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.

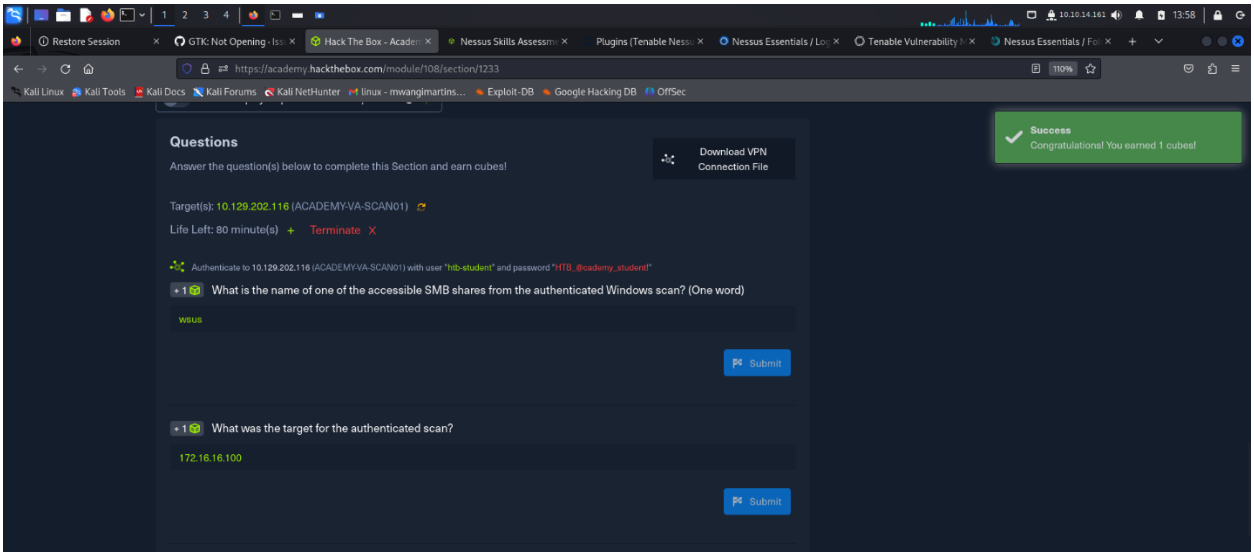
1.4 Nessus Skills Assessment

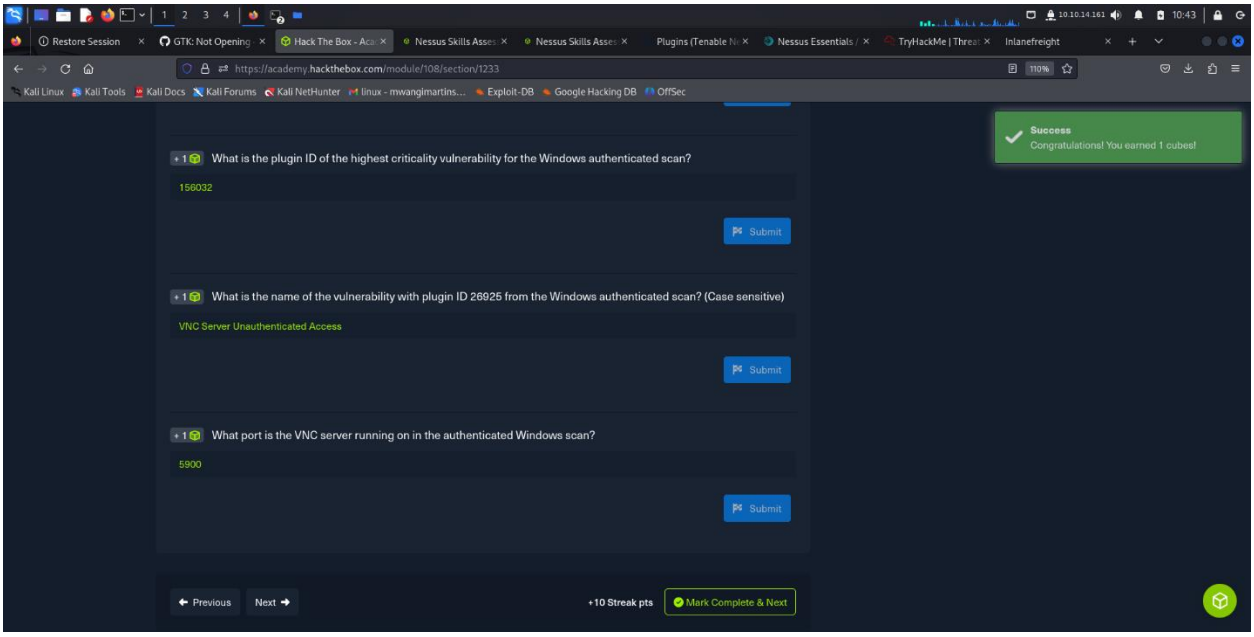
Scenario

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.

