

## **Vulnerability Assessment**

### **Introduction**

In the realm of cybersecurity, protecting sensitive information is paramount. One of the critical vulnerabilities is the transmission of sensitive information in cleartext via HTTP. This report delves into the details of this vulnerability, outlines the processes involved in security assessments, and discusses the tools and methods used for vulnerability scoring and reporting, with a focus on Nessus and OpenVAS.

### **Cleartext Transmission of Sensitive Information via HTTP**

### **Understanding the Vulnerability**

The transmission of sensitive information in cleartext via HTTP is a significant security risk. HTTP, unlike HTTPS, does not encrypt the data being transmitted between the client and the server. This lack of encryption means that any sensitive information, such as passwords, personal data, or financial information, can be easily intercepted by malicious actors during transit.

### **Implications**

**Data Interception:** Attackers can use packet sniffing tools to capture sensitive information

**Man-in-the-Middle Attacks:** Without encryption, attackers can insert themselves between the client and server to intercept or alter the data being transmitted.

**Compliance Issues:** Many regulations and standards, such as GDPR and PCI-DSS, mandate the protection of sensitive information during transmission. Failure to encrypt data can lead to non-compliance and severe penalties.

## Security Assessments

### The Importance of Security Assessments

Security assessments are crucial in identifying and mitigating vulnerabilities within an organization's IT infrastructure. These assessments help in understanding the security posture of the systems and in taking proactive measures to secure sensitive information.

### Steps Involved in Security Assessments

1. **Planning and Scoping:** Define the scope of the assessment, including the systems and networks to be tested, and set clear objectives.
2. **Information Gathering:** Collect data about the target systems, including network configurations, software versions, and existing security measures.
3. **Vulnerability Detection:** Use automated tools and manual techniques to identify potential vulnerabilities.
4. **Exploitation (Optional):** Attempt to exploit identified vulnerabilities to understand their potential impact (often part of penetration testing).
5. **Analysis and Reporting:** Analyze the findings, assess the risk associated with each vulnerability, and compile a comprehensive report with recommendations for remediation.

## Vulnerability Scoring and Reporting

### Vulnerability Scoring

Vulnerability scoring is an essential part of the assessment process. It helps in prioritizing the vulnerabilities based on their severity and potential impact. The Common Vulnerability Scoring System (CVSS) is widely used for this purpose. CVSS assigns a score to each vulnerability based on factors such as:

**Base Score:** Reflects the intrinsic characteristics of a vulnerability.

**Temporal Score:** Considers factors that may change over time, such as the availability of exploits.

**Environmental Score:** Takes into account the specific context and environment of the affected system.

## Reporting

A comprehensive vulnerability report should include:

**Executive Summary:** A high-level overview of the findings and their implications.

**Detailed Findings:** In-depth information about each identified vulnerability, including description, CVSS score, and potential impact.

**Recommendations:** Specific steps for mitigating each vulnerability.

**Conclusion:** Summary of the overall security posture and suggested next steps.

## Tools for Vulnerability Assessment

### Nessus

Nessus is a widely used vulnerability scanner that helps in identifying and managing security vulnerabilities across various IT environments.

### Features

- Comprehensive scanning capabilities for servers, networks, and applications.
- Regular updates with new vulnerability checks.

- Detailed reporting and analysis tools.

#### Advantages:

- User-friendly interface.
- High accuracy in vulnerability detection.
- Extensive plugin library for various types of vulnerabilities.

### OpenVAS

OpenVAS (Open Vulnerability Assessment System) is an open-source tool that provides comprehensive vulnerability scanning and management.

