VULNERABILITY ASSESSMENT (HACK THE BOX)

Introduction.

This is a path where I will get to understand different types of security assessments, vulnerability scoring, and reporting, using network vulnerability scanning tools like Nessus, OpenVAS, and reporting.

Table of Contents

Contents

Module Sections.

Security Assessments.

Black box pentesting is done with no knowledge of a network's configuration or applications.

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.

White box pentesting is typically conducted by giving the penetration tester full access to all systems, configurations, build documents, etc., and source code if web applications are in-scope.

Application pentesters assess web applications, thick-client applications, APIs, and mobile applications.

Network or infrastructure pentesters assess all aspects of a computer network, including its networking devices such as routers and firewalls, workstations, servers, and applications.

Physical 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 pentesters test human beings.

Vulnerability assessments look for vulnerabilities in networks without simulating cyber attacks. During a vulnerability assessment, the assessor will typically run a vulnerability scan and then perform validation on critical, high, and medium-risk vulnerabilities. This means that they will show evidence that the vulnerability exists and is not a false positive, often using other tools, but will not seek to perform privilege escalation, lateral movement, post-exploitation, etc., if they validate, for example, a remote code execution vulnerability.

Penetration tests, depending on their type, evaluate the security of different assets and the impact of the issues present in the environment. Penetration tests can include manual and automated tactics to assess an organization's security posture. A pentest is a simulated cyber attack to see if and how the network can be penetrated. Regardless of a company's size, industry, or network design, pentests should only be performed after some vulnerability assessments have been conducted successfully and with fixes.

Security audits are typically requirements from outside the organization, and they're typically mandated by government agencies or industry associations to assure that an organization is compliant with specific security regulations.

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.

A **red team** is a type of evasive black box pentesting, simulating all kinds of cyber attacks from the perspective of an external threat actor.

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.

Vulnerability Scanning Overview.

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 would determine a vulnerability if the identified version of a particular asset has a public CVE.

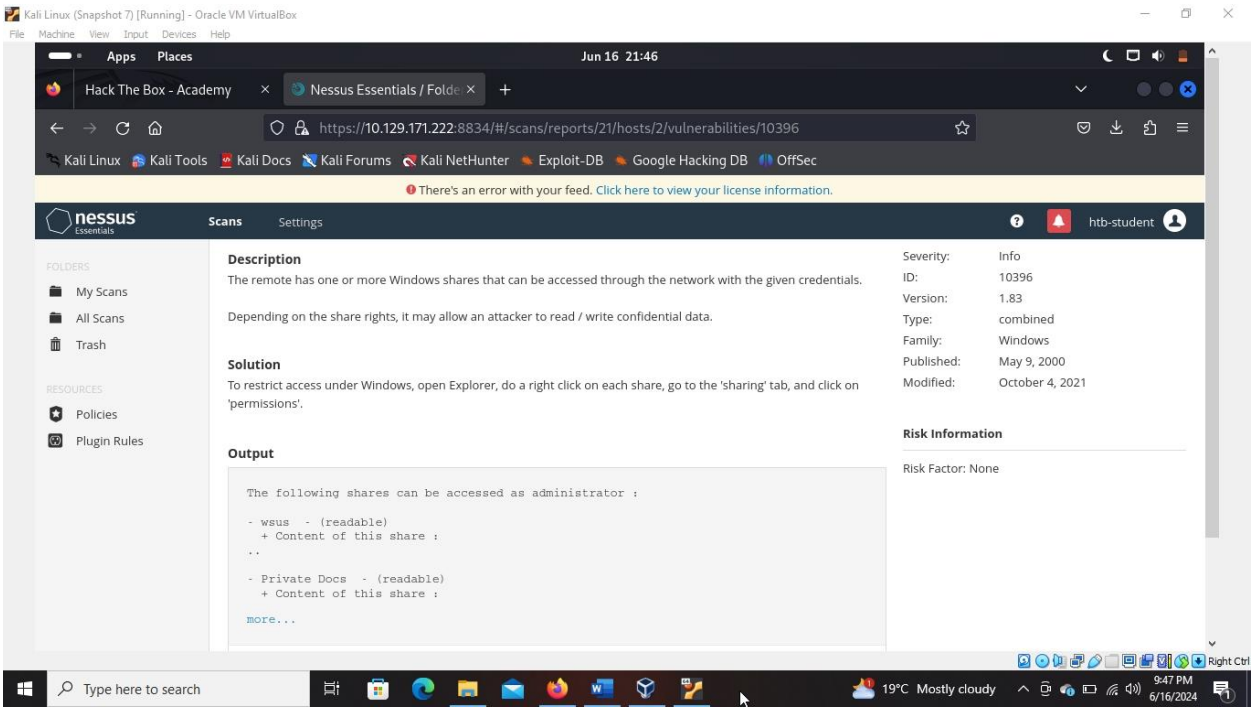
dynamic test tries specific (usually benign) payloads such as weak credentials, SQL injection, or command injection on the target (i.e., a web application). If any payload returns a hit, then there's a good chance that it is vulnerable.

Getting Started With Nessus

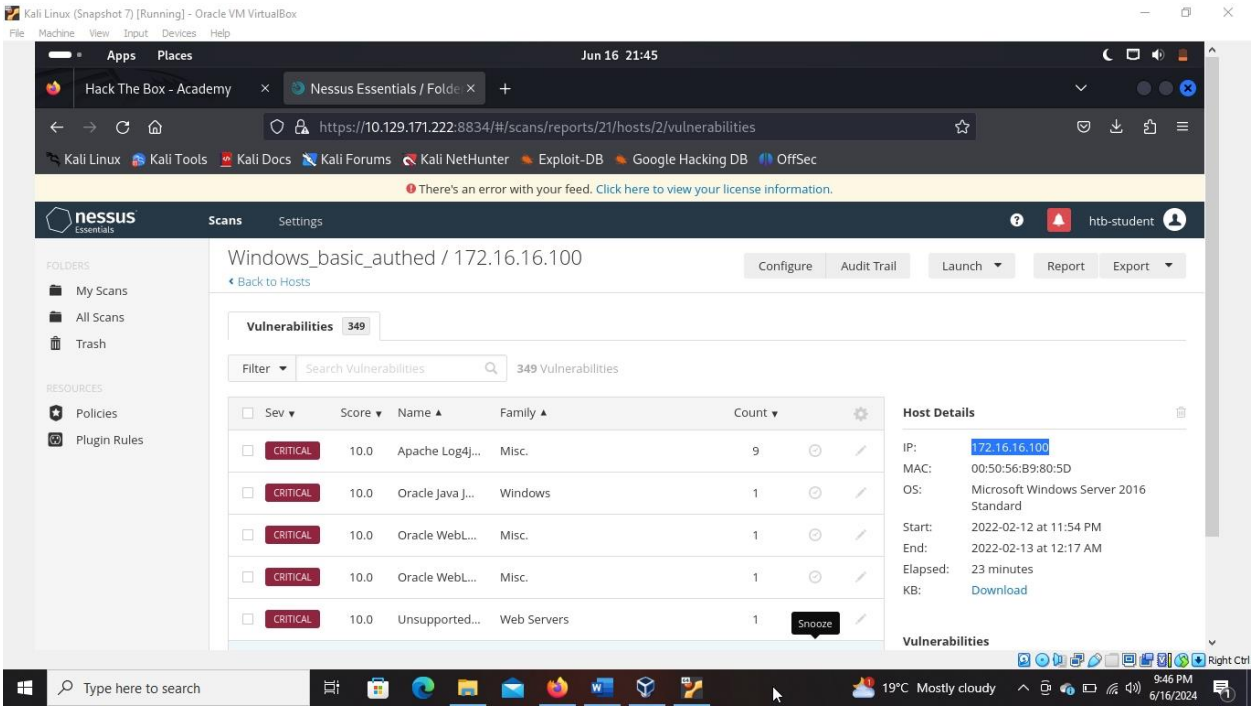
Nessus Skills Assessment.

