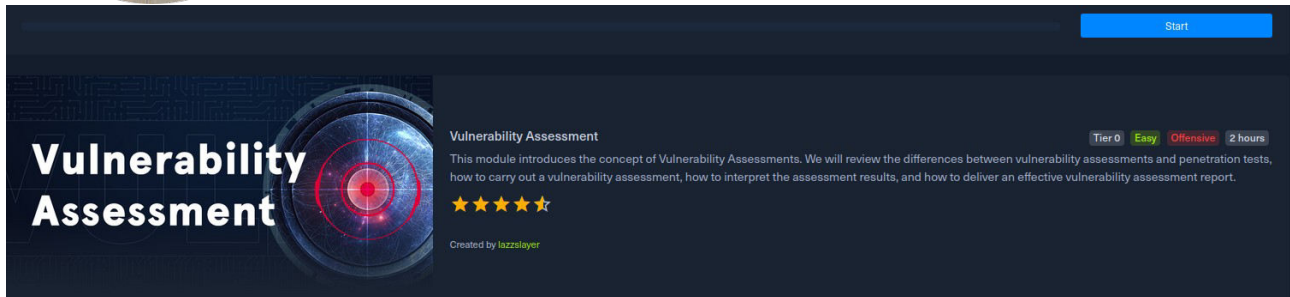




Eric Mwenda

VULNERABILITY ASSESSMENT

<https://academy.hackthebox.com/achievement/596337/108>



Security Assessments

Security assessment is very key to any institution, company or organisation. An assessment has to be made now and then on their networks, computers and applications to find and confirm vulnerabilities are present, so that they can be patched, mitigated or removed from the system.

A vulnerability assessment is based on a particular security standard and compliance with these standards is analyzed for example going through a checklist.

Defining which standards apply to a particular network will depend on many factors for organizations are different too.

Penetration Test

A pentest is a type of simulated cyber attack and pentesters conduct actions that a threat actor may perform to see if certain kinds of exploits are possible.

The key difference is that for a pentest there is a full legal consent of the entity being pentested. Whether a pentester is an employee or a third-party contractor, they will need to sign a lengthy legal document with the target company that describes what they're allowed to do and what they're not allowed to do.

A cyber threat intrudes into the system without legal rights from the target.

There are several kinds of pentests.

1. Black box
2. Grey box
3. white box

Black box – This kind of pentest is done without the knowledge of a network's configuration or applications. In this kind of cases a pentester will only be given as little as the company's name or an ethernet port and have to bypass Network Access Control (NAC) and nothing else (requiring them to perform their own discovery for IP addresses).

This kind of pentest is carried out with minimal information.

Grey box - pentesting is done with a little bit of knowledge of the network they're testing, from a perspective equivalent to an employee who doesn't work in the IT department, such as a receptionist

or customer service agent. The customer will typically give the tester in-scope network ranges or individual IP addresses in a grey box situation.

White box – In this penetration, the pentester is provided with a huge information about the system that is full access to all systems, configurations, build documents, etc., and source code if web applications are in-scope. The goal here is to discover as many flaws as possible that would be difficult or impossible to discover blindly in a reasonable amount of time.

A pentester has to know several fields and technologies but it is best to have a specialty.

We also have:-

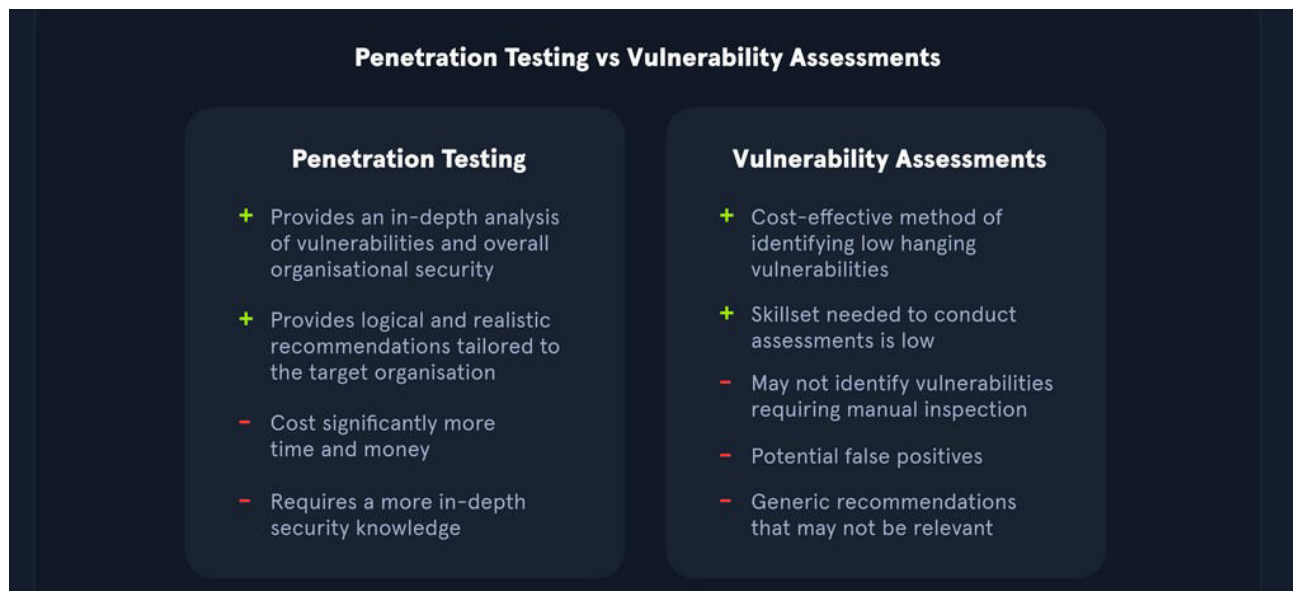
- Application Pentesters.
- Network or Infrastructure Pentesters.
- Physical Pentesters.
- Social Engineering.

Application Pentesters - assess web applications, thick-client applications, APIs, and mobile applications. They will often be well-versed in source code review and able to assess a given web application from a black box or white box standpoint.

Network or Infrastructure Pentesters - assess all aspects of a computer network, including its networking devices such as routers and firewalls, workstations, servers, and applications. These types of penetration testers typically must have a strong understanding of networking, Windows, Linux, Active Directory, and at least one scripting language. In this type of pentest, tools such as Nessus are very handy in this kind of work.

Physical pentesters – This pentesters try to leverage physical security weaknesses and breakdowns in processes to gain access to a facility such as a data center or office building.

Social Engineering – This is whereby a pentester uses his/her interaction skills with human beings with the aim of getting valuable information indirectly from the target without their knowledge or without raising suspicions.



An organization may benefit more from a vulnerability assessment over a penetration test if they want to receive a view of commonly known issues monthly or quarterly from a third-party vendor. However, an organization would benefit more from a penetration test if they are looking for an

approach that utilizes manual and automated techniques to identify issues outside of what a vulnerability scanner would identify during a vulnerability assessment.

Other Types of Security Assessments

Security Audits

Vulnerability assessments are performed because an organization chooses to conduct them, and they can control how and when they're assessed. Security audits are different.

Bug Bounties

Bug bounty programs are implemented by all kinds of organizations. They invite members of the general public, with some restrictions (usually no automated scanning), to find security vulnerabilities in their applications. Bug bounty hunters can be paid anywhere from a few hundred dollars to hundreds of thousands of dollars for their findings, which is a small price to pay for a company to avoid a critical remote code execution vulnerability from falling into the wrong hands.

Red Team Assessment

Companies with larger budgets and more resources can hire their own dedicated red teams or use the services of third-party consulting firms to perform red team assessments. A red team consists of offensive security professionals who have considerable experience with penetration testing. A red team plays a vital role in an organization's security posture.

Vulnerability Assessment

A Vulnerability Assessment aims to identify and categorize risks for security weaknesses related to assets within an environment. It is important to note that there is little to no manual exploitation during a vulnerability assessment. A vulnerability assessment also provides remediation steps to fix the issues.

The purpose of a Vulnerability Assessment is to understand, identify, and categorize the risk for the more apparent issues present in an environment without actually exploiting them to gain further access.

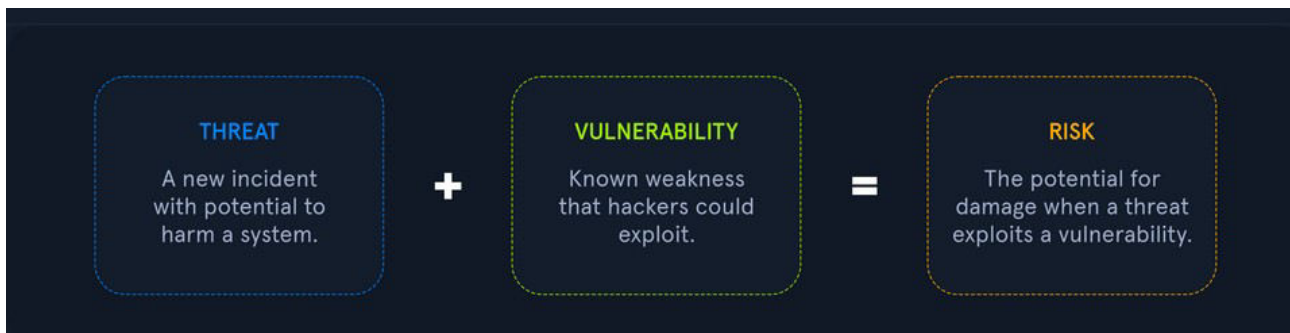
Methodology

Methodologies may vary slightly from organization to organization.