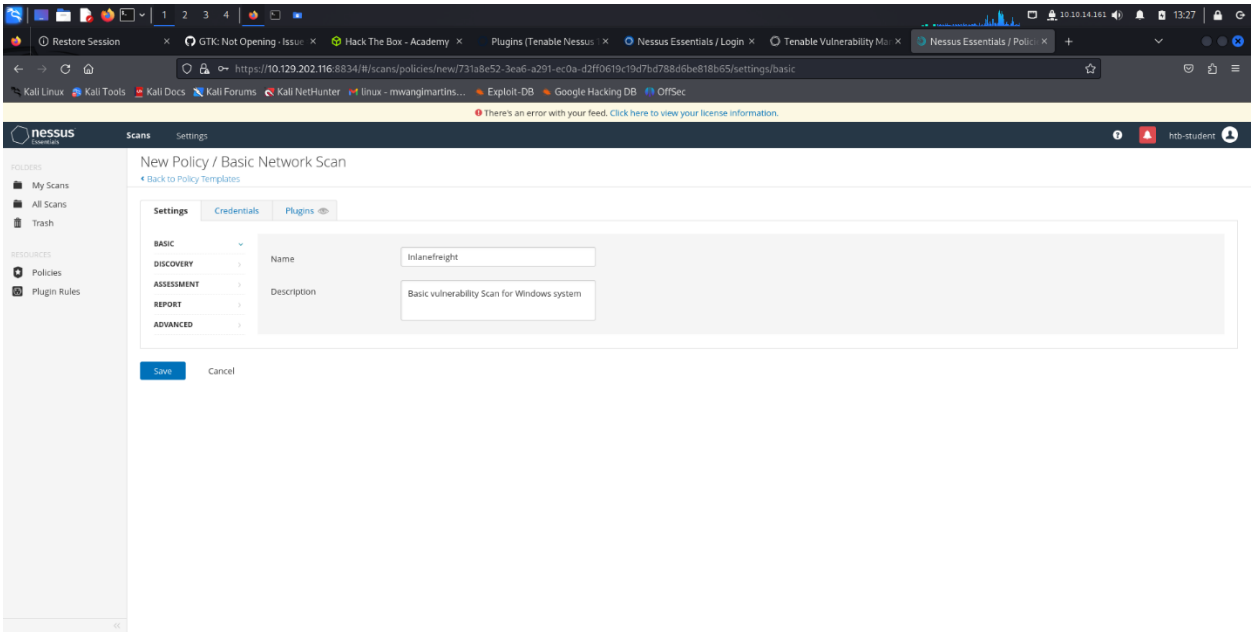
The target server is a Windows Server host used as a development server.

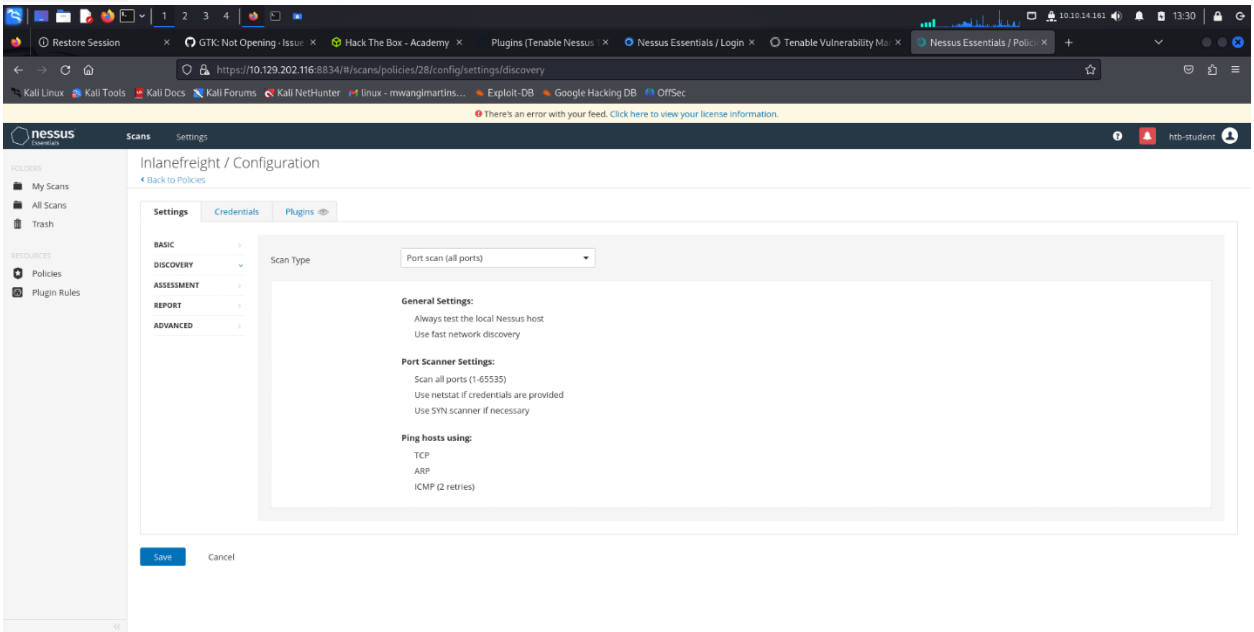
Questions



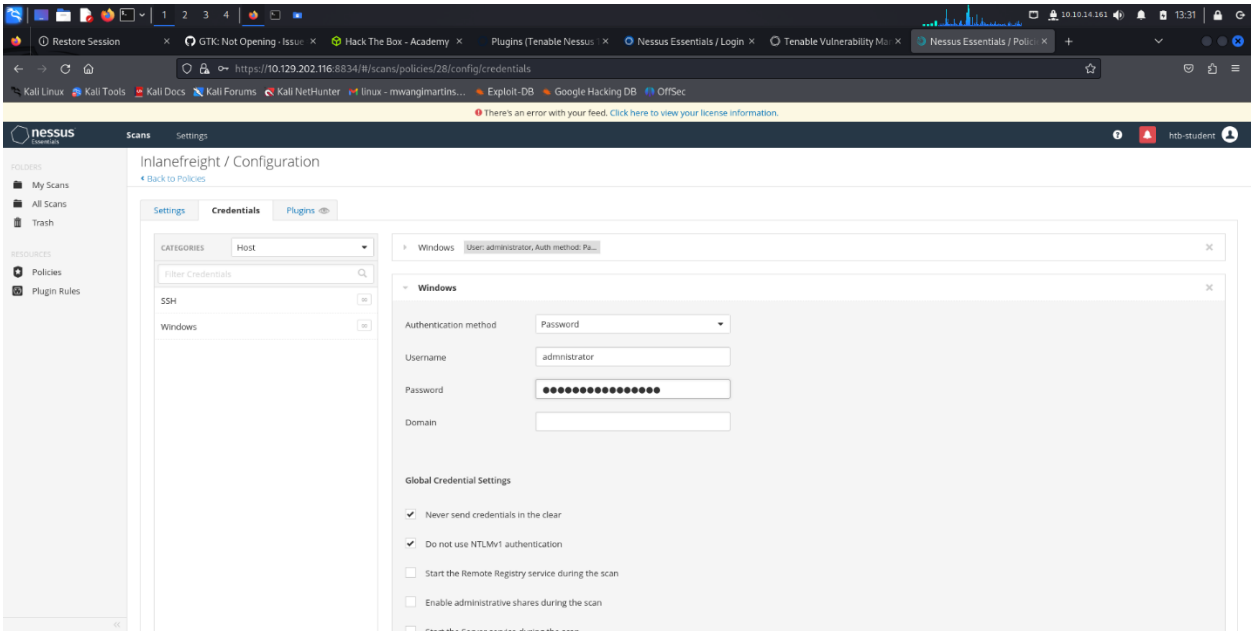


After successful login, I created a policy that suited my target scan with using The Basic Network Scan, to specify the scope of the scan, By navigating to the Policies section, I created my new policy, with giving it a name “Inlanefreight” and a description, setting up to scan all ports.

