedure will enable a business to receive a continual overview of the vulnerabilities and related hazards in its IT environment. A company can only prevent attackers from infiltrating their networks and stealing sensitive data by discovering and mitigating IT environment vulnerabilities.

The process encompassing vulnerability scanning and other factors, such as risk acceptance, is called?

Answer: **Vulnerability Management**

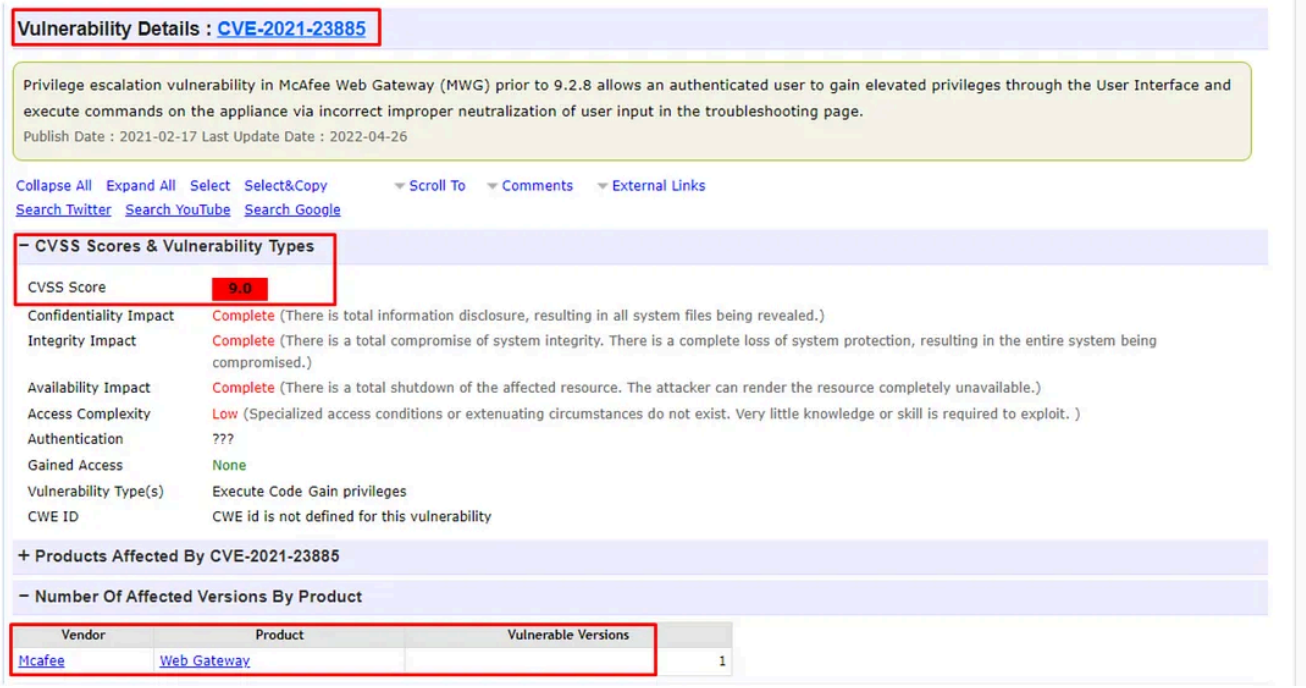
Is the overall objective of vulnerability management to increase an organisation’s risk exposure? (yea/nay)

Answer: **Nay**

Task 3: **Vulnerability Classification**

While security vendors often prefer to develop their own vulnerability specifications, vulnerability management is generally viewed as an open, standards-based approach employing the National Institute of Standards and Technology's (NIST) Security Content Automation Protocol (SCAP) standard. The primary components of SCAP are as follows:

- **Common Vulnerabilities and Exposures (CVE):** MITRE maintains the CVE list of publicly documented vulnerabilities and exposures. Each of the CVEs identifies a vulnerability that may be exploited to launch an attack. With a unique identifier, a description, and at least one public reference, CVE seeks to standardise the identification of security vulnerabilities. Anyone can access the CVE system at no cost, making it a valuable resource for security management professionals and organizations. CVE Details is also a renowned website for searching CVEs and their impact.



Vulnerability Details : CVE-2021-23885

Privilege escalation vulnerability in McAfee Web Gateway (MWG) prior to 9.2.8 allows an authenticated user to gain elevated privileges through the User Interface and execute commands on the appliance via incorrect improper neutralization of user input in the troubleshooting page.
Publish Date : 2021-02-17 Last Update Date : 2022-04-26

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

− CVSS Scores & Vulnerability Types

CVSS Score	9.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	???
Gained Access	None
Vulnerability Type(s)	Execute Code Gain privileges
CWE ID	CWE id is not defined for this vulnerability

+ Products Affected By CVE-2021-23885

− Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions	
Mcafee	Web Gateway		1

For example, CVE-2021-23885 illustrates a CVE identifier consisting of the CVE prefix, the year the CVE ID was given, and the sequence number. Furthermore, the CVE description includes the affected product name, the affected versions, the product manufacturer, the vulnerability's nature, the overall impact, the access an attacker would need to exploit the vulnerability, and the crucial code inputs required.

- **Common Configuration Enumeration (CCE):** A CCE gives system configuration issues unique identifiers to quickly and accurately link configuration data from different information sources and tools. For instance, CCE identifiers can be used to match up configuration assessment tool results with recommended best practices. This is comparable to the CVE list, which gives publicly reported system vulnerability IDs.
- **Common Platform Enumeration (CPE):** CPE is a method for classifying and identifying devices, operating systems (OS), and application types inside an infrastructure. CPE is widely used in security and vulnerability management tools to identify various assets and to take accurate automated decisions through correlation with CVE and CCE.
- **Common Vulnerability Scoring System (CVSS):** CVSS is a scoring system that rates the severity of vulnerabilities and identifies their characteristics. It assigns severity scores to all defined vulnerabilities, which is used to prioritise mitigation efforts and the required resources based on the severity. The range of possible scores is 0 to 10, with 10 representing the most severe.

CVSS(3) Score	Severity Rating
0	None
0.1 to 3.9	Low
4.0 to 6.9	Medium
7.0 to 8.9	High
9.0 to 10	Critical

There are numerous public sites with information on vulnerabilities; however, the National Vulnerability Database (NVD) administered by NIST is a comprehensive database of CVE-assigned known vulnerabilities. Although NVD and CVE are frequently used interchangeably, they differ in many ways. CVE is just a list of all the entries for known vulnerabilities. Nevertheless, NVD is a more comprehensive database based on and fully synchronised with the CVE list, guaranteeing that any updates to the CVE list are represented in NVD. Besides the analysis of CVEs, the NVD also allocates a CVSS score to each vulnerability.

What is the CVSS for CVE-2013–1048?

Base Score	Base Severity	CVSS Vector	Exploitability Score	Impact Score	Source
4.6	MEDIUM	AV:L/AC:L/Au:N/C:P/I:P/A:P	3.9	6.4	nvd@nist.gov

Access Vector:	Access Complexity:	Authentication:	Confidentiality Impact:	Integrity Impact:	Availability Impact:
Local	Low	None	Partial	Partial	Partial

Answer: **4.6**

What is the Access Complexity for CVE-2013–1048?

Answer: **low**

With the fictional CVE-2023–2022, what would the CVE ID assign year be?

Answer: **2023**

Task 4: **Vulnerability Management Life Cycle — Discover & Prioritise**

There are six essential phases in the vulnerability management lifecycle that can be mapped out from the NIST Cybersecurity Framework; each includes its sub-processes and activities. These stages can be used by organisations wishing to develop or enhance their vulnerability management program. To showcase the execution process for vulnerability management, let's examine a real-world situation.

Start Machine

Connecting to the Machine

We will use Ubuntu as a test machine and Greenbone Community Edition (GCE) throughout the room. You can start the virtual machine by clicking `Start Machine`. The machine takes about 4 minutes to boot; additionally, please wait 1 - 2 minutes for OpenVAS to be configured in the background.

First, we will see a case study and then we will practically test an Ubuntu machine. In the case study, we will be scanning a Windows machine hosting a web application using `XAMPP`; however, for the exercise part, we will be going through the scan report of an Ubuntu machine. Since this study aims to implement a vulnerability management system, the basic commands and the installation process are exempted. You can learn more about its installation in this room.

