Assignment 1 Information Security

M Ali Awan

21L-5648

BDS – 7C

Table of Contents

1. Prerequisites

2. Virtual Machines Setup and Configuration

3. Identifying Target Machine's IP Address

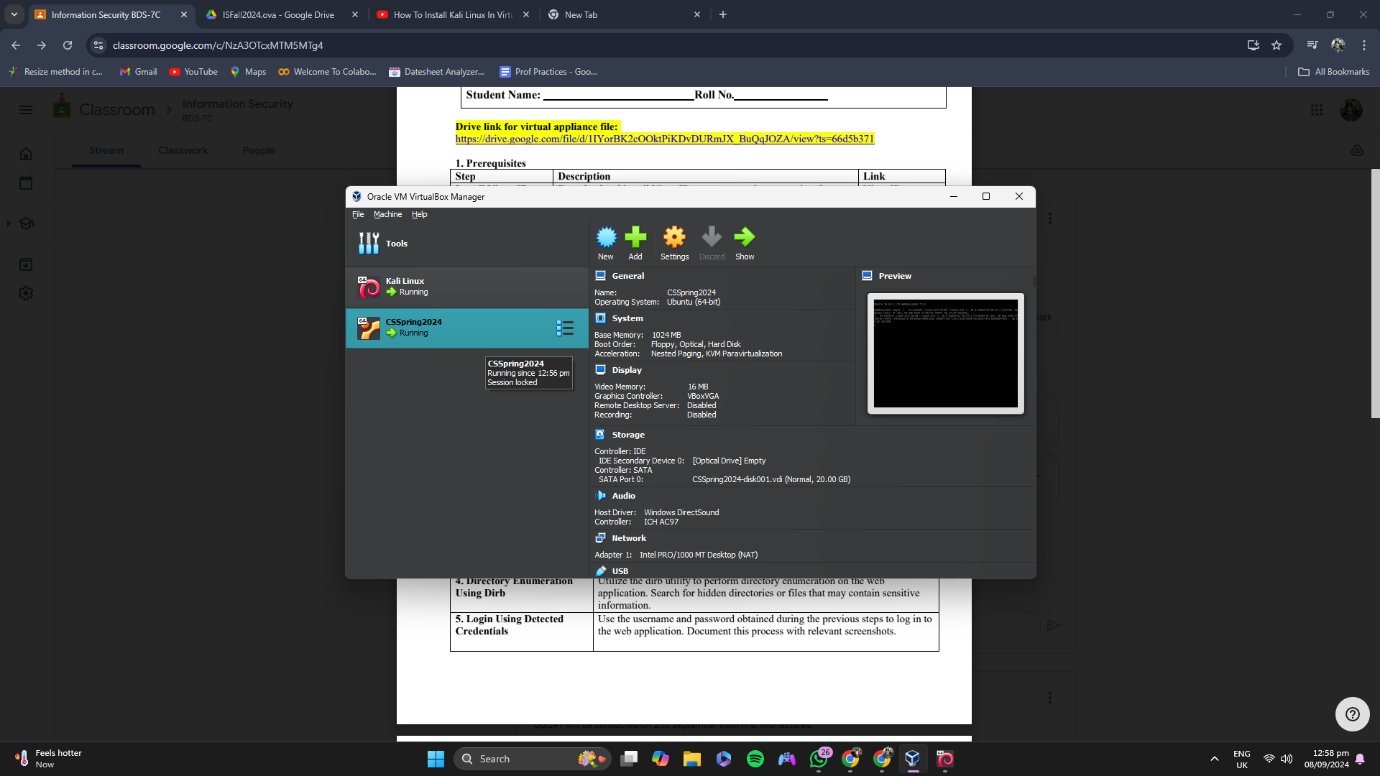