I logged in into Nessus Scanner and started a new scan that is a Basic Network Scan. I modified the scan template to scan all ports against the target 172.16.16.100. I later set an authenticated scan using an administrator user credentials.

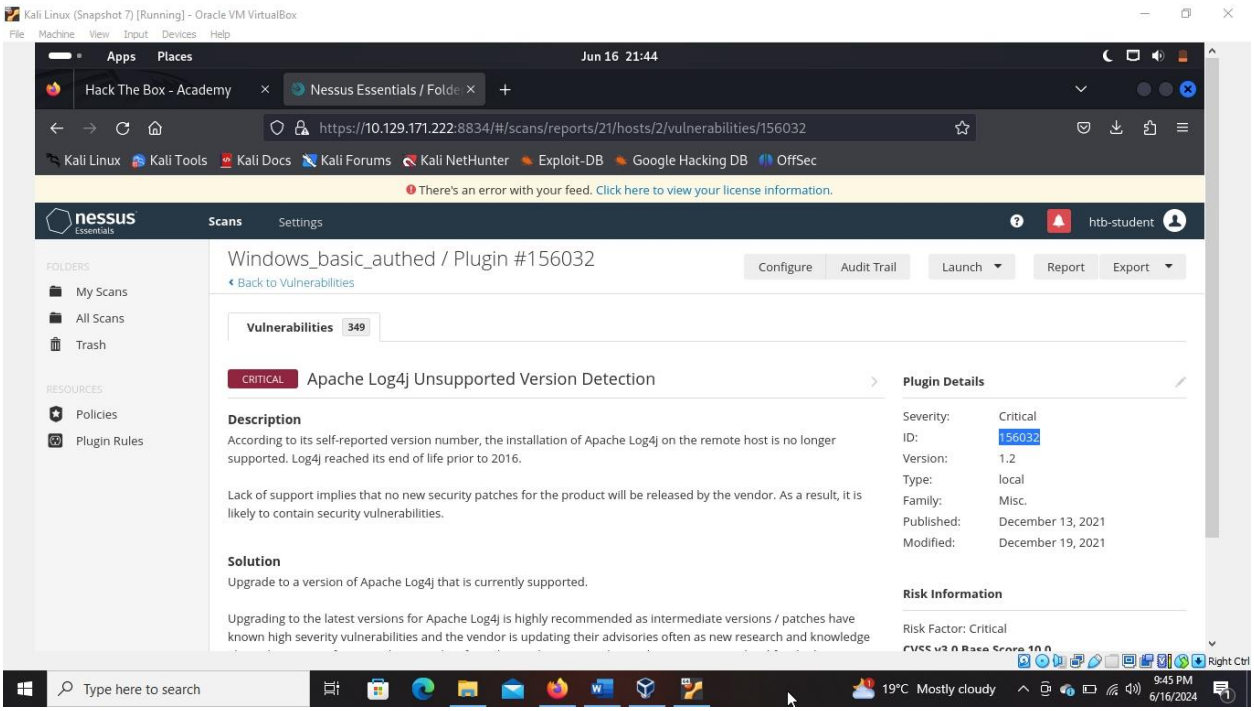
After the scan has finished, I went into the vulnerabilities tab and searched for shares where I saw two shares through SMB that an attacker can read or write confidential data as an administrator.



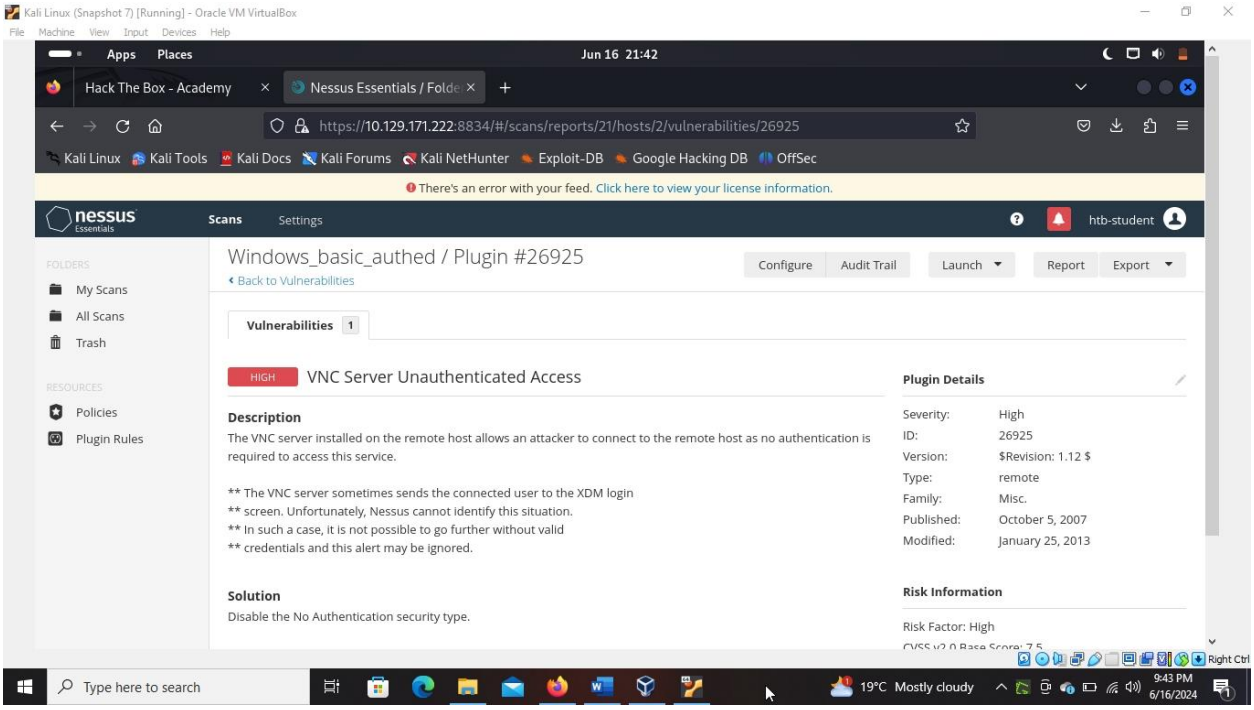
The target for the authenticated scan can be seen when you click on the windows authenticated scan under hosts.