In this section we covered 8 main steps of a methodology from identifying assets to creating a remediation plan.

1. Conduct Risk Identification Analysis.
2. Develop Vulnerability Scanning Policies
3. Identify the type of scans
4. Configure the scan
5. Perform the scanning
6. Evaluate and consider possible risks
7. Interpret the scan results.
8. create a remediation and mitigation plan.

Afterwards we differentiated between Threat, Vulnerability and Risk.



1. Threat - A Threat is a process that amplifies the potential of an adverse event, such as a threat actor exploiting a vulnerability. Some vulnerabilities raise more threat concerns over others due to the probability of the vulnerability being exploited. For example, the higher the reward of the outcome and ease of exploitation, the more likely the issue would be exploited by threat actors. Exploit

2. Exploit - An Exploit is any code or resources that can be used to take advantage of an asset's weakness. Many exploits are available through open-source platforms such as Exploit-db or the Rapid7 Vulnerability and Exploit Database. We will often see exploit code hosted on sites such as GitHub and GitLab as well. Risk

3. Risk - Risk is the possibility of assets or data being harmed or destroyed by threat actors.

Assessment Standards

In this section we discussed as far as both penetration tests and vulnerability assessments is concerned, they should comply with specific standards to be accredited and accepted by governments and legal authorities. Such standards help ensure that the assessment is carried out thoroughly in a generally agreed-upon manner to increase the efficiency of these assessments and reduce the likelihood of an attack on the organization.

Compliance Standards

Every organisation has those standards they should adhere to. Most known information security compliance standards are **PCI, HIPAA, FISMA, and ISO 27001**.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a commonly known standard in information security that implements requirements for organizations that handle credit cards. This is not a government regulation but organizations that store, process or transmit cardholder data must still implement PCI DSS guidelines.



Health Insurance Portability and Accountability Act (HIPAA) – used to protect patients data. HIPAA does not necessarily require vulnerability scans or assessments; however, a risk assessment and vulnerability identification are required to maintain HIPAA accreditation.

Federal Information Security Management Act (FISMA) – This is a set of standards and guidelines used to safeguard government operations and information. The act requires an organization to provide documentation and proof of a vulnerability management program to maintain information technology systems' proper availability, confidentiality, and integrity.

ISO 27001 - This is a standard used worldwide to manage information security. ISO 27001 requires organizations to perform quarterly external and internal scans.

Penetration Testing Standards - Penetration tests should not be performed without any rules or guidelines. There must always be a specifically defined scope for a pentest, and the owner of a network must have a signed legal contract with pentesters outlining what they're allowed to do and what they're not allowed to do.

We also looked at various pentesting standards, depending on what kind of computer system is being assessed.

Commonly used standards by pentesters:-

1. PETS (Penetration Testing Execution Standard) - can be applied to all types of penetration tests. It outlines the phases of a penetration test and how they should be conducted.

2. OSSTNM (Open Source Security Testing Methodology Manual) – This standard has a set of guidelines pentesters can use to ensure they're doing their jobs properly. It can be used alongside other pentest standards.

3. NIST (National Institute of Standards and Technology) – This standard is well known for their NIST Cybersecurity Framework system for designing incident response policies and procedures. NIST also has a Penetration Testing Framework

4. OWSAP (Open Web Application Security Project) – This are the go-to organization for defining testing standards and classifying risks to web applications.

Common Vulnerability Scoring System (CVSS)

Every vulnerability has a score value.

The CVSS are often used together with the so-called Microsoft DREAD. DREAD is a risk assessment system developed by Microsoft to help IT security professionals evaluate the severity of security threats and vulnerabilities. It is used to perform a risk analysis by using a scale of 10 points to assess the severity of security threats and vulnerabilities.

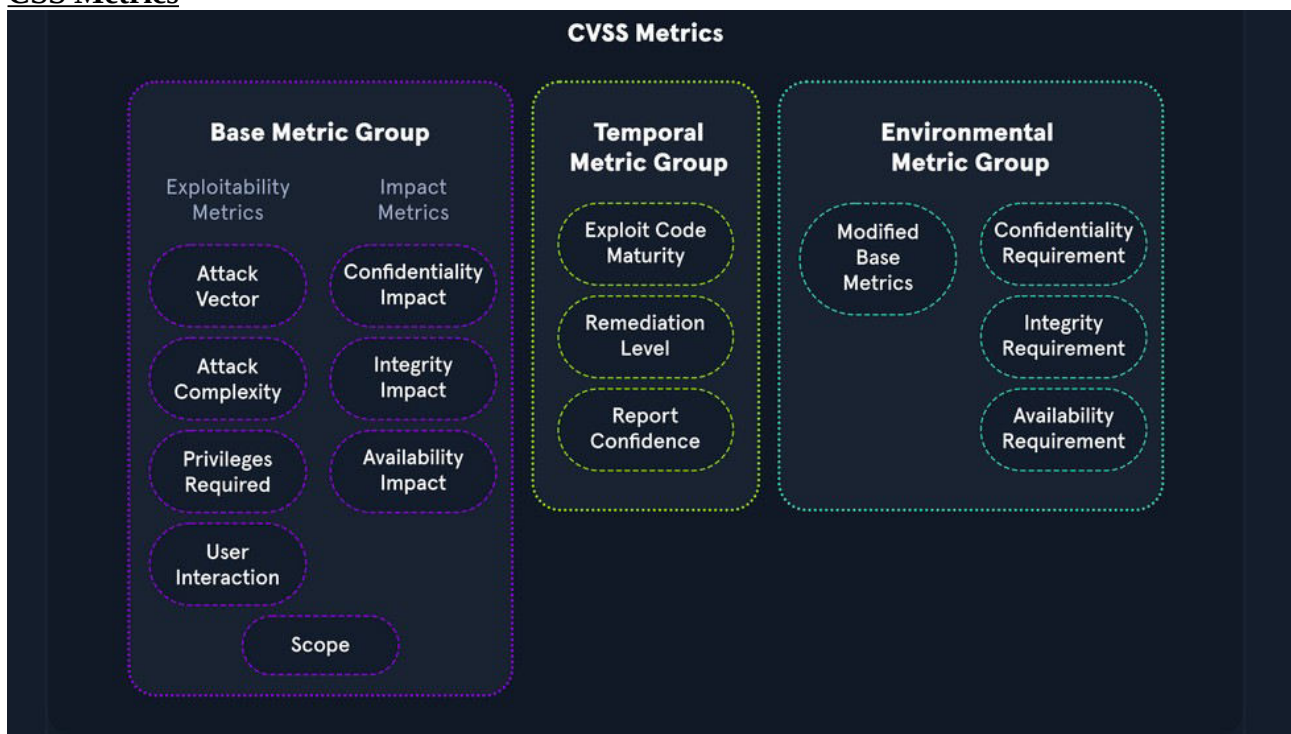
With DREAD, we calculate the risk of a threat or vulnerability based on five main factors:

- Damage Potential
- Reproducibility
- Exploitability
- Affected Users
- Discoverability

Risk Scoring

The CVSS system helps categorize the risk associated with an issue and allows organizations to prioritize issues based on the rating. The CVSS scoring consists of the exploitability and impact of an issue. The exploitability measurements consist of access vector, access complexity, and authentication. The impact metrics consist of the CIA triad, including confidentiality, integrity, and availability.

CSS Metrics



Base Metric Group

The CVSS base metric group represents the vulnerability characteristics and consists of exploitability metrics and impact metrics.

Exploitability Metrics

The Exploitability metrics are a way to evaluate the technical means needed to exploit the issue using the metrics such as Attack Vector, Attack Complexity, Privileges Required and User Interaction.

Impact Metrics

The Impact metrics represent the repercussions of successfully exploiting an issue and what is impacted in an environment, and it is based on the CIA triad. The CIA triad is an acronym for Confidentiality, Integrity, and Availability.

Temporal Metric Group

The Temporal Metric Group details the availability of exploits or patches regarding the issue.

Exploit Code Maturity

The Exploit Code Maturity metric represents the probability of an issue being exploited based on ease of exploitation techniques. There are various metric values associated with this metric, including Not Defined, High, Functional, Proof-of-Concept, and Unproven.

