

VULNERABILITY ASSESSTMENT

1.1 Vulnerability Assessment

Vulnerability assessments is about looking for vulnerabilities in networks without simulating cyber-attacks. It can be based on various security standards, such as GDPR compliance or OWASP web application security standards. It's like going through a checklist.

1.2 Nessus Scan

Nessus provides separate templates for scanners and agents, depending on which sensor you want to use for scanning: scanner template, web App template and agent template,

Scanner Template

Discovery scans to see what hosts are on a network, and associated information such as IP address, FQDN, operating systems, and open ports, if available.

Includes, Host discovery, Attack surface Discovery.

Vulnerability scan templates allow you to scan your network for a specific vulnerability or group of vulnerabilities. Includes, Basic Network Scan, Advanced Scan, Malware Scan,

Compliance/configuration scan templates to check whether host configurations are compliant with various industry standards. Includes, specific CVEs and audit & compliance standards, Audit Cloud Infrastructure, Internal PCI Network Scan.

Web App template

Uses vulnerability scans and they include, API, Web App Config Audit, Quick Scans, SSL TLS, Log4Shell.

Agent template

Uses both vulnerability scans which includes Basic Agent Scan, Advanced Agent Scan, Agent Log4Shell, Malware Scan. And Compliance Scans which include Policy Compliance Auditing, SCAP and OVAL Auditing.

1.3 Advanced Settings

We can configure Nessus with advanced settings in its scans, like scan policies, plugins, and credentials.

Scan policies 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. Thus, the ability to create targeted scans for any number of scenarios.

Nessus plugins contain information such as the vulnerability name, impact, remediation, and a way to test for the presence of a particular issue.

We can also configure an authenticated scans with the use of the credentials section when configuring a new scan.

1.4 Nessus Skills Assessment

Scenario

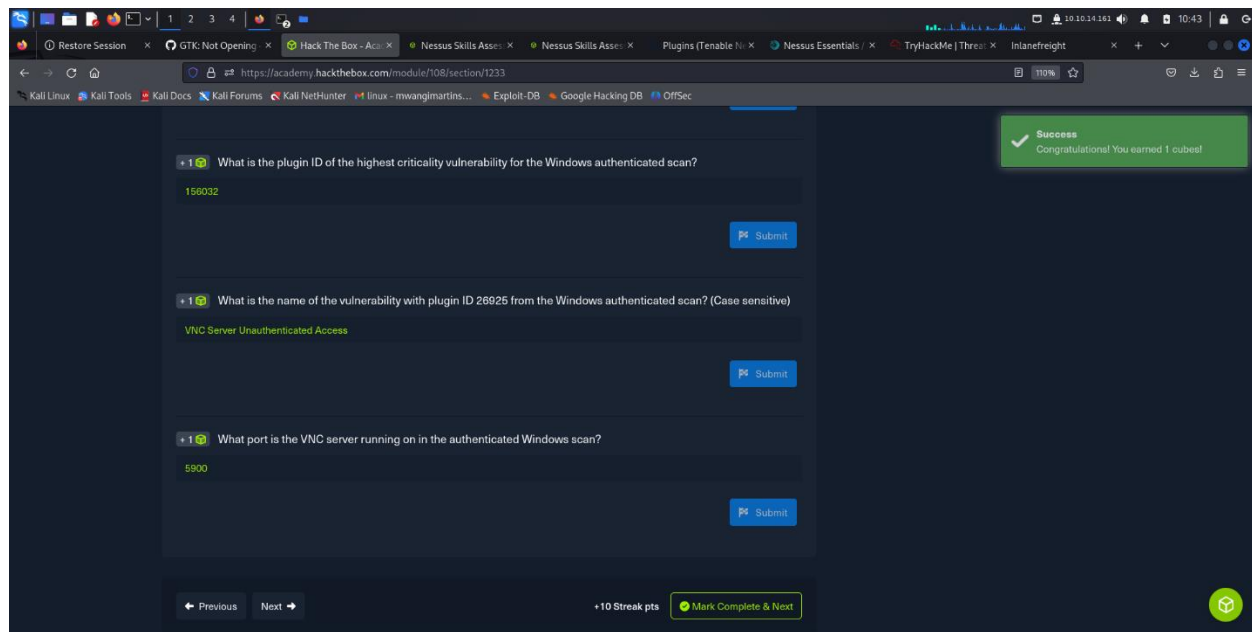
You have been contracted by the company InlaneFreight to perform an internal vulnerability assessment against one of their servers. They have asked for a cursory assessment to be performed to identify any significant vulnerabilities as they do not have the budget for a full-scale penetration test this year. The results of this vulnerability assessment may enable the CISO to push for additional funding from the Board of Directors to perform more in-depth security testing.

The target server is a Windows Server host used as a development server.