4. Determining Open Ports and Services

5. Identifying Vulnerabilities in Web Application

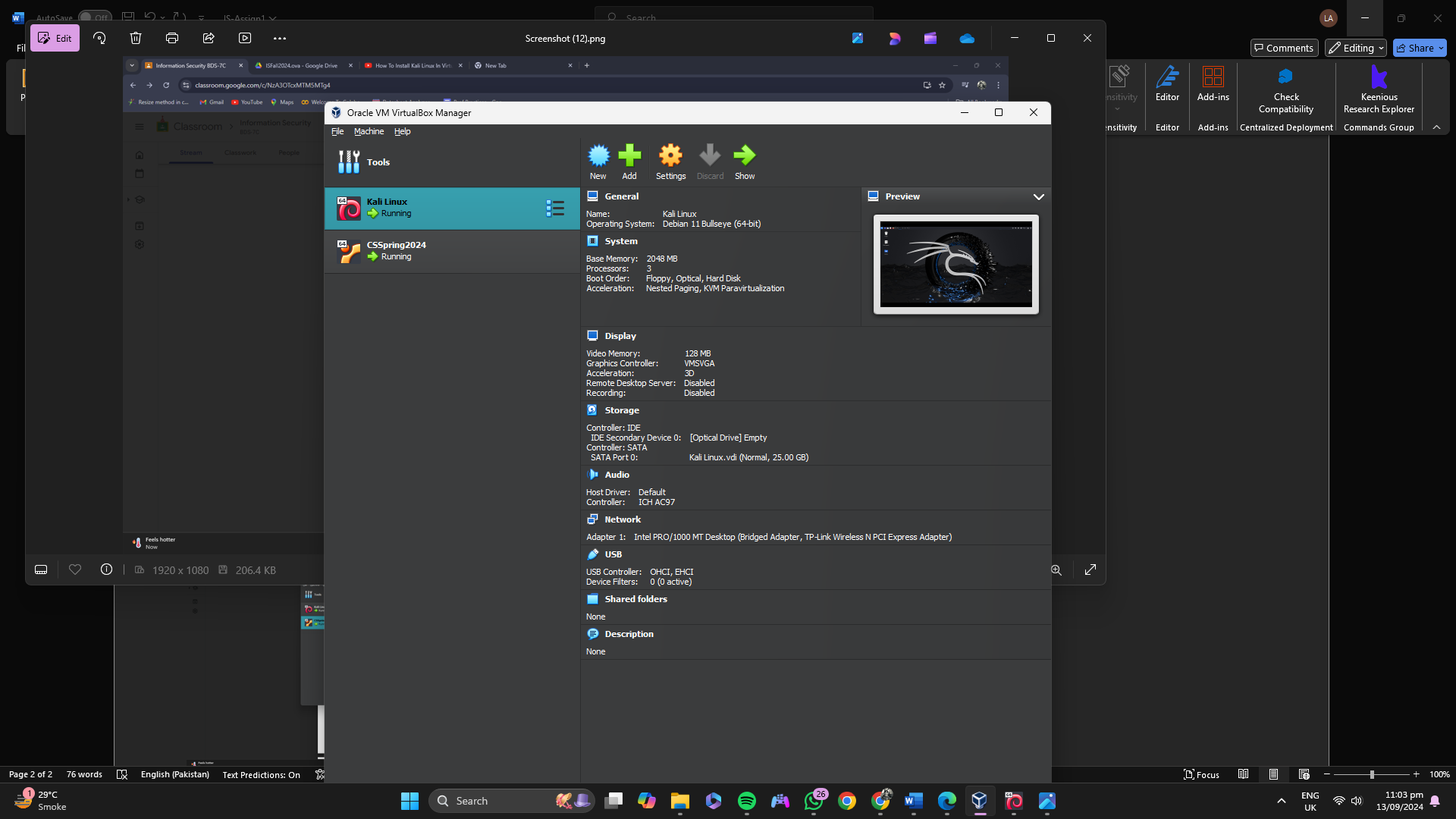
6. Directory Enumeration Using Dirb

7. Logging In Using Detected Credentials