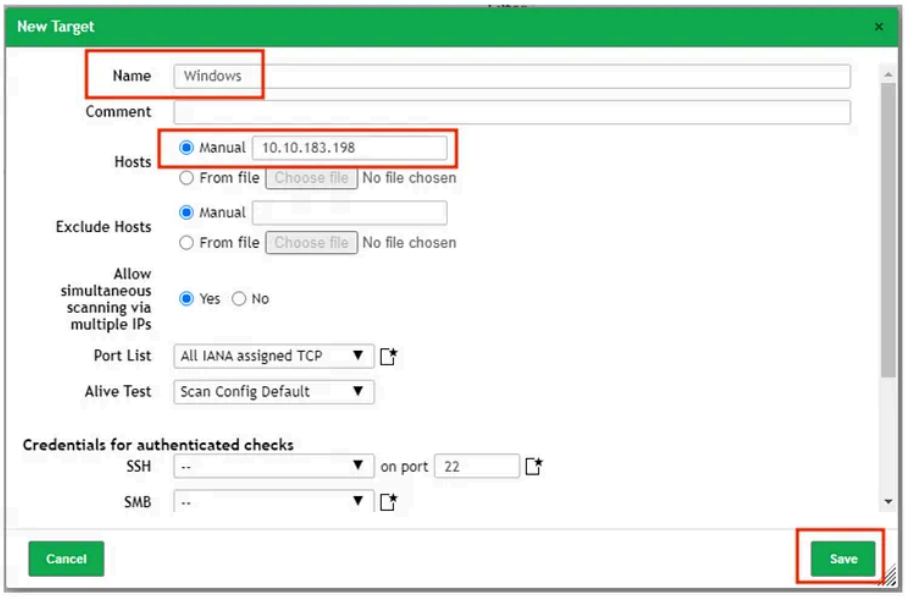
Using a practical example, let's dig deeper into various phases of vulnerability management. Open the web panel for the GCE by visiting the URL `http://MACHINE_IP:9392`. The default credentials for the platform are `admin:admin`. Ignore the unencrypted connection message on the screen, as this is for demonstration purposes only.

Step 1: Discover

The first step is to compile a list of all the environment's resources/assets, including the applications, services, operating systems, and configurations, to identify vulnerabilities. Typically, this combines both a network scan and a system scan and enables you against any potential threat to the organisation's information and critical infrastructure. For this purpose, organisation-wide scanning should be planned and conducted regularly.

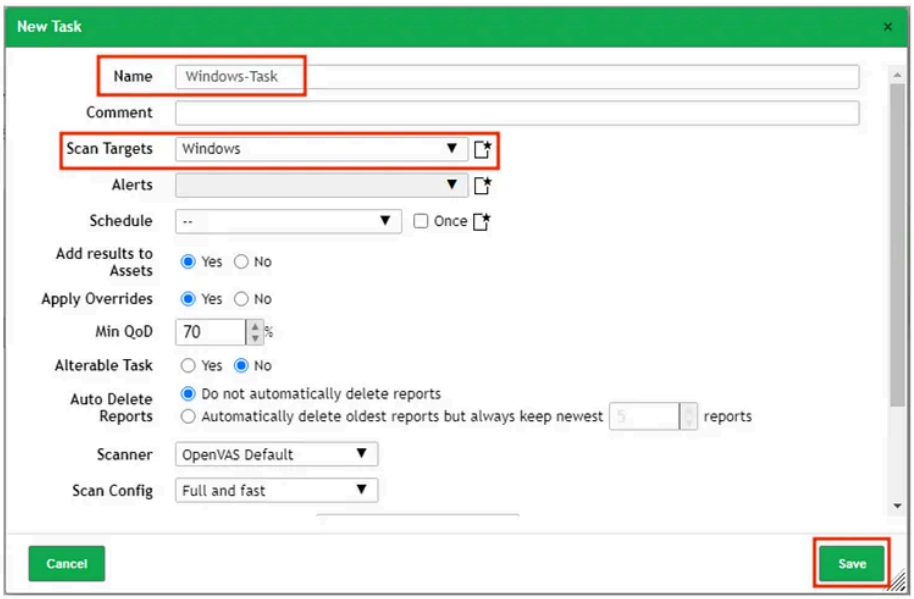
Consider we are working as a Security Engineer in a cybersecurity company and have been tasked to perform vulnerability management of the company's assets. We can perform the discovery using the following steps in GCE:

Add Target: Once logged in to GCE, open the **Configuration** menu, and click on **Targets**. Once the page is opened, click the **page with a star** icon on the left side to add a new target. In the example, we will add the IP address **10.10.183.198**, which belongs to a Windows-based machine. We can scan all the subnets and networks of the company; however, for the sake of this task, we added only a single IP, as shown below:



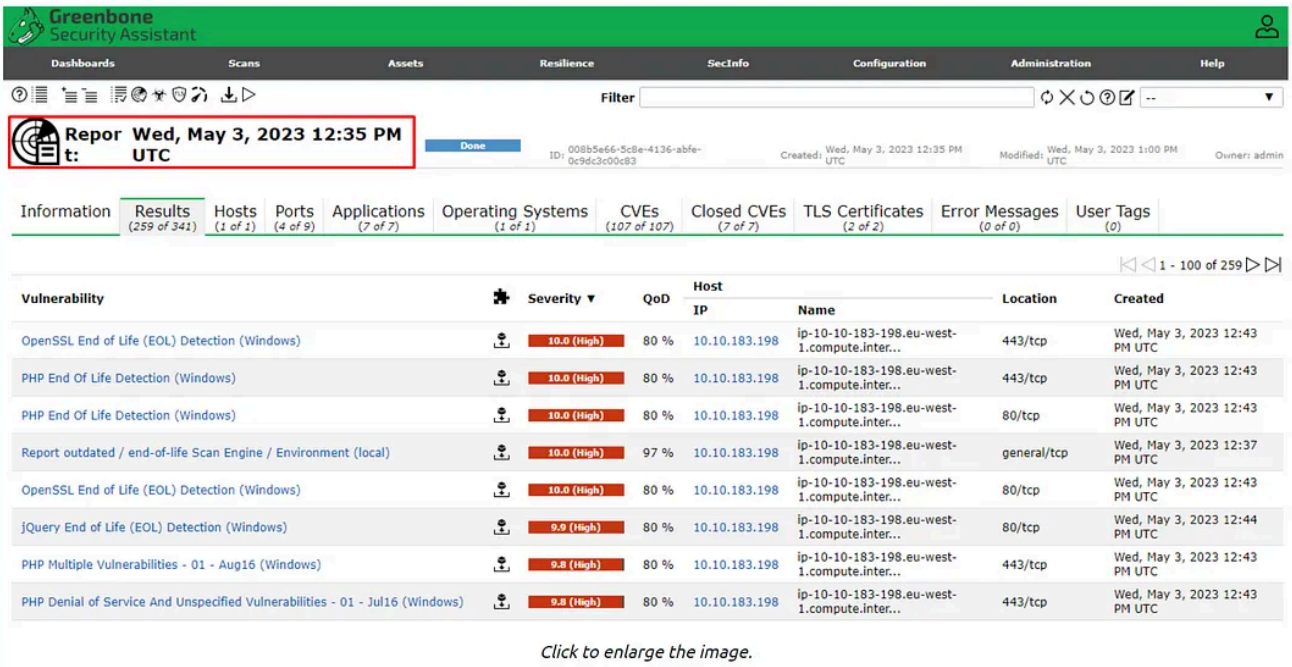
Click to enlarge the image.

Add Task: Next, open the **Scans** menu, and click on **Tasks** to configure the tool to scan all the assets running on the specified target (**10.10.183.198**). Once the page is opened, click the **page with a star** icon on the left side to add a new task, as shown below. We can run the task by clicking the **start** button next to the respective task.



Click to enlarge the image.

