THEREDUSERS PVT. LMT.

INTERNSHIP REPORT

SUBMITTED BY

MD AURANGJEB ALAM

Under Supervision

of

Mohammad Narimanov

NALANDA COLLEGE OF ENGINEERING, CHANDI

A Major Project Report On

"CYBER SECURITY ANALYST"

Submitted in partial fulfillment of the requirement for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

AERONAUTICAL ENGINEERING

By:

MD AURANGJEB ALAM

Under The Guidance Of

MOHAMMAD NARIMANOV

Duration – 1 month

Connect us - LinkedIn , Mail

Task 1: Introduction To Network Security

❖Introduction

During my internship, I explored the different types of network threads and how to implement security measures.

I installed virtual machine on window also installed **Wireshark** on Linux for used to monitor suspicious network traffic. I attempted to manually exploit the vulnerabilities identified by Wireshark.

❖ Configuration

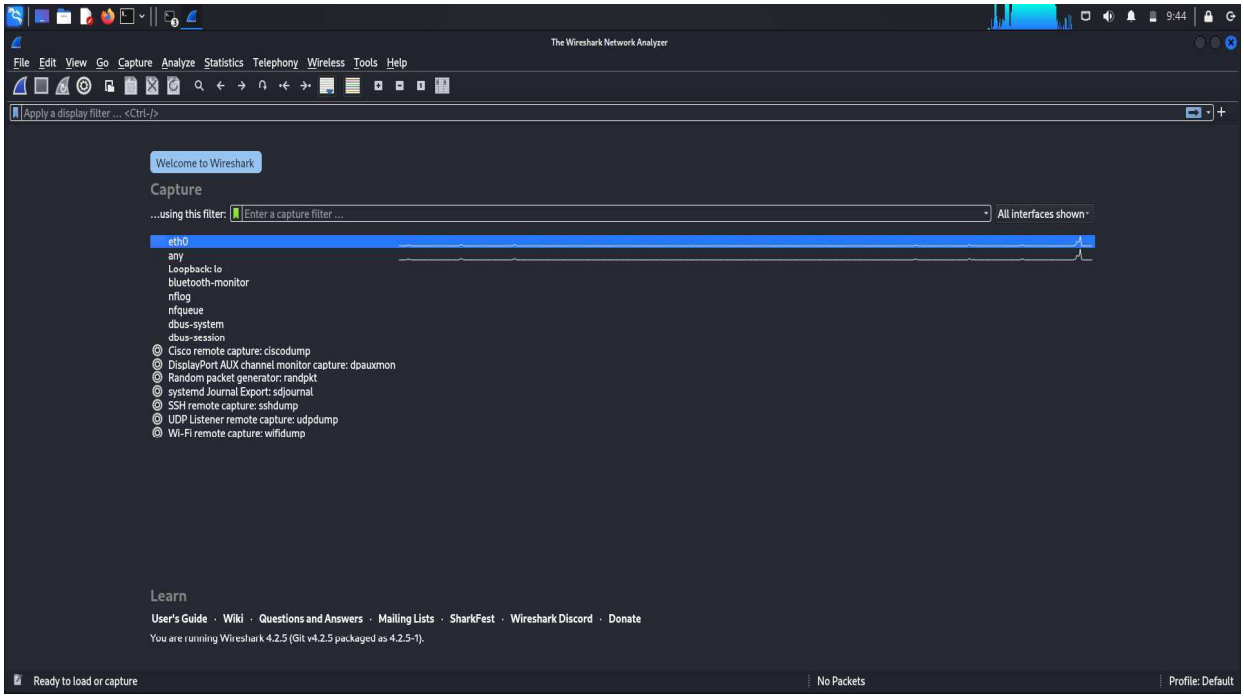
◆ Objective

Wireshark was chosen as the primary learning tool because it is designed to identify malicious activity on network. It is a deliberately, making it a perfect platform for practicing real-world attack scenarios in a controlled environment