# Screenshot and Table

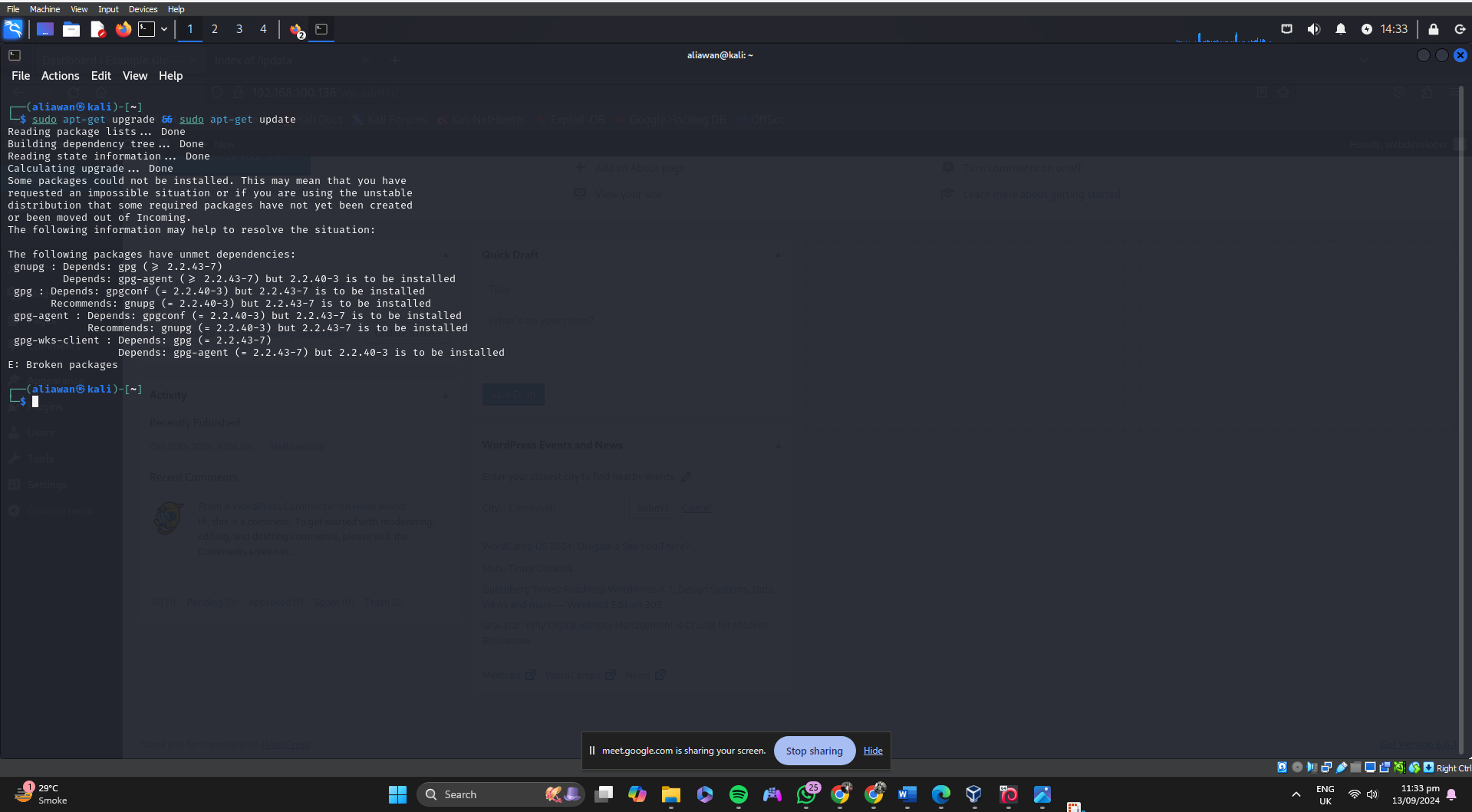


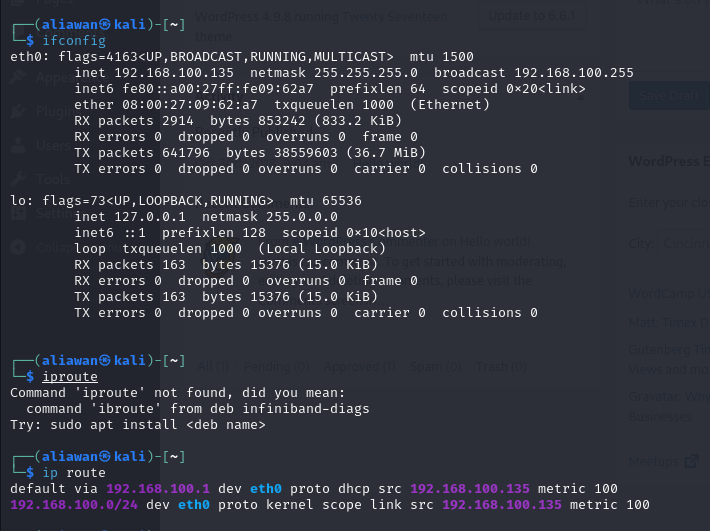
This shows that I have both kali Linux and CSspring 2024 which is my target machine installed into my virtual box.