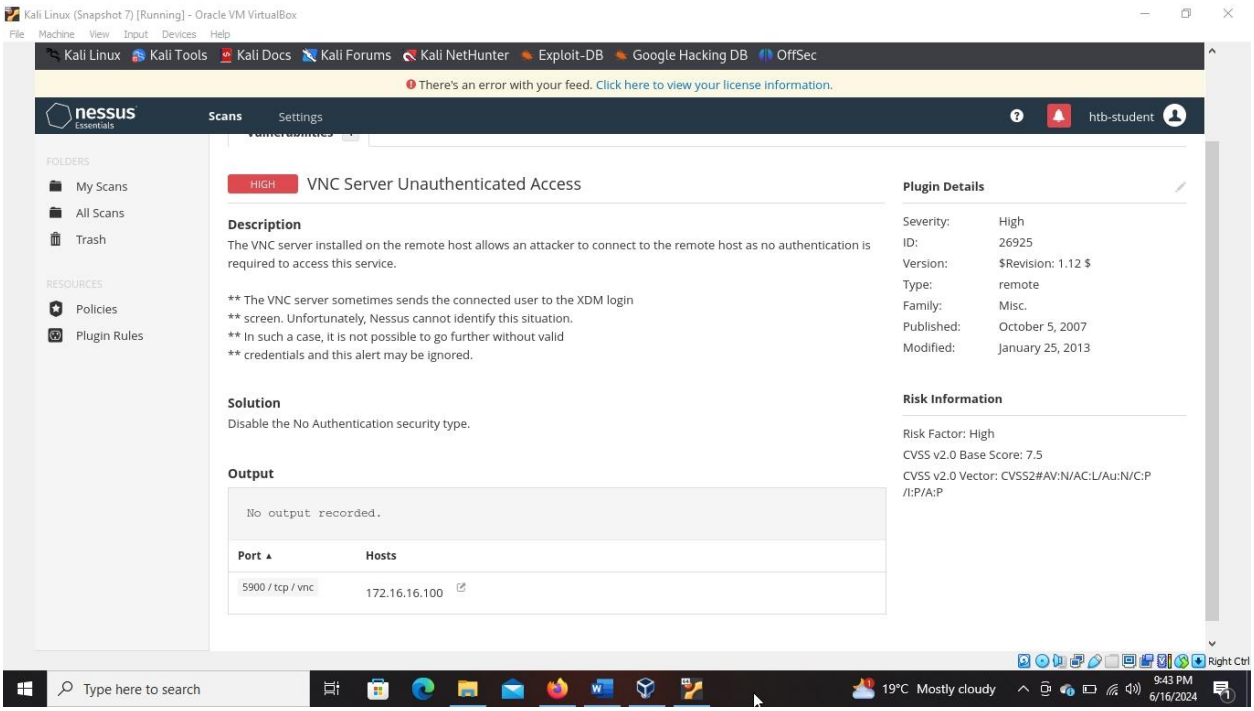
The most critical vulnerability was the Apache Log4j and to get the plugin ID, it can be seen on the right under Plugin details.

