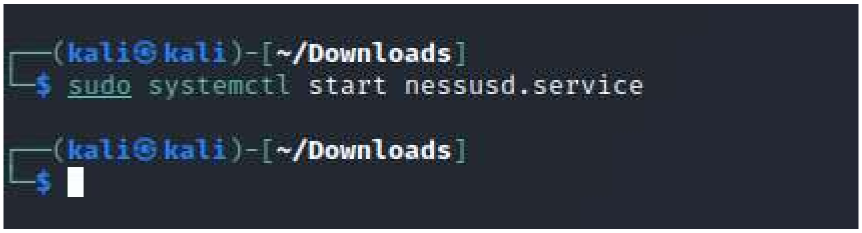
Write-Up On TryHackMe Nessus Lab - Written By Luke Hauersperger

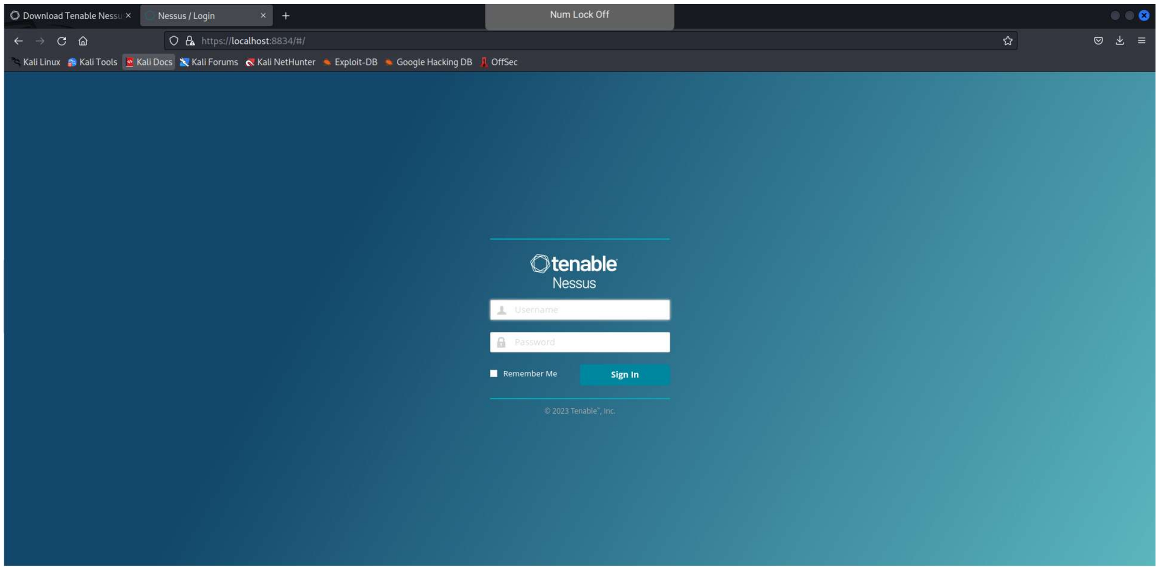
In order to start this lab I needed to set up my Kali lab and download the Nessus file, which I then ran.