We have initiated the scanning process to discover all the assets and vulnerabilities of the target. The status of all the scan tasks is available through the `Scan > Reports` menu of the tool. As soon as the scan is finished, we can click on the corresponding scan from the same page to see all identified assets and vulnerability details. *You can ignore the vulnerabilities related to GCE.*



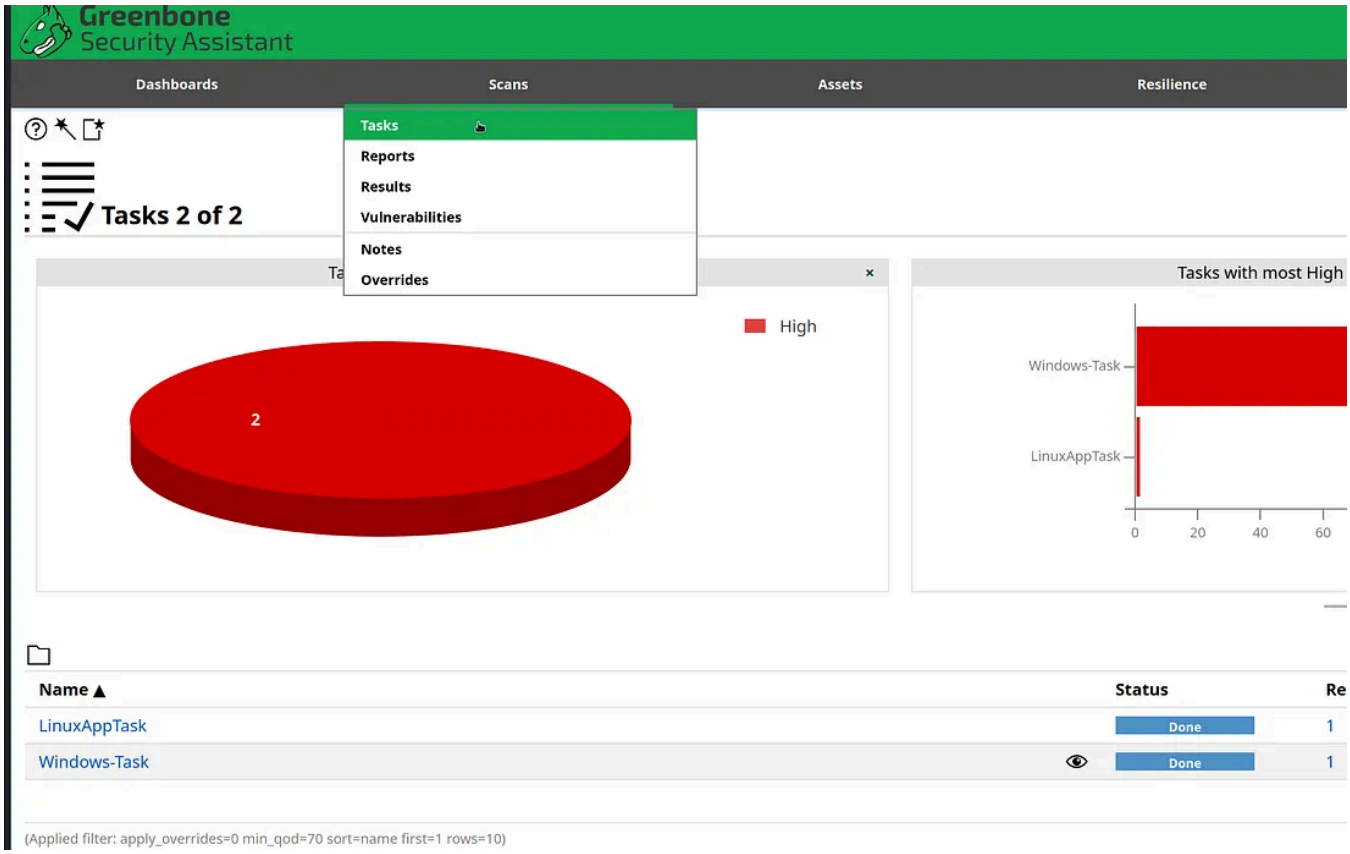
Click to enlarge the image.

Step 2: Prioritise

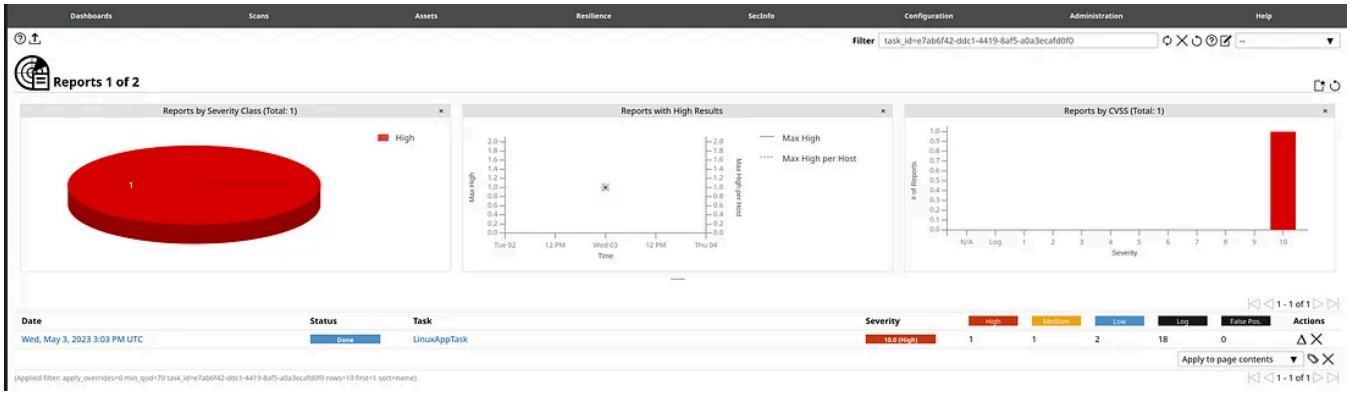
The second step involves grouping and assigning a risk-based priority to the assets (identified during the discovery phase) based on how crucial they are to the business. This can significantly assist the organisation in determining which groups require special attention and thus will aid in the decision-making process when distributing resources.

Once the results are identified, we will prioritise the identified vulnerabilities in different assets based on their operational importance. Asset vulnerabilities leading to data breaches and DB access are rated as **Top** risk priority since the breach of sensitive organisation records would damage the organisation's reputation and may also have legal or regulatory consequences.

The THM Team has already ran a scan, so once logged in, we just need to access the Linux App Task

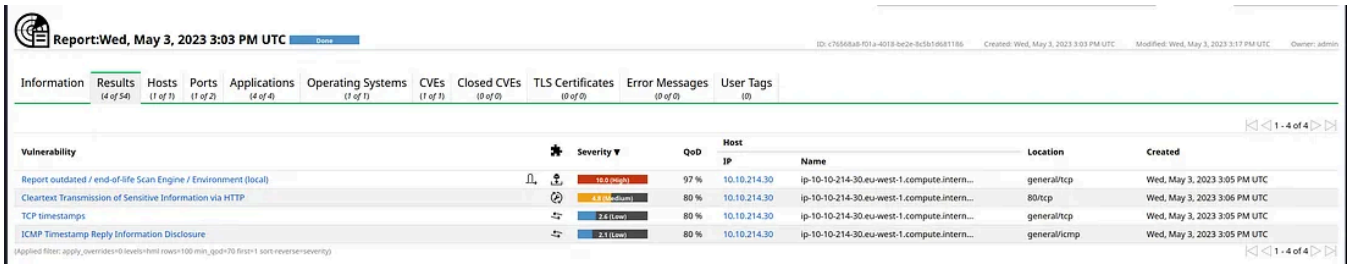


After scanning, what is the total number of medium-level vulnerabilities?



Answer: **1**

What is the severity score for the vulnerability “**ICMP Timestamp Reply Information Disclosure**”?



Answer: **2.1**

What is the operating system and the version number of the target machine?