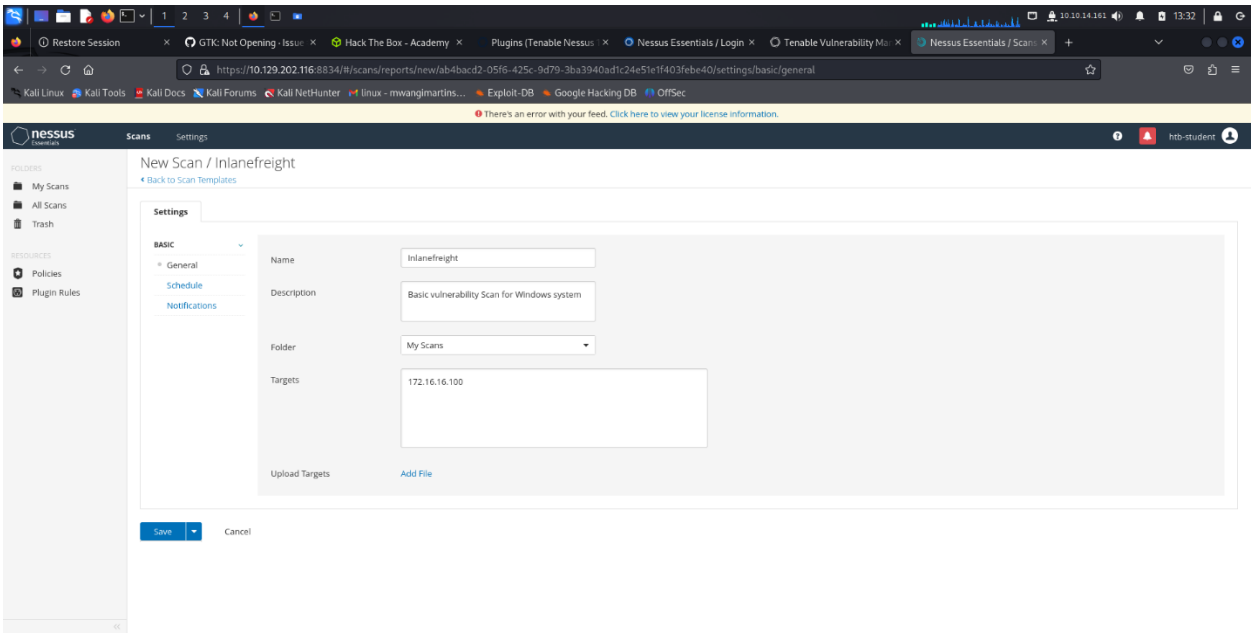

https://10.129.202.116:8834/#/scans/policies/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic
There's an error with your feed. Click here to view your license information.
nessus
Scans
Settings
htb-student
New Policy / Basic Network Scan
Back to Policy Templates
My Scans
All Scans
Trash
Policies
Plugin Rules
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
Inlanefreight
Description
Basic vulnerability Scan for Windows system
Save
Cancel

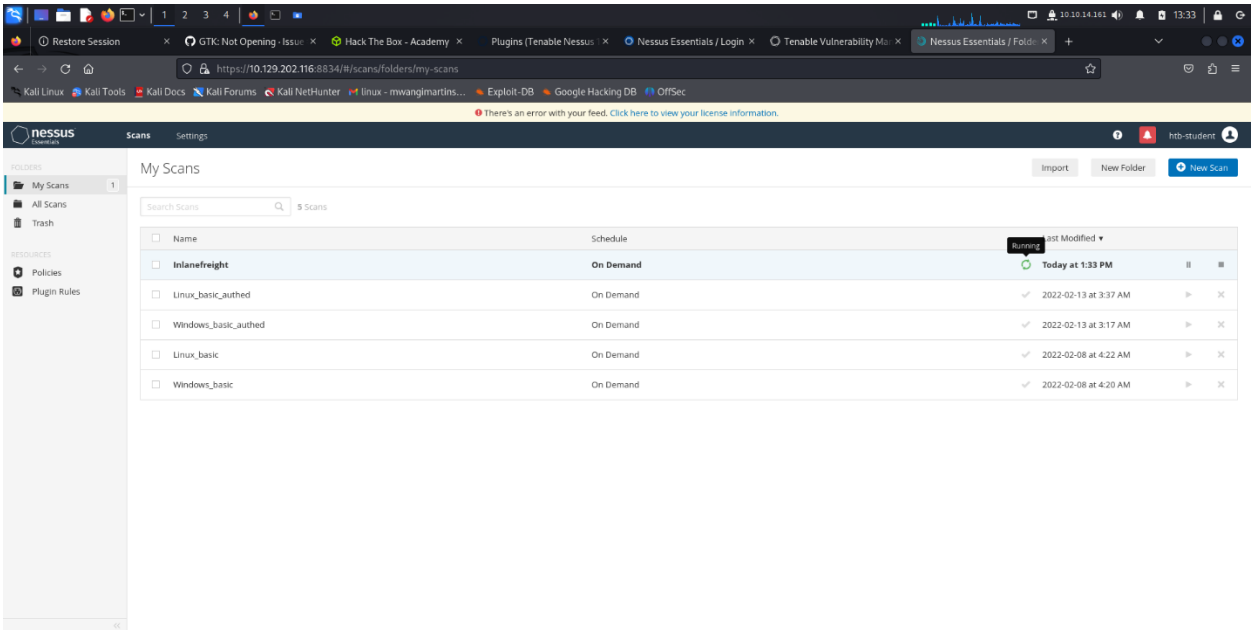

https://10.129.202.116:8834/#/scans/policies/28/config/settings/discovery
There's an error with your feed. Click here to view your license information.
nessus
Scans
Settings
htb-student
Inlanefreight / Configuration
Back to Policies
My Scans
All Scans
Trash
Policies
Plugin Rules
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Port scan (all ports)
General Settings:
Always test the local Nessus host
Use fast network discovery
Port Scanner Settings:
Scan all ports (1-65535)
Use netstat if credentials are provided
Use SYN scanner if necessary
Ping hosts using:
TCP
ARP
ICMP (2 retries)
Save
Cancel