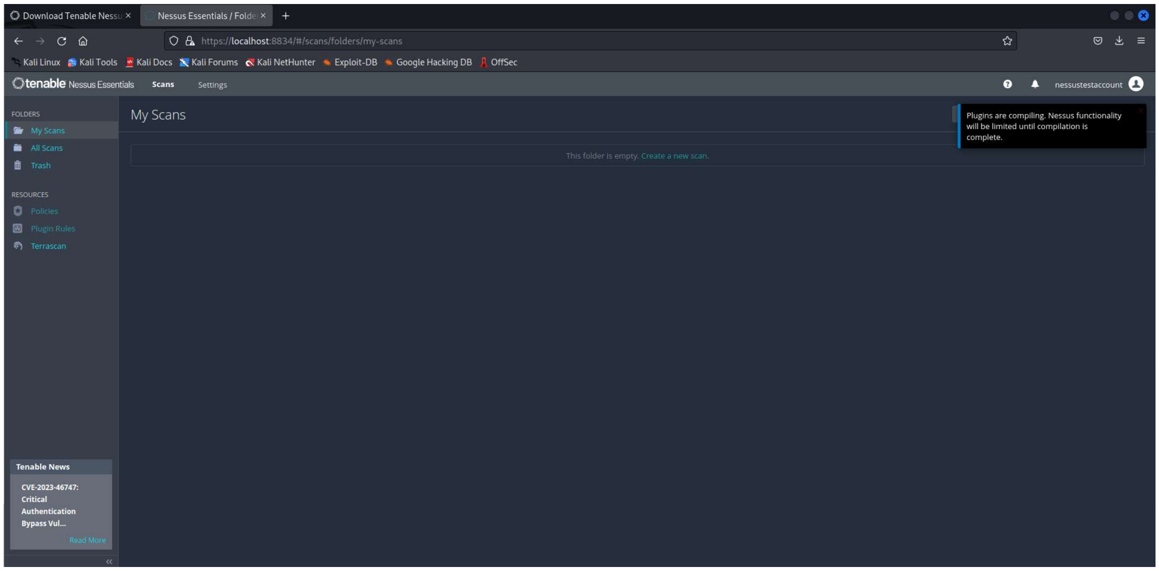
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo systemctl start nessusd.service

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

After setting up the Nessus file, I was able to go to the localhost link, in order to open up the Nessus GUI.   I then created an account on the image shown below.



After setting up my account, below is what the screenshot looked like.



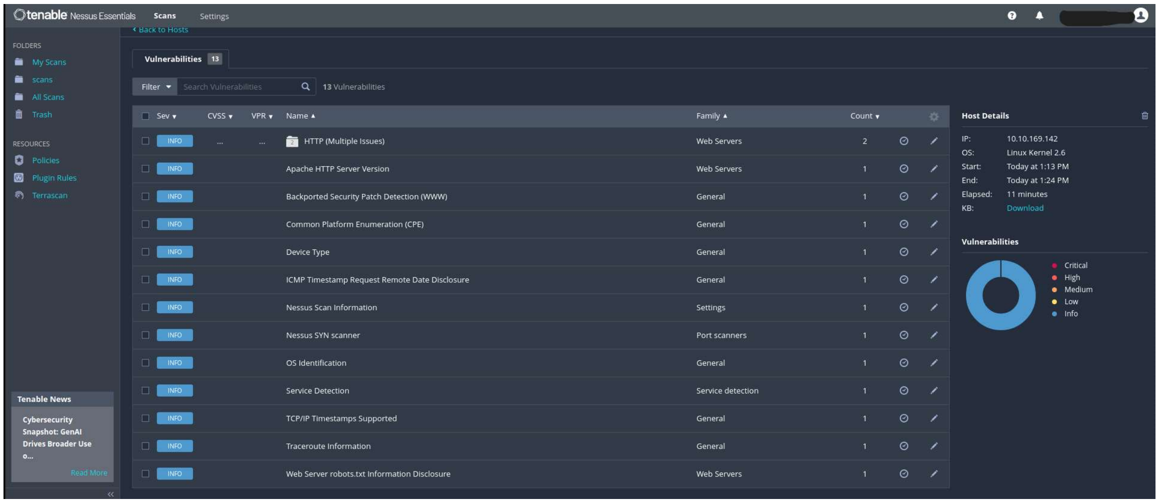
My Scans

Plugins are compiling. Nessus functionality will be limited until compilation is complete.

This folder is empty. Create a new scan.

CVE-2023-46747: Critical Authentication Bypass Vul...

I ran a full port scan using low bandwidth settings on the web application, and here are the vulnerabilities that I found.



Cybersecurity Snapshot: GenAI Drives Broader Use o...