We can see the network settings for both kali Linux and csspring 2024 , Kali Linux settings where changed according to the settings in the Yt video.

## Updating and Upgrading



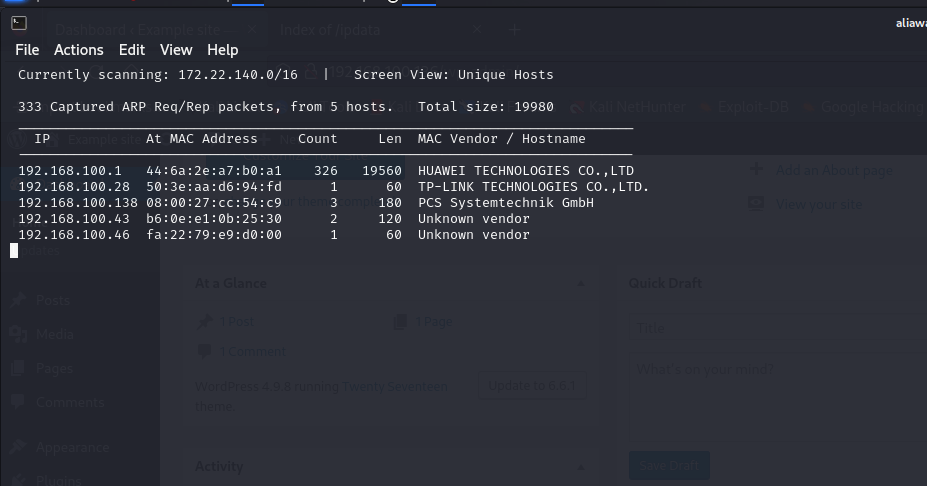


|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VM | IP Address | Subnet mask | Default Gateway | Network Adapter |
| Kali Linux | 192.168.100.135 | 255.255.255.0 | 192.168.100.1 | Bridge Adapter |
| CSspring | 192.168.100.136 | 255.255.255.0 | 192.168.100.1 | Bridge Adapter |

## 3. Target Machine Ip Address

I have used netdiscover tool to identify the target machine IP address in my case which was a wordpress site. We use this command to scan and find devices connected to same subnet.

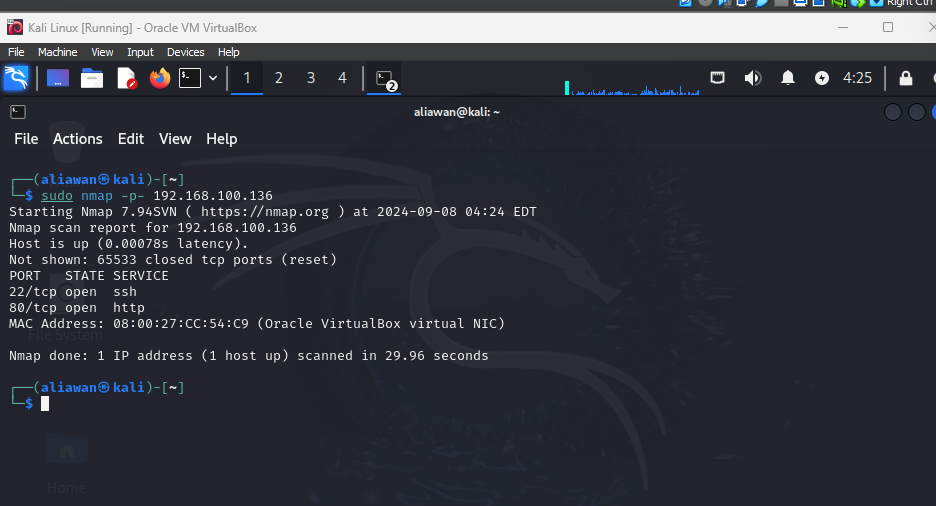
It will list devices along with their IP and Mac Address.