This how to set up a authenticated scan,

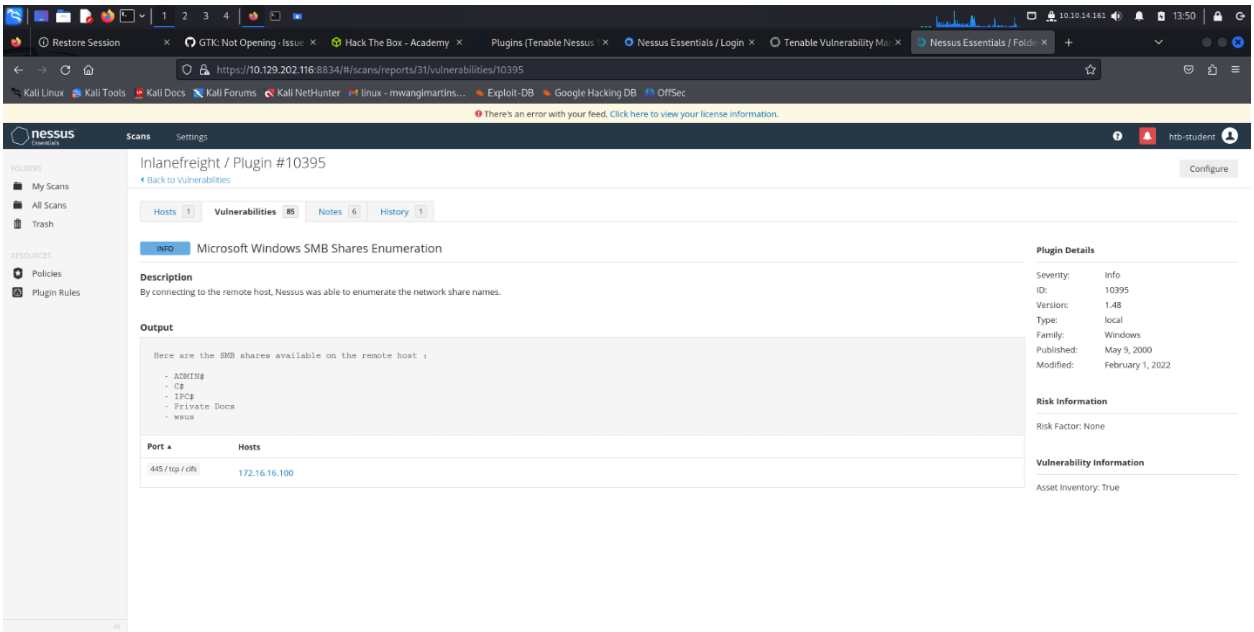


Created a new scan, with my target,

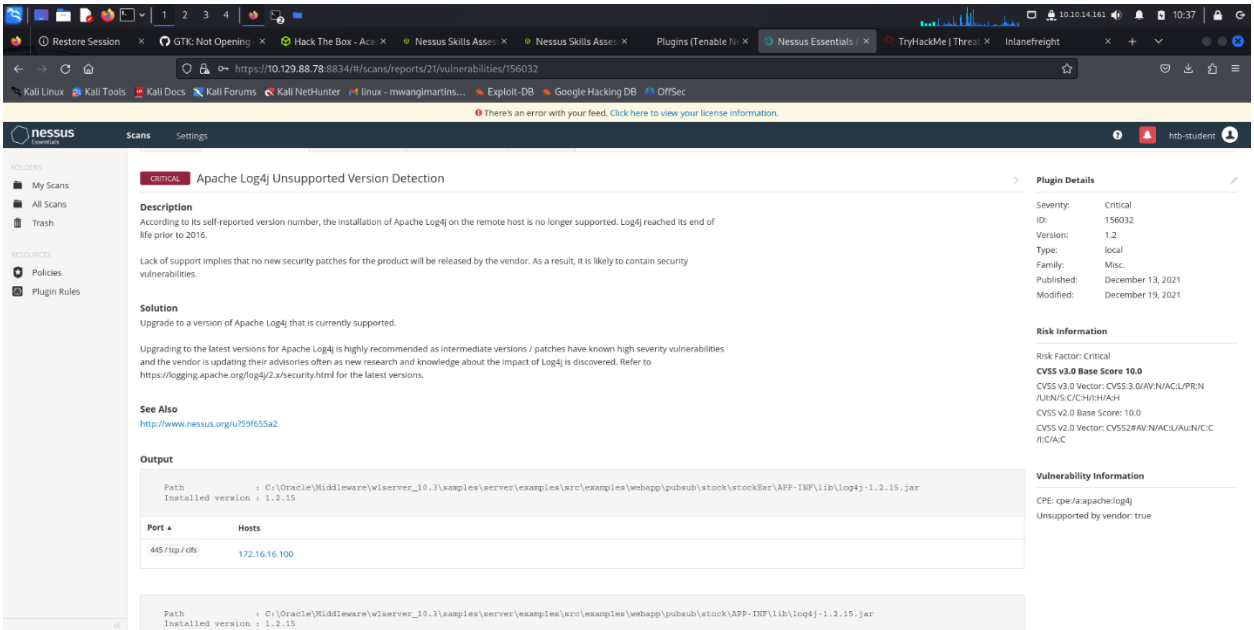




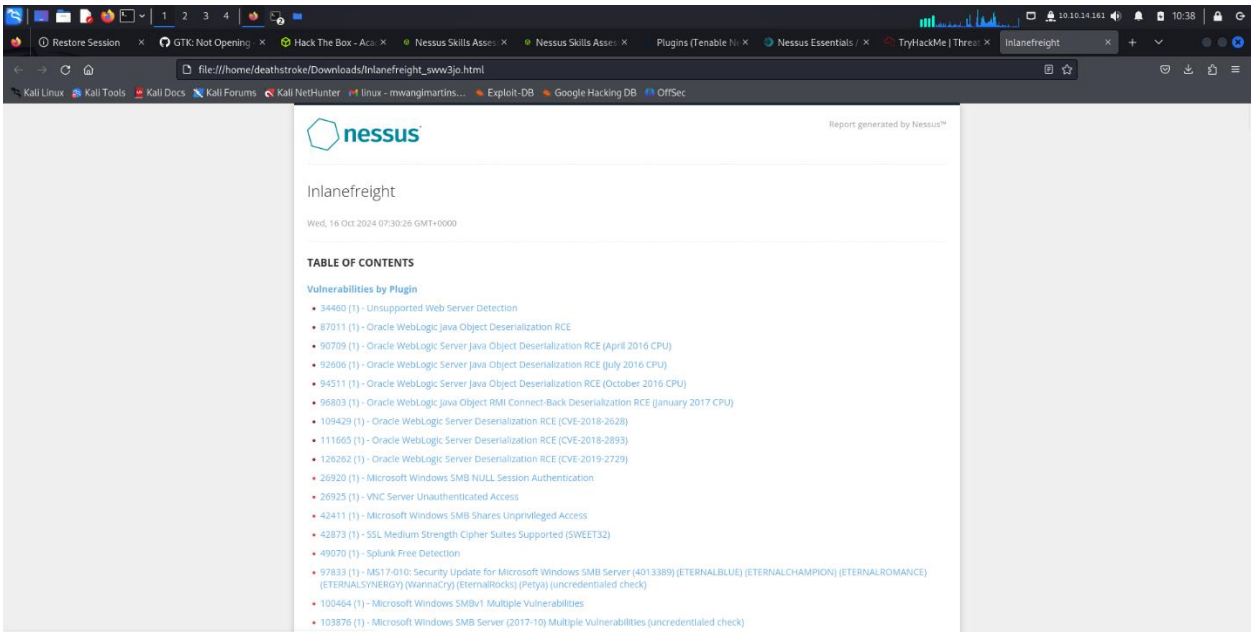
filtered the results based on SMB share to find the shares that can be accesses with any credentials,



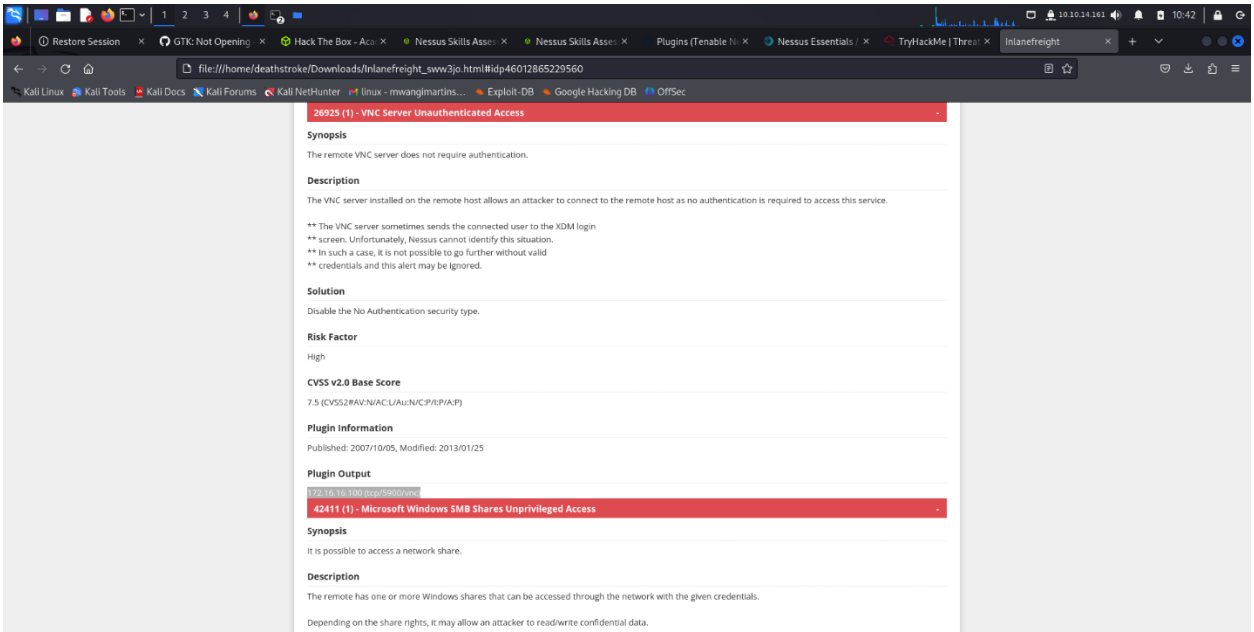
From the results I found the highest vulnerability as they were ranked according to Score 10 being highest and critical,



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



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



26925 (1) - VNC Server Unauthenticated Access

Synopsis

The remote VNC server does not require authentication.

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.

** The VNC server sometimes sends the connected user to the XDM login
** screen. Unfortunately, Nessus cannot identify this situation.
** In such a case, it is not possible to go further without valid
** credentials and this alert may be ignored.

Solution

Disable the No Authentication security type.

Risk Factor

High

CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

Plugin Information

Published: 2007/10/05, Modified: 2013/01/25

Plugin Output

172.16.16.100 (tcp/5900/vnc)

42411 (1) - Microsoft Windows SMB Shares Unprivileged Access

Synopsis

It is possible to access a network share.

Description

The remote has one or more Windows shares that can be accessed through the network with the given credentials.

Depending on the share rights, it may allow an attacker to read/write confidential data.

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.