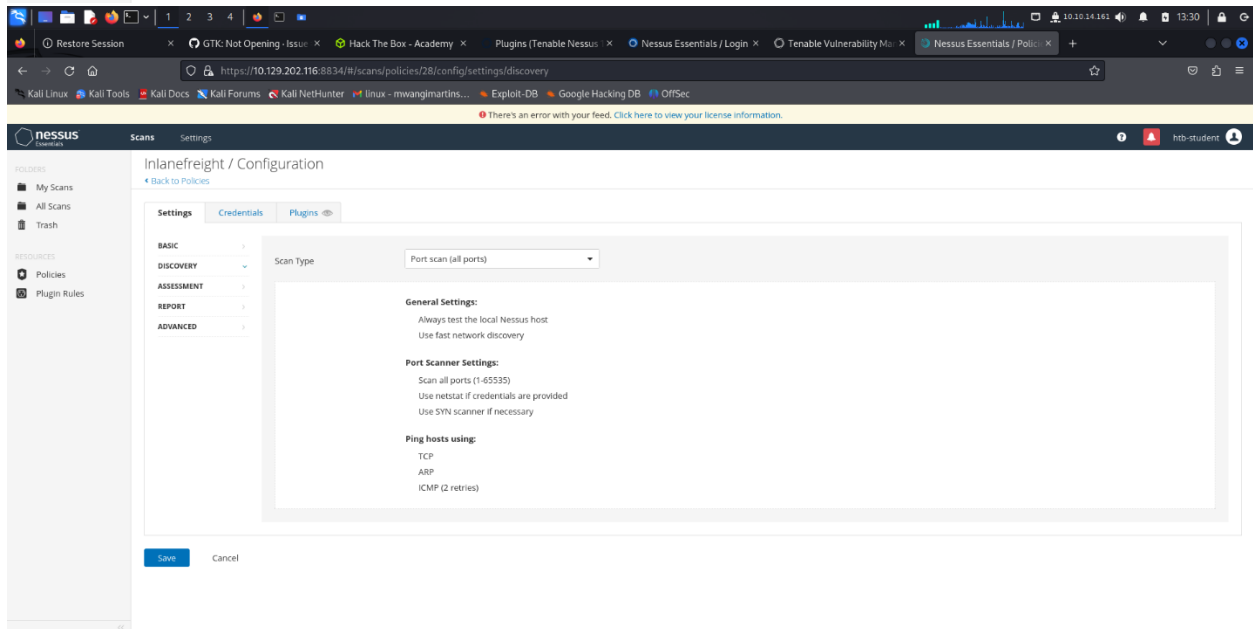
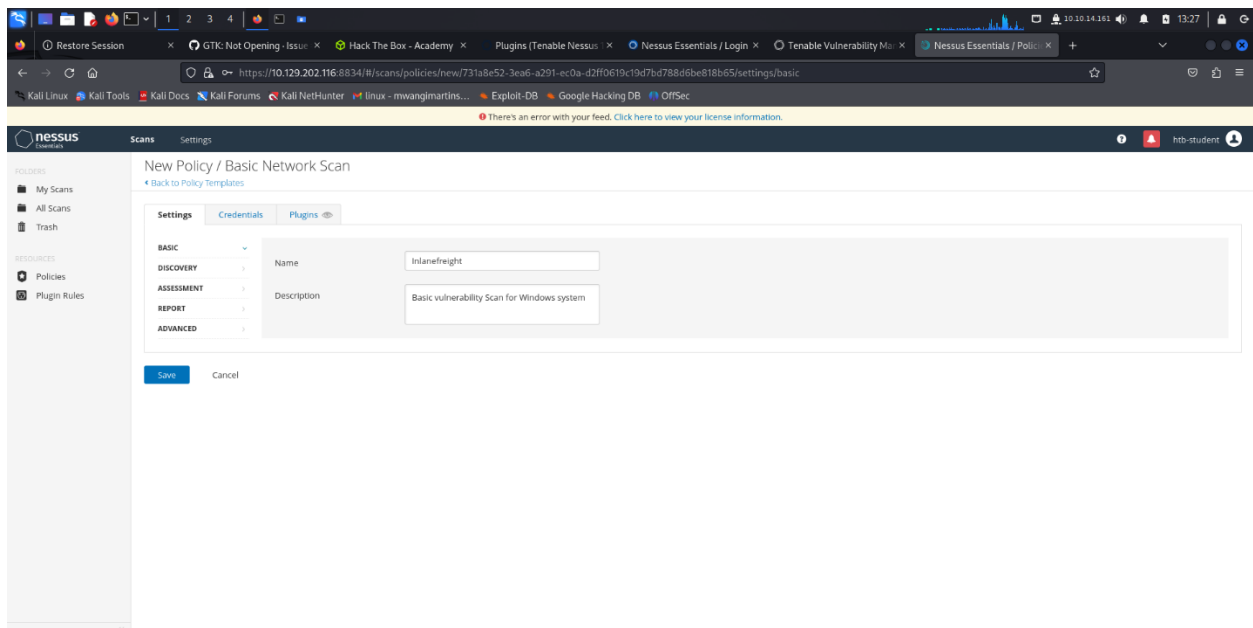
Questions

The screenshot shows a web browser window with the URL <https://academy.hackthebox.com/module/108/section/1233>. The page is titled "Questions" and contains the following information:

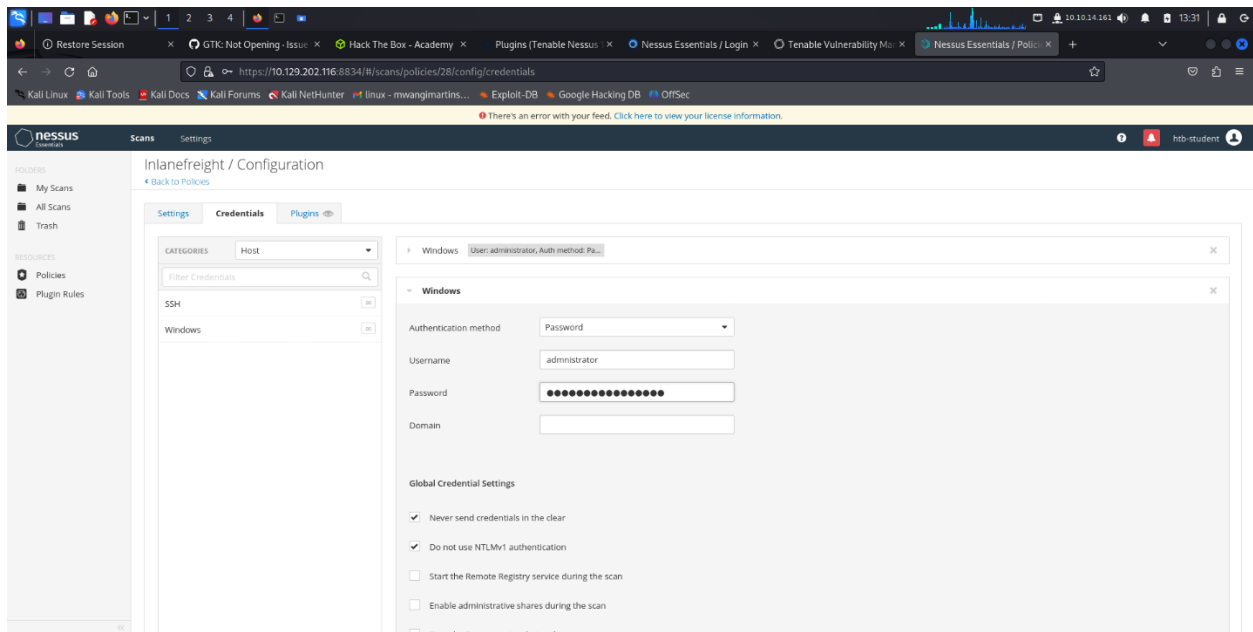
- A green success message: "Success Congratulations! You earned 1 cube!"
- A "Download VPN Connection File" button.
- Target(s): 10.129.202.116 (ACADEMY-VA-SCAN01)
- Life Left: 80 minute(s) + Terminate X
- Authentication instructions: Authenticate to 10.129.202.116 (ACADEMY-VA-SCAN01) with user "htb-student" and password "HTB_@cademy_student!"
- Question 1: "What is the name of one of the accessible SMB shares from the authenticated Windows scan? (One word)"
Answer: wslus
- Question 2: "What was the target for the authenticated scan?"
Answer: 172.16.16.100



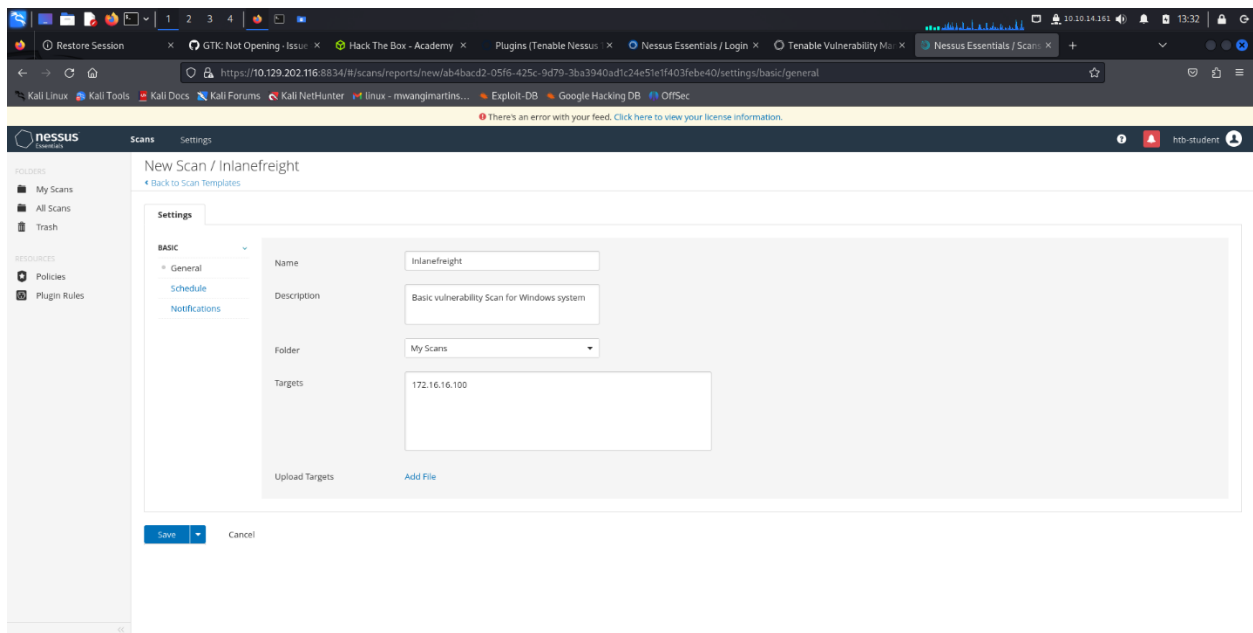
After successful login, I created a policy that suited my target scan with using The Basic Network Scan, to specify the scope of the scan, By navigating to the Policies section, I created my new policy, with giving it a name “Inlanefreight” and a description, setting up to scan all ports.