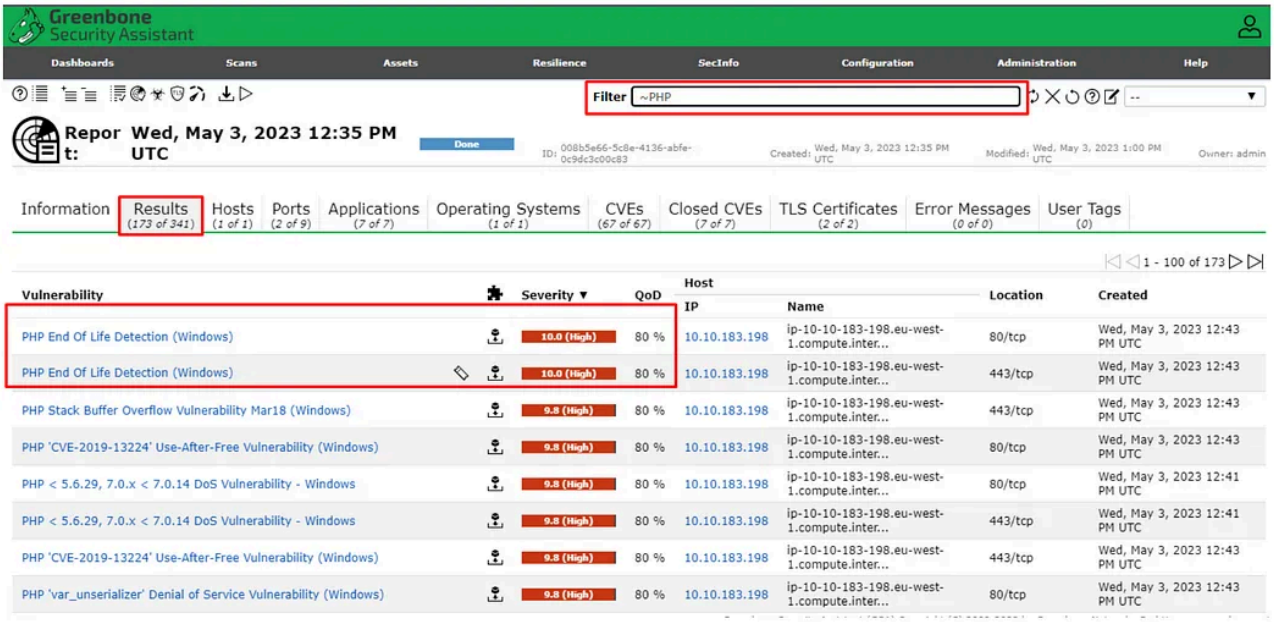
Answer: **Ubuntu 20.04**

Task 5: **Vulnerability Management Life Cycle — Assess & Report**

Step 3: Assess

The third phase involves creating a risk baseline by evaluating your assets to determine how severe each is. The process lets organisations decide which risks to eliminate based on factors such as their classification, criticality level, and vulnerability level. In the longer run, assessments help organisations establish a consistent baseline.

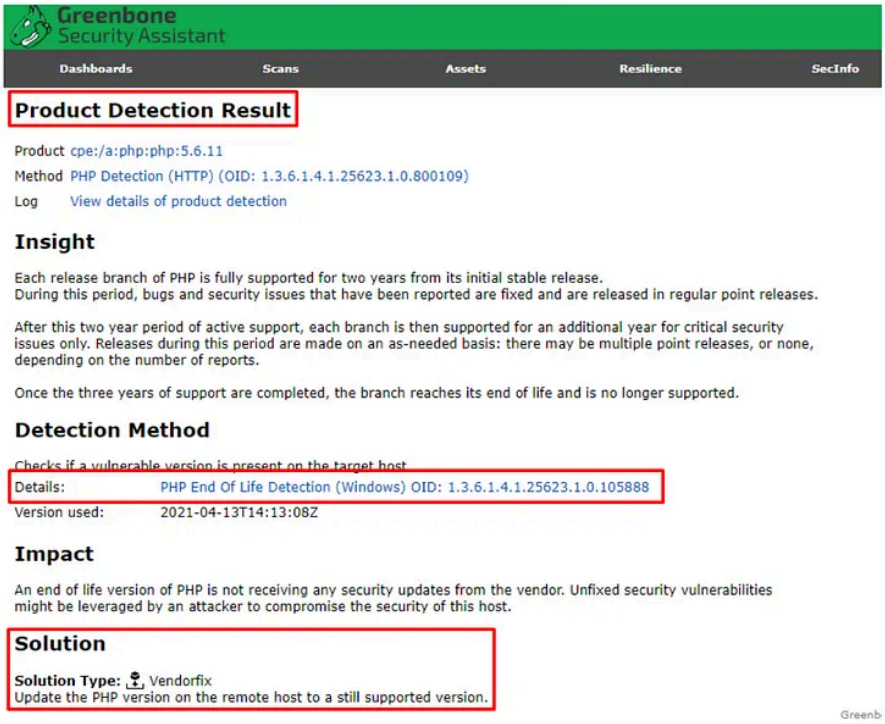
For this purpose, we looked at the **Top** risk-rated assets and noticed that most of them are associated with `PHP` (a server-side scripting language); therefore, we decided to look into the vulnerabilities of this asset first. A list of identified vulnerabilities filtered with `PHP` is shown below. It can be seen that a total of **173 vulnerabilities** are associated with this asset by the GVM OpenVAS scanner. Most of them are rated as **High** severity, whereas others were rated as **Medium** severity. Only two of the vulnerabilities associated with `PHP` are rated as **Low** severity.



Step 4: Reporting

The next step is to use the assessment results to determine the risk levels associated with each vulnerability. **Documenting and reporting** known vulnerabilities is crucial. It makes it easier for security engineers to monitor vulnerability dynamics throughout their networks and guarantees that businesses continue to adhere to all applicable security requirements and regulations.

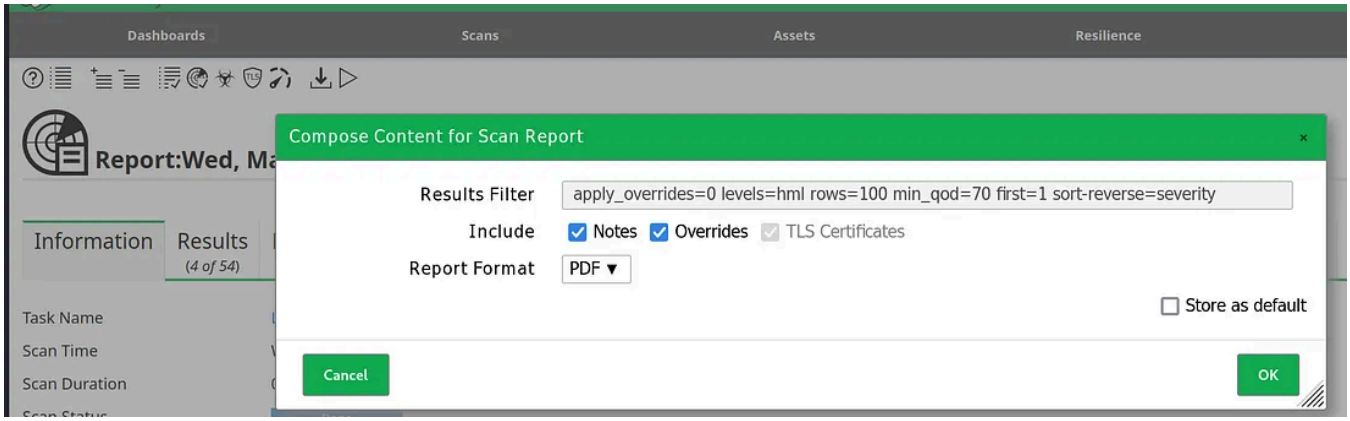
For this purpose, we inspected the top **High** severity vulnerability with a CVSS score of 10.0. We can do this by clicking on the corresponding vulnerability from the GUI to get more details about the vulnerability and the possible impact. The following image shows that the GVM has provided information on the vulnerability and **suggested remedial measures to fix it**. Similarly, we inspected the "Buffer Overflow vulnerability" and several other critical vulnerabilities associated with PHP in the scan results and found that all of them can be fixed by upgrading the PHP to its latest version.



Click to enlarge the image.

Before reporting a vulnerability for remediation, it is highly advised to confirm that it is not a false positive since vulnerability scanners are prone to such errors. While some vulnerabilities might be straightforward to confirm, such as those identified with default credentials that could be easily verified remotely, others might require some effort remotely or from the client end. In any case, when a vulnerability is identified as a false positive, it is recommended to flag it in the report in the tool for future reference.

Download the **LinuxAppTask** report in PDF format. What is the severity rating of the vulnerability in the report, where the solution type is "**Workaround**"?



2.1.2 Medium 80/tcp

Medium (CVSS: 4.8) NVT: Cleartext Transmission of Sensitive Information via HTTP
Summary The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result
`The following input fields where identified (URL:input name):`
`http://ip-10-10-214-30.eu-west-1.compute.internal/phpmyadmin/:pma_password`
`http://ip-10-10-214-30.eu-west-1.compute.internal/phpmyadmin/?D=A:pma_password`

Impact An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.
Solution: **Solution type:** Workaround Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.
Affected Software/OS Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Answer: **Medium**

What is the solution type for the "**TCP timestamps**" vulnerability?