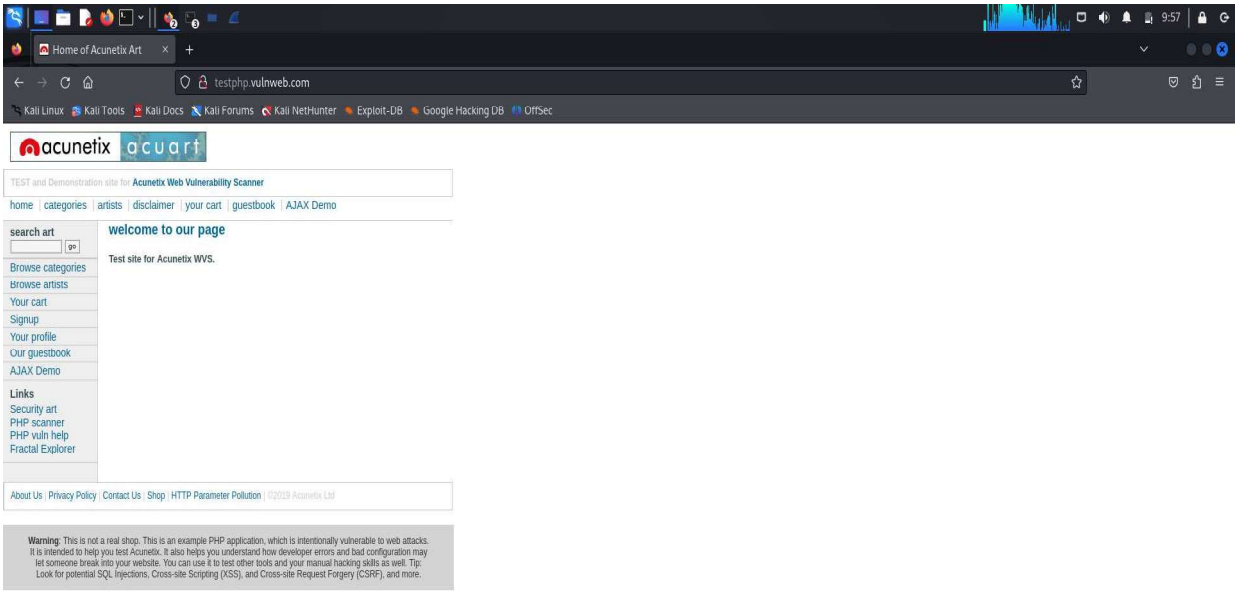
◆ Steps for Installation

- First install Virtual machine (VM ware) / Virtual Box on Window.
- Installed **Kali Linux** on Window machine.
- Set up the virtual environment and download **Wireshark** (pre-installed in kali Linux).
- Configured the kali network set to bridge adapter this allow your host system (window) to communicate with your kali on a network.
- Launch Wireshark on your host system, configure to capture traffic base on your network connection. For instance, 'WIFI'
- Open your kali terminal. Type 'ifconfig' and press inter key. We can see kali **IP** address which are going to lookout in your Wireshark.

- Type '**Wireshark**' in command terminal, Launch Wireshark and choose '**eth0**' interface. All traffic passes through the interface.



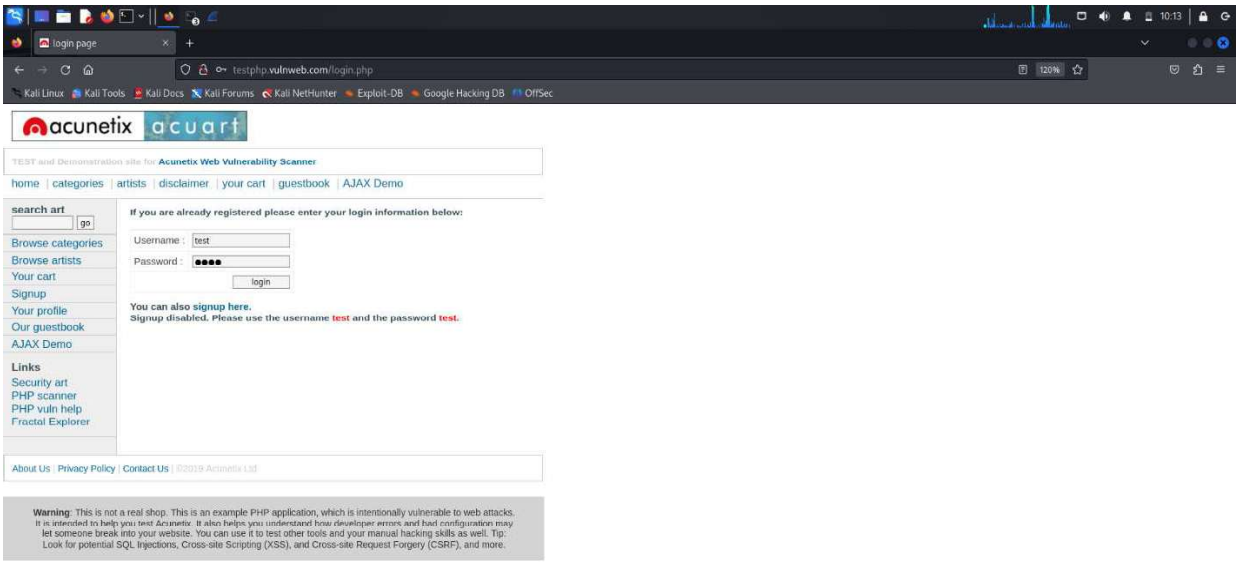
- Open Firefox browser in virtual machine and visit ***http://testphp.vulnweb.com/.***