#### Features:

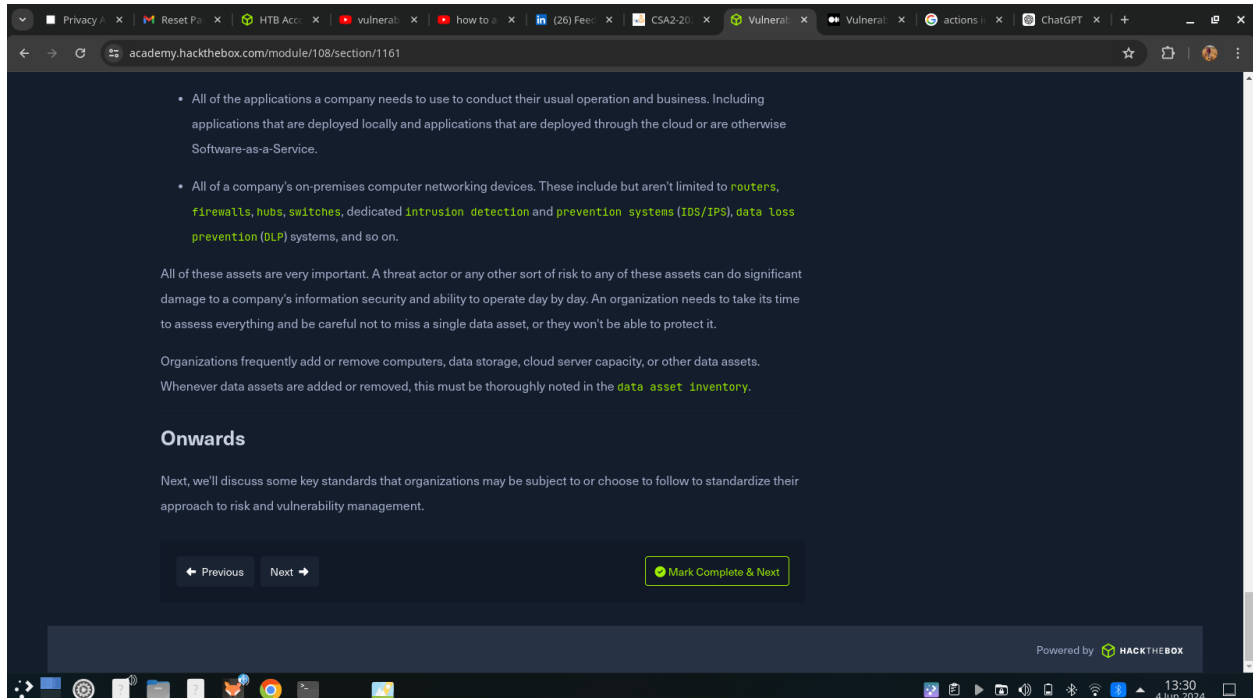
- Wide range of vulnerability tests covering various network services and applications.
- Regular updates and community support.
- Flexible configuration options for custom scans.

#### Advantages:

- Open-source and free to use.
- Strong community support.
- Extensive documentation and resources.

cs-sa07-24019

John\_Mbithi\_Mutave



The screenshot shows a web browser window with multiple tabs. The active tab is 'Vulneral:'. The address bar shows 'academy.hackthebox.com/module/108/section/1161'. The page content includes a list of assets, a paragraph about their importance, and a section titled 'Onwards'.

- All of the applications a company needs to use to conduct their usual operation and business. Including applications that are deployed locally and applications that are deployed through the cloud or are otherwise Software-as-a-Service.
- All of a company's on-premises computer networking devices. These include but aren't limited to **routers**, **firewalls**, **hubs**, **switches**, dedicated **intrusion detection and prevention systems (IDS/IPS)**, **data loss prevention (DLP)** systems, and so on.

All of these assets are very important. A threat actor or any other sort of risk to any of these assets can do significant damage to a company's information security and ability to operate day by day. An organization needs to take its time to assess everything and be careful not to miss a single data asset, or they won't be able to protect it.