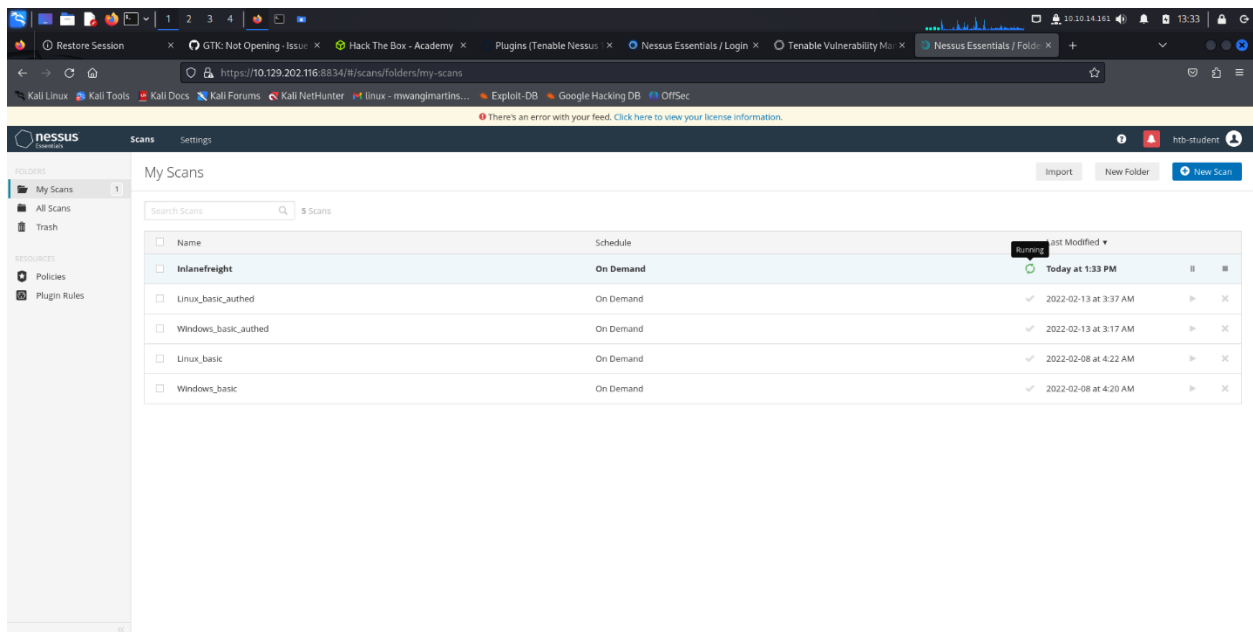


This how to set up a authenticated scan,

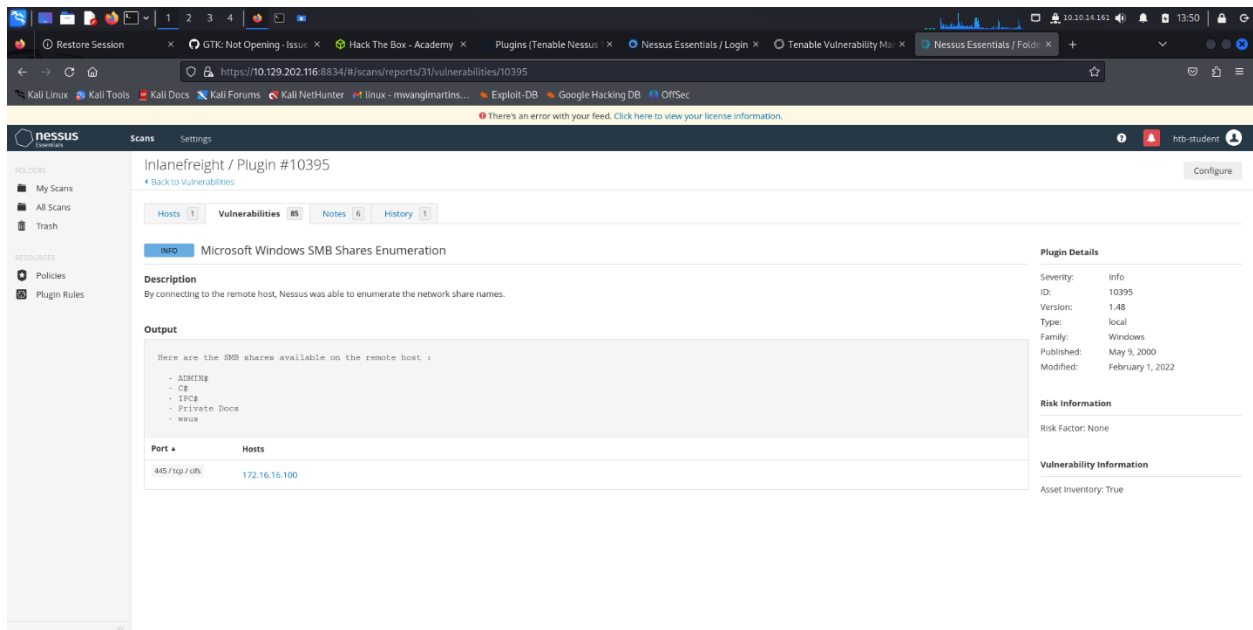


Created a new scan, with my target,





filtered the results based on SMB share to find the shares that can be accesses with any credentials,



From the results I found the highest vulnerability as they were ranked according to Score 10 being highest and critical,

CRITICAL Apache Log4j Unsupported Version Detection

Description
According to its self-reported version number, the installation of Apache Log4j on the remote host is no longer supported. Log4j reached its end of life prior to 2016.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution
Upgrade to a version of Apache Log4j that is currently supported.

Upgrading to the latest versions for Apache Log4j is highly recommended as intermediate versions / patches have known high severity vulnerabilities and the vendor is updating their advisories often as new research and knowledge about the impact of Log4j is discovered. Refer to <https://logging.apache.org/log4j/2.x/security.html> for the latest versions.