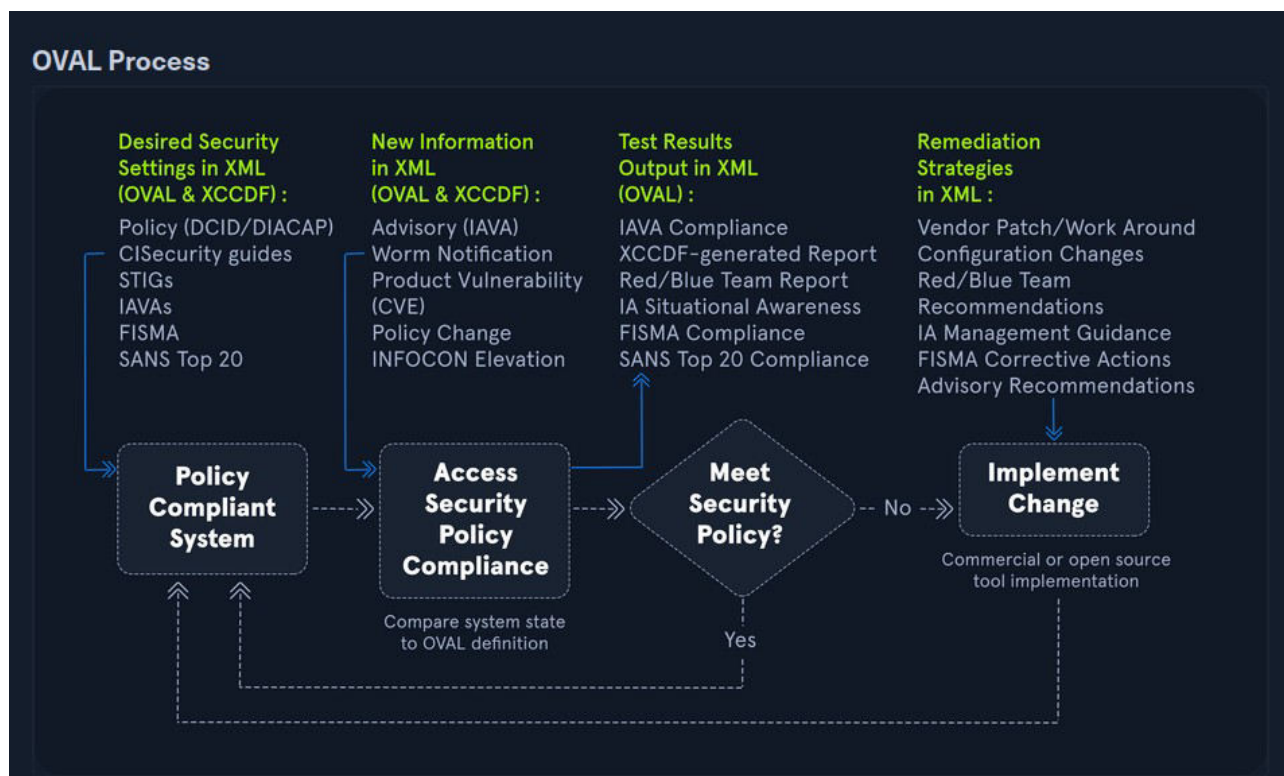
Remediation Level

The Remediation level is used to identify the prioritization of a vulnerability. The metric values associated with this metric include Not Defined, Unavailable, Workaround, Temporary Fix, and Official Fix.

Common Vulnerabilities and Exposures (CVE)

In this section we began by discussing about OVAL (Open Vulnerability Assessment Language). OVAL is a publicly available information security international standard used to evaluate and detail the system's current state and issues.

OVAL provides a language to understand encoding system attributes and various content repositories shared within the security community.

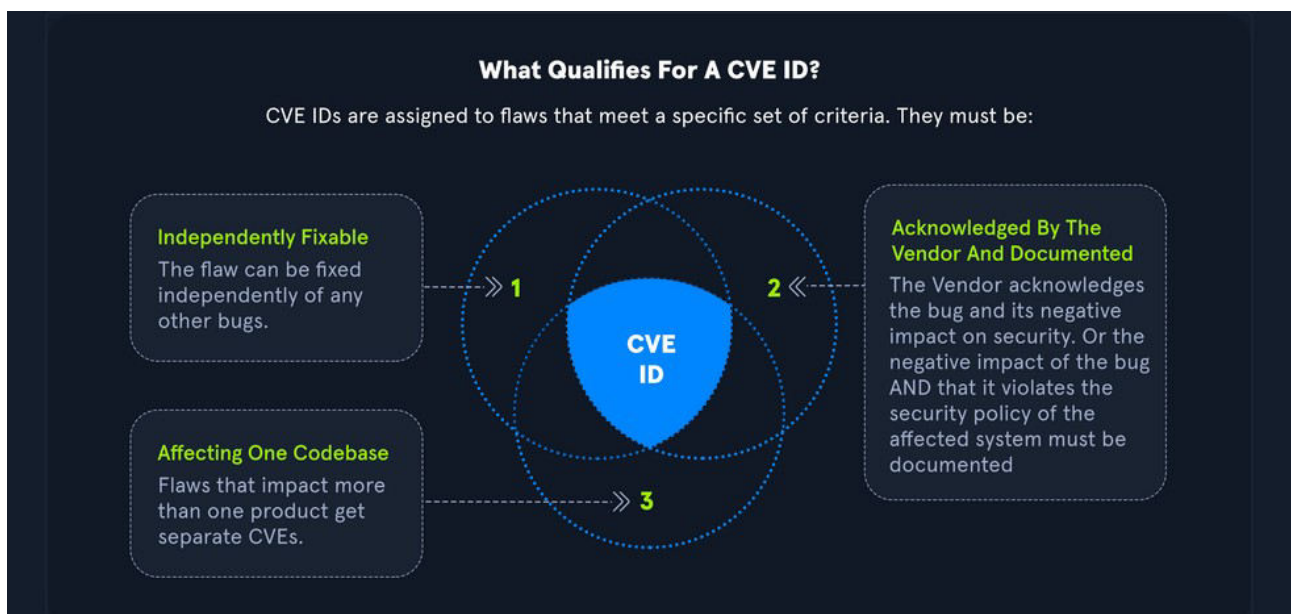


The goal of the OVAL language is to have a three-step structure during the assessment process that consists of:

- Identifying a system's configurations for testing
- Evaluating the current system's state
- Disclosing the information in a report

Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) is a publicly available catalog of security issues. Each security issue has a unique CVE ID number assigned by the CVE Numbering Authority (CNA). The purpose of creating a unique CVE ID number is to create a standardization for a vulnerability or exposure as a researcher identifies it. A CVE consists of critical information regarding a vulnerability or exposure, including a description and references about the issue. The information in a CVE allows an organization's IT team to understand how detrimental a problem could be to their environment.



There are 9 stages of Obtaining a CVE, they are:-

1. Identify if CVE is Required and Relevant.
2. Reach Out to Affected Product Vendor.
3. Identify if Request Should Be For Vendor CNA or Third Party CNA.
4. Requesting CVE ID Through CVE Web Form.
5. Confirmation of CVE Form.
6. Receival of CVE ID.
7. Public Disclosure of CVE ID.
8. Announcing the CVE.
9. Providing Information to The CVE Team.

Vulnerability Scanning Overview

Vulnerability scanning is performed to identify potential vulnerabilities in network devices such as routers, firewalls, switches, as well as servers, workstations, and applications.

Vulnerabilities scanners typically do not exploit vulnerabilities (with some exceptions) but need a human to manually validate scan issues to determine whether or not a particular scan returned real issues that need to be fixed or false positives that can be ignored and excluded from future scans against the same target.

The type of scans run varies from one tool to another, but most tools run a combination of dynamic and static tests, depending on the target and the vulnerability.

A static test is supposed to determine a vulnerability if the identified version of a particular asset has a public CVE. However, this is not always accurate as a patch may have been applied, or the target isn't specifically vulnerable to that CVE

A dynamic test tries specific payloads such as weak credentials, SQL injection, or command injection on the target like a web application. If any payload returns a hit, then there's a good chance that it is vulnerable.

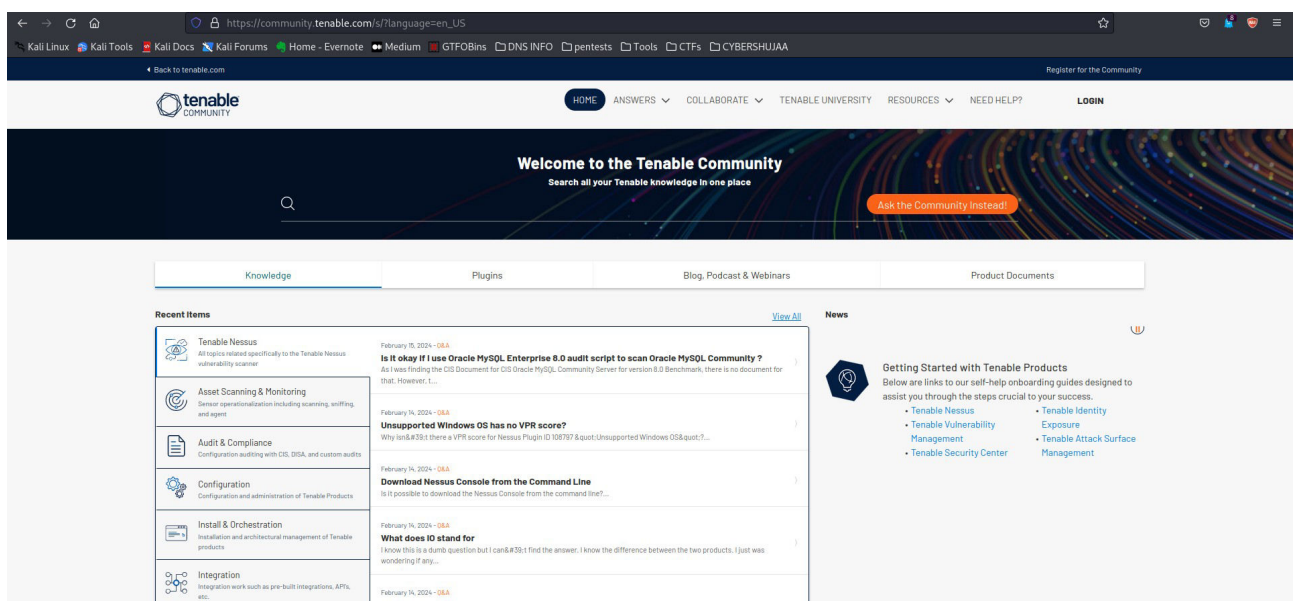
It is advised that organizations should run both unauthenticated and authenticated scans on a continuous schedule to ensure that assets are patched as new vulnerabilities are discovered and that any new assets added to the network do not have missing patches or other configuration/patching issues.