Low (CVSS: 2.6)
NVT: TCP timestamps

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result
```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 535979669
Packet 2: 535980749
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled' Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Answer: **Mitigation**

What is the CVE for "**ICMP Timestamp Reply Information Disclosure**"?

Low (CVSS: 2.1)
NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generators in other services.

Vulnerability Detection Method
Details: `ICMP Timestamp Reply Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: `2022-11-18T10:11:40Z`

References
`cve: CVE-1999-0524`
`url: http://www.ietf.org/rfc/rfc0792.txt`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`
`dfn-cert: DFN-CERT-2014-0658`

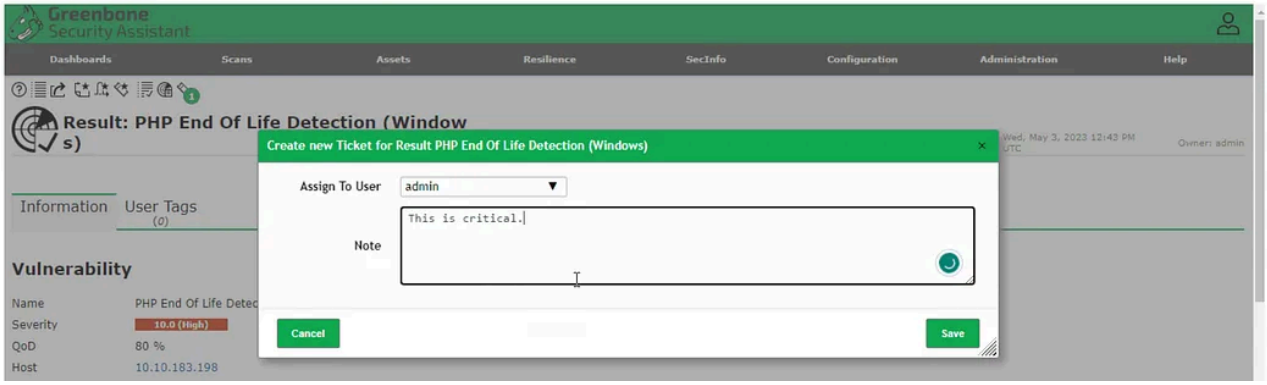
Answer: **CVE-1999–0524**

Task 6: **Vulnerability Management Life Cycle — Remediate & Verify**

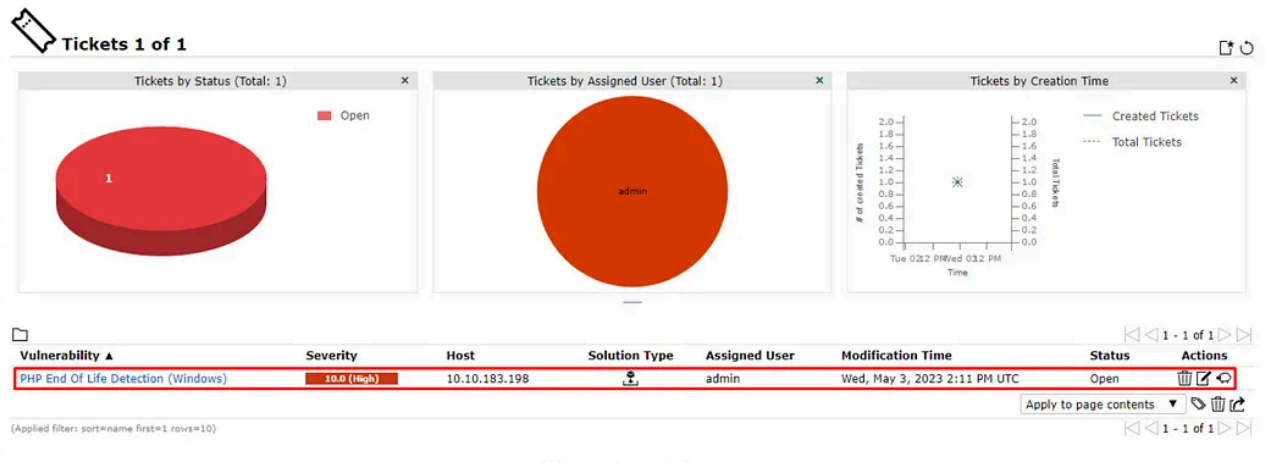
Step 5: Remediation

This phase involves fixing the vulnerabilities discovered earlier, beginning with the most severe ones. The identified vulnerabilities should be reported to the concerned stakeholders for remediation. A few approaches are available to organisations for dealing with known vulnerabilities and configuration errors. **Remedial action, such as thoroughly addressing or patching vulnerabilities, is the best course of action**. If complete remediation is not feasible, businesses might mitigate, which entails lowering the risk of exploitation or minimising the potential harm. Finally, security engineers can acknowledge their vulnerability, for instance, when the risk involved is low, and choose to do nothing.

Now that we are aware of the most critical vulnerabilities in the organisation, it is time to report them to the stakeholders for remediation. For this purpose, we will create a ticket for the `PHP` vulnerability and assign it to the responsible team. Tickets in the GVM can be created from the `Detail View` GUI of the corresponding vulnerability, as shown below.



The responsible team received the ticket and will resolve the issue by upgrading `PHP` to the latest version. Once they resolved it, they will change the status to **Fixed**. The remediation ticket's status can be tracked from the `Resilience > Remediation Tickets` menu, as shown below.



Click to enlarge the image.

Step 6: Verification & Monitoring

In the last step of vulnerability management, regular audits and process monitoring are used to guarantee that all threats have been eradicated. For this purpose, we will rescan the target after applying the fix. If the results are satisfactory, we will close the remediation ticket.

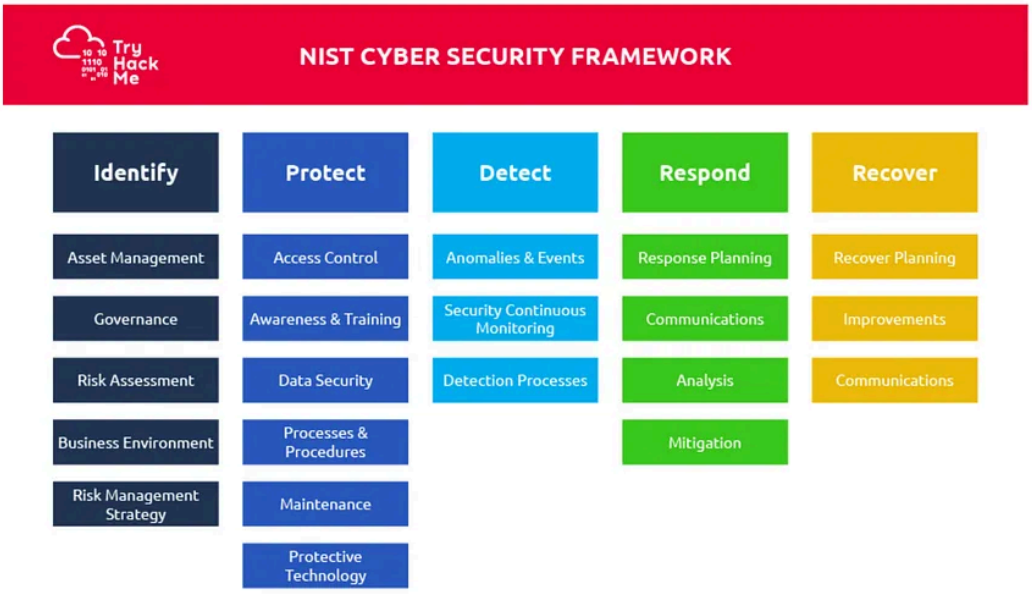
As a Security Engineer, the priority of a remediation ticket for a critical vulnerability must be (high/medium/low)?

Answer: **high**

Task 7: **Vulnerability Management Framework**

This task will briefly discuss a renowned framework used worldwide for vulnerability management. The National Institute of Standards and Technology (NIST) created the Cybersecurity Framework (CSF) as a guidance for organisations to better manage and reduce their cybersecurity risks. The NIST Cybersecurity Framework is intended as a comprehensive cyber strategy and has become a helpful risk management resource for corporate sector businesses and government entities. The fundamental components of the NIST Cybersecurity Framework are broken down into five areas applicable to vulnerability management that help to achieve the cybersecurity objectives of an organisation.

- **Identify**: What assets and processes require security?
- **Protect:** Put the right security measures in place to protect the organisation's assets.
- **Detect:** Implement adequate procedures to detect cybersecurity events.
