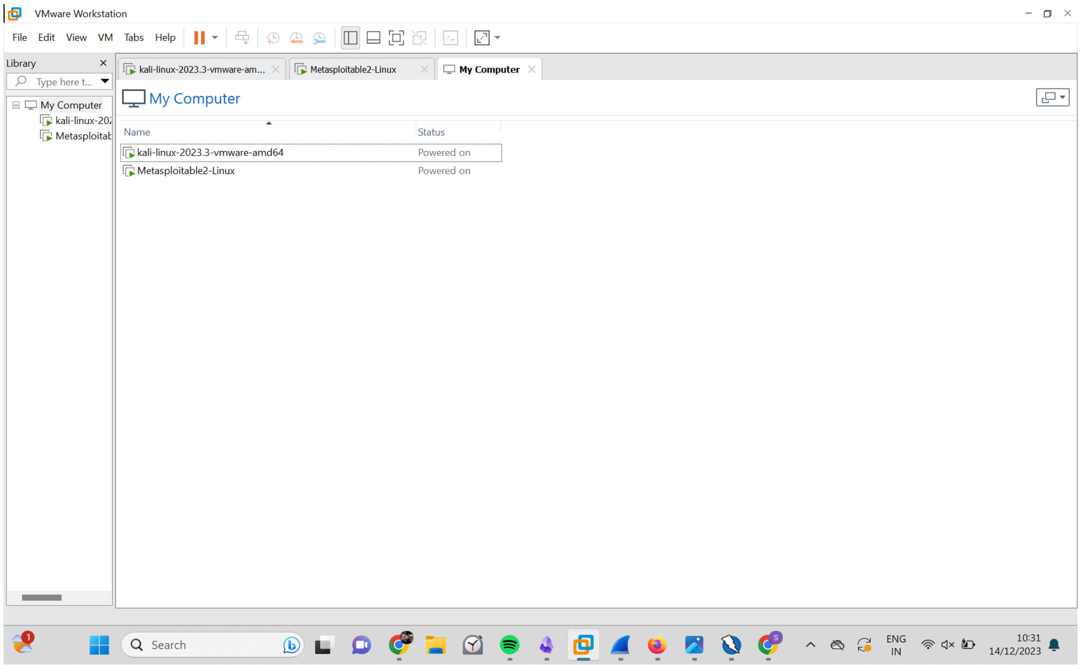
REPORT

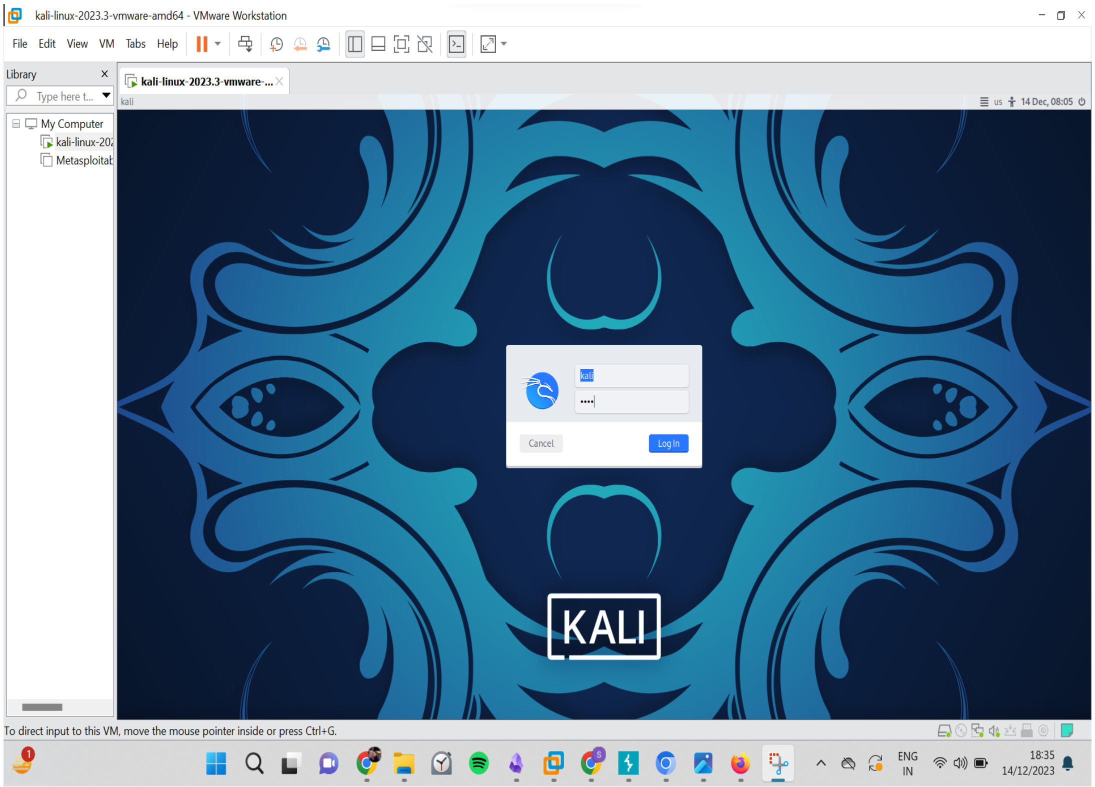
Setup Hacking Lab

1. Setting up VMware

- Open Get into PC in any browser
- Download VMWARE
- Install Metasploitable 2 and Kali Linux in system and add it into Vmware
- Login with the credentials
    - For Kali - Id and pass - kali
    - For metasploit - Id and pass - msfadmin



Name	Status
kali-linux-2023.3-vmware-amd64	Powered on
Metasploitable2-Linux	Powered on



kali

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2. Setting up Wireshark

What is Wireshark?

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

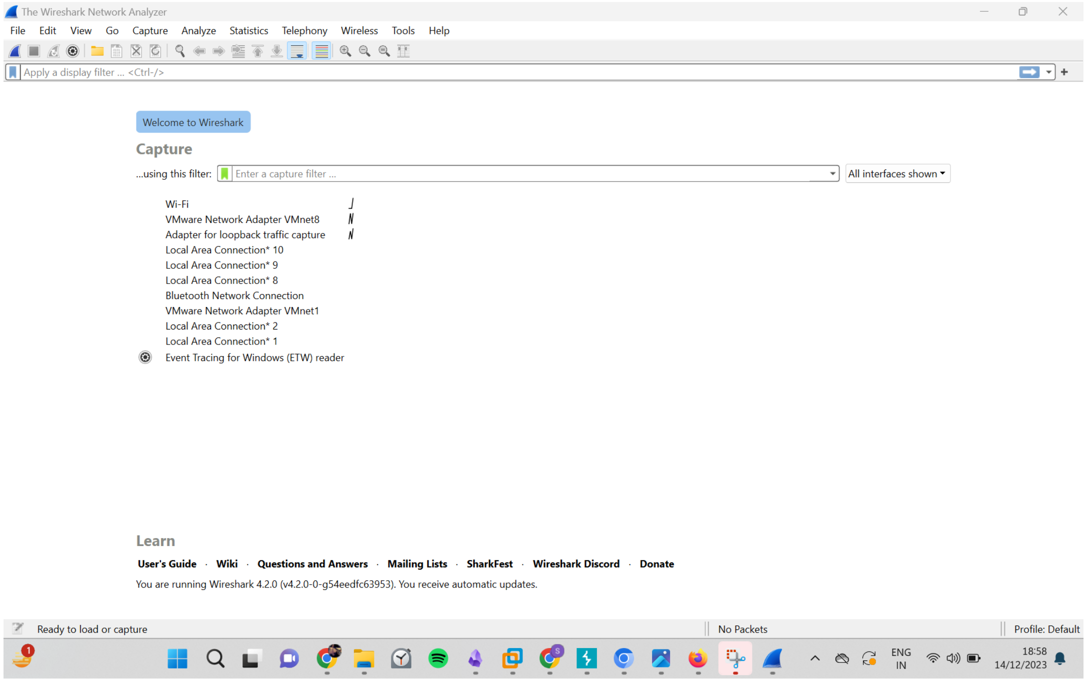
Installation and Configuration steps:

Step 1: Download and Install Wireshark

- Visit Wireshark Download Page.
- Download the appropriate installer (32-bit or 64-bit).
- Run the installer, follow on-screen instructions, and install WinPcap or Npcap if prompted.

Step 2: Launch Wireshark and Capture Packets

- Open Wireshark.
- Choose a network interface.
- Click the green shark fin icon to start capturing packets.
- Analyze captured data.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ... All interfaces shown

Wi-Fi
VMware Network Adapter VMnet8
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
VMware Network Adapter VMnet1
Local Area Connection* 2
Local Area Connection* 1
Event Tracing for Windows (ETW) reader

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.2.0 (v4.2.0-0-g54eedfc63953). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

3. Setting up Nessus

What is Nessus?

Nessus is a vulnerability scanner developed by Tenable, and the steps may vary depending on your operating system. Below are generic steps that should give you a good starting point.

Installation of Nessus Community Edition:

Step 1: Download Nessus:

- Visit the official Tenable website (https://www.tenable.com/products/nessus/nessus-essentials) and locate the download page for Nessus Community Edition.
- Download the appropriate version for your operating system (Windows, Linux, or macOS).

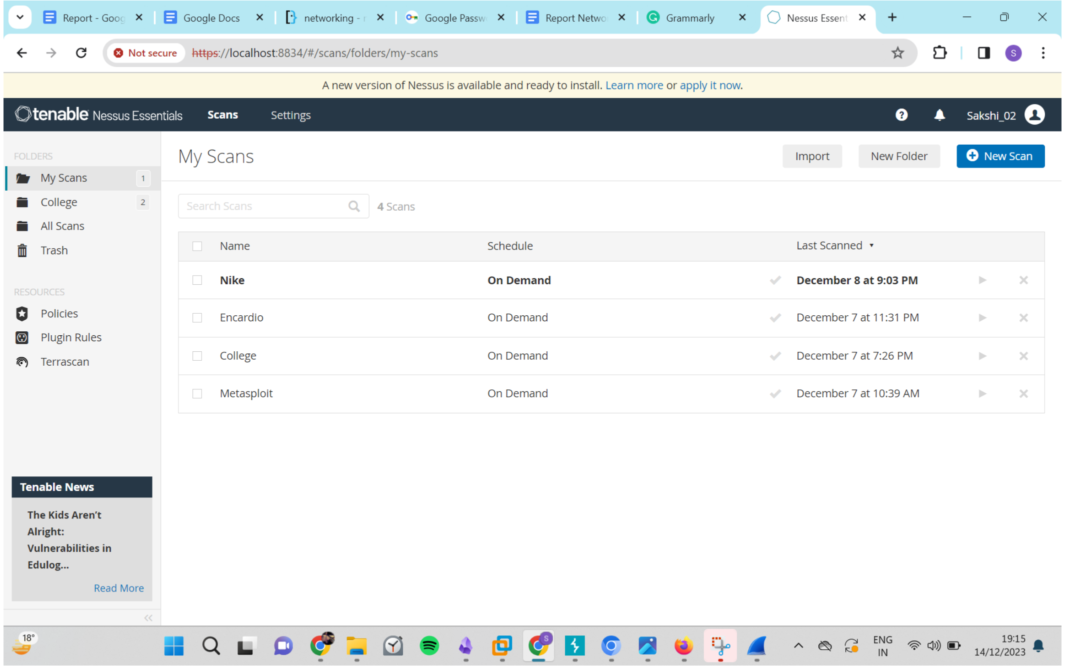
Step 2: Install Nessus:

- Follow the installation instructions provided for your specific operating system.
- On Linux, you may need to use terminal commands to install the package. On Windows, run the installer and follow the on-screen instructions.

Step 3: Setting up Nessus Community Edition:

- Access the Web Interface:
  - Once installed, open a web browser and navigate to https://<your-nessus-server-ip>:8834.
  - The default port for Nessus is 8834.
- Accept License Agreement:

  - Log in with the default credentials (username: tenable, password: tenable).
  - Accept the license agreement and change the password for the default account.
- Product Activation:
  - If required, enter the activation code provided during the download process.
  - Follow any additional prompts to complete the activation process.
- Update Plugins:
  - After logging in, Nessus will check for plugin updates. Allow it to update to ensure you have the latest vulnerability checks.
- Configure Nessus:
  - Configure the scanning preferences, including target hosts, scan type, and other relevant settings.
  - Set up scan schedules and notification preferences as needed.
- Create a Scan:
  - Create a new scan by specifying the target hosts and configuring scan options.
  - Choose from various scan templates based on your requirements.
- Run a Scan:
  - Initiate the scan and monitor the progress.
  - Review the scan results to identify vulnerabilities on the scanned systems.
- Generate Reports:
  - After the scan completes, generate reports detailing the vulnerabilities discovered.
  - Customize reports based on your needs.
- Regular Maintenance:
  - Periodically update Nessus and its plugins to ensure you have the latest security checks.



A new version of Nessus is available and ready to install. Learn more or apply it now.

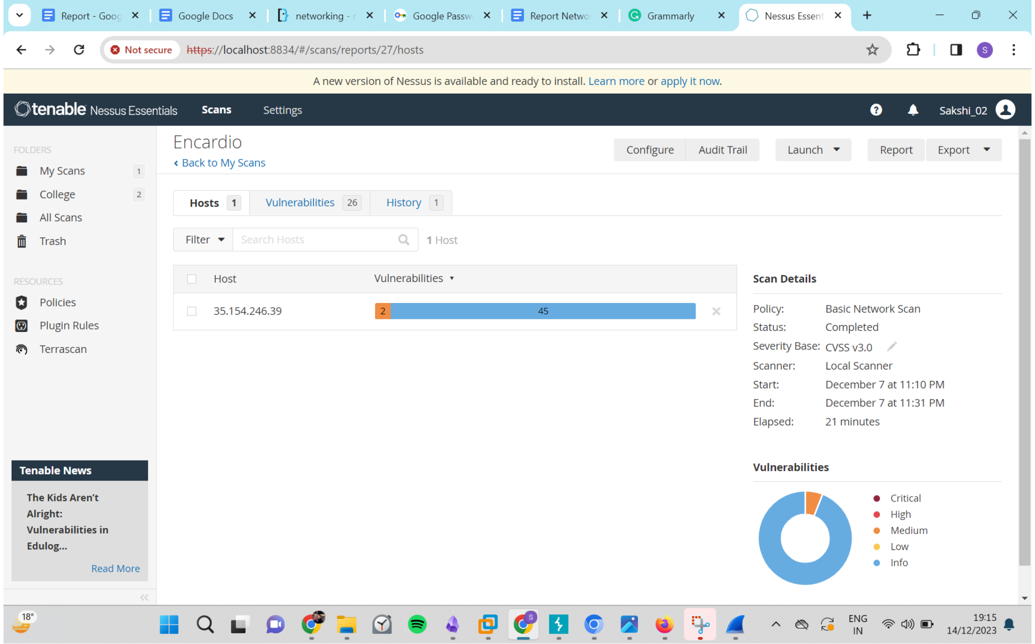
My Scans

4 Scans

Name	Schedule	Last Scanned ▾
Nike	**On Demand**	**December 8 at 9:03 PM**
Encardio	On Demand	December 7 at 11:31 PM
College	On Demand	December 7 at 7:26 PM
Metasploit	On Demand	December 7 at 10:39 AM

Tenable News

The Kids Aren't Alright: Vulnerabilities in Edulog...



localhost:8834/#/scans/reports/27/hosts

A new version of Nessus is available and ready to install. Learn more or apply it now.

Encardio

‹ Back to My Scans

Hosts 1 | Vulnerabilities 26 | History 1

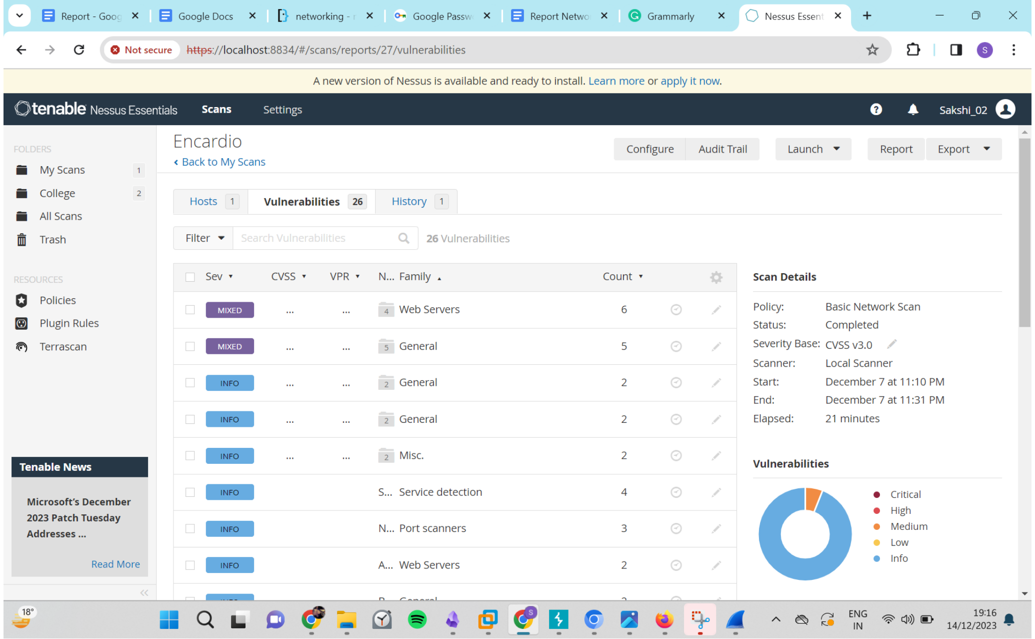
1 Host

Host	Vulnerabilities
35.154.246.39	2 · 45

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: December 7 at 11:10 PM
End: December 7 at 11:31 PM
Elapsed: 21 minutes

Vulnerabilities



localhost:8834/#/scans/reports/27/vulnerabilities

A new version of Nessus is available and ready to install. Learn more or apply it now.

Encardio

‹ Back to My Scans

Hosts 1 | Vulnerabilities 26 | History 1

26 Vulnerabilities

Sev	CVSS	VPR	N...	Family	Count
MIXED	...	...	4	Web Servers	6
MIXED	...	...	5	General	5
INFO	...	...	2	General	2
INFO	...	...	2	General	2
INFO	...	...	2	Misc.	2
INFO			S...	Service detection	4
INFO			N...	Port scanners	3
INFO			A...	Web Servers	2

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: December 7 at 11:10 PM
End: December 7 at 11:31 PM
Elapsed: 21 minutes

Vulnerabilities