Nessus, **Nexpose** and **Qualys** are well-known vulnerability scanning platforms that also provide free community editions.

Another open-source alternatives is **OpenVAS**.

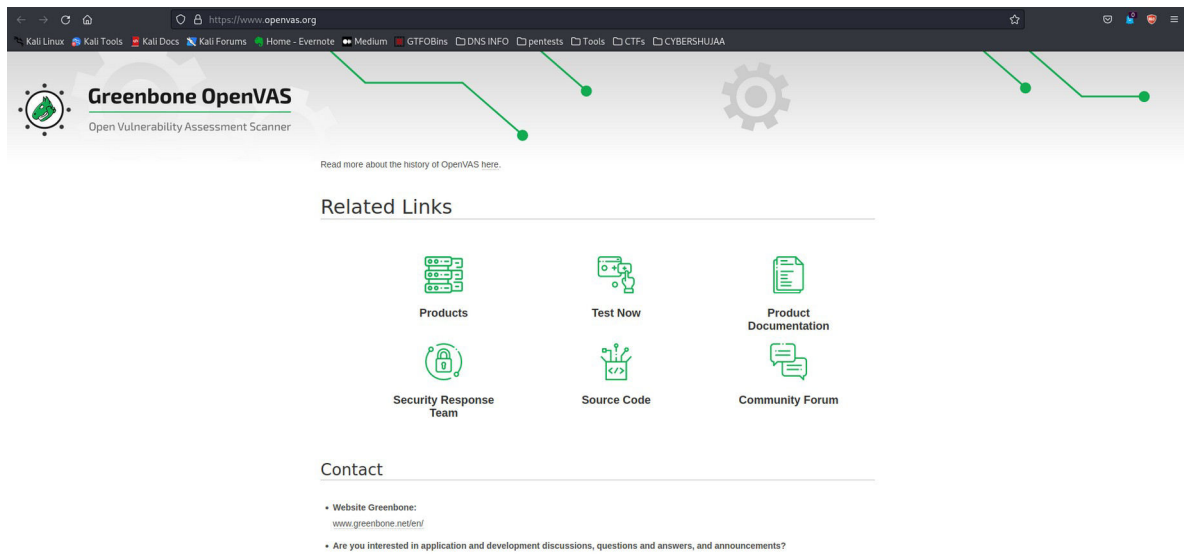
Nessus Overview

The free version for Nessus is the Nessus Essentials by Tenable.



OpenVAS Overview

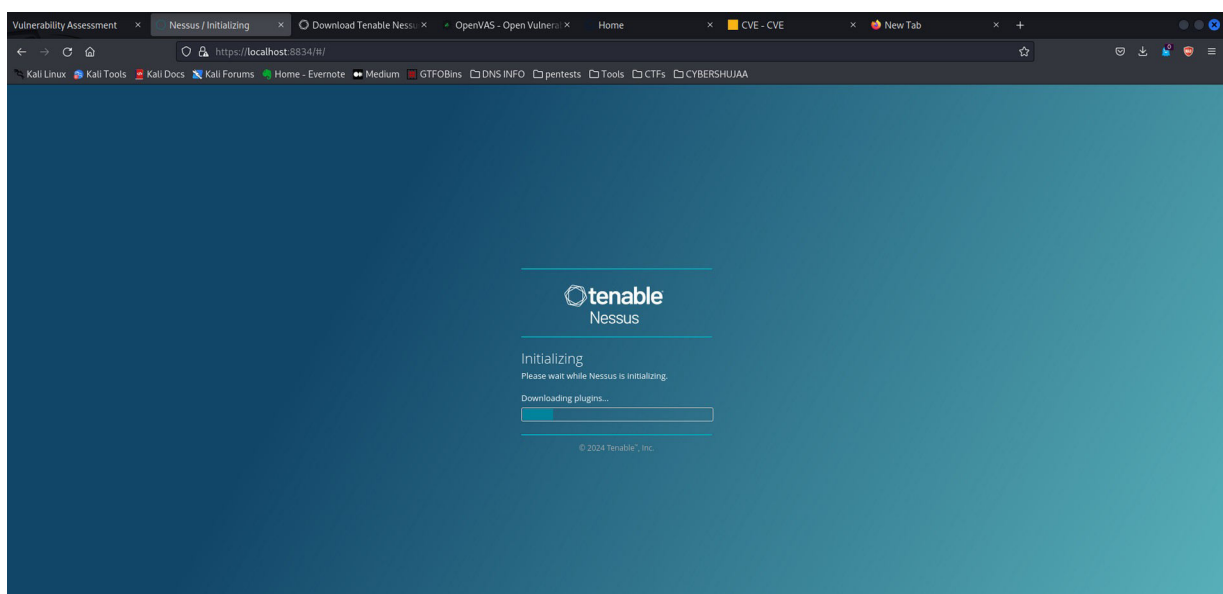
OpenVAS by Greenbone Networks is a publicly available open-source vulnerability scanner. OpenVAS can perform network scans, including authenticated and unauthenticated testing.



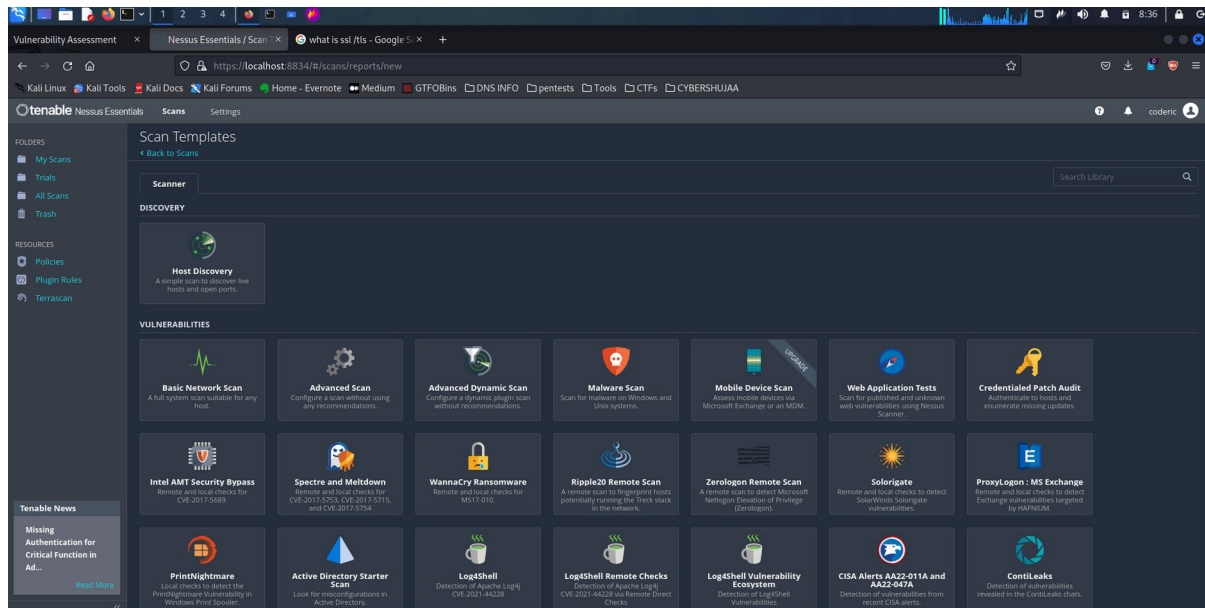
Getting Started with Nessus

In this section we looked on how to:-

- Register into a Nessus account.
- How to get an activation key for Nessus Essentials.
- Download Nessus into our local machine.
- How to install Nessus from our kali terminal.
- How to start Nessus services using command:- **sudo systemctl start nessusd.service**
- How to access Nessus from the web browser. **https://localhost:8834**
- How to initialize Nessus and key in our activation key.



Installed.



Nessus Scan

A new Nessus scan can be configured by clicking New Scan, and selecting a scan type. Scan templates fall into three categories: Discovery, Vulnerabilities, and Compliance.

New Scan

New scan has a basic Host Discovery scan to identify live hosts/open ports or a variety of scan types such as the Basic Network Scan, Advanced Scan, Malware Scan, Web Application Tests, as well as scans targeted at specific CVEs and audit & compliance standards

Discovery

We also discussed about Discovery section, under Host Discovery, where we are presented with the option to enable scanning for fragile devices.

I noted that scanning devices such as network printers often result in them printing out reams of paper with garbage text, leaving the devices unusable therefore it is advised to leave the setting disabled:

Within the **Service Discovery** subsection, the **Probe all ports to find services option** is selected by default. It's possible that a poorly designed application or service could crash as a result of this probing, but most applications should be robust enough to handle this. Searching for SSL/TLS services is also enabled by default on a custom scan, and Nessus can additionally be instructed to identify expiring and revoked certificates.

Assessment

Under the Assessment category, web application scanning can also be enabled if required and a custom user agent and various other web application scanning options can be specified like a URL for Remote File Inclusion (RFI) testing.

Advanced

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.