13 Vulnerabilities

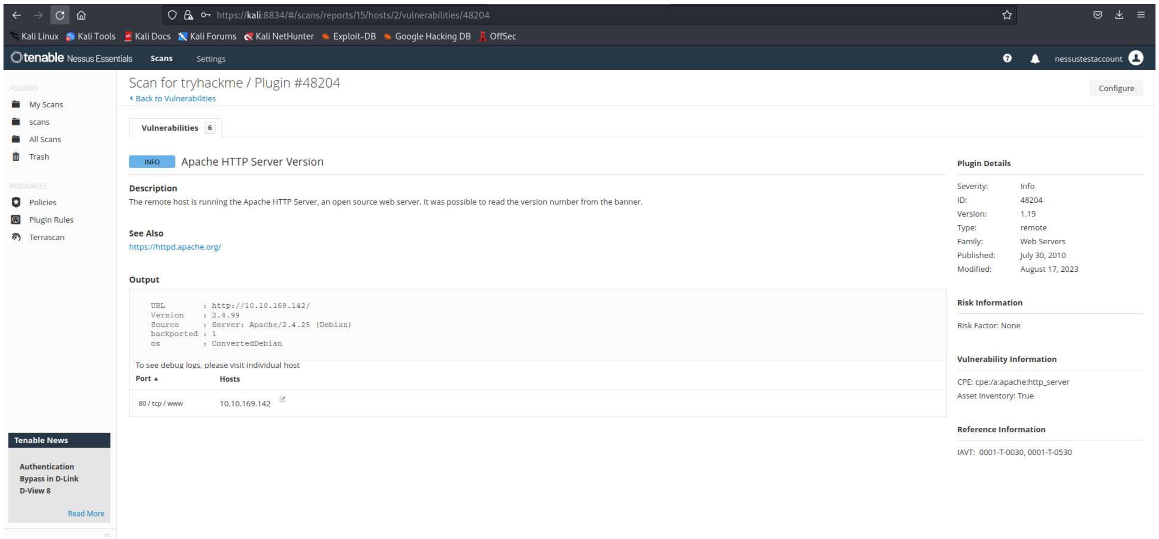
Sev	CVSS	VPR	Name	Family	Count
INFO	...	...	HTTP (Multiple Issues)	Web Servers	2
INFO			Apache HTTP Server Version	Web Servers	1
INFO			Backported Security Patch Detection (WWW)	General	1
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	General	1
INFO			ICMP Timestamp Request Remote Date Disclosure	General	1
INFO			Nessus Scan Information	Settings	1
INFO			Nessus SYN scanner	Port scanners	1
INFO			OS Identification	General	1
INFO			Service Detection	Service detection	1
INFO			TCP/IP Timestamps Supported	General	1
INFO			Traceroute Information	General	1
INFO			Web Server robots.txt Information Disclosure	Web Servers	1

Host Details

IP:	10.10.169.142
OS:	Linux Kernel 2.6
Start:	Today at 1:13 PM
End:	Today at 1:24 PM
Elapsed:	11 minutes
KB:	Download

Vulnerabilities

Below is one of the specific vulnerabilities that I found, and if this was my environment, I would need to move forward by resolving this vulnerability.



Scan for tryhackme / Plugin #48204

Apache HTTP Server Version

Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

See Also

https://httpd.apache.org/

Output

```
  URL        : http://10.10.169.142/
  Version    : 2.4.99
  Source     : Server: Apache/2.4.25 (Debian)
  backported : 1
  os         : ConvertedDebian
```

To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	10.10.169.142

Plugin Details

Severity:	Info
ID:	48204
Version:	1.19
Type:	remote
Family:	Web Servers
Published:	July 30, 2010
Modified:	August 17, 2023

Risk Information

Risk Factor: None

Vulnerability Information

CPE: cpe:/a:apache:http_server
Asset Inventory: True

Reference Information

IAVT: 0001-T-0030, 0001-T-0530