- **Respond**: Develop methods for mitigating the effects of cybersecurity incidents.
- **Recover**: Implement the proper procedures for restoring capabilities and services impacted by cybersecurity incidents.



The NIST CSF comprises guidelines, standards, and best practices for managing cybersecurity risk. In recent years, it gained immense popularity, and many organisations now employ the CSF to govern their cybersecurity state. Even though the NIST CSF has a broader range of applications, let's examine how to exploit its fundamental elements for vulnerability management.

Identify

The framework's first and foremost objective is to provide a solid basis for a cybersecurity program. This stage addresses the query, "**What assets require protection?**" in the context of vulnerability management. This phase may involve the following steps:

- **Develop asset discovery methodologies**: You cannot safeguard what you do not know. Implement the required tools and procedures to achieve complete insight over enterprise assets, including those on-premises and cloud assets.
- **Discover assets in real-time:** The process of discovering assets should be automated to get a near real-time picture of all the assets within the organisation.
- **Ascertain the criticality of assets:** Adding security and business relevance to the assets would assist you in prioritising their significance to your business. It's crucial to analyse as much data as possible. Unfortunately, most companies use a subjective method to estimate the importance of their assets to the business. They tend to make cybersecurity decisions based on intuition rather than data, which yields poor results.

Protect

This phase encompasses limiting or reducing the effects of a potential cyber incident and deploying the appropriate safeguards to secure the provision of IT infrastructure services. For vulnerability management, this phase addresses the query, "**Have you adopted the necessary measures to secure the assets of your organisation?**" This phase may involve the following steps:

- **Deploy security safeguards**: Make use of security systems and technology, and follow best practices, including proactive security (email security, network security, ransomware and anti-malware protection), preventative security (encryption, regular backups) and Information Security Management Systems (ISMS) (patch management solutions, Identity Access Management (IAM), Security Information and Event Management (SIEM), and Data Loss Prevention (DLP)).
- Deploy vulnerability management software.

Detect

This phase outlines the operations performed to promptly recognise a cybersecurity incident's presence. To vulnerability management, this stage addresses the query, "**Have you put in place suitable measures to discover security vulnerabilities?**" This phase may involve the following steps:

- **Detect vulnerabilities**: After you have mapped the attack surface, you must implement tools and methods to detect vulnerabilities and shortcomings in the IT infrastructure. Discovering vulnerabilities is a crucial part of a program for managing vulnerabilities.
- **Prioritise vulnerabilities**: Since every enterprise has a large number of vulnerabilities, it is essential to prioritise vulnerabilities for remediation, ensuring that the responsible team takes adequate measures to fix vulnerabilities based on their priority.
- **Quantify risks:** Once vulnerabilities are prioritised, the associated risks can be quantified by assigning a score to each vulnerability, which can be customised based on the organisation's mission. Estimating cyber risk in quantified terms gives a consistent vocabulary for prioritising initiatives and tracking the efficacy of the overall cybersecurity program.