Advanced Settings

There are a couple of settings on the advanced tab but here are a few options explained:-

Scan Policies

Nessus gives us the option to create scan policies. Essentially these are customized scans that allow us to define specific scan options, save the policy configuration, and have them available to us under Scan Templates when creating a new scan. This gives us the ability to create targeted scans for any number of scenarios, such as a slower, more evasive scan, a web-focused scan, or a scan for a particular client using one or several sets of credentials. Scan policies can be imported from other Nessus scanners or exported to be later imported into another Nessus scanner.

Nessus Plugins

Nessus works with plugins written in the Nessus Attack Scripting Language (NASL) and can target new vulnerabilities and CVEs. These plugins contain information such as the vulnerability name, impact, remediation, and a way to test for the presence of a particular issue.

Scanning with Credentials

Nessus also supports credentialed scanning and provides a lot of flexibility by supporting LM/NTLM hashes, Kerberos authentication, and password authentication.

Working with Nessus Scan Output

Nessus gives us the option to export scan results in a variety of report formats as well as the option to export raw Nessus scan results to be imported into other tools, archived, or passed to tools, such as EyeWitness, which can be used to take screenshots of all web applications identified by Nessus and greatly assist us with working through the results and finding more value in them.

Nessus Reports

Once a scan is completed we can choose to export a report in **.pdf, .html or .csv** formats.

Exporting Nessus Scans

Nessus also gives the option to export scans into two formats Nessus (scan.nessus) or Nessus DB (scan.db). The .nessus file is an .xml file and includes a copy of the scan settings and plugin outputs. The .db file contains the .nessus file and the scan's KB, plugin Audit Trail, and any scan attachments.

Scanning Issues

Nessus scans can cause issues on sensitive networks and provide false positives, no results, or have an unfavorable impact on the network.

It is advised that it is always best to communicate with your client (or internal stakeholders if running a scan against your own network) on whether any sensitive/legacy hosts should be excluded from the scan or if any high priority/high availability hosts should be scanned separately, outside of regular business hours, or with different scan configurations to avoid potential issues.

Mitigating Issues

1. In the case one receive scan results showing either all ports open or no ports open, it may be as a result of firewalls present in that network, therefore we are advised to configure an Advanced Scan and disable the Ping the remote host option. This will stop the scan from using ICMP to verify that the host is "live" and instead proceed with the scan. Some firewalls may return an "ICMP Unreachable" message that Nessus will interpret as a live host and provide many false-positive informational findings.

2. In sensitive networks, we can use rate-limiting to minimize impact. For example, we can adjust Performance Options and modify Max Concurrent Checks Per Host if the target host is often under heavy load, such as a widely used web application. This will limit the number of plugins used concurrently against the host.

3. We should avoid scanning legacy systems and choose the option not to scan printers. From the previous section we saw that a vulnerable system can prompt printers to print large amount of useless papers rendering the machine unusable.

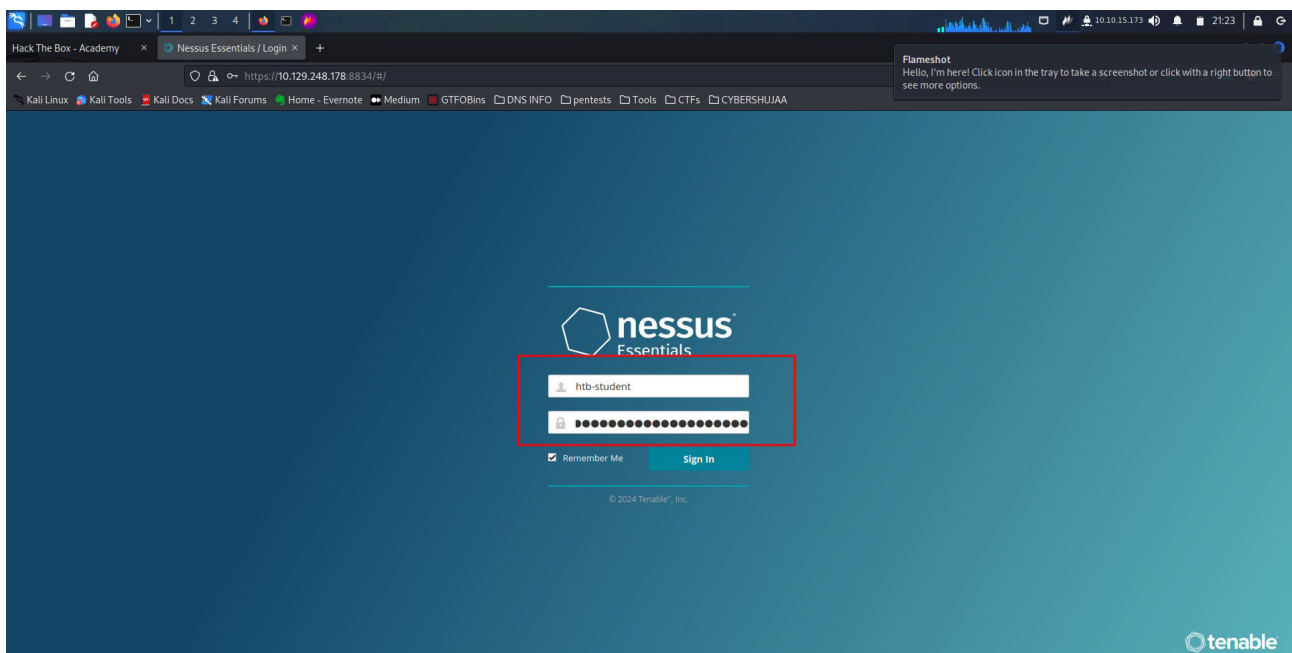
If a host is of particular concern, it should be left out of the target scope as Nessus does not have an option for an "exclusion list" of hosts within a CIDR range like we can do with tools like Nmap.

4. Unless specifically requested, we should never perform Denial of Service checks. We can ensure that these types of plugins are not used by always enabling the "safe checks" option when performing scans to avoid any network plugins that can have a negative impact on a target, such as crashing a network daemon.

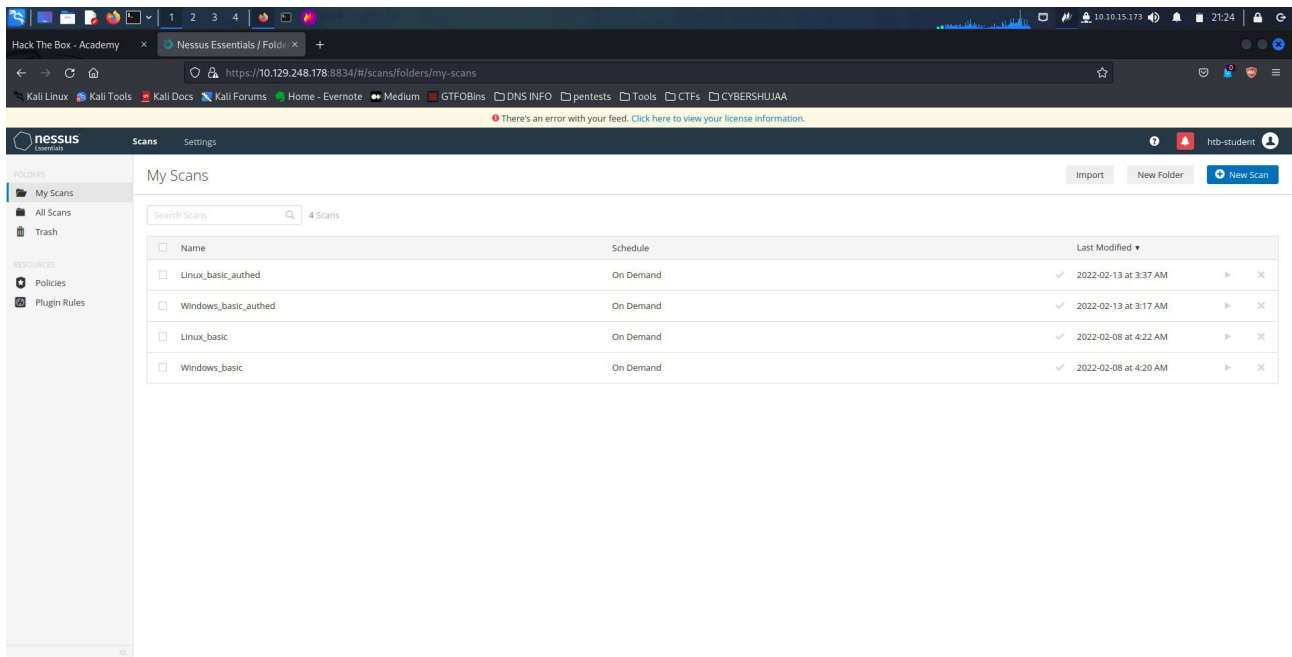
Questions

First was to login to the Nessus web Application using my spawning target and credentials given

Address: <https://10.129.248.178:8834> **Username:** htb-student **Pass:** HTB_@cademy_student!