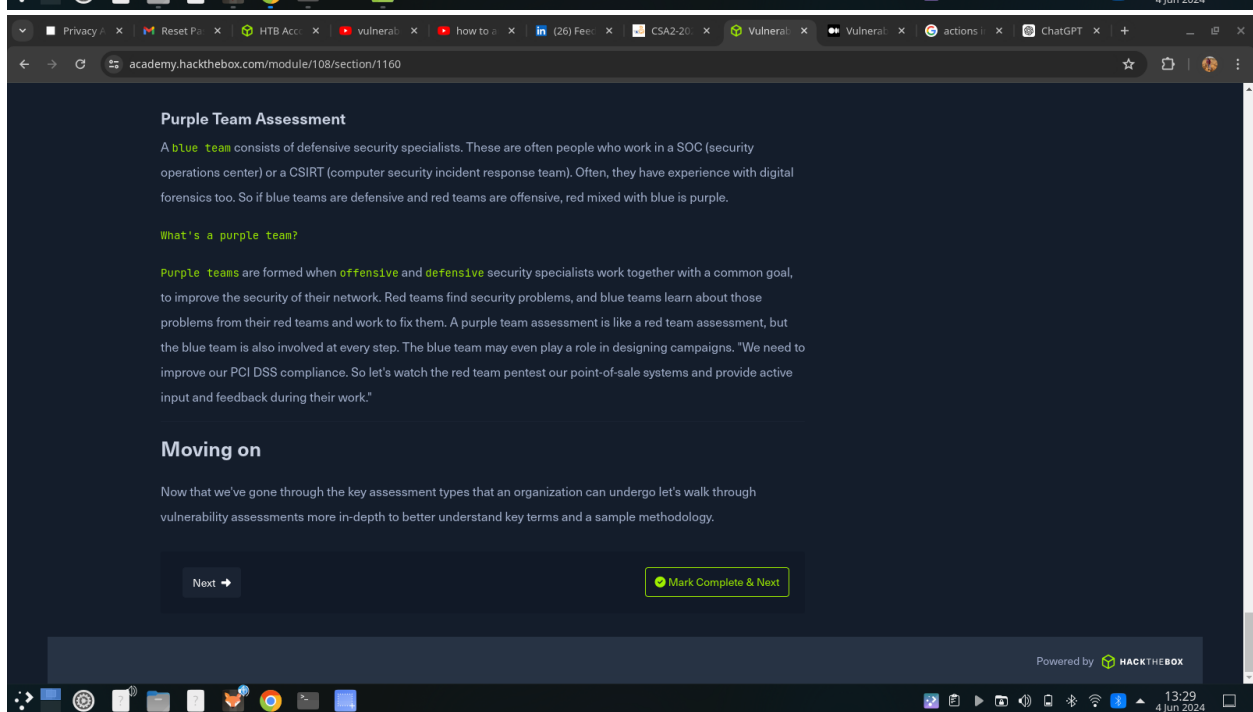
Organizations frequently add or remove computers, data storage, cloud server capacity, or other data assets. Whenever data assets are added or removed, this must be thoroughly noted in the **data asset inventory**.

### Onwards

Next, we'll discuss some key standards that organizations may be subject to or choose to follow to standardize their approach to risk and vulnerability management.

Navigation buttons: Previous, Next, Mark Complete & Next.

Powered by HACKTHEBOX



The screenshot shows the same web browser window with the active tab 'Vulneral:'. The address bar shows 'academy.hackthebox.com/module/108/section/1160'. The page content includes a section titled 'Purple Team Assessment' and a section titled 'Moving on'.

### Purple Team Assessment

A **blue team** consists of defensive security specialists. These are often people who work in a SOC (security operations center) or a CSIRT (computer security incident response team). Often, they have experience with digital forensics too. So if blue teams are defensive and red teams are offensive, red mixed with blue is purple.

**What's a purple team?**

**Purple teams** are formed when **offensive** and **defensive** security specialists work together with a common goal, to improve the security of their network. Red teams find security problems, and blue teams learn about those problems from their red teams and work to fix them. A purple team assessment is like a red team assessment, but the blue team is also involved at every step. The blue team may even play a role in designing campaigns. "We need to improve our PCI DSS compliance. So let's watch the red team pentest our point-of-sale systems and provide active input and feedback during their work."

### Moving on

Now that we've gone through the key assessment types that an organization can undergo let's walk through vulnerability assessments more in-depth to better understand key terms and a sample methodology.

Navigation buttons: Next, Mark Complete & Next.

Powered by HACKTHEBOX

cs-sa07-24019

John\_Mbithi\_Mutave

The screenshot shows a web browser with multiple tabs open. The active tab is 'Vulneral' and the URL is 'academy.hackthebox.com/module/108/section/1027'. The page content is about the NIST Cybersecurity Framework. It states that NIST (National Institute of Standards and Technology) is well known for their NIST Cybersecurity Framework, a system for designing incident response policies and procedures. NIST also has a Penetration Testing Framework. The phases of the NIST framework include:

- Planning
- Discovery
- Attack
- Reporting

Below this, there is a section for OWASP. It states that OWASP stands for the Open Web Application Security Project. They're typically the go-to organization for defining testing standards and classifying risks to web applications. OWASP maintains a few different standards and helpful guides for assessment various technologies:

- Web Security Testing Guide (WSTG)
- Mobile Security Testing Guide (MSTG)
- Firmware Security Testing Methodology

At the bottom of the page, there are navigation buttons: 'Previous', 'Next', and 'Mark Complete & Next'. The page is powered by HACKTHEBOX.