See Also
<http://www.nessus.org/u/59f655a2>

Output

Path	Installed version
C:\Oracle\Middleware\wserver_10.3\examples\server\examples\src\examples\webapp\pubsub\stock\stockBar\APP-INF\lib\log4j-1.2.15.jar	1.2.15

Plugin Details

Severity: Critical
ID: 156032
Version: 1.2
Type: local
Family: Misc.
Published: December 13, 2021
Modified: December 19, 2021

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:CC/H/I/HA/H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CPE: cpe:/a:apache:log4j
Unsupported by vendor: true

Decided to generate a report with .html, with the table of contents being vulnerability by plugins, This made it easy to locate the vulnerability with this plugin ID 26925

Report generated by nessus™

Inlanefreight

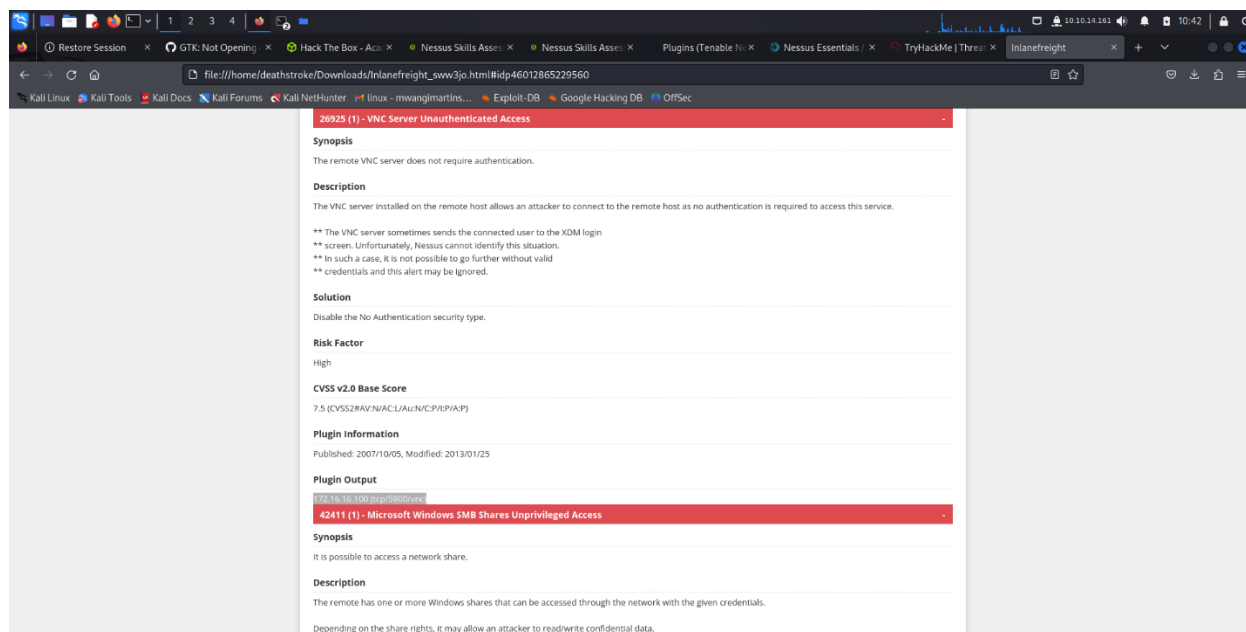
Wed, 16 Oct 2024 07:30:26 GMT+0000

TABLE OF CONTENTS

Vulnerabilities by Plugin

- 34460 (1) - Unsupported Web Server Detection
- 87071 (1) - Oracle WebLogic Java Object Deserialization RCE
- 80709 (1) - Oracle WebLogic Server Java Object Deserialization RCE (April 2016 CPU)
- 82606 (1) - Oracle WebLogic Server Java Object Deserialization RCE (July 2016 CPU)
- 84511 (1) - Oracle WebLogic Server Java Object Deserialization RCE (October 2016 CPU)
- 96803 (1) - Oracle WebLogic Server RMI Connect-Back Deserialization RCE (January 2017 CPU)
- 109429 (1) - Oracle WebLogic Server Deserialization RCE (CVE-2018-2628)
- 111665 (1) - Oracle WebLogic Server Deserialization RCE (CVE-2018-2893)
- 126262 (1) - Oracle WebLogic Server Deserialization RCE (CVE-2019-2729)
- 26920 (1) - Microsoft Windows SMB NULL Session Authentication
- 26925 (1) - VNC Server Unauthenticated Access
- 42411 (1) - Microsoft Windows SMB Shares Unprivileged Access
- 42873 (1) - SSL Medium Strength Cipher Suites Supported (SWEET32)
- 49070 (1) - Splunk Free Detection
- 97833 (1) - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannanCry) (EternalRocks) (Petya) (uncredentialed check)
- 100464 (1) - Microsoft Windows SMBv1 Multiple Vulnerabilities
- 103876 (1) - Microsoft Windows SMB Server (2017-10) Multiple Vulnerabilities (uncredentialed check)

From the same report found the port Number that VNC server was running on



1.5 OpenVAS Scan

Before setting up any scans, it is best to configure the targets for the scan by navigating to configurations tabs and target options.

Authenticated scan leverages a high privileged user such as root or Administrator depending on the permission level for the user.

OpenVAS has various scan configurations to choose from for scanning a network such as;

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

Discovery scan configuration to enumerate information about the system. It identifies the host's services, hardware, accessible ports, and software being used on the system. Does not check for vulnerabilities.

Host Discovery scan configuration solely tests whether the host is alive and determines what devices are active on the network. does not check for vulnerabilities.

System Discovery 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 scan is the safest option and leverages intelligence to use the best NVT checks for the host(s) based on the accessible ports.