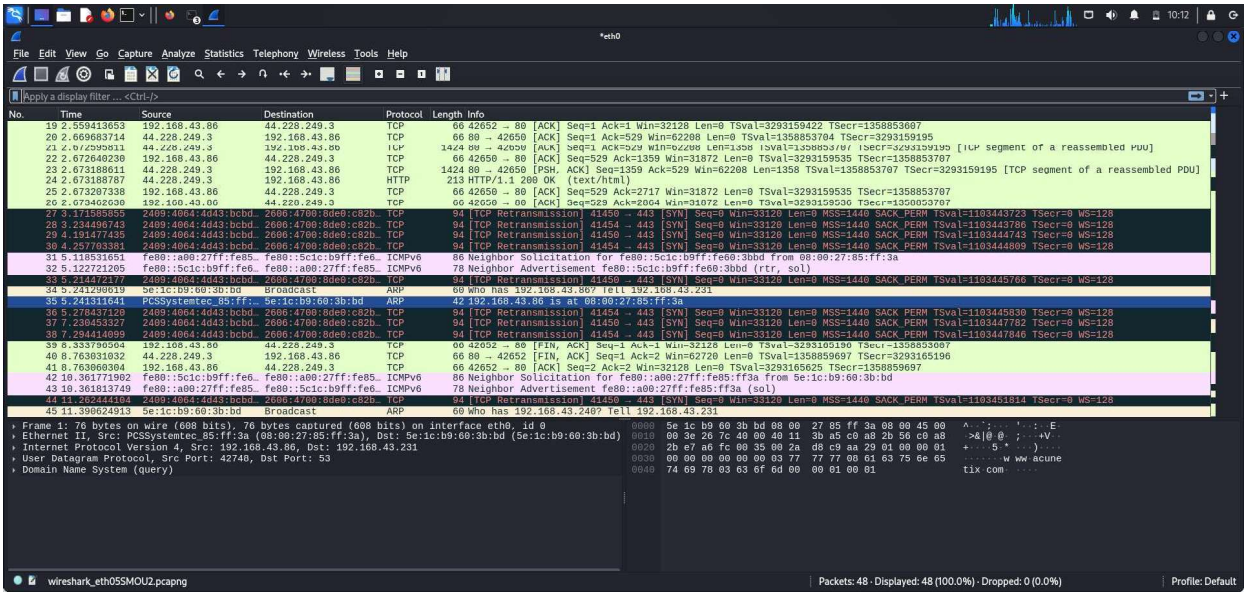
- Go to signup button and login with **credentials**