The screenshot shows a web browser with multiple tabs open. The active tab is 'Vulneral' and the URL is 'academy.hackthebox.com/module/108/section/1228'. The page content is about Calculating CVSS Severity. It explains that a 'Not Defined' value would indicate skipping this metric, a 'High' value would mean one of the elements of the CIA triad would have astronomical effects on the overall organization and customers, a 'Medium' value would indicate one of the elements of the CIA triad would have significant effects on the overall organization and customers, and a 'Low' value would mean one of the elements of the CIA triad would have minimal effects on the overall organization and customers.

### Calculating CVSS Severity

The calculation of a CVSS v3.1 score takes into account all the metrics discussed in this section. The National Vulnerability Database has a calculator available to the public [here](#).

### CVSS Calculation Example

For example, for the Windows Print Spooler Remote Code Execution Vulnerability, CVSS Base Metrics is 8.8. You can reference the values of each metric value [here](#).

### Next Steps

Next, we'll discuss how vulnerabilities are classified in a standard way that scanning tools can use to include an external reference to the particular vulnerability.

At the bottom of the page, there are navigation buttons: 'Previous', 'Next', and 'Mark Complete & Next'. The page is powered by HACKTHEBOX.

be able to leverage the issues for criminal use, also referred to as a **zero day** or an **0-day**.

## Examples

### CVE-2020-5902

CVE-2020-5902 is an unauthenticated, remote code execution vulnerability in the BIG-IP Traffic Management User Interface (TMUI). The issue is exploitable when TMUI is available through the BIG-IP management port and leads to a complete system takeover since an attacker could execute code, edit files, and enable or disable services on the remote host.

### CVE-2021-34527

CVE-2021-34527, also known as PrintNightmare, is a remote code execution vulnerability within the Windows Print Spooler service. The Windows Print Spooler service can be abused due to the service improperly handling privileges file operations. The issue requires a user to be authenticated but allows complete takeover of a system from remote or local code execution. The issue is extremely dangerous since it allows an attacker to fully control a domain since it exploits servers (including domain controllers) and workstations.

## Getting Hands-on

Now that we've defined key terms, discussed assessment types, vulnerability scoring, and disclosure, let's move on to getting familiar with two popular vulnerability scanning tools: Nessus and OpenVAS.

[← Previous](#) [Next →](#) [Mark Complete & Next](#)

academy.hackthebox.com/module/108/section/1230

## Dashboards

Overview

### Tasks by Severity Class (Total: 5)

Severity	Count
Low	4
High	1

### Tasks by Status (Total: 5)

Status	Count
Done	5

### CVEs by Creation Time

Year	Created CVEs	Total CVEs
1990	0	0
1995	0	0
2000	0	0
2005	0	0
2010	0	0
2015	0	0
2020	0	0

### CVEs by Severity Class (Total: 95318)

Severity	Count
Low	55312
High	33848
Medium	7148

[← Previous](#) [Next →](#) [Mark Complete & Next](#)

Powered by **HACKTHEBOX**

Privacy x Reset Pa x HTB Acc x vulneral x how to x (26) Fe x CSA2-20 x Vulneral x Vulneral x actions x ChatGPT x

academy.hackthebox.com/module/108/section/1029

On the **Advanced** tab, safe checks are enabled by default. This prevents Nessus from running checks that may negatively impact the target device or network. We can also choose to slow or throttle the scan if Nessus detects any network congestion, stop attempting to scan any hosts that become unresponsive, and even choose to have Nessus scan our target IP list in random order:

BASIC >  
DISCOVERY >  
ASSESSMENT >  
REPORT >  
ADVANCED >  
    General

General Settings

☒ Enable safe checks  
☐ Stop scanning hosts that become unresponsive during the scan  
☐ Scan IP addresses in a random order

Performance Options

☐ Slow down the scan when network congestion is detected

Network timeout (in seconds)   
Max simultaneous checks per host   
Max simultaneous hosts per scan

Previous Next

Mark Complete & Next

Privacy x Reset Pa x HTB Acc x vulneral x how to x (26) Fe x CSA2-20 x Vulneral x Vulneral x actions x ChatGPT x

academy.hackthebox.com/module/108/section/1231

may also use these credentials to SSH into the target VM to configure Nessus.