Once I was in this was my first page to receive:

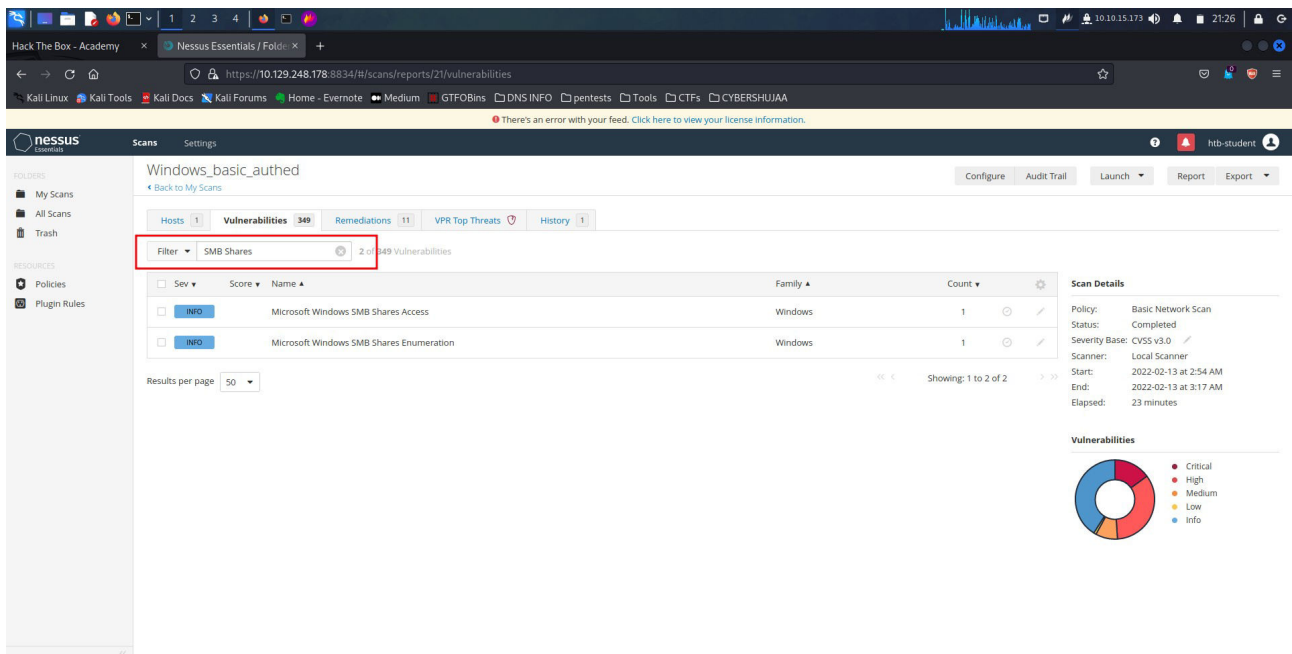


Next step was to answer the questions provided in this assessment.

What is the name of one of the accessible SMB shares from the authenticated Windows scan? (One word)

ANS: wsus

For faster navigation I used the filter tab to find SMB Shares, From the Windows SMB Shares Enumeration I was able to get the list of accessible shares.



All SMB Shares list:

The screenshot shows the Nessus Essentials interface for the 'Windows_basic_authed / Plugin #10395' scan. The 'Output' tab is selected, displaying the results of the SMB Shares Enumeration. The output text indicates that the scan was performed as an administrator and lists the available SMB shares: ADMIN\$, C\$, IPC\$, Private_Docs, and 172.16.16.100. The 172.16.16.100 share is highlighted with a red box. Below the output, a table shows the port (445 / tcp / cifs) and the host (172.16.16.100).

Windows_basic_authed / Plugin #10395

Back to Vulnerabilities

Hosts 1 Vulnerabilities 349 Remediations 11 VPR Top Threats History 1

INFO Microsoft Windows SMB Shares Enumeration

Description

By connecting to the remote host, Nessus was able to enumerate the network share names.

Output

Here are the SMB shares available on the remote host when logged in as administrator:

- ADMIN\$
- C\$
- IPC\$
- Private_Docs
- 172.16.16.100

Port Hosts

445 / tcp / cifs	172.16.16.100
------------------	---------------

Plugin Details

Severity: Info

ID: 10395

Version: 1.48

Type: local

Family: Windows

Published: May 9, 2000

Modified: February 1, 2022

Risk Information

Risk Factor: None

Vulnerability Information

Asset Inventory: True

What was the target for the authenticated scan?

ANS: 172.16.16.100

The first tab is the host, which shows the target that was used.

The screenshot shows the Nessus Essentials interface for the 'Windows_basic_authed' scan. The 'Hosts' tab is selected, displaying a list of hosts. The host '172.16.16.100' is highlighted with a red box. To the right of the host list, a bar chart shows the distribution of vulnerabilities: 67 Critical, 136 High, 40 Medium, and 266 Low. The 'Scan Details' section on the right provides information about the scan, including the policy (Basic Network Scan), status (Completed), severity base (CVSS v3.0), scanner (Local Scanner), start time (2022-02-13 at 2:54 AM), end time (2022-02-13 at 3:17 AM), and elapsed time (23 minutes). A donut chart shows the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Windows_basic_authed

Back to My Scans

Hosts 1 Vulnerabilities 349 Remediations 11 VPR Top Threats History 1

Filter Search Hosts 1 Host

<input type="checkbox"/> Host	Vulnerabilities
<input type="checkbox"/> 172.16.16.100	67 136 40 266

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: 2022-02-13 at 2:54 AM

End: 2022-02-13 at 3:17 AM

Elapsed: 23 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

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

ANS: 156032

The first scan result shows the highest criticality vulnerability.

The screenshot displays the Nessus Essentials interface for a scan named 'Windows_basic_authed'. The 'Vulnerabilities' tab is active, showing a list of 349 vulnerabilities. The first vulnerability, 'Apache Log4j Unsupported Version Detection', is highlighted with a red box and labeled 'Plugin ID: 156032'. The 'Scan Details' panel on the right shows the scan was completed on 2022-02-13 at 2:54 AM.

Sev	Score	Name	Family	Count
CRITICAL	10.0	Apache Log4j Unsupported Version Detection	Misc.	9
CRITICAL	10.0	Oracle Java JRE Unsupported Version Detection	Windows	1
CRITICAL	10.0	Oracle WebLogic Server Multiple Vulnerabilities (April 2017 CPU)	Misc.	1
CRITICAL	10.0	Oracle WebLogic Server Multiple Vulnerabilities (July 2017 CPU)	Misc.	1
CRITICAL	10.0	Unsupported Web Server Detection	Web Servers	1
CRITICAL	9.9	Oracle WebLogic Server Multiple Vulnerabilities (October 2017 CPU)	Misc.	1
CRITICAL	9.8	Apache Log4j 1.x Multiple Vulnerabilities	Misc.	9
CRITICAL	9.8	Jenkins LTS < 2.303.3 / Jenkins weekly < 2.319 Multiple Vulnerabilities	CGI abuses	1
CRITICAL	9.8	KB4022715: Windows 10 Version 1607 and Windows Server 2016 June 2017 Cumulative Update	Windows : Microsoft Bulletins	1
CRITICAL	9.8	KB4025339: Windows 10 Version 1607 and Windows Server 2016 July 2017 Cumulative Update	Windows : Microsoft Bulletins	1
CRITICAL	9.8	KB4041691: Windows 10 Version 1607 and Windows Server 2016 October 2017 Cumulative Update (KRACK)	Windows : Microsoft Bulletins	1
CRITICAL	9.8	KB4457131: Windows 10 Version 1607 and Windows Server 2016 September 2018 Security Update	Windows : Microsoft Bulletins	1

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

ANS: VNC Server Unauthenticated Access

Sev	Score	Name	Plugin ID: 26925	Family	Count
HIGH	7.5 *	VNC Server Unauthenticated Access		Misc.	1

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

ANS: 5900

The screenshot displays the Nessus Essentials interface for the vulnerability 'VNC Server Unauthenticated Access' (Plugin ID: 26925). The 'Description' section states that the VNC server installed on the remote host allows an attacker to connect to the remote host as no authentication is required to access this service. The 'Solution' section suggests disabling the No Authentication security type. The 'Output' section shows the port 5900/tcp on host 172.16.16.100.

Description
The VNC server installed on the remote host allows an attacker to connect to the remote host as no authentication is required to access this service.

Solution
Disable the No Authentication security type.

Output
No output recorded.

Port	Hosts
5900 / tcp / vnc	172.16.16.100

OpenVAS

OpenVAS has various scan configurations to choose from for scanning a network. We recommend only leveraging the ones below, as other options could cause system disruptions on a network:

Base: This scan configuration is meant to enumerate information about the host's status and operating system information. This scan configuration does not check for vulnerabilities.

Discovery: This scan configuration is meant to enumerate information about the system. The configuration identifies the host's services, hardware, accessible ports, and software being used on the system. This scan configuration also does not check for vulnerabilities.

Host Discovery: This scan configuration solely tests whether the host is alive and determines what devices are active on the network. This scan configuration does not check for vulnerabilities as well. OpenVAS leverages ping to identify if the host is alive.

System Discovery: This scan enumerates the target host further than the 'Discovery Scan' and attempts to identify the operating system and hardware associated with the host.

Full and fast: This configuration is recommended by OpenVAS as the safest option and leverages intelligence to use the best NVT checks for the host(s) based on the accessible ports.