  Username = **test**

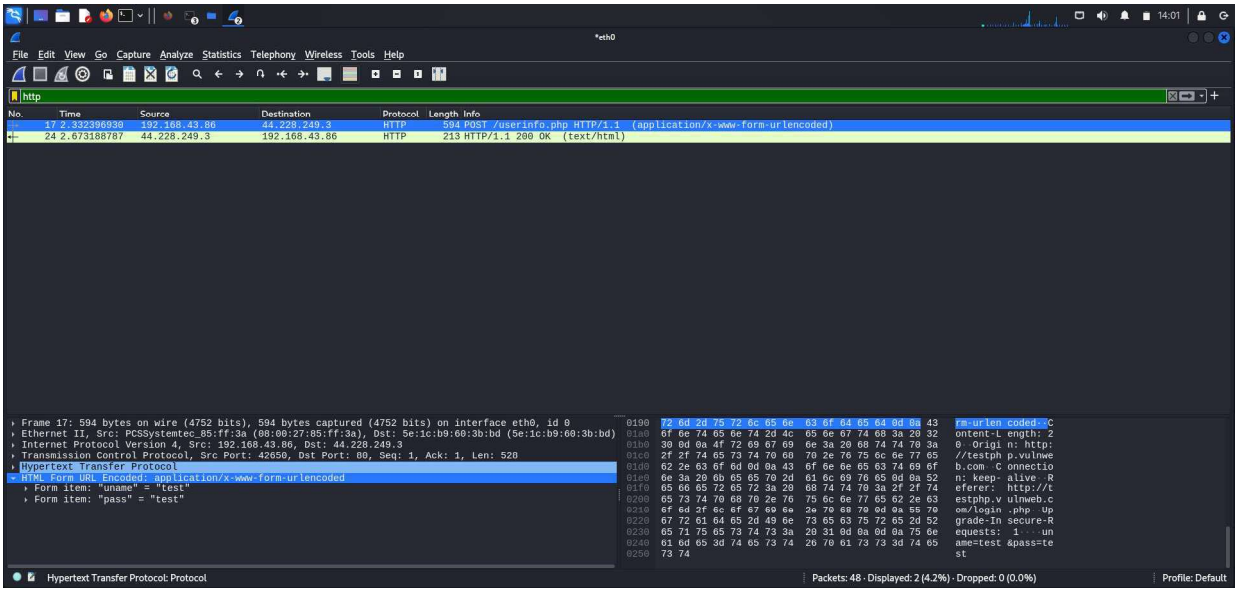
  Password = **test**



- Capture the traffic using Wireshark (looking out for source which is our kali IP address and the destination).

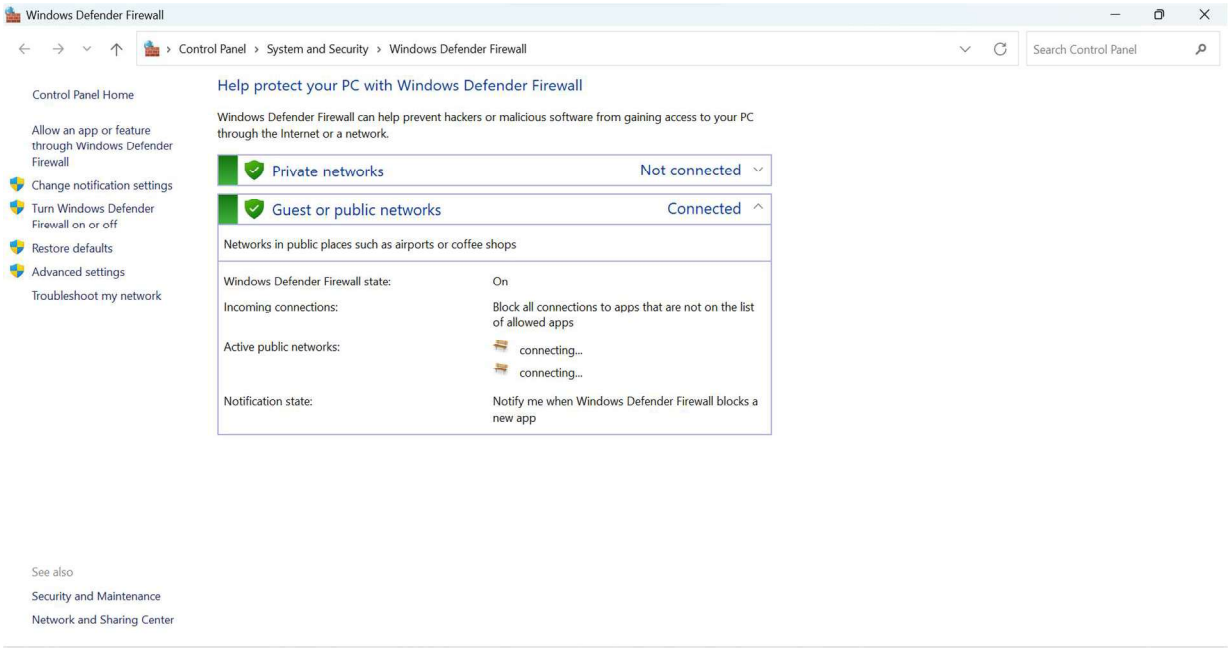


- Using filter option filter for **‘http’** and find post request. The login credentials are visible because http protocol is **unsecured**.

