

**KING’S OWN INSTITUTE\***

**Success in Higher Education**

# 

# INDIVIDUAL ASSIGNMENT COVERSHEET

Family Name: AUSTRIA Given Name: JOHN BENNY

Student Number: 12301175 Lecturer’s Name: DR. PRABHU JYOT SINGH

Subject Name: ICT740 Applied Cybersecurity

Assignment Title: Assessment 2: Vulnerability Testing

**Declaration**

(This declaration must be completed by the student or the assignment will not be marked.)

I certify the following:

* I have read and understood the *Student Academic Misconduct Policy*
* This assignment is my own work based on my personal study and or research.
* I have acknowledged all material and sources used in the preparation of this assignment including any material generated in the course of my employment.
* The assignment has not previously been submitted for assessment.
* I have not copied in part or in whole or otherwise plagiarised the work of other students.
* I have read and I understand the criteria used for assessment.
* The assignment is within the word and page limits specified in the unit outline.
* The use of any material in this assignment does not infringe the intellectual property / copyright of a third party.
* I understand that this assignment may undergo electronic detection for plagiarism, and an anonymous copy of the assignment may be retained on the database and used to make comparisons with other assignments in future.
* By completing this coversheet in full and submitting this assignment electronically, I am bound by the conditions of the KOI’s *Student Academic Misconduct Policy* and the declaration on this coversheet.

J\_AUST

01 / 09 / 2024

Signature Date

----------------------------------------------------------------------------

**Assignment Receipt**

Family Name: AUSTRIA Student Number: 12301175

Given Name:(s) JOHN BENNY

Lecturer’s Name: DR. PRABHU JYOT SINGH

Subject Name: ICT740 Applied Cybersecurity

Assignment Title: Assessment 2: Vulnerability Testing

J\_AUST

01 / 09 / 2024

Signature Date

INDIVIDUAL ASSIGNMENT COVER SHEET \* AUSTRALIAN INSTITUTE OF BUSINESS AND MANAGEMENT PTY LTD PAGE **1** OF **1**

1. JULY 2015 CRICOS 03171A ABN: 72 132 629

# TABLE OF CONTENTS

[INDIVIDUAL ASSIGNMENT COVERSHEET 1](#_Toc176047042)

[TABLE OF CONTENTS 2](#_Toc176047043)

[1.0. INTRODUCTION 3](#_Toc176047044)

[2.0. VULNERABILITY ANALYSIS 4](#_Toc176047045)

[2.1. Port 25: SMTP 8](#_Toc176047046)

[2.2. Port 80: http 9](#_Toc176047047)

[2.2.1. Browser Version 13](#_Toc176047048)

[2.3. Port 5900: VNC 15](#_Toc176047049)

[2.4. Port 3306: MySQL 17](#_Toc176047050)

[3.0. SUMMARY 20](#_Toc176047051)

[4.0. REFERENCES 21](#_Toc176047052)

# INTRODUCTION

Cyber risk rises as the number of interconnected systems of technology expands each day. Impacting one or more of the three attributes of information, Confidentiality – Integrity – Availability, is a result of cyber risk. System developers must prioritize in predicting the exploitability of such vulnerabilities to contain rich semantic information and develop a patch for the vulnerabilities discovered.

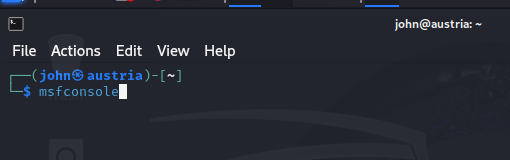
The Metasploit Framework is a testing platform for modular penetration that enables users to test, write and execute exploit code. Testing the security vulnerabilities, enumerating networks, executing attacks and evading detection are some of the suites of tools that Metasploit offers to its users. The core of Metasploit Framework is to provide users an environment for penetration testing and exploit development (Rapid7, 2022).

Metasploitable2 as defined by Kumar (2023) is “a tool developed by Rapid7 for the purpose of developing and executing exploits against vulnerable systems.” Metasploitable2 is a virtual machine that aids users for penetration testing and configuring of exploits in open ports. It is a signature development in Intrusion Detection System.

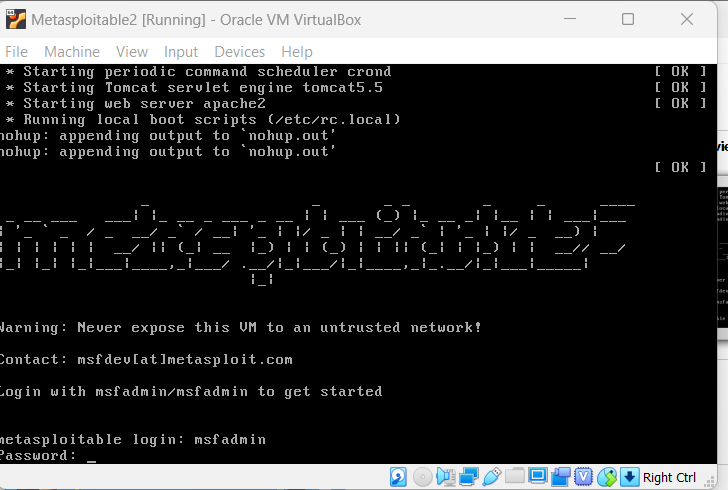
This paper will look at Metasploit Framework in Kali Linux as the host to exploit vulnerabilities in Metasploitable2. The network connection between the two virtual machine is ensured by making a new Nat Network in the Tools of the Oracle Virtual Box Manager. Metasploitable2 will be scanned by Nmap to determine the IP Address, Open Ports and OS running in the virtual machine. Metasploit