## 4.Determining Open Ports and Services

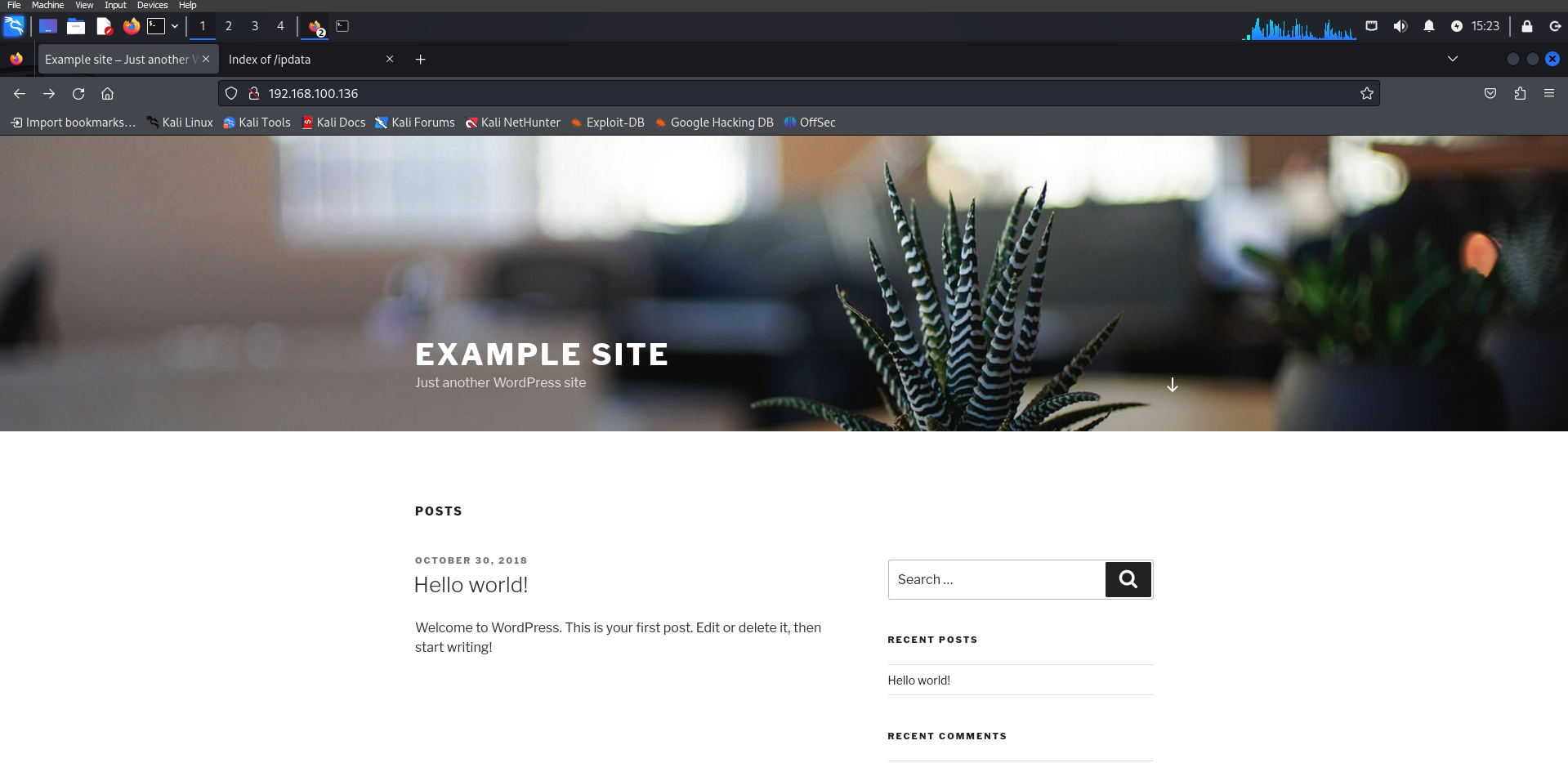
I have used nmap tool that give me port, state and service of my targeted virtual machine.

The command i used is sudo nmap -p- 192.168.100.136



## 5. Identifying the Vulnerabilities

In our given case I was not able to log in to Word press site because we did not have the credentials. It was running on port 80. I tried to hack into the site by brute force approach of getting the password combination but it also did not work , but somehow I managed to get the login



Login = webdeveloper

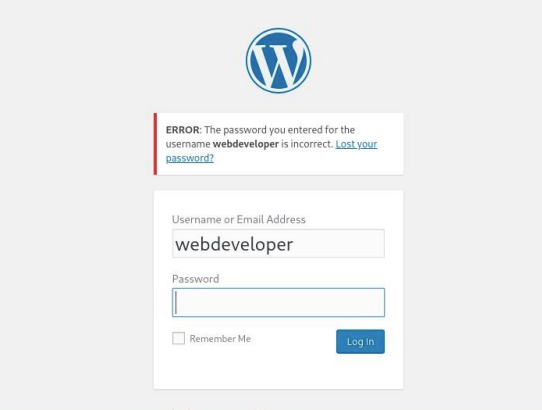
Password = We can’t figure out till now.