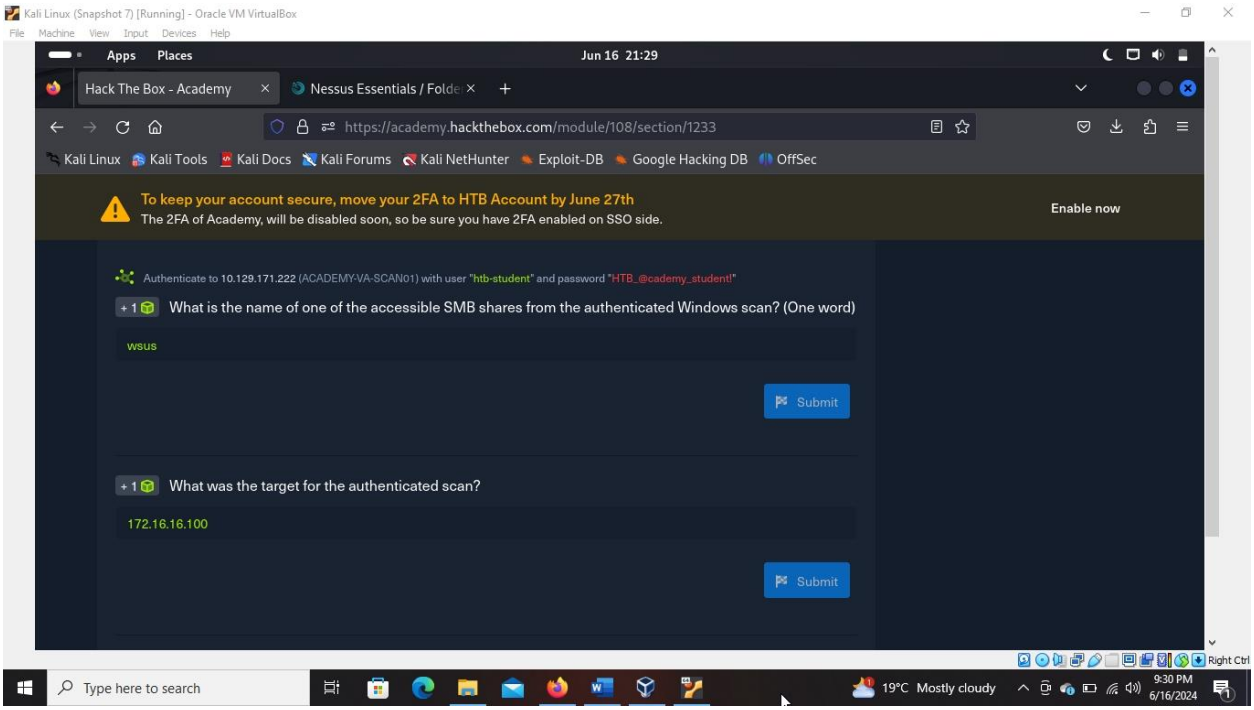


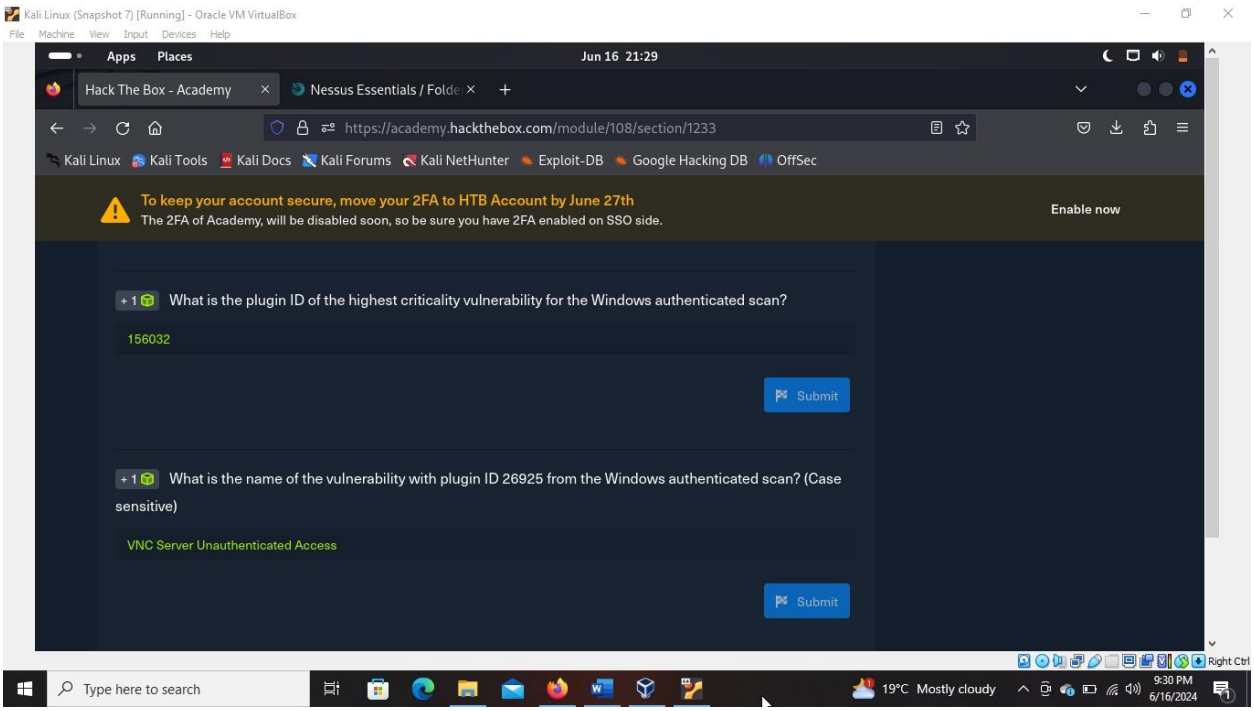
I went ahead and applied a filter to search for a plugin ID where I was able to get the vulnerability with the searched plugin ID.

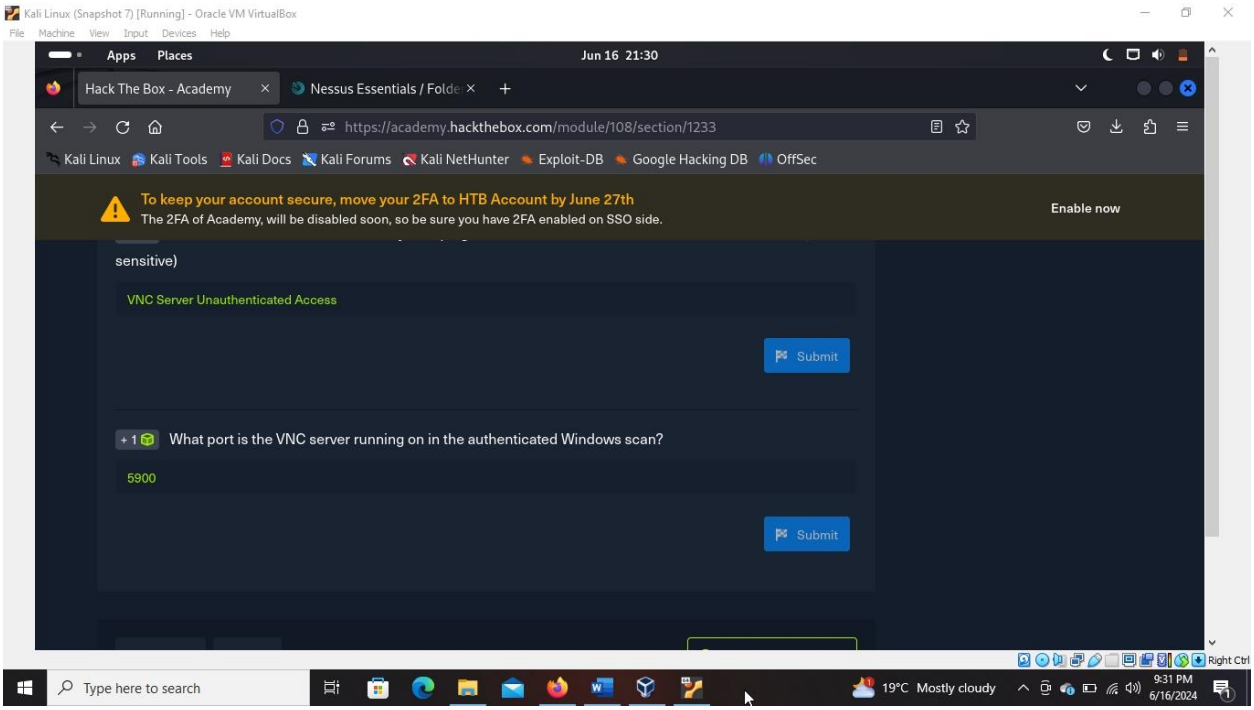


I was able to find the port under which the VNC server ran on which I was able to found at the bottom of the scan under output.