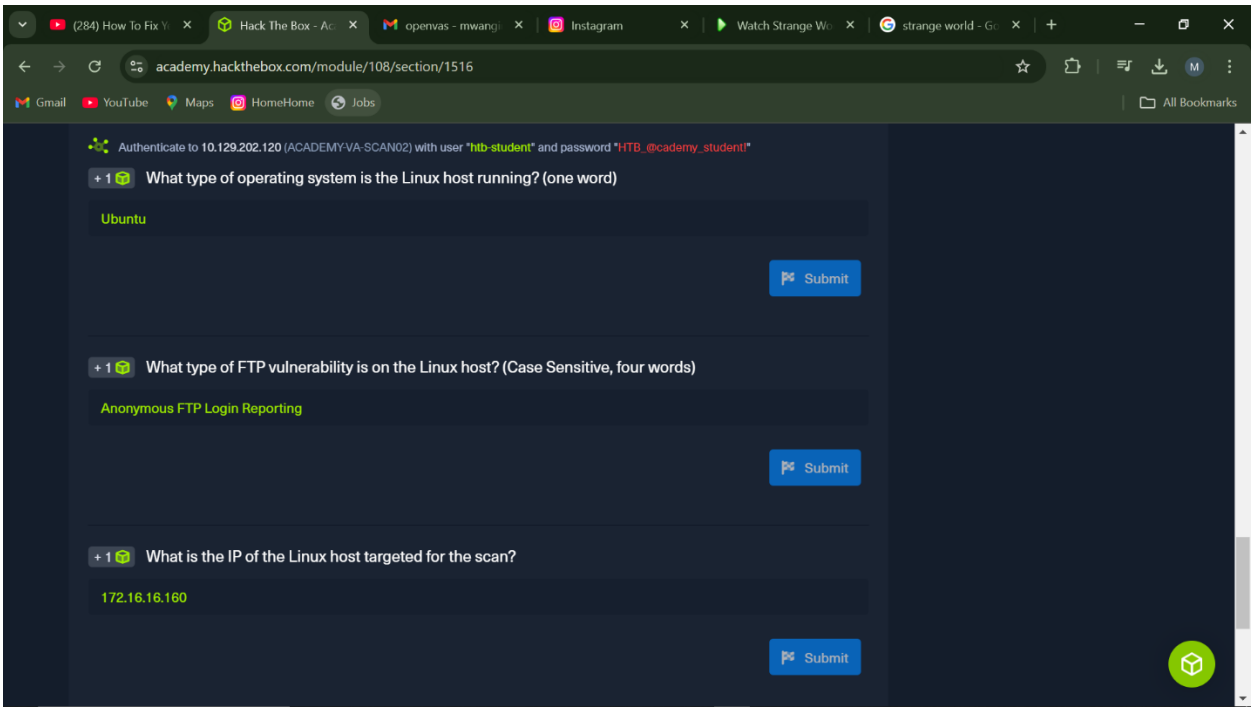
1.6 OpenVAS Skills Assessment

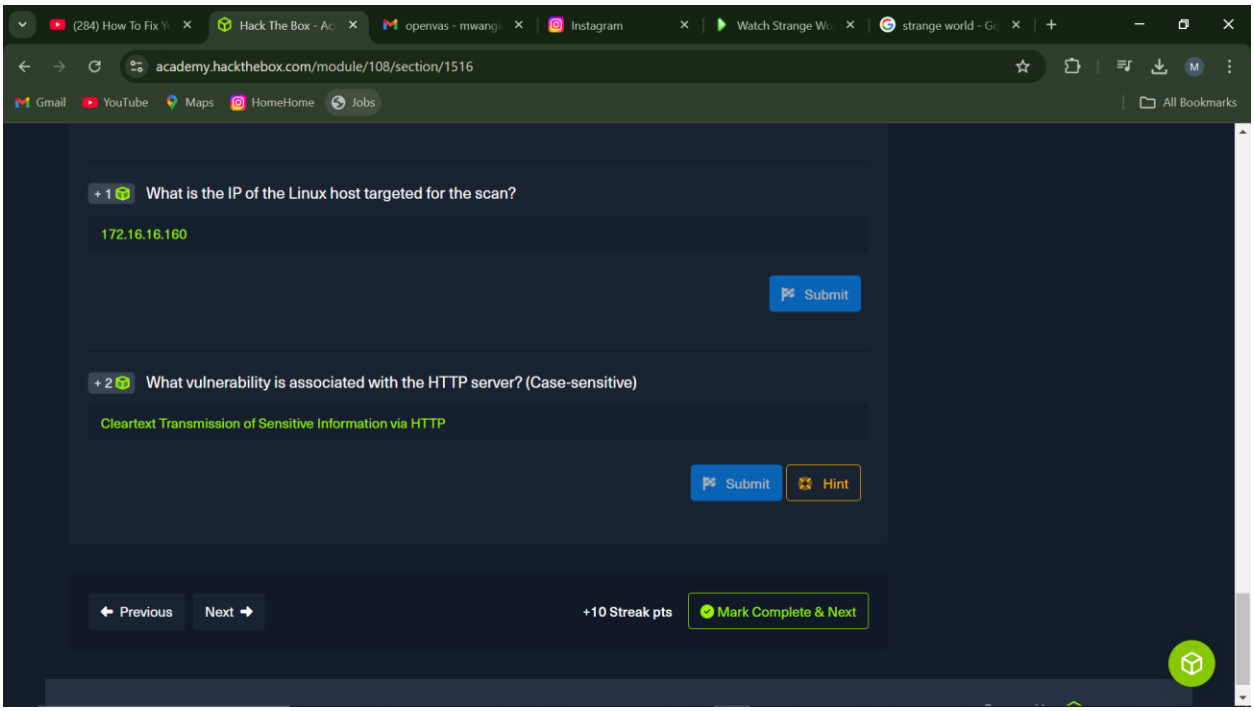
Scenario

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.