To access the password i tried this method of brute force using hydra

hydra -l webdeveloper -P /usr/share/wordlists/rockyou.txt 192.168.100.136 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^:F=Invalid username"

This command was used to get the login id

$ wpscan --url http://192.168.100.136 --enumerate u



## 6. Directory Enumeration Using Dirb

I used dirb command to uncover hidden information and perform directory enumeration and to find sensitive files and data.

**dirb** [**http://192.168.100.136**](http://192.168.100.136)

****

These are the few results I obtained from this drib command

----------------- DIRB v2.22 By The Dark Raver ----------------- START\_TIME: Sun Sep 8 05:27:54 2024 URL\_BASE: http://192.168.100.136/ WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt ----------------- GENERATED WORDS: 4612 ---- Scanning URL: http://192.168.100.136/ ---- + http://192.168.100.136/index.php (CODE:301|SIZE:0) ==> DIRECTORY: http://192.168.100.136/ipdata/ + http://192.168.100.136/server-status (CODE:403|SIZE:303) ==> DIRECTORY: http://192.168.100.136/wp-admin/ ==> DIRECTORY: http://192.168.100.136/wp-content/ ==> DIRECTORY: http://192.168.100.136/wp-includes/ + http://192.168.100.136/xmlrpc.php (CODE:405|SIZE:42)

Vulnerabilities and Weaknesses:

The key findings were that they were using an outdated version 4.9.8

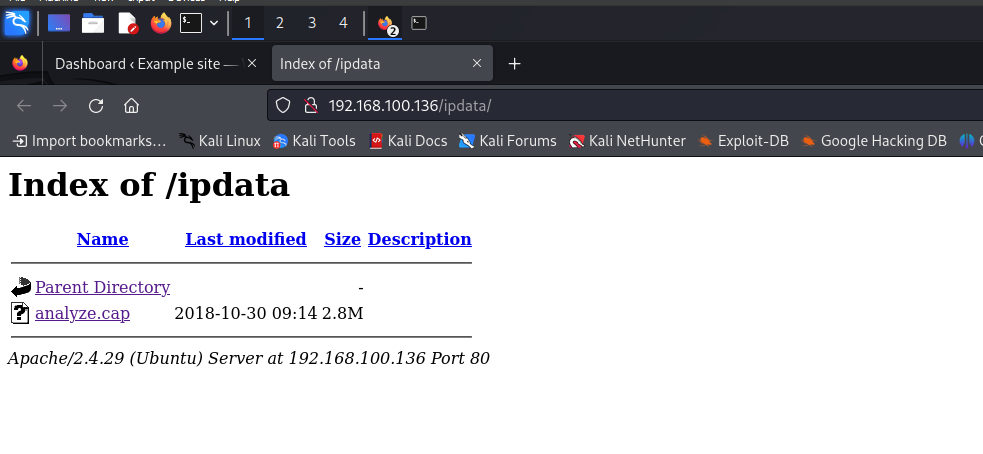
The theme of wordpress was also outdated

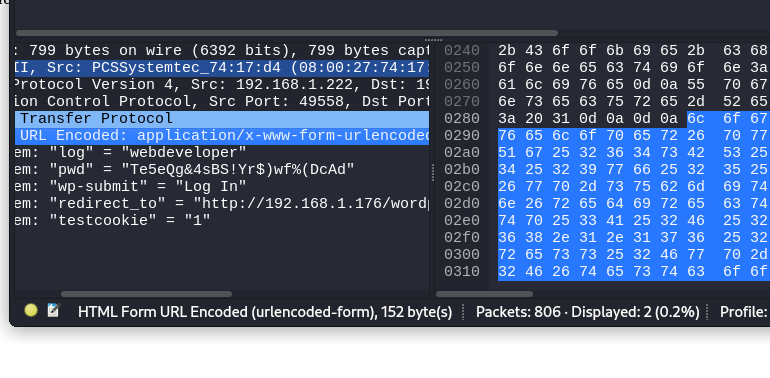
There were open Ports

## 7. Login using credentials

I found a **.cap** file in the **/ipdata/** directory and opened it in **Wireshark**. By filtering the HTTP POST requests, I was able to spot some interesting traffic that might contain sensitive information.