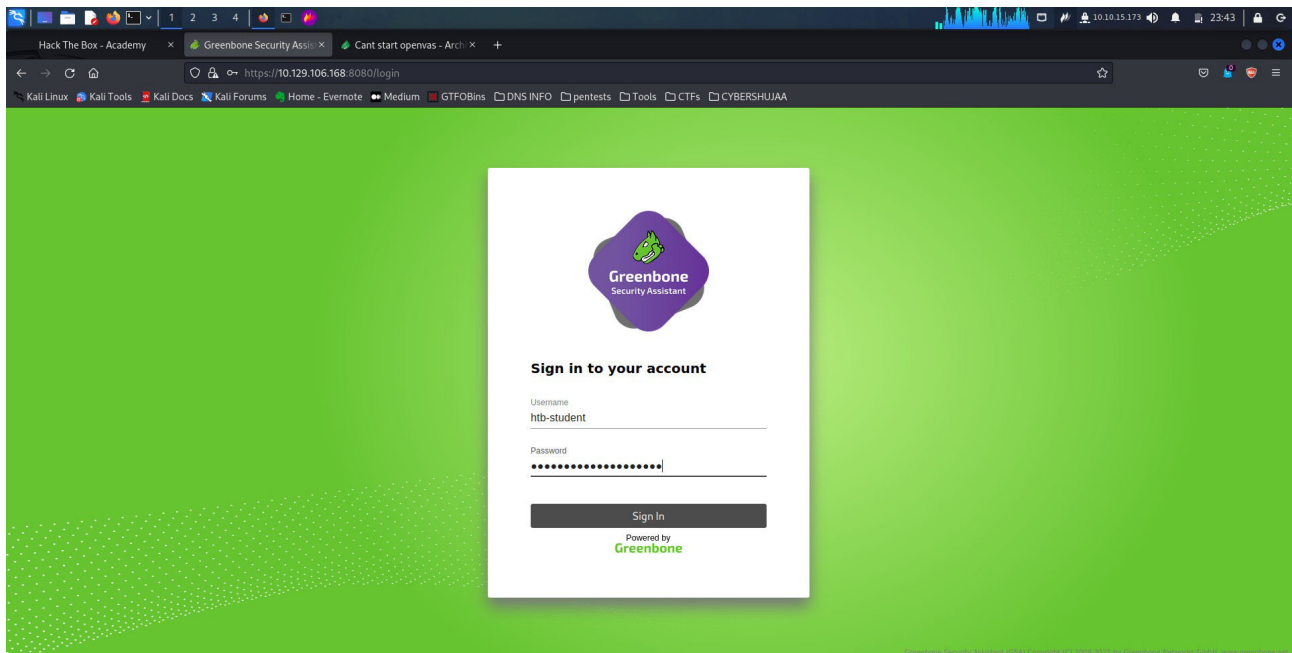
Questions

After a few events without luck, I kept refreshing my page as I understood the IP target host was still loading to be up, but finally I was able to get a login page in the end.

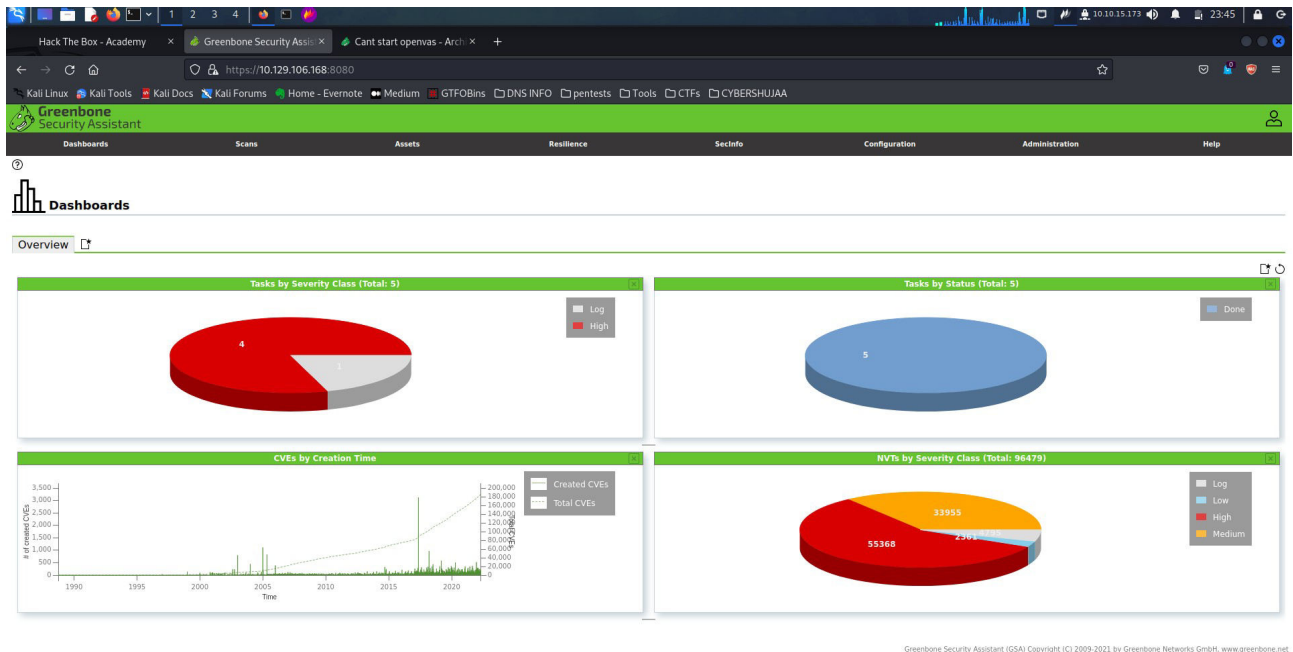
First i needed to login using credentials provided

Address used: <https://10.129.106.168:8080/>

Username: htb-student **Pass:** HTB_@cademy_student!



First page after login looks like this:-

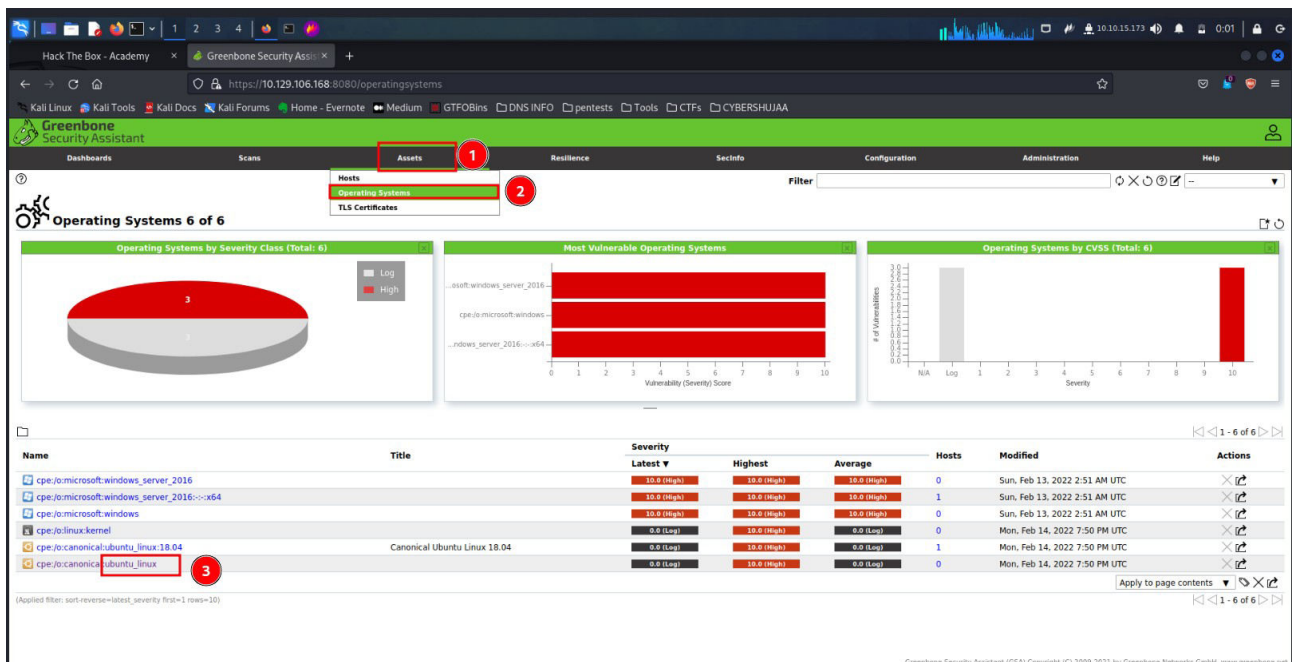


Now that we had an openVAS Scan next was to answer the questions.

What type of operating system is the Linux host running? (one word)

ANS: Ubuntu

To answer this I had to open the Assets tab, choose the operating system option and since we are looking for a Linux host, Ubuntu was the only option there was.



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

ANS: Anonymous FTP Login Reporting

To find this I looked on the Linux host vulnerabilities tab and came across this FTP vulnerability.

The screenshot shows the Greenbone Security Assistant interface. The top navigation bar includes tabs for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. The main content area displays the details of a vulnerability titled "Anonymous FTP Login Reporting".

Account: "ftp":
drwxr-xr-x 2 ftp ftp 4096 Feb 07 01:10 pub

Insight
A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.
Remark: NIST don't see 'configuration issues' as software flaws so the referenced CVE has a severity of 0.0. The severity of this VT has been raised by Greenbone to still report a configuration issue on the target.

Detection Method
Details: **Anonymous FTP Login Reporting** OID: 1.3.6.1.4.1.25623.1.0.900600
Version used: 2021-10-20T00:00:29Z

Impact
Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:
- gain access to sensitive files
- upload or delete files.

Solution
Solution Type: Mitigation
If you do not want to share files, you should disable anonymous logins.