Kali Linux (Snapshot 7) [Running] - Oracle VM VirtualBox
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
There's an error with your feed. Click here to view your license information.
nessus Essentials
Scans
Settings
htb-student
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
HIGH
VNC Server Unauthenticated Access
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.
Output
No output recorded.
Port
Hosts
5900 / tcp / vnc
172.16.16.100
Plugin Details
Severity: High
ID: 26925
Version: $Revision: 1.12 $
Type: remote
Family: Misc.
Published: October 5, 2007
Modified: January 25, 2013
Risk Information
Risk Factor: High
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
Type here to search
19°C Mostly cloudy
9:43 PM
6/16/2024


Kali Linux (Snapshot 7) [Running] - Oracle VM VirtualBox
Apps Places
Jun 16 21:29
Hack The Box - Academy
Nessus Essentials / Folde
https://academy.hackthebox.com/module/108/section/1233
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
Authenticate to 10.129.171.222 (ACADEMY-VA-SCAN01) with user "htb-student" and password "HTB_@cademy_student!"
+1 What is the name of one of the accessible SMB shares from the authenticated Windows scan? (One word)
wsus
Submit
+1 What was the target for the authenticated scan?
172.16.16.100
Submit
Type here to search
19°C Mostly cloudy
9:30 PM
6/16/2024


Kali Linux (Snapshot 7) [Running] - Oracle VM VirtualBox
Apps Places
Jun 16 21:29
Hack The Box - Academy
Nessus Essentials / Folde
https://academy.hackthebox.com/module/108/section/1233
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
+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
Type here to search
19°C Mostly cloudy
9:30 PM
6/16/2024


Kali Linux (Snapshot 7) [Running] - Oracle VM VirtualBox
Apps Places
Jun 16 21:30
Hack The Box - Academy
Nessus Essentials / Folde
https://academy.hackthebox.com/module/108/section/1233
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
To keep your account secure, move your 2FA to HTB Account by June 27th
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.
Enable now
sensitive)
VNC Server Unauthenticated Access
Submit
+1 What port is the VNC server running on in the authenticated Windows scan?
5900
Submit
Type here to search
19°C Mostly cloudy
9:31 PM
6/16/2024

OpenVAS

OpenVAS Scan

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.

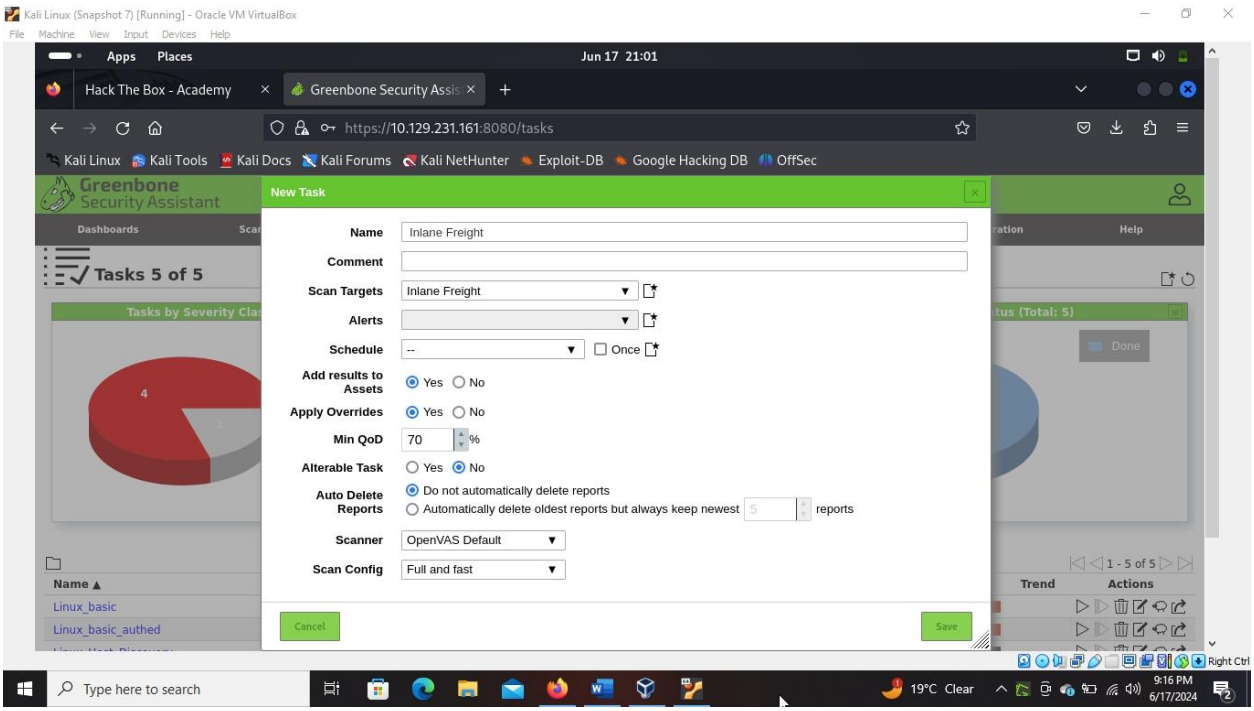
Host Discovery: This scan configuration solely tests whether the host is alive and determines what devices are active on the network. This scan configuration does not check for vulnerabilities as well. *OpenVAS leverages ping to identify if the host is alive.*

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.

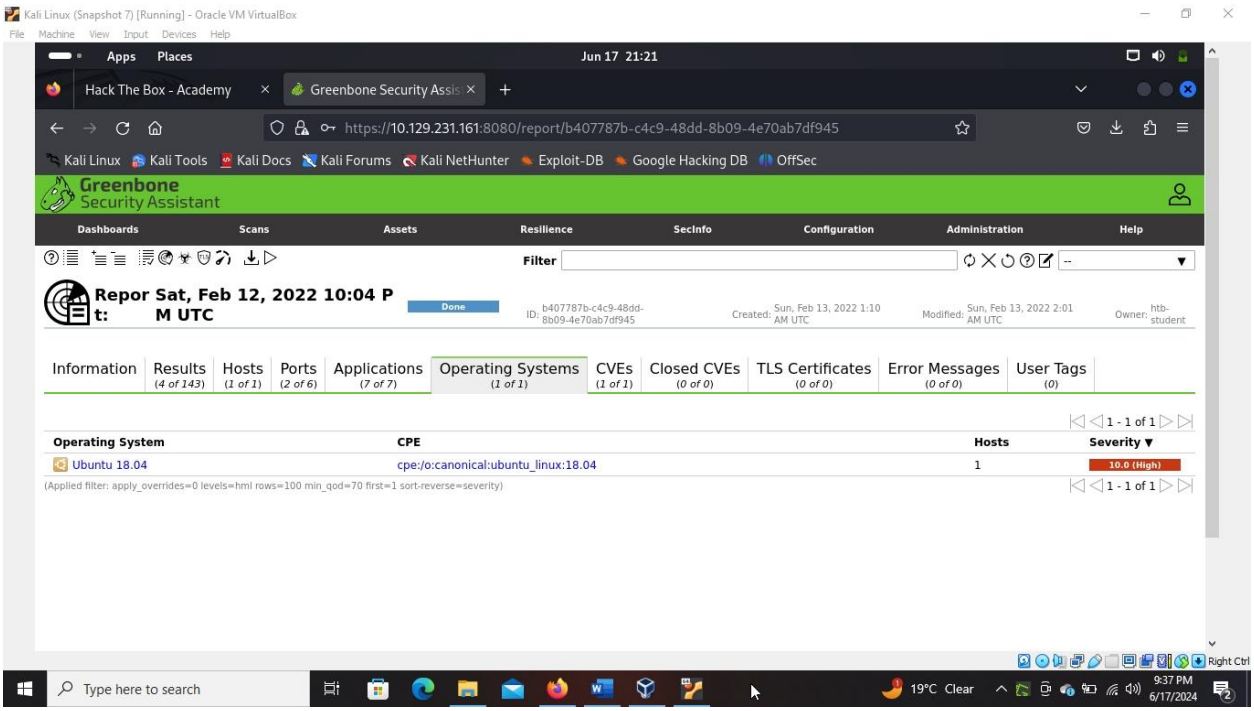
Full and fast: This configuration is recommended by OpenVAS as the safest option and leverages intelligence to use the best NVT checks for the host(s) based on the accessible ports.