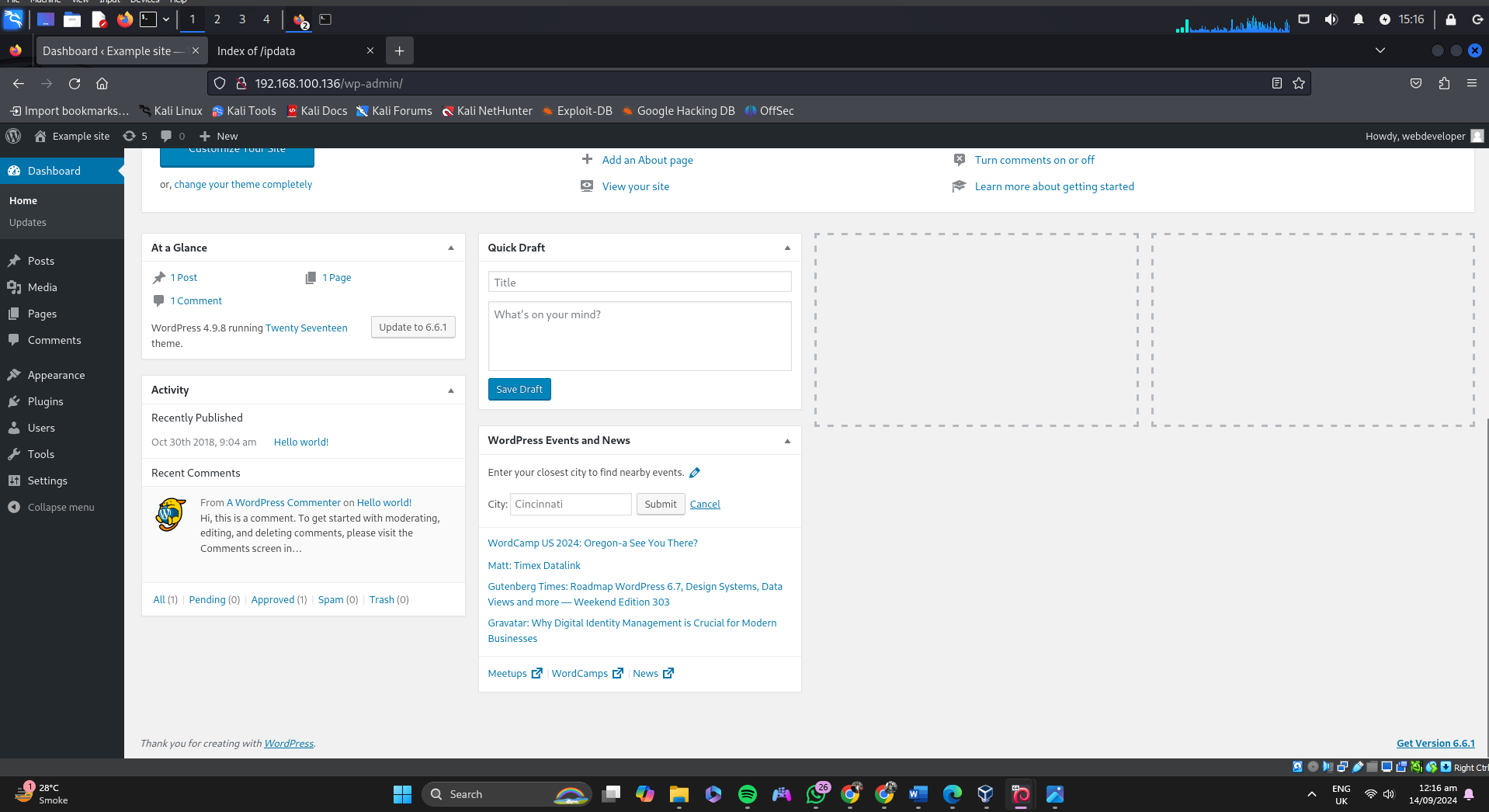
After going through the data carefully, I discovered login credentials in a POST request sent to **/wordpress/wp-login.php**. Using these credentials, I was able to log into the WordPress admin panel.





A screenshot of a computer

Description automatically generated



Here is an attached snap i sent on Sunday out of excitement for competing this assignment before time. I hope you will not mind me attaching this screenshot of my snap 😊

A computer screen with a screenshot

Description automatically generated