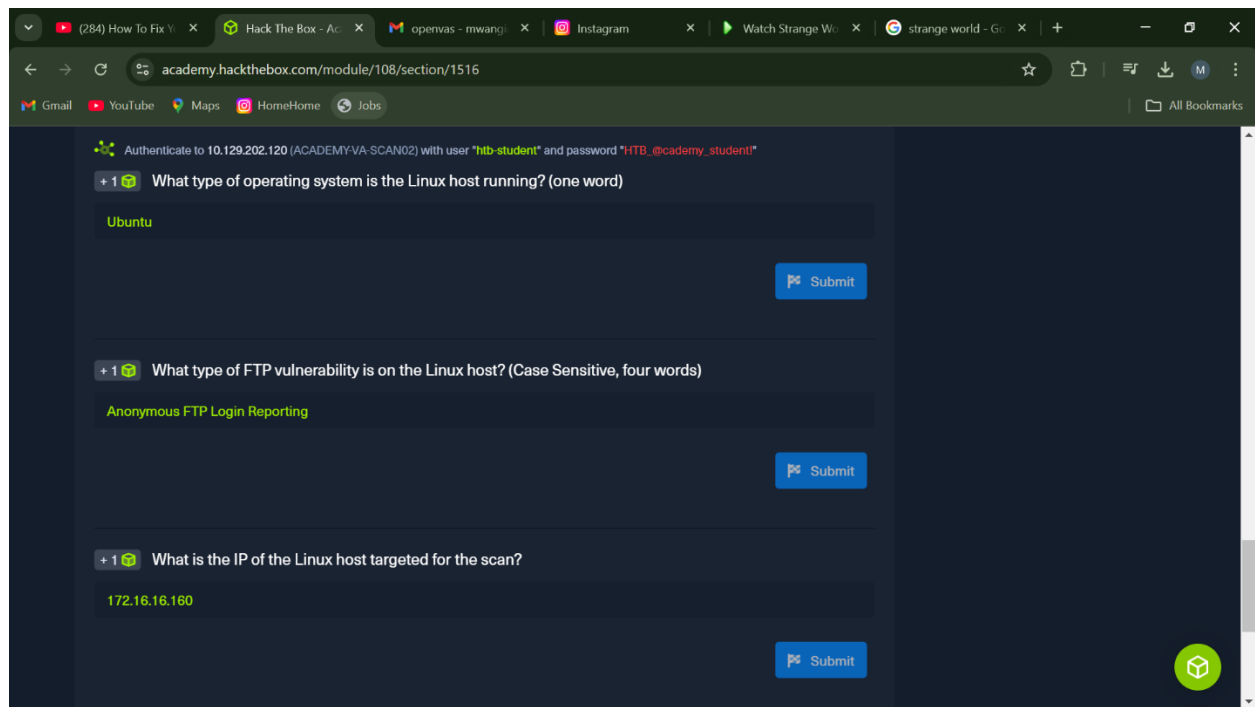
1.6 OpenVAS Skills Assessment

Scenario

You have been contracted by the company InlaneFreight to perform an internal vulnerability assessment against one of their servers. They have asked for a cursory assessment to be performed to identify any significant vulnerabilities as they do not have the budget for a full-scale penetration test this year. The results of this vulnerability assessment may enable the CISO to push for additional funding from the Board of Directors to perform more in-depth security testing.

The target server is a Linux Server host.

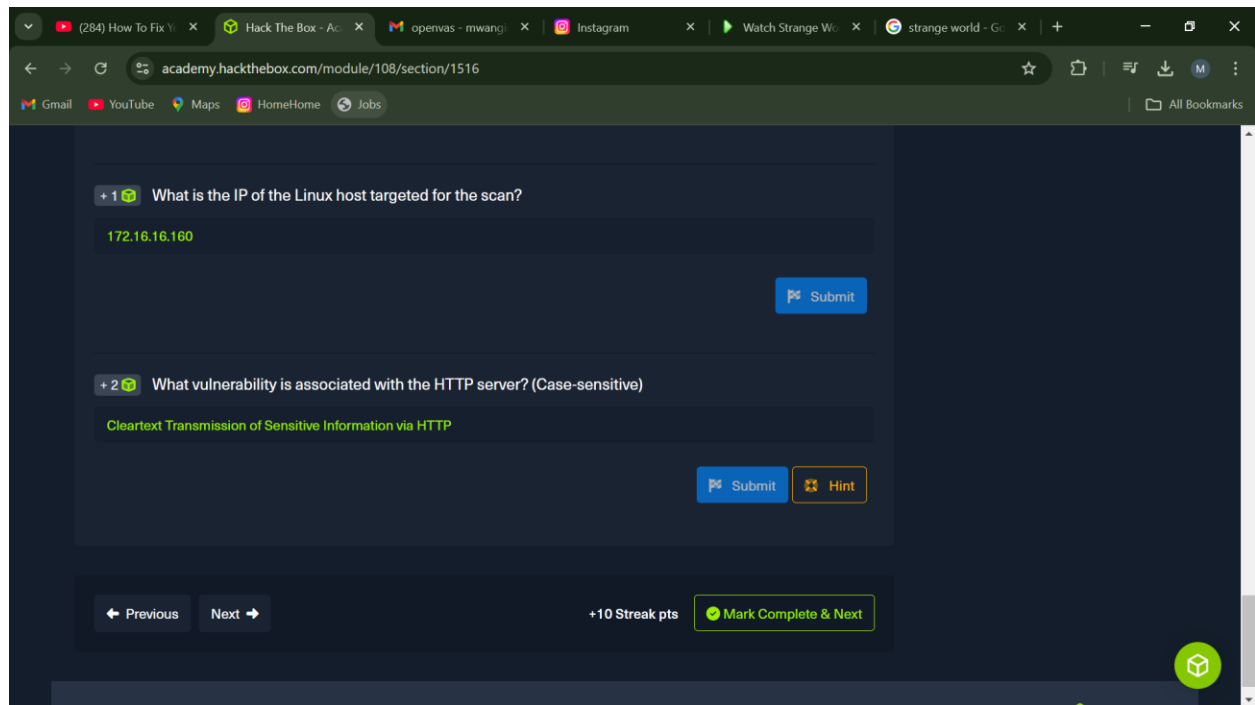
Questions



The screenshot shows a web browser window with multiple tabs. The active tab is 'Hack The Box - Academy' with the URL 'academy.hackthebox.com/module/108/section/1516'. The page content is a dark-themed interface with a header bar containing navigation links like 'Gmail', 'YouTube', 'Maps', 'HomeHome', and 'Jobs'. Below the header, there is a green banner with the text: 'Authenticate to 10.129.202.120 (ACADEMY-VA-SCAN02) with user "hdb-student" and password "HTB_@cademy_student"'. The main content area contains three questions, each with a '+1' icon and a 'Submit' button:

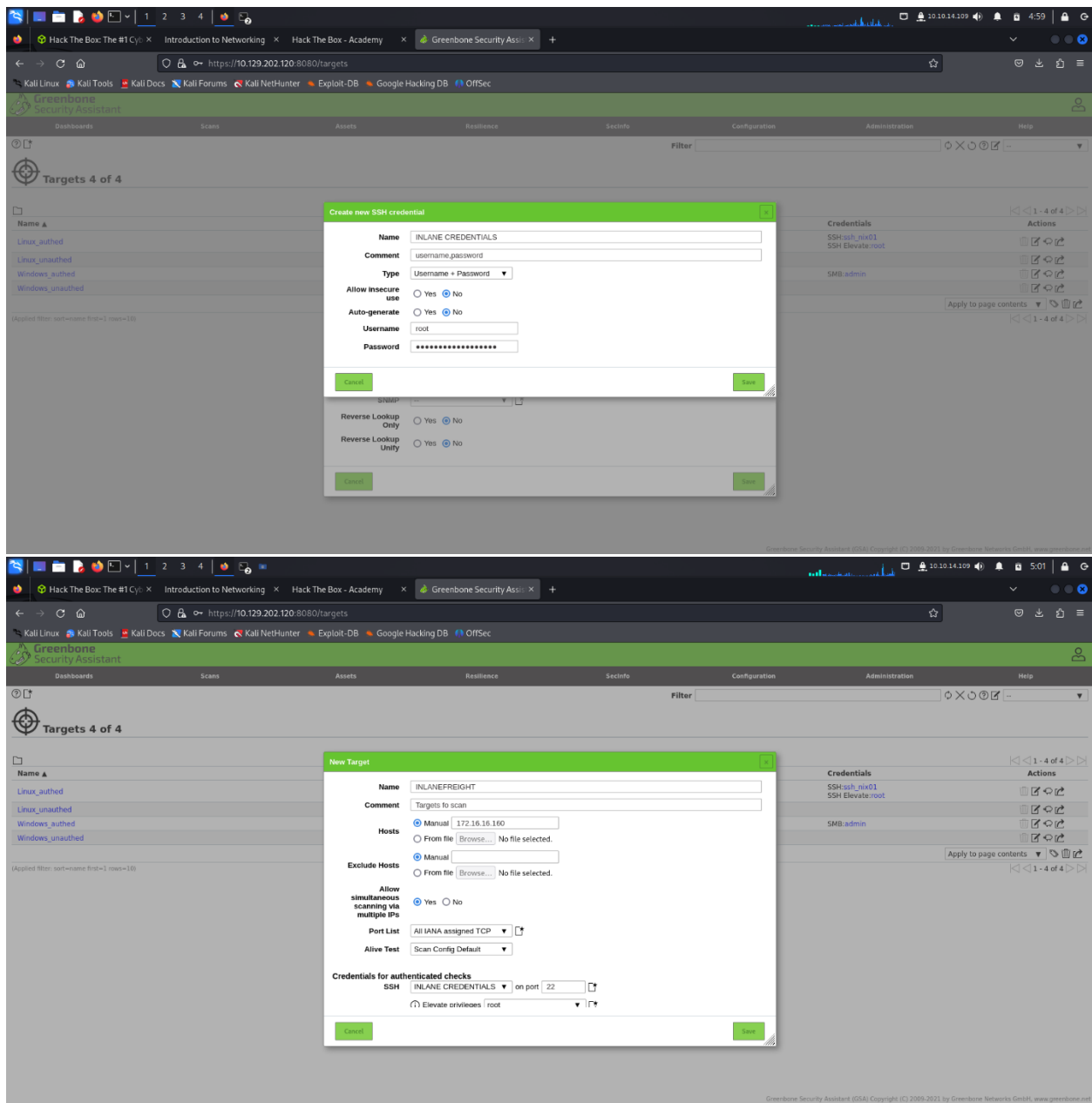
- Question 1: 'What type of operating system is the Linux host running? (one word)'. The answer 'Ubuntu' is entered in the text field.
- Question 2: 'What type of FTP vulnerability is on the Linux host? (Case Sensitive, four words)'. The answer 'Anonymous FTP Login Reporting' is entered in the text field.
- Question 3: 'What is the IP of the Linux host targeted for the scan?'. The answer '172.16.16.160' is entered in the text field.

A green cube icon is visible in the bottom right corner of the page.