OpenVAS Skills Assessment

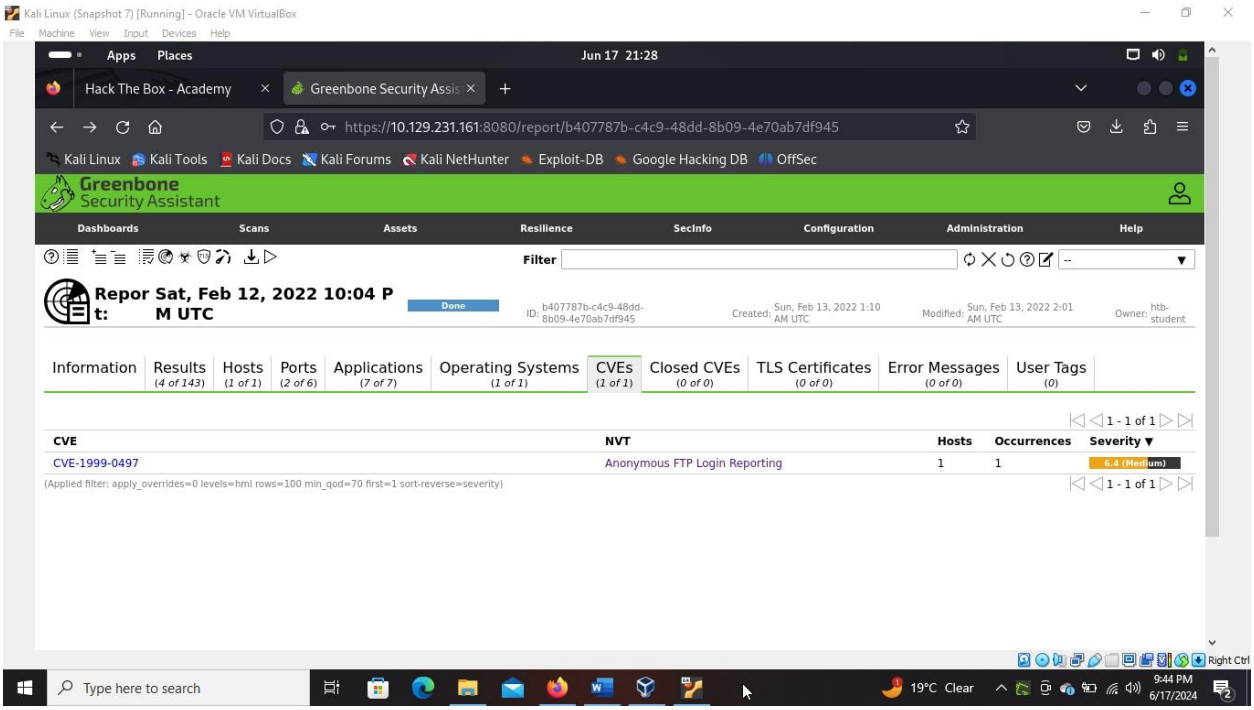
I logged into the remote machine using ssh and logged into OpenVAS and set the target IP, the OpenVAS default scanner and used the full and fast config. I later set the scanner to run as an authenticated user.



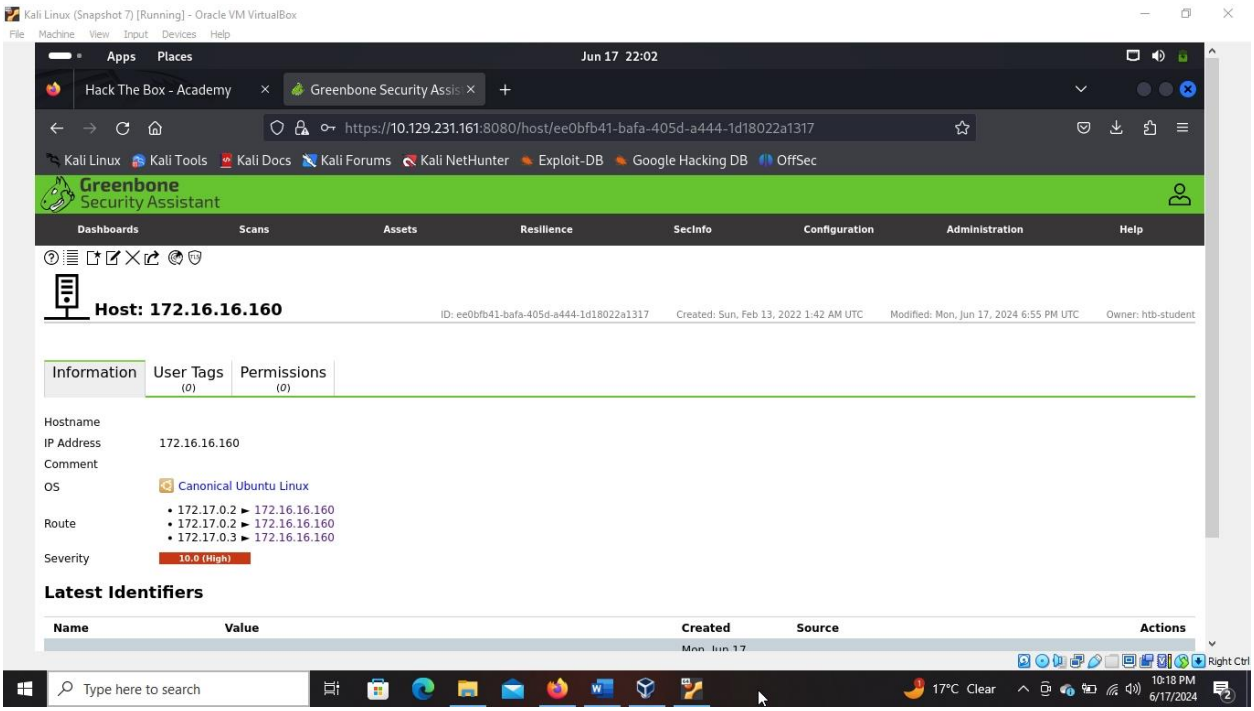
I selected the linux authenticated scan and selected the Operating Systems tab to check what OS the linux host is running.