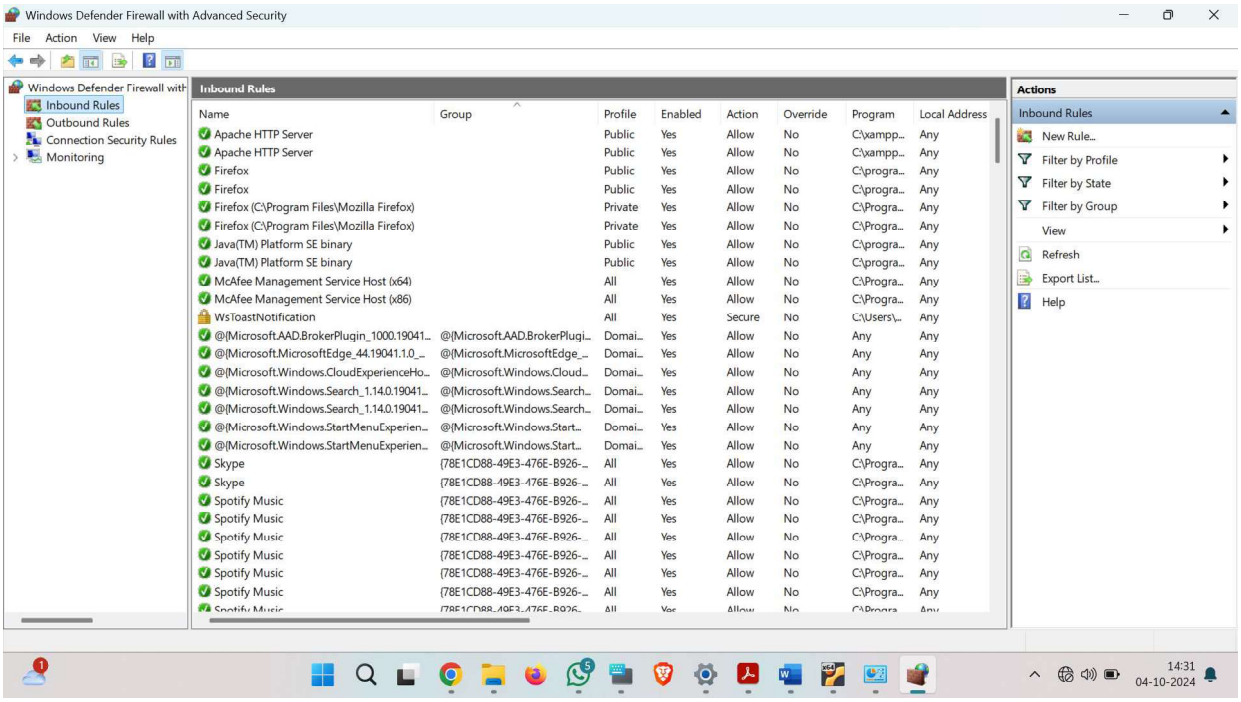


◆ Security measure

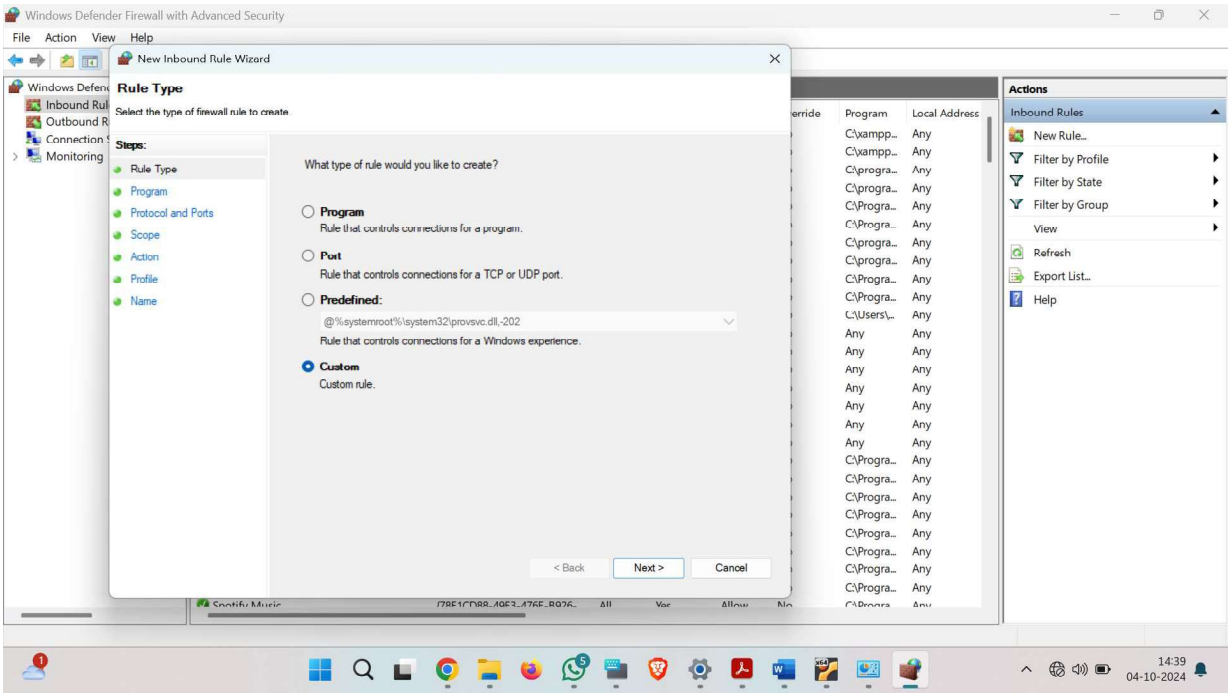
- To implement security measures by using window **Firewall** on