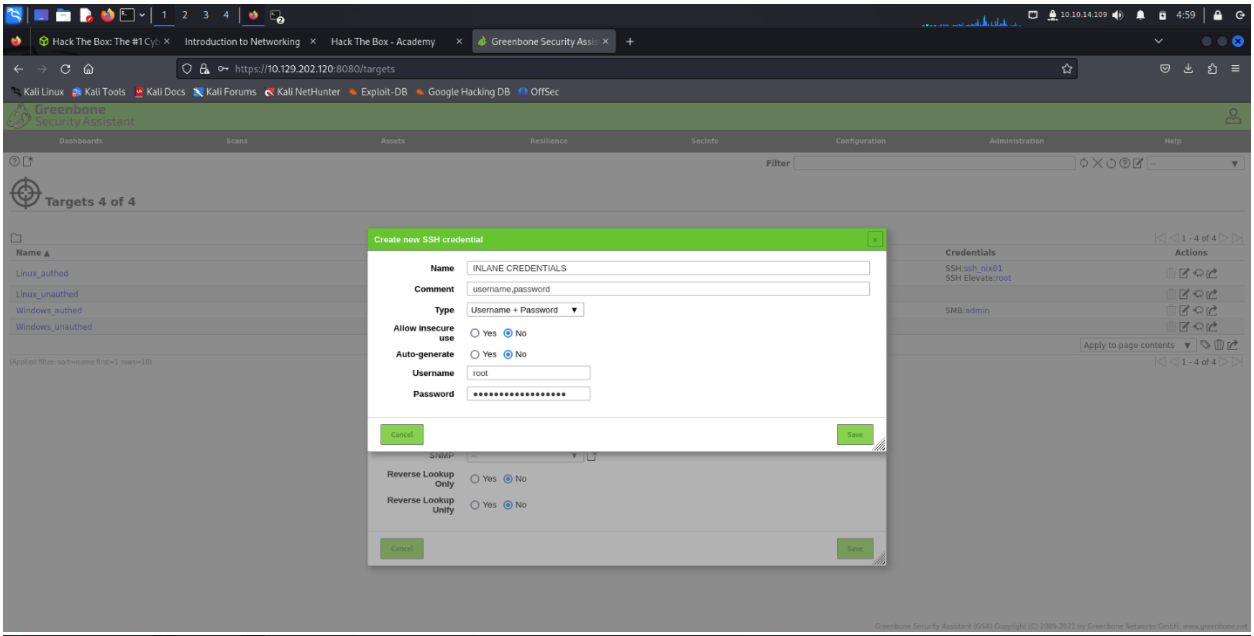
Questions

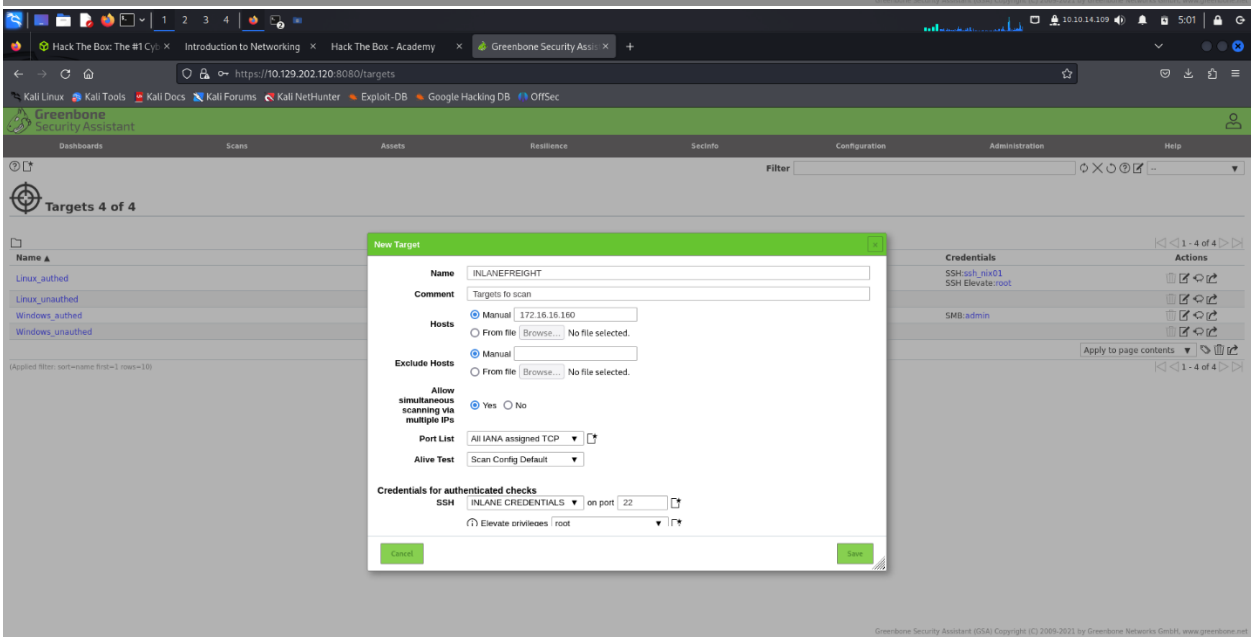




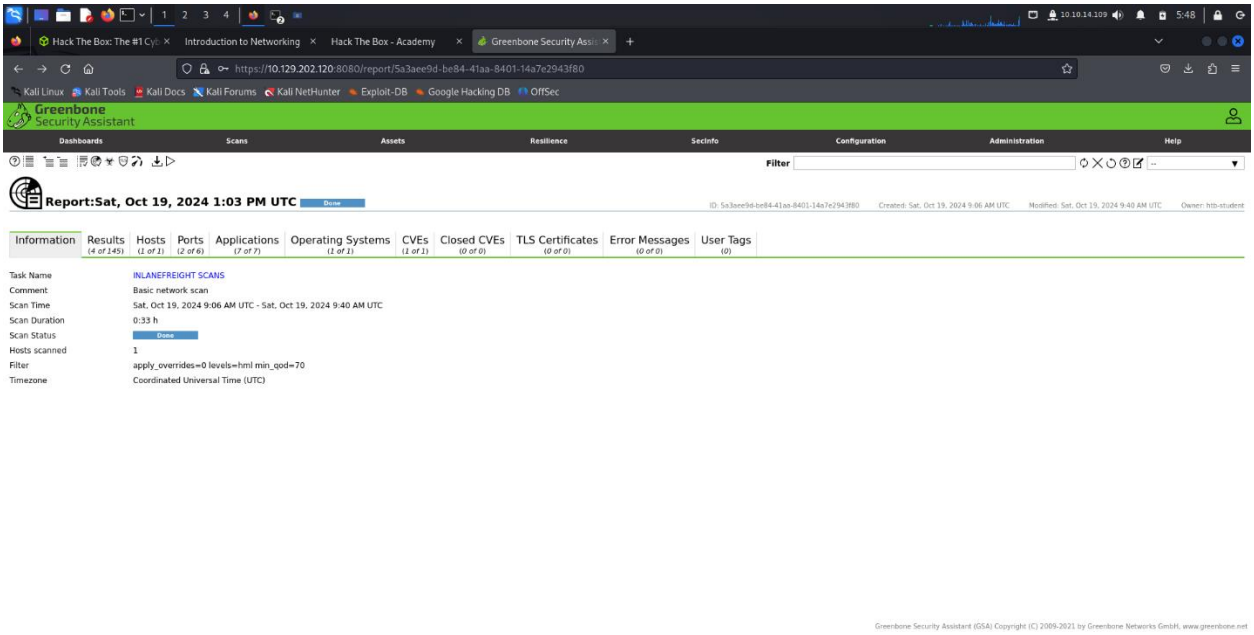
Started off by login to the OpenVAS with credentials provided.