Finally, once the setup is complete, we can start creating scans, scan policies, plugin rules, and customizing settings. The **Settings** page has a wealth of options such as setting up a Proxy Server or SMTP server, standard account management options, and advanced settings to customize the user interface, scanning, logging, performance, and security options.

Overview  
About  
Account  
Proxy Server  
Reverse Link  
SMTP Server  
Custom GAs  
Upgrade Assistant  
Password Mgmt  
System Health  
Notifications  
My Account

Advanced Settings

Advanced settings allow you to manually configure global settings. In order for these settings to take effect, a restart of the Nessus service or server may be required. NOTICE: Settings configured in scans or policies will override these values.

User Interface Scanning Logging Performance Security Miscellaneous

Setting	Modifier	Value
Allow Post-Scan Raising	allow_post_scan_raising	Yes
Disable API	disable_api	No
Disable Firewall	disable_firewall	No
Login Banner	login_banner	
Maximum Concurrent Web Users	global_max_web_users	100
Nessus Web Server IP	scan_address	0.0.0.0
Nessus Web Server Port	webui_listen_port	8834

Previous Next

Mark Complete & Next

Powered by HACKTHEBOX

13:35  
4 Jun 2024



cs-sa07-24019

John\_Mbithi\_Mutave

academy.hackthebox.com/module/108/section/1232

Finally, we can check the Nessus output to confirm whether the authentication to the target application or service with the supplied credentials was successful:

**INFO** Microsoft SQL Server Login Possible

**Description**  
Nessus was able to log into the remote MS SQL server using the supplied credentials.

**See Also**  
[https://azure.microsoft.com/en-us/?ocid=cloudplat\\_hp](https://azure.microsoft.com/en-us/?ocid=cloudplat_hp)

**Output**

```
Credentialed checks have been enabled for MSSQL server on port 1433.
SQL Server Version   : 14.0.1000.0
SQL Server Instance  :
```

← Previous   Next →   **Mark Complete & Next**

Powered by HACKTHEBOX

academy.hackthebox.com/module/108/section/1024

Scan ID	Name	Last Modified	Status
1	Windows_basic	Aug 22, 2020 22:07 +00:00	completed

Enter the report(s) you want to download (comma separate list) or 'all': 1

Choose File Type(s) to Download:  
[0] Nessus (No chapter selection)  
[1] HTML  
[2] PDF  
[3] CSV (No chapter selection)  
[4] DB (No chapter selection)

Enter the file type(s) you want to download (comma separate list) or 'all': 3

Path to save reports to (without trailing slash): /assessment\_data/inlanefreight/scans/nessus

Downloading report(s). Please wait...

```
[+] Exporting scan report, scan id: 1, type: csv
[+] Checking export status...
[+] Report ready for download...
[+] Downloading report to: /assessment_data/inlanefreight/scans/nessus/inlanefreight_basic_5y3hx
Report Download Completed!
```

We can also write our own scripts to automate many Nessus features.

← Previous   Next →   **Mark Complete & Next**

Powered by HACKTHEBOX

cs-sa07-24019  
John\_Mbithi\_Mutave

Privacy xReset Po xHTB Acc xvulneral xhow to x(26) Fee xCSA2-20 xVulneral xVulneral xactions xChatGPT x

academy.hackthebox.com/module/108/section/1028

rx | tx

bytes

1.04 MiB | 1.34 MiB

max

414.81 kbit/s | 480.59 kbit/s

average

230.57 kbit/s | 296.72 kbit/s

min

0 bit/s | 0 bit/s

packets

18252 | 22733

max

864 p/s | 969 p/s

average

480 p/s | 598 p/s

min

0 p/s | 0 p/s

time

38 seconds

real

0m38.588s

user

0m0.002s

sys

0m0.010s

When comparing the results, we can see that the number of bytes and packets transferred during a vulnerability scan is quite significant and can severely impact a network if not tuned properly or performed against fragile/sensitive devices.