References
CVE CVE-1999-0497

Apache HTTP Server Detection Consolidation	0.0 (Log)	80 %	172.16.16.160	general/tcp	Sun, Feb 13, 2022 1:09 AM UTC
Apache Tomcat Detection Consolidation	0.0 (Log)	80 %	172.16.16.160	general/tcp	Sun, Feb 13, 2022 1:09 AM UTC
CGI Scanning Consolidation	0.0 (Log)	80 %	172.16.16.160	80/tcp	Sun, Feb 13, 2022 1:21 AM UTC

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

What is the IP of the Linux host targeted for the scan?

ANS: 172.16.16.160

To find this I clicked on the tab Assets > Hosts which gave me two IP addresses (172.16.16.100 and 172.16.16.160), but only one was indicated as the targeted host.

The screenshot shows the Greenbone Security Assistant interface with the "Assets" tab selected and the "Hosts" sub-tab active. Two hosts are listed:

Name	Hostname	IP Address	OS	Severity	Modified	Actions
172.16.16.100		172.16.16.100		10.0 (High)	Sun, Feb 13, 2022 2:51 AM UTC	
172.16.16.160		172.16.16.160		0.0 (Log)	Sat, Mar 26, 2022 6:34 PM UTC	

Latest Identifiers

Name	Value	Created	Source
OS	cpe:/microsoft:windows_server_2016-...x64	Sun, Feb 13, 2022 2:51 AM UTC	Report d0de5c80-8ea9-456c-b91d-384f28c56b4d (NVT 1.3.6.1.4.1.25623.1.0.103621)
OS	cpe:/microsoft:windows_server_2016	Sun, Feb 13, 2022 2:51 AM UTC	Report d0de5c80-8ea9-456c-b91d-384f28c56b4d (NVT 1.3.6.1.4.1.25623.1.0.102011)
OS	cpe:/microsoft:windows	Sun, Feb 13, 2022 2:51 AM UTC	Report d0de5c80-8ea9-456c-b91d-384f28c56b4d (NVT 1.3.6.1.4.1.25623.1.0.111067)
OS	cpe:/microsoft:windows	Sun, Feb 13, 2022 2:51 AM UTC	Report d0de5c80-8ea9-456c-b91d-384f28c56b4d (NVT 1.3.6.1.4.1.25623.1.0.105355)
OS	cpe:/microsoft:windows	Sun, Feb 13, 2022 2:51 AM UTC	Report d0de5c80-8ea9-456c-b91d-384f28c56b4d (NVT 1.3.6.1.4.1.25623.1.0.108044)
ip	172.16.16.100	Sun, Feb 13, 2022 2:51 AM UTC	Report d0de5c80-8ea9-456c-b91d-384f28c56b4d (Target Host)

Latest Identifiers

Name	Value	Created	Source
ip	172.16.16.160	Sat, Mar 26, 2022 6:34 PM UTC	Report 4df92cf4-974c-4e65-b8e5-206285ee9720 (Target Host)

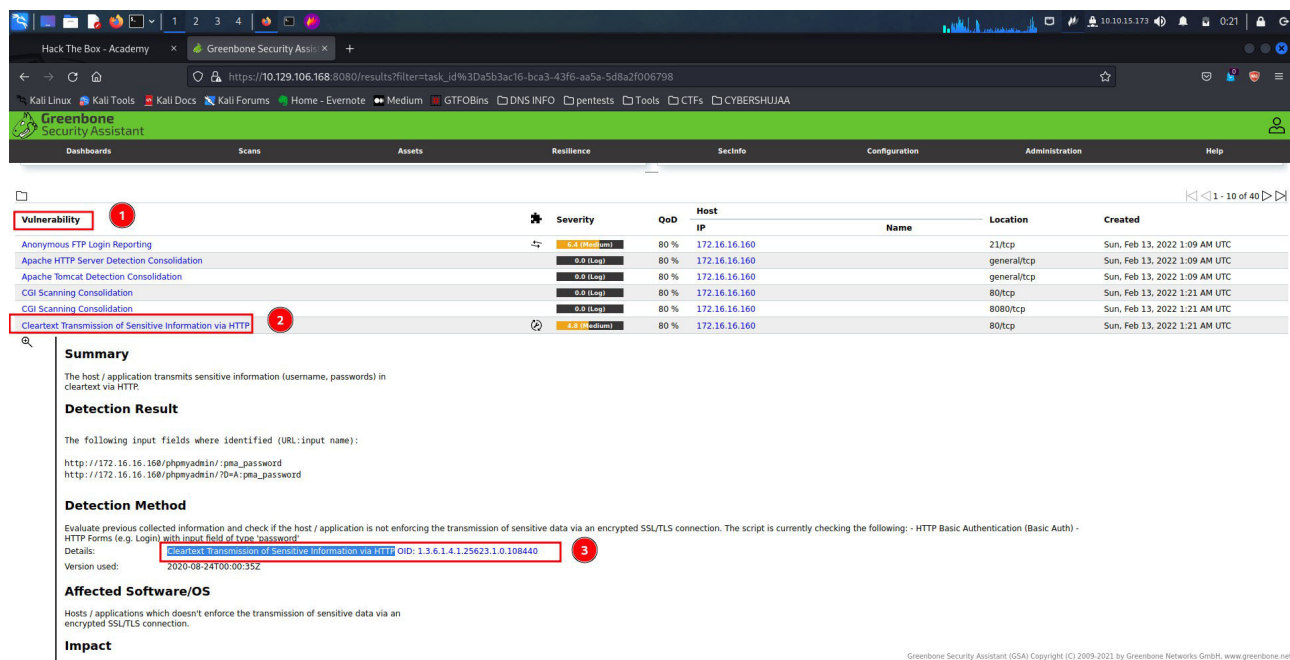
Apply to page contents

Greenbone Security Assistant (GSA) Copyright (C) 2009-2021 by Greenbone Networks GmbH, www.greenbone.net

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

ANS: Cleartext Transmission of Sensitive Information via HTTP

To find this Vulnerability I clicked on the Linux_basics then searched for the vulnerabilities tab which after clicking it it displayed a number of vulnerabilities one of it being involved with the HTTP server.



The screenshot shows the Greenbone Security Assistant (GSA) interface. The 'Vulnerability' tab is selected, and a list of vulnerabilities is displayed. The vulnerability 'Cleartext Transmission of Sensitive Information via HTTP' is highlighted with a red box and a red circle labeled '2'. The 'Summary' section for this vulnerability is expanded, showing details about the host, detection result, and method. A red box and red circle labeled '3' highlight the 'Details' section, which mentions the 'HTTP Basic Authentication (Basic Auth)' and the 'password' field.

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
Anonymous FTP Login Reporting	0.0 (Low)	80 %	172.16.16.160	21/tcp	general/tcp	Sun, Feb 13, 2022 1:09 AM UTC
Apache HTTP Server Detection Consolidation	0.0 (Log)	80 %	172.16.16.160	general/tcp	general/tcp	Sun, Feb 13, 2022 1:09 AM UTC
Apache Tomcat Detection Consolidation	0.0 (Log)	80 %	172.16.16.160	80/tcp	80/tcp	Sun, Feb 13, 2022 1:21 AM UTC
CGI Scanning Consolidation	0.0 (Log)	80 %	172.16.16.160	8080/tcp	8080/tcp	Sun, Feb 13, 2022 1:21 AM UTC
Cleartext Transmission of Sensitive Information via HTTP	0.4 (Medium)	80 %	172.16.16.160	80/tcp	80/tcp	Sun, Feb 13, 2022 1:21 AM UTC

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Detection Result
The following input fields were identified (URL:input name):
http://172.16.16.160/phpmyadmin/:pma_password
http://172.16.16.160/phpmyadmin/?db=pma_password

Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection. The script is currently checking the following: - HTTP Basic Authentication (Basic Auth) - HTTP Forms (e.g. Login) with input field of type "password".
Details: [https://www.greenbone.net/vulnerability/CVE-2019-11340](#) OID: 1.3.6.1.4.1.25623.1.0.108440
Version used: 2020-08-24T00:00:35Z

Affected Software/OS
Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Impact

Reporting

This was the last section for this module and it talked about writing a report after carrying out a target scan.

This section indicated a strong report should consist of the following sections:-

1. Executive Summary - The Executive Summary of a vulnerability assessment report is intended to be readable by an executive who needs a high-level overview of the details and what is the most important items to fix immediately, depending on the severity. This section allows an executive to look at the report and prioritize remediation based on the summary.
2. Overview of Assessment - The Overview of the Assessment should include any methodology leveraged during the assessment. The methodology should detail the execution of the assessment during the testing period, such as discussing the process and tools used for the project such as Nessus and openVAS.
3. Scope - The Scope and Duration section of the report should include everything the client authorized for the assessment, including the target scope and the testing period.
4. Vulnerabilities and Recommendations - The Vulnerabilities and Recommendations section should detail the findings discovered during the vulnerability assessment once you've eliminated any false positives by manually testing them. It is best to group findings that relate to each other based on the type of issues or their severity.

For every issue found it is supposed to be reported with the following elements:

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

Conclusion.

In conclusion, Hack The Box Academy's Vulnerability Assessment module has provided me with valuable resources to enhance my skills in identifying and addressing security vulnerabilities. By providing hands-on experiences, practical scenarios and comprehensive learning materials, the module has equipped me with the knowledge and tools necessary to conduct effective vulnerability assessments.

Am quite convinced that the practical nature of the module is likely to be beneficial in preparing me for real-world cyberneticist challenges, contributing to my overall skills in securing systems and networks. With the new tools learnt that is Nessus and openVAS I can proudly say I have added a skill in my course of learning.

Thank You.