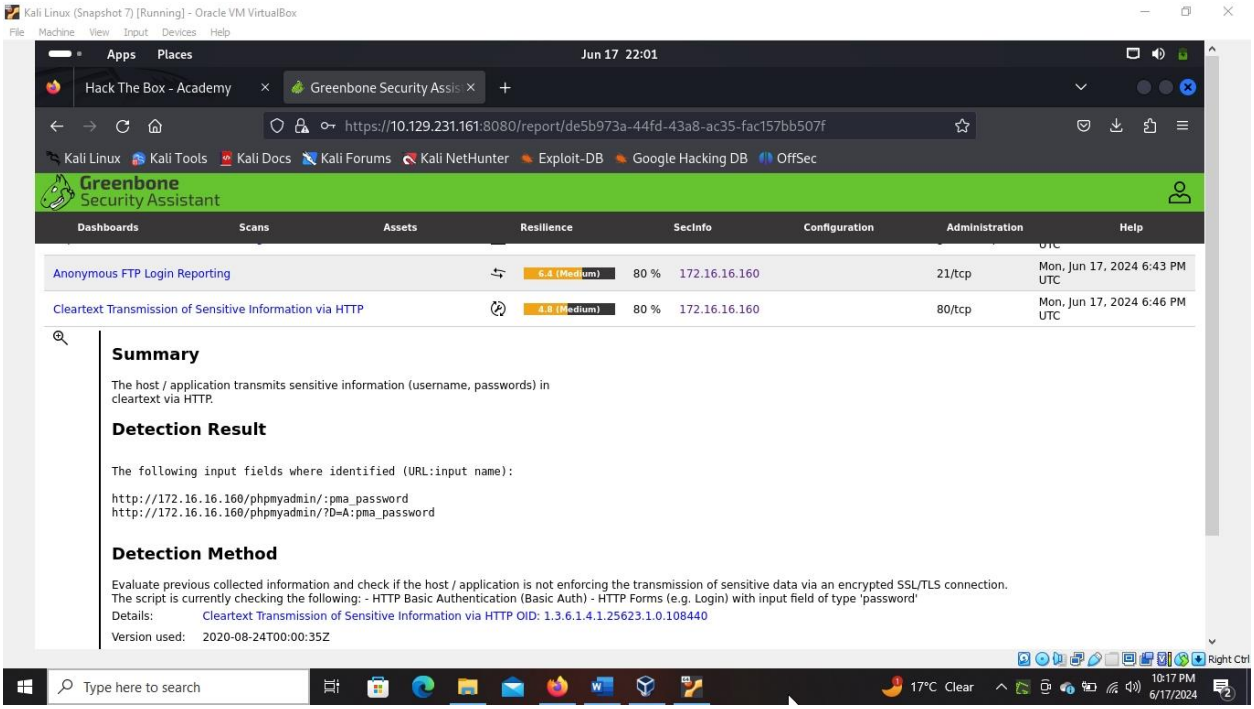
I went ahead to check the type of FTP vulnerability that is on the host linux machine which was under the vulnerability tab.