PreviousNext

Mark Complete & Next

Powered by HACKTHEBOX

13:37

4 Jun 2024

John\_Mbithi\_Mutave

acade

myhackthebox.com/module/108/section/1026

You might need to refresh your browser once it opens.

[\*] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

greenbone-security-assistant.service - Greenbone Security Assistant (gsad)

Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; disabled; vendor preset: disabled)

Active: active (running) since Mon 2021-12-27 21:40:17 GMT; 11ms ago

Docs: man:gsad(8)  
https://www.greenbone.net

Process: 24626 ExecStart=/usr/sbin/gsad --listen=127.0.0.1 --port=9392 (code=exited, status=0/SUCCESS)

Main PID: 24627 (gsad)

Tasks: 2 (limit: 4605)

Memory: 2.2M

CPU: 20ms

CGroup: /system.slice/greenbone-security-assistant.service  
└─24627 /usr/sbin/gsad --listen=127.0.0.1 --port=9392

Dec 27 21:48:17 parrot systemd[1]: Starting Greenbone Security Assistant (gsad)...  
Dec 27 21:48:17 parrot gsad[24626]: Oops, secure memory pool already initialized  
Dec 27 21:48:17 parrot systemd[1]: Started Greenbone Security Assistant (gsad).

gvm.service - Greenbone Vulnerability Manager daemon (gvm)

Loaded: loaded (/lib/systemd/system/gvm.service; disabled; vendor preset: disabled)

Note: The VM provided in the OpenVAS Skills Assessment section has OpenVAS pre-installed and the targets running. You can go to that section and start the VM and use OpenVAS throughout the module, which can be accessed at <https://< IP >:8080>. The OpenVAS credentials are: [http-student:HTB\\_@cademy\\_student!.](#) You may also use these credentials to SSH into the target VM to configure OpenVAS.

Previous

Next

Mark Complete & Next

Powered by HACKTHEBOX

Privacy Reset P HTB Acc vulnural how to (26) Fee CSA2-20 Hack Th Vulnural actions ChatGPT

acade myhackthebox.com/module/108/section/1233

+1 What is the plugin ID of the highest criticality vulnerability for the Windows authenticated scan?

156032

Submit

+1 What is the name of the vulnerability with plugin ID 26925 from the Windows authenticated scan? (Case sensitive)

VNC Server Unauthenticated Access

Submit

+1 What port is the VNC server running on in the authenticated Windows scan?

5900

Submit

Previous

Next

Mark Complete & Next

academy.hackthebox.com/module/108/section/1026

```
[*] You might need to refresh your browser once it opens.
[*] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

• greenbone-security-assistant.service - Greenbone Security Assistant (gsad)
  Loaded: loaded (/lib/systemd/system/greenbone-security-assistant.service; disabled; vendor preset: disabled)
  Active: active (running) since Mon 2021-12-27 21:40:17 GMT; 11ms ago
  Docs: man:gsad(8)
        https://www.greenbone.net
  Process: 24626 ExecStart=/usr/sbin/gsad --listen=127.0.0.1 --port=9392 (code=exited, status=0/SUCCESS)
  Main PID: 24627 (gsad)
  Tasks: 2 (limit: 4609)
  Memory: 2.2M
  CPU: 20ms
  CGroup: /system.slice/greenbone-security-assistant.service
          └─24627 /usr/sbin/gsad --listen=127.0.0.1 --port=9392

Dec 27 21:40:17 parrot systemd[1]: Starting Greenbone Security Assistant (gsad)...
Dec 27 21:40:17 parrot gsad[24626]: Oops, secure memory pool already initialized
Dec 27 21:40:17 parrot systemd[1]: Started Greenbone Security Assistant (gsad).

• gvm.service - Greenbone Vulnerability Manager daemon (gvm)
  Loaded: loaded (/lib/systemd/system/gvm.service; disabled; vendor preset: disabled)
```

**Note:** The VM provided in the [OpenVAS Skills Assessment](#) section has OpenVAS pre-installed and the targets running. You can go to that section and start the VM and use OpenVAS throughout the module, which can be accessed at <https://< IP >:8080>. The OpenVAS credentials are: [htb-student:HTB\\_@cademy\\_student!](#). You may also use these credentials to SSH into the target VM to configure OpenVAS.