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,

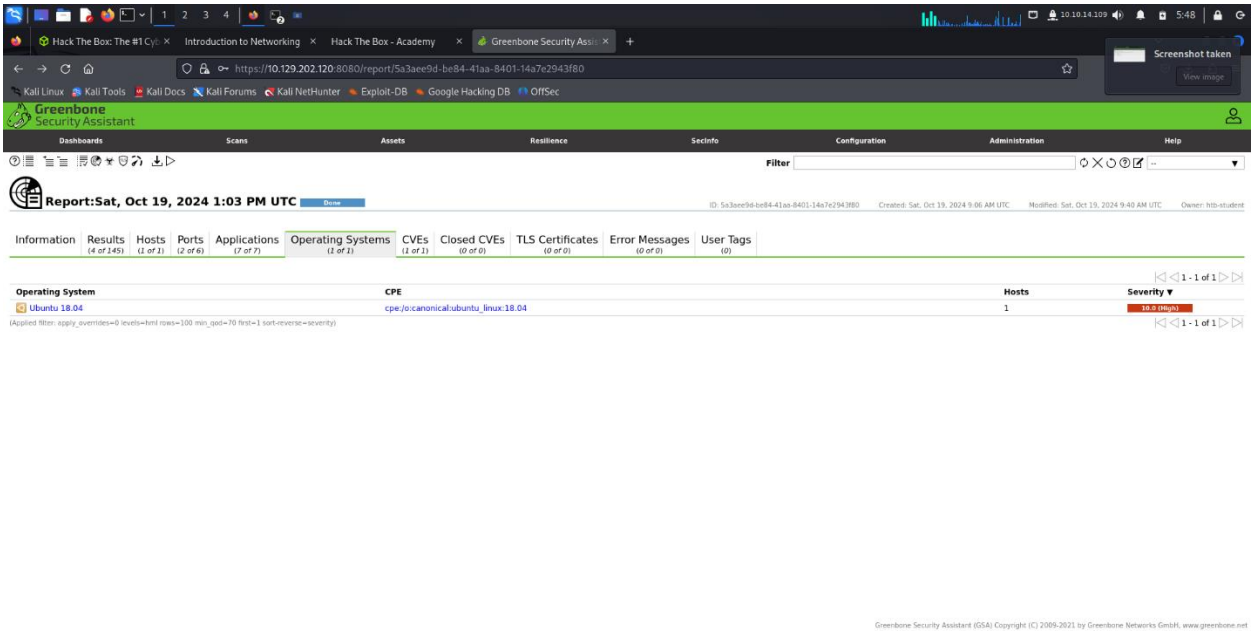




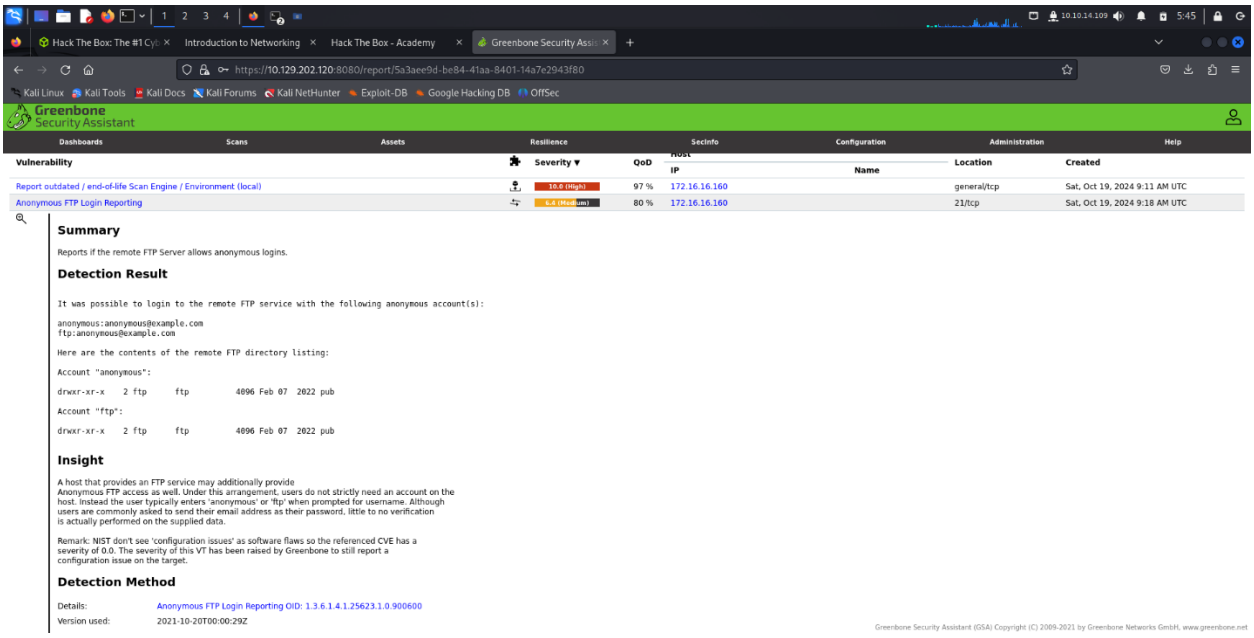
This was the results upon completion of the scan,



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,



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