host system. Open window firewall and go to advance setting.



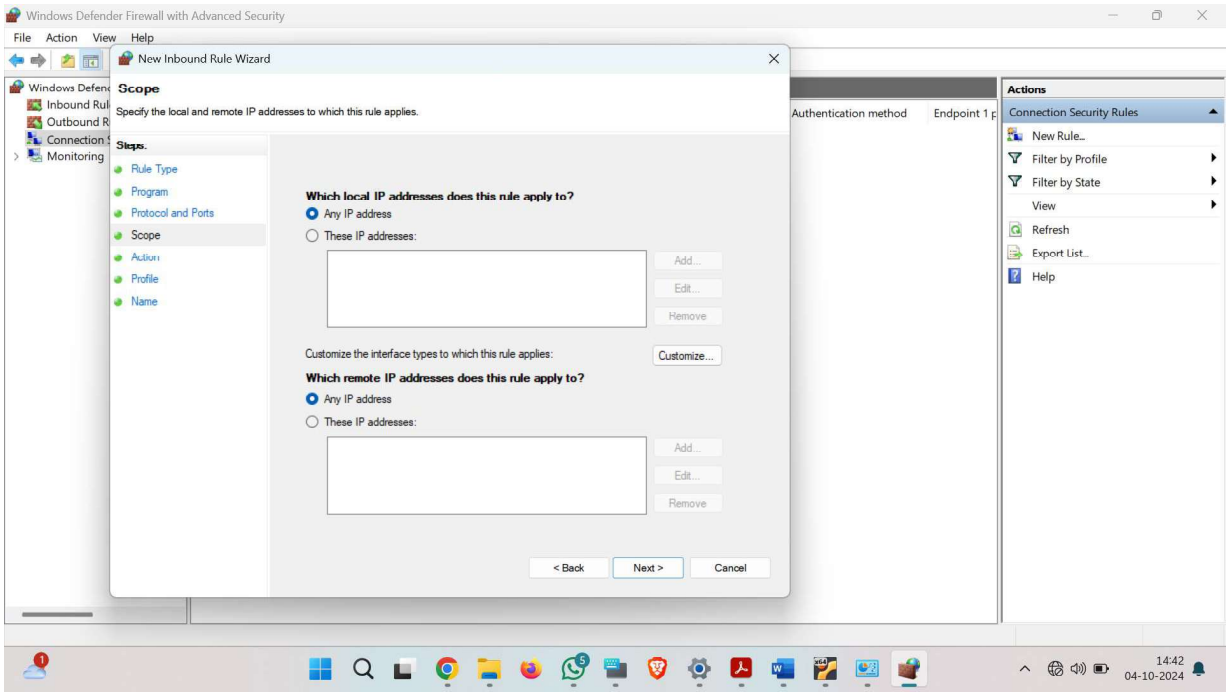
- After click on advanced setting go to inbound rules.