← Previous   Next →   [Mark Complete & Next](#)

Powered by **HACKTHEBOX**

academy.hackthebox.com/module/108/section/1463

## HOSTS

Included	172.16.16.160
Maximum Number of Hosts	1
Allow simultaneous scanning via multiple IPs	Yes
Reverse Lookup Only	No
Reverse Lookup Unify	No
Alive Test	Scan Config Default
Port List	All IANA assigned TCP

## Tasks using this Target (2)

[Linux\\_Host\\_Discovery](#) • [Linux\\_basic](#)

← Previous   Next →   [Mark Complete & Next](#)

Powered by **HACKTHEBOX**

John\_Mbithi\_Mutave

Privacy / xReset Po / xHTB Acc / xvulnerab / xhow to / x(26) Fee / xCSA2-20 / xHack Th / xVulneral / xactions / xChatGPT / x+ / x

academy.hackthebox.com/module/108/section/1516

☆🔖👤⋮

+ 1 🟢 What type of FTP vulnerability is on the Linux host? (Case Sensitive, four words)

Anonymous FTP Login Reporting

Submit

+ 1 🟢 What is the IP of the Linux host targeted for the scan?

172.16.16.160

Submit

+ 2 🟢 What vulnerability is associated with the HTTP server? (Case-sensitive)

Cleartext Transmission of Sensitive Information via HTTP

SubmitHint

← PreviousNext →

🟢 Mark Complete & Next

cs-sa07-24019  
John\_Mbithi\_Mutave

The screenshot shows a web browser window with the URL `academy.hackthebox.com/module/108/section/1030`. The page content includes a list of elements for each issue: Vulnerability Name, CVE, CVSS, Description of Issue, References, Remediation Steps, Proof of Concept, and Affected Systems. Below this is a section titled "Closing" with a paragraph of text. At the bottom, there are buttons for "Previous", "+10 Streak pts", and "Finish". The page is powered by HACKTHEBOX.

Each issue should have the following elements:

- Vulnerability Name
- CVE
- CVSS
- Description of Issue
- References
- Remediation Steps
- Proof of Concept
- Affected Systems

### Closing

The reporting portion of any assessment is the most crucial part of the project. Always make sure you are writing your reports such that any audience can read them. When discussing technical information, always reference what you describe for the reader to understand or reproduce what you are talking about in the report. Additionally, sentences should be to the point with proper grammar as well. The strongest reports are concise and clear for a reader.

[Previous](#) [+10 Streak pts](#) [Finish](#)

Powered by **HACKTHEBOX**

The screenshot shows the HTB Academy dashboard. A large modal window is displayed in the center, titled "Vulnerability Assessment" and "Great job Alb0GreenN!". The modal contains a congratulatory message and a prompt to share success with everyone, with buttons for "Share on LinkedIn", "Share on X", "Share on Facebook", and "Get a shareable link". The background shows the user's profile (Alb0GreenN, Free, 40 cubes), a sidebar with navigation links (Dashboard, Exams, Modules, Paths, Academy x HTB Labs), and a list of modules. The "Vulnerability Assessment" module is highlighted, showing its conclusion and key takeaways.

## Vulnerability Assessment

Great job Alb0GreenN!

Completed / Congrats!

in Share on LinkedIn

Conclusion

This module covered various vulnerability types of compliance bodies and to Nessus and OpenVAS.

### Module Key takeaways

- Defining a Vulnerability Assessment
- Vulnerability scoring systems
- Installing and using Nessus
- Installing and using OpenVAS

Here are a few suggestions to try out based on the path you've just completed!

Suggested Modules

Alb0GreenN Free 40

LEARN

- Dashboard
- Exams
- Modules
- Paths
- Academy x HTB Labs

MY ACHIEVEMENTS

- My Certificates
- My Badges

REFERRALS

in Share on LinkedIn

Share on X

Share on Facebook

Get a shareable link

Change Log

Retake Module

Shareable link - <https://academy.hackthebox.com/achievement/1296187/108>

## Conclusion

Cleartext transmission of sensitive information via HTTP is a critical vulnerability that poses significant risks to organizations. Conducting thorough security assessments using tools like Nessus and OpenVAS, combined with effective vulnerability scoring and reporting, is essential in identifying and mitigating these risks. By adopting a proactive approach to vulnerability management, organizations can protect their sensitive information and maintain compliance with relevant regulations and standards.