- **Monitor constantly**: Implement tools for continuous monitoring to detect newly found vulnerabilities, new assets, and other changes in your environment.

Respond

This stage emphasises the steps required once a cybersecurity vulnerability has been identified. This process addresses the query: "**Have you implemented the necessary techniques and mechanisms to mitigate the vulnerability's impact?**" This phase may involve the following steps:

- **Define ownership**: It is essential to determine who is responsible for addressing each vulnerability. Clarity regarding ownership warrants accountability and encourages action.
- **Establish reporting**: Reports present relevant stakeholders with the extent of vulnerabilities that have been identified. Creating risk-owner-specific reports enables progress comparisons. Leaderboards, warnings, and reminders can be utilised to encourage the concerned team member to fulfil their responsibilities for the assigned duties.
- **Share status regularly**: Provide stakeholders with timely updates on the remedial queue. A further part of status sharing is the ability to provide reports that demonstrate progress on risk mitigation and the commercial value the security program is bringing.
- **Adopt a risk acceptance approach:** Swiftly eliminating all discovered vulnerabilities is impossible. There could be circumstances where business-critical assets must be taken offline to address a vulnerability. One should establish a strategy for risk acceptance based on risk threshold and business requirements.
- **Establish remedial measures**: During normal operations, security teams should concentrate on eradicating large quantities of critical vulnerabilities and eliminating security holes swiftly and effectively. However, when adversaries actively exploit a newly discovered critical vulnerability, the security team should focus on finding and releasing patches or swift mitigations to address these severe vulnerabilities.

Recover

This is the final step of the NIST CSF. This phase entails updating and strengthening resilience plans and restoring any compromised capabilities or services caused by a cybersecurity event. For vulnerability management, it addresses the query, "**Have you implemented the processes and technologies necessary for detecting and resolving future vulnerabilities?**" This phase may involve the following steps:

- **Implement sophisticated search capabilities**: Having the power to look for affected assets is one of the preventive measures required for vulnerability management remediation. In the detect stage, you must be able to quickly and precisely identify all compromised assets. Similarly, you should be able to confirm that vulnerability occurrences have been addressed during the Recover phase.
- **Extend security to unmanaged areas:** The expanding use of cloud infrastructure fuels the explosion of attack surfaces within organisations. In the recovery stage, it may be required to increase insight across conventional assets (e.g. laptops, desktops) and assets not currently covered by your solutions (e.g. IoT devices, cloud assets). A Cyber Asset Attack Surface Management (CAASM) solution can fill this void and offer your organisation an accurate and almost real-time picture of its assets.
- **Record lessons**: Revise your procedures to take account of the learnings from security events and improve the current cybersecurity strategy.

The process of listing vulnerabilities as per their order of priority is called?

Answer: **Prioritise vulnerabilities**

Which phase entails updating and strengthening resilience plans and restoring any compromised capabilities or services caused by a cybersecurity event?

Answer: **Recover**

Task 8: **Conclusion**

In this room, we learnt different stages of the **vulnerability management life cycle** and how to protect your assets from vulnerabilities by following a renowned vulnerability management framework. An organization's management is at risk of being unaware of potential security risks associated with its IT infrastructure if it does not have a vulnerability management approach in place.

Implementing a program for vulnerability management is all about risk management. By implementing a well-defined program, a company can gain a continuous perspective of the risk posed by security vulnerabilities in its IT infrastructure. It enables **management to make well-informed decisions regarding the risk-reduction measures** that could be undertaken.

Any organisation that wishes to understand the security threats posed by the technology it employs should implement a vulnerability management program. **Implementing a new vulnerability management approach within an enterprise can be challenging for a security engineer**. Various factors must be considered to ensure the success of a vulnerability management program, like choosing a **vulnerability scanning technique** that meets the organisation's demands or configuring and fine-tuning the vulnerability scanning technology. Finally, it is advised that early vulnerability scans be limited in scope when beginning vulnerability management. This stops initial scans from finding a large number of vulnerabilities. A preferable strategy would be only to **select a small range of vulnerabilities** (such as OWASP Top 10) or just those issues that the vulnerability scanning program identifies as **High** severity .

Stay tuned and keep finding and patching vulnerabilities.

Tryhackme Walkthrough Tryhackme Writeup

Follow

Written by Daniel Schwarzentraub

116 Followers · 4 Following

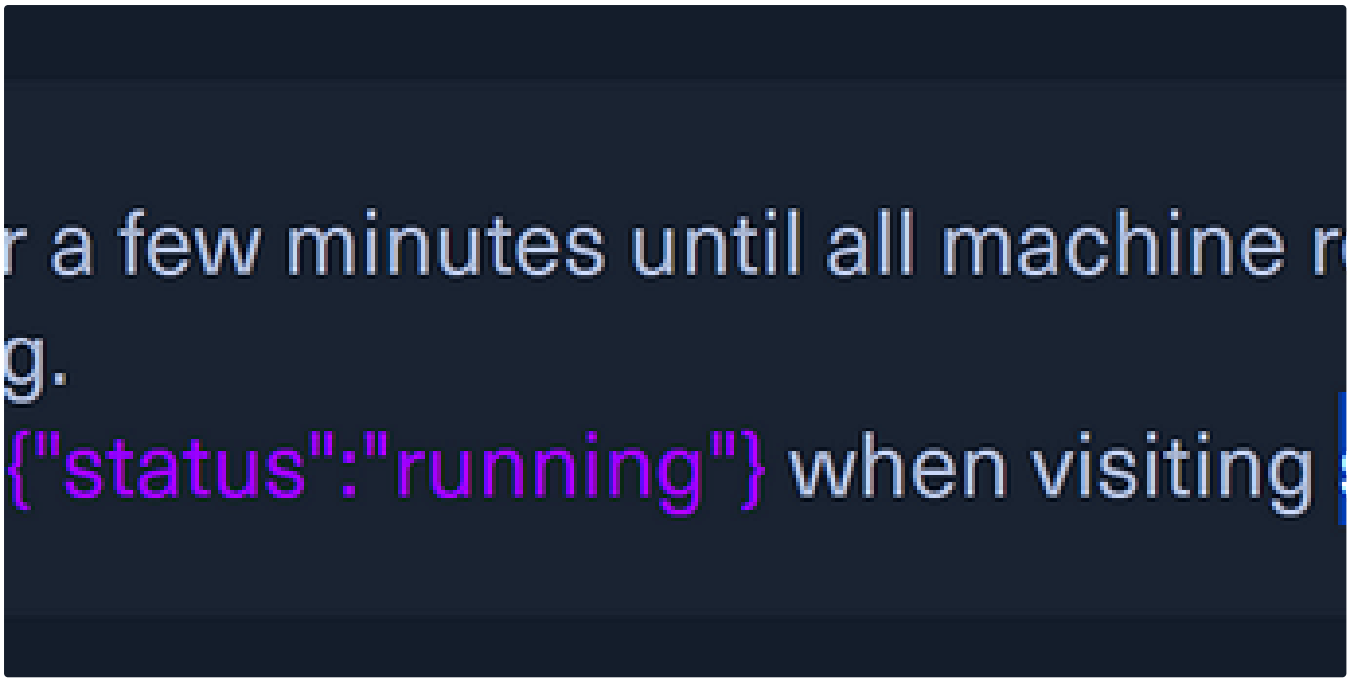
PNW_Hacker

No responses yet

What are your thoughts?

Respond

More from Daniel Schwarzentraub

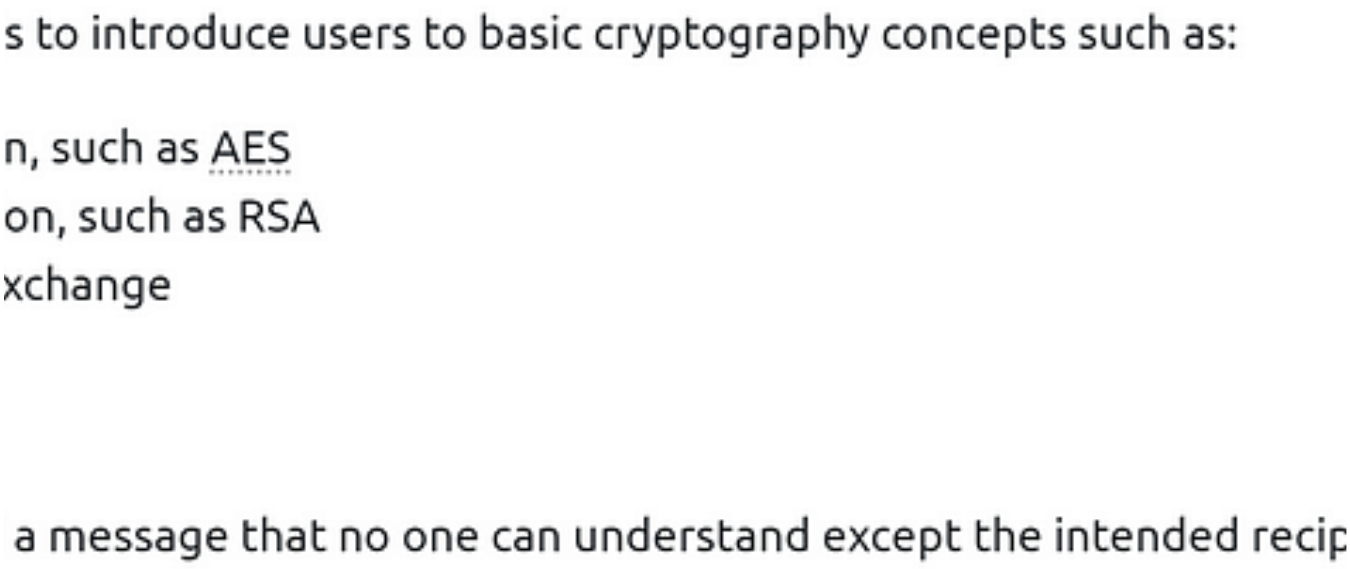


Daniel Schwarzentraub

HTB—Tier 1 Starting Point: Three

HTB—Tier 1 Starting Point: Three

Jul 20, 2023 4 2

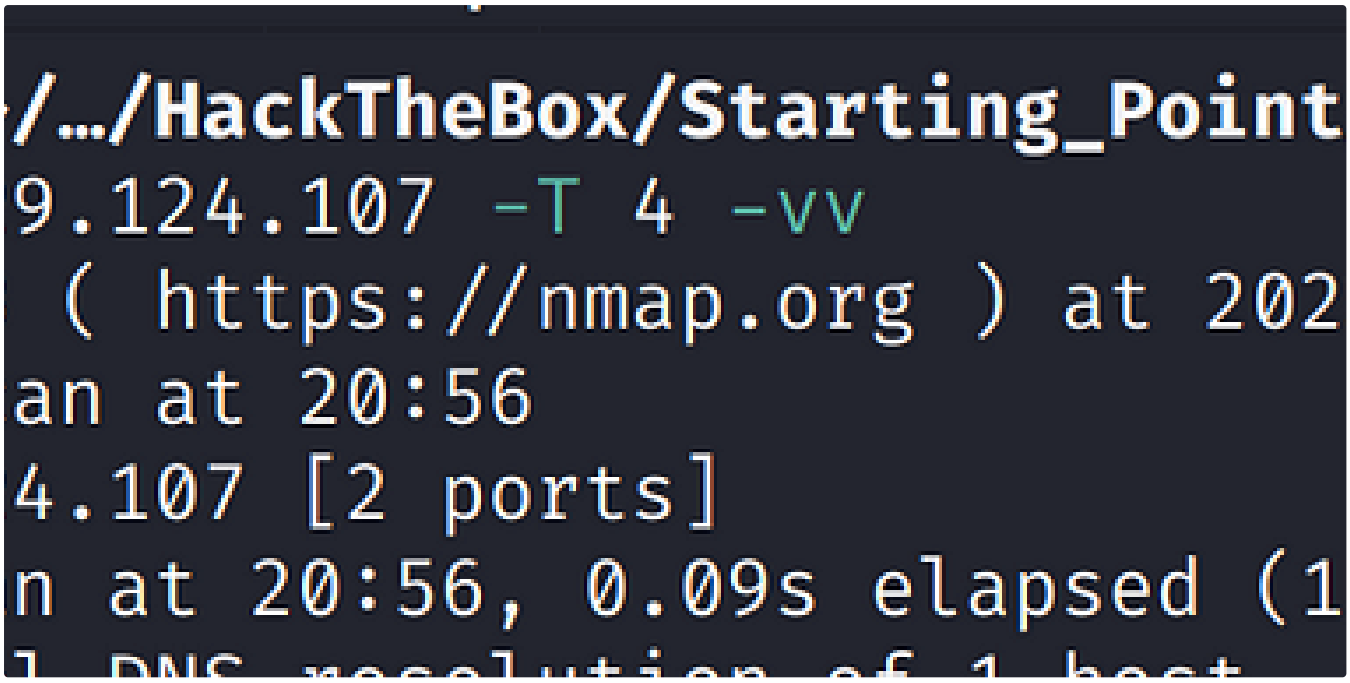


Daniel Schwarzentraub

Tryhackme: Introduction to Cryptography

Tryhackme: Introduction to Cryptography

Sep 26, 2023 2



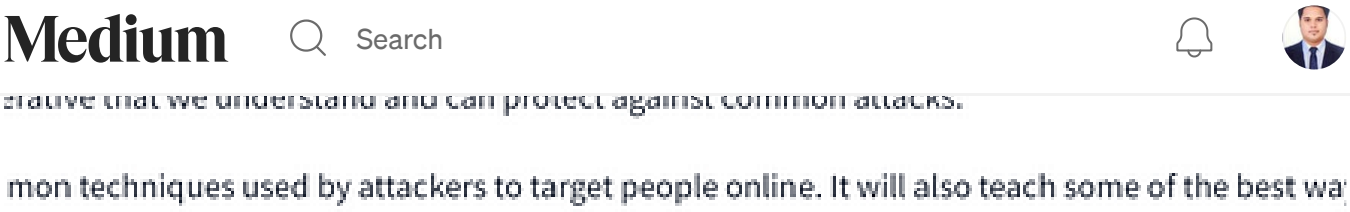
Daniel Schwarzentraub

HTB—Tier 2 Starting Point: Archetype

HTB—Tier 2 Starting Point: Archetype

Open in app ↗

Medium Search



Daniel Schwarzentraub

Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024

See all from Daniel Schwarzentraub

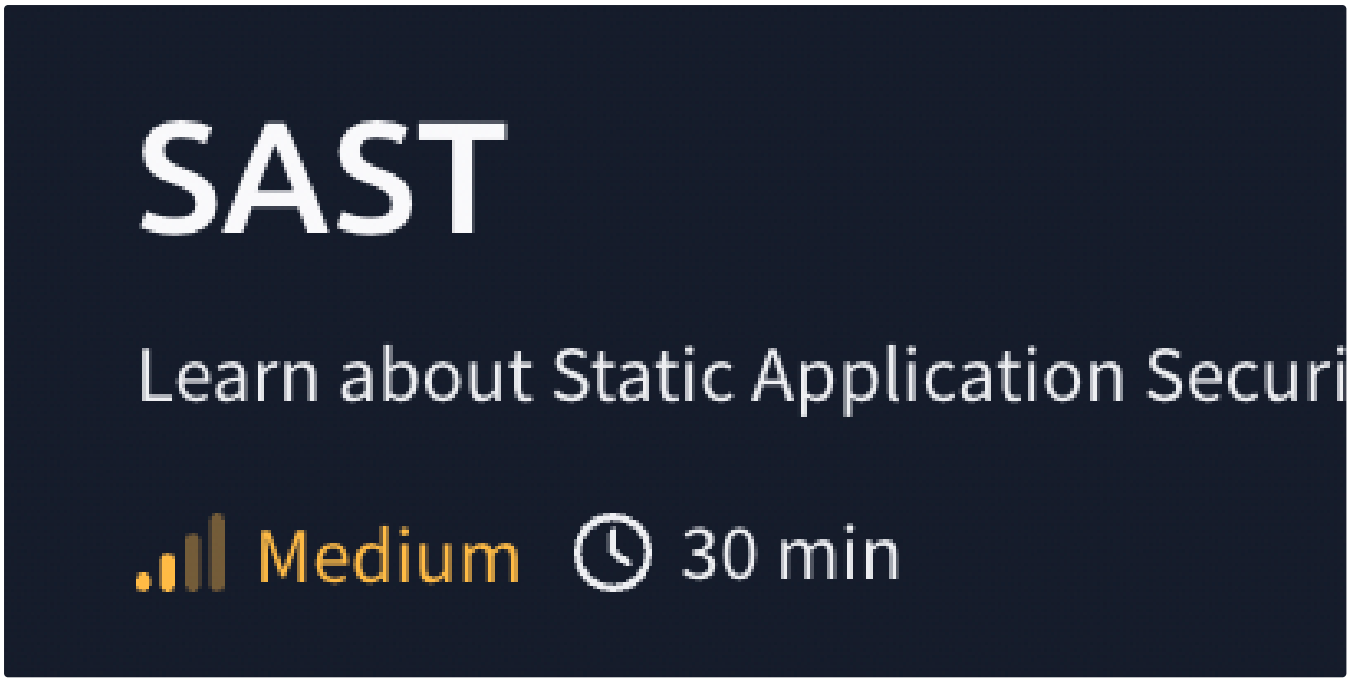
Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60



In OSINT Team by Angie

SAST TryHackMe Writeup | THM Walkthrough

Hello everyone! For today, I will do a TryHackMe walkthrough of the SAST room. I will note that this is a paid room. The SAST room is from...

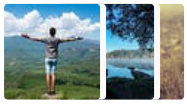
Aug 23, 2024 131

Lists

Staff picks
796 stories · 1560 saves

Stories to Help You Level-Up at Work
19 stories · 912 saves

Self-Improvement 101
20 stories · 3196 saves



Productivity 101
20 stories · 2707 saves

IritT

Nmap—TryHackMe Insights &Walkthrough

An in depth look at scanning with Nmap, a powerful network scanning tool.

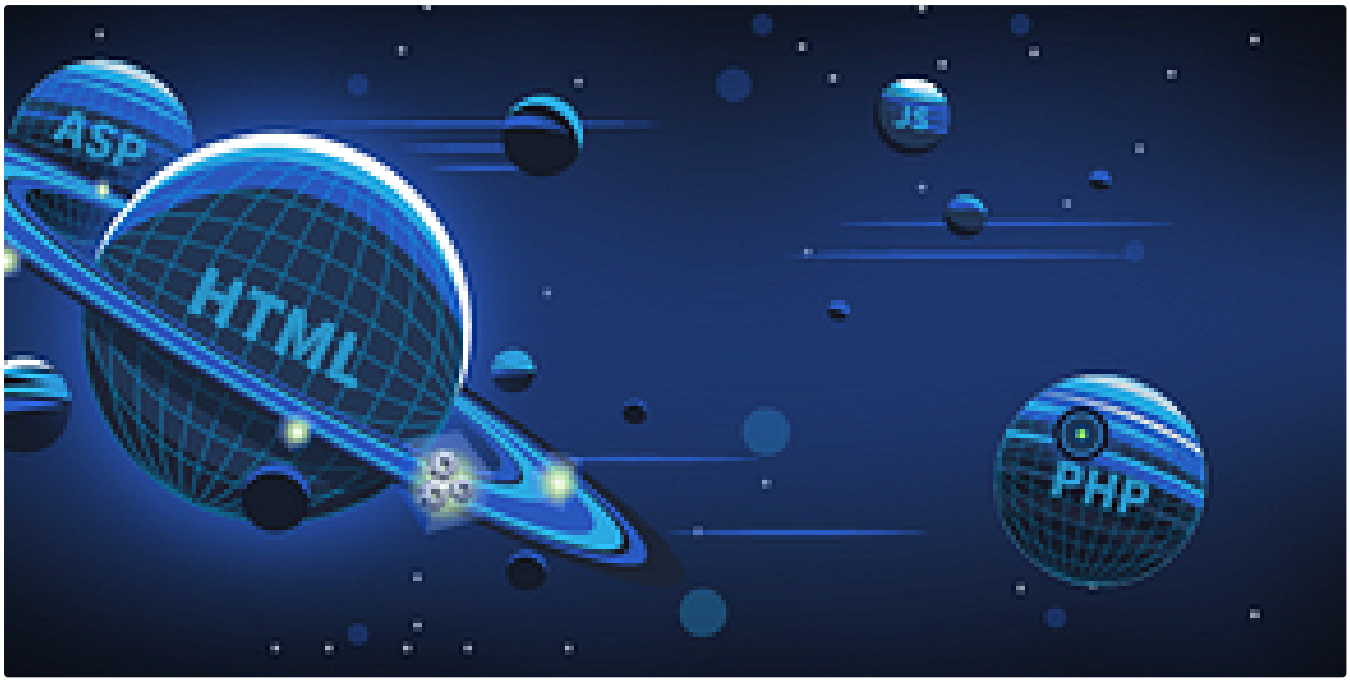
Dec 23, 2024

In T3CH by Axoloth

TryHackMe | Vulnerability Scanner Overview | WriteUp

Learn about vulnerability scanners and how they work in a practical scenario

Nov 23, 2024 50



In T3CH by Axoloth

TryHackMe | Web Application Basics | WriteUp

Learn the basics of web applications: HTTP, URLs, request methods, response codes, and headers

Oct 26, 2024 56

In T3CH by Axoloth

TryHackMe | K8s Runtime Security | WriteUp

Secure a Kubernetes environment using in-house offerings and runtime security tools like Falco.

Sep 15, 2024 50

See more recommendations