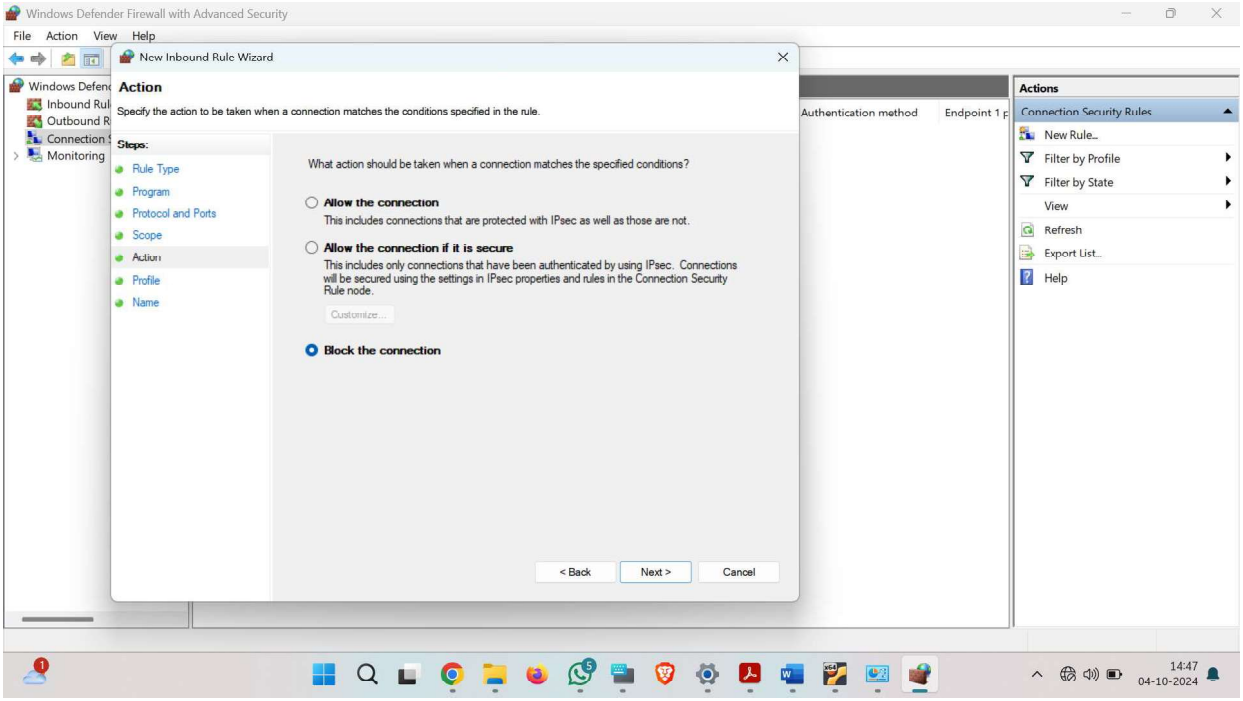
- Click on New Rules in right side and select ‘Custom’ from rule type.



- Click on ‘scope’ you have local and remote IP address sections.



- Set the rule on local IP address input your desired device IP address which you intend to block it access to your local network.
- Go to the ‘**Action**’ section and block the connection.



- Again, go to '**Name**' section and input name to identify the rule you just created. Click finish.
- You can see your added inbound Rule. We add a **test** name inbounded rule for demo purpose.