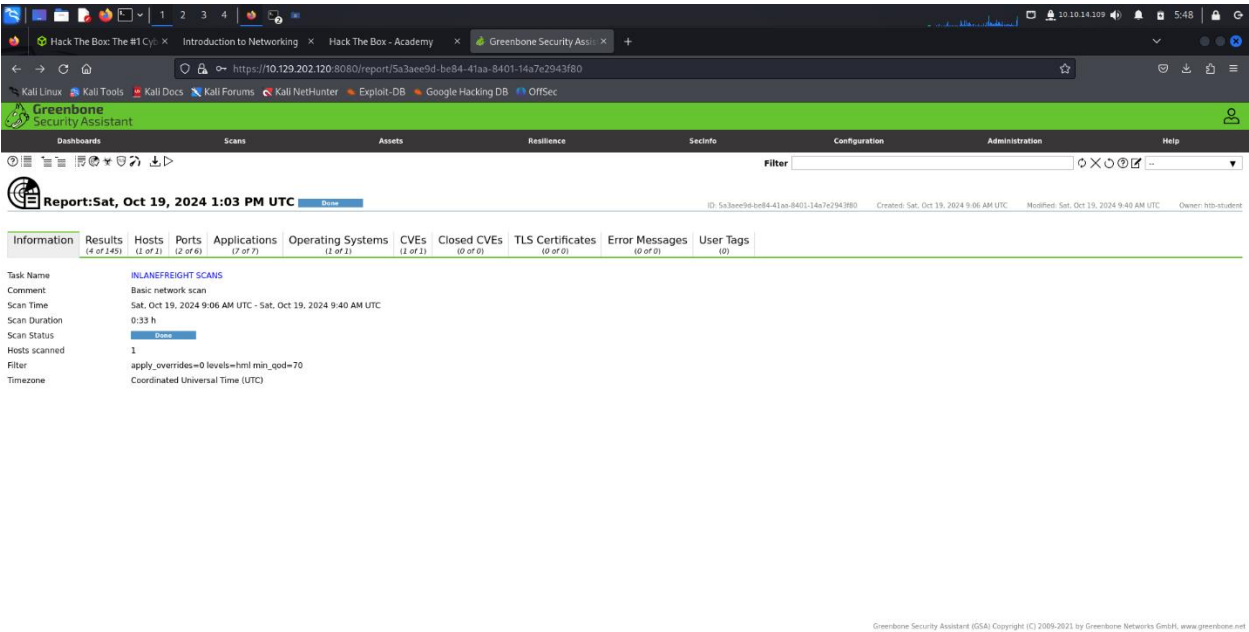


Started off by login to the OpenVAS with credentials provided.

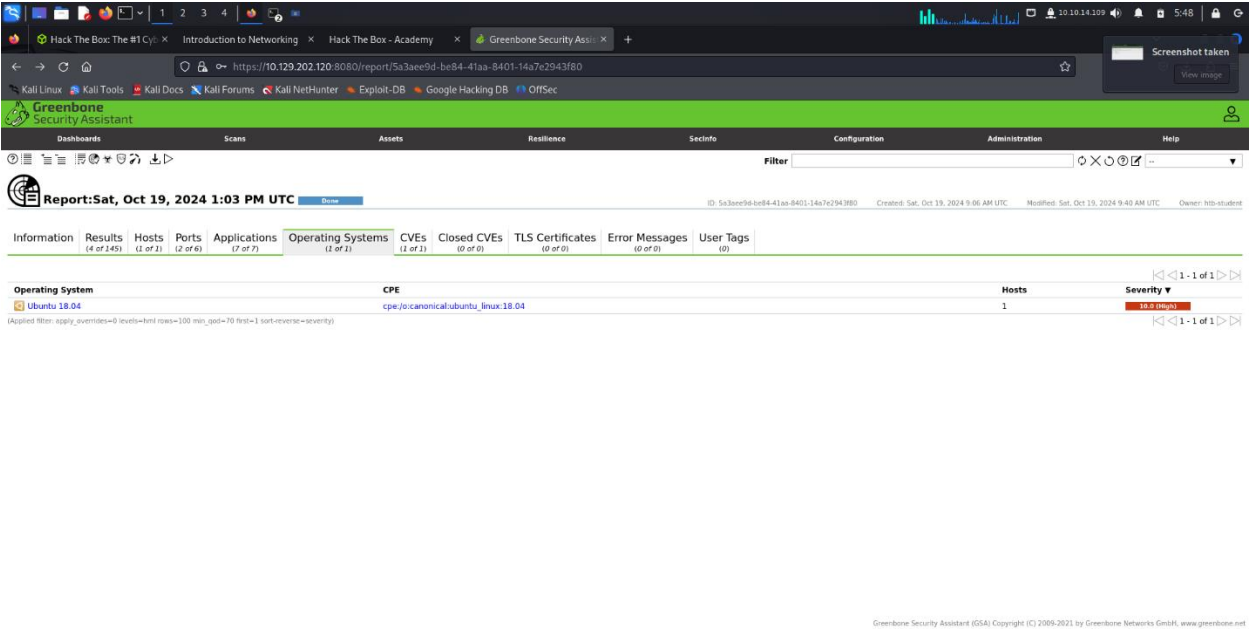
Continued to set up an authenticated scan with Username and a password, and created a target which was going to be scanned and including the credentials which have root access to retrieve more information about system,



This was the results upon completion of the scan,



From the results found the OS running, Ubuntu



From the results found the FTP vulnerability to be anonymous Login, Can be exploited by just login to ftp server without any credentials,

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

Summary
Reports if the remote FTP Server allows anonymous logins.

Detection Result
It was possible to login to the remote FTP service with the following anonymous account(s):
anonymous:anonymous@example.com
ftp:anonymous@example.com
Here are the contents of the remote FTP directory listing:
Account "anonymous":
drwxr-xr-x 2 ftp ftp 4096 Feb 07 2022 pub
Account "ftp":
drwxr-xr-x 2 ftp ftp 4096 Feb 07 2022 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 added 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

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

From the results found the HTTP server vulnerability which was cleartext transmission, which can be exploited with Man-In-the-Middle Attack,

The screenshot shows the Greenbone Security Assistant (GSA) interface. The top navigation bar includes tabs for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. The main content area displays the results of a scan titled "Cleartext Transmission of Sensitive Information via HTTP".

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/:pea_password
http://172.16.16.160/phpmyadmin/:pea_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: Cleartext Transmission of Sensitive Information via HTTP OID: 1.3.6.1.4.1.25623.1.0.108440
Version used: 2020-08-24T00:00:35Z

Affected Software/OS
Note: / application which doesn't enforce the transmission of sensitive data via an

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