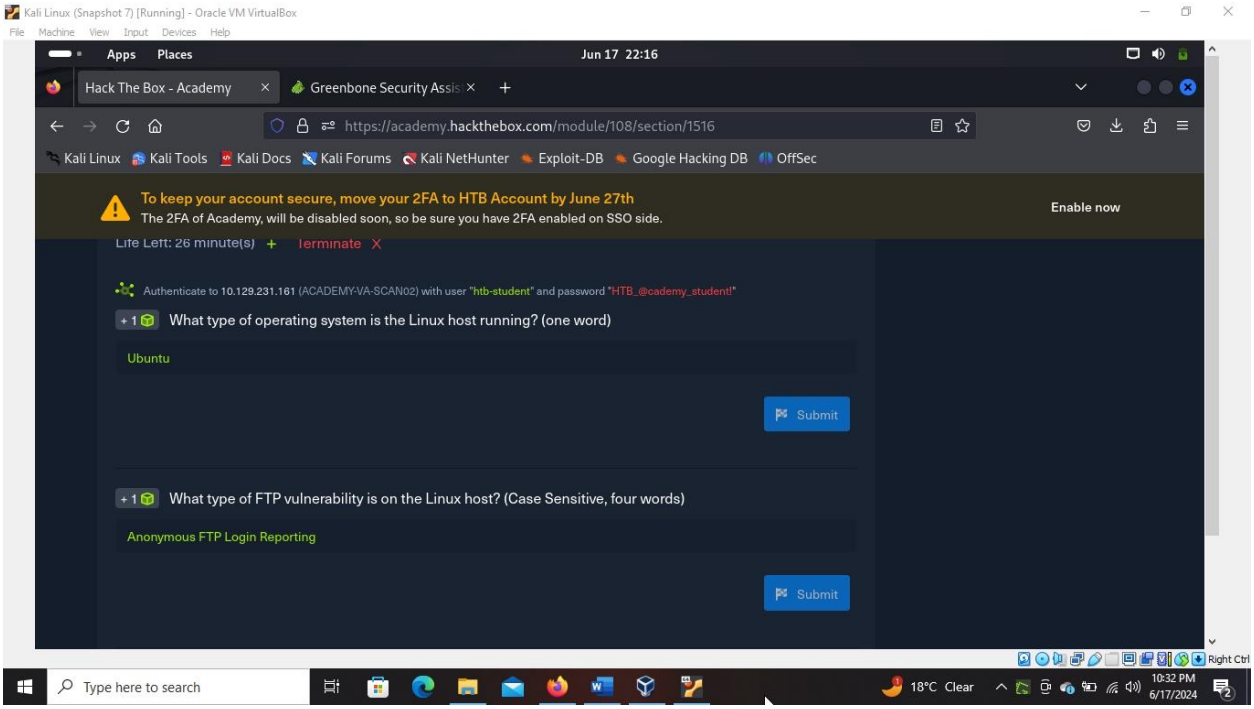


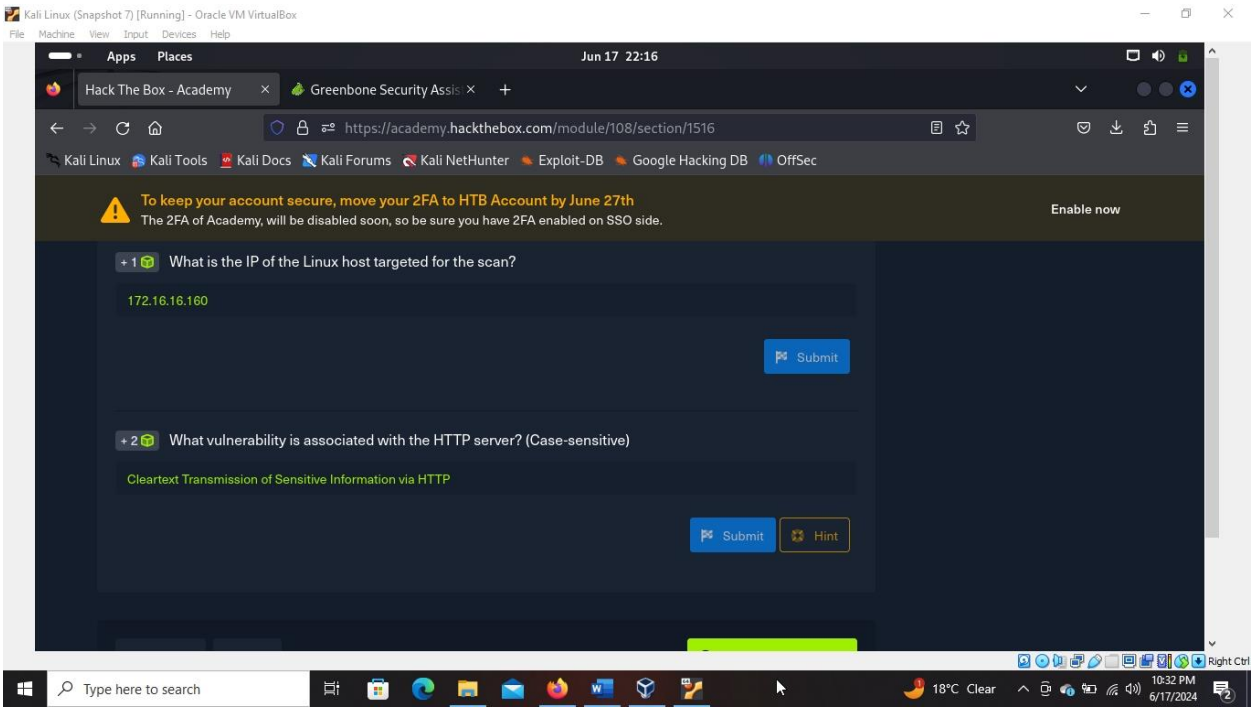
Under the hosts tab, I could see the target IP address listed.



Under the vulnerability tab, I got the type of vulnerability associated with the HTTP server which involved sending sensitive information through cleartext.

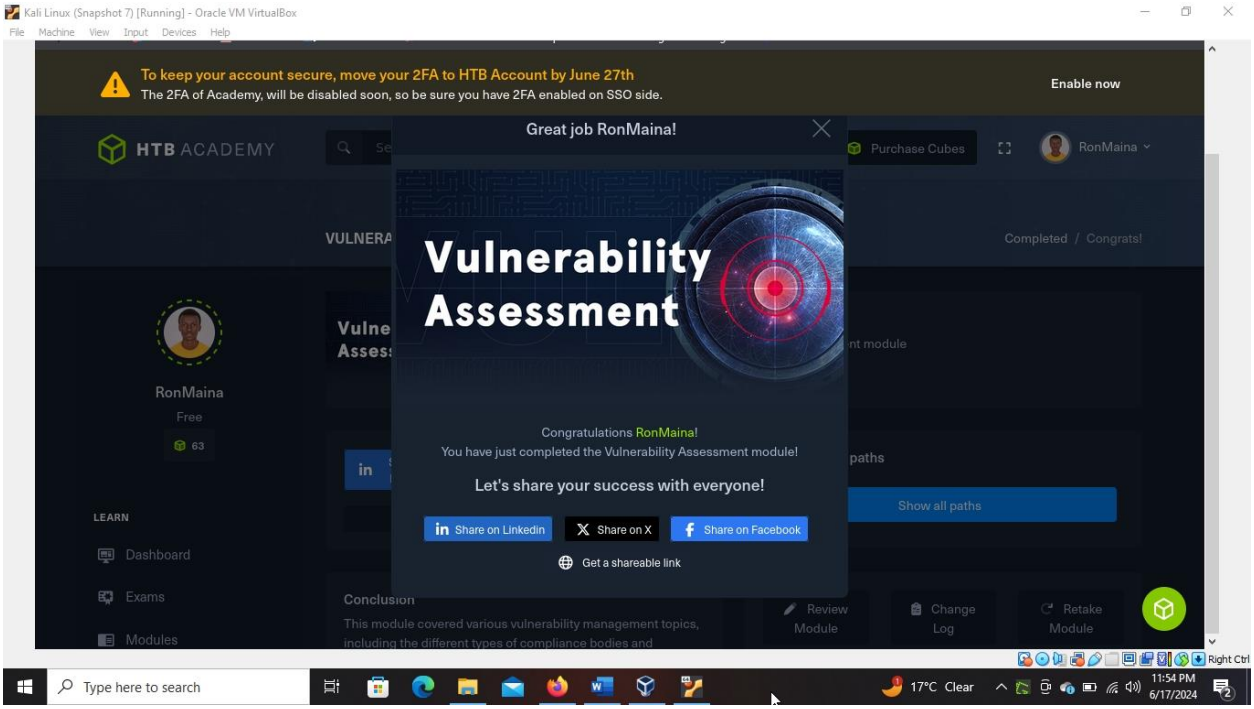






Final Completion

This is a screenshot of my completion of the paths.



Conclusion.

I have learned about the different types of security assessments, vulnerability scoring, and reporting, using network vulnerability scanning tools like Nessus, OpenVAS, and reporting.

Shareable link

https://academy.hackthebox.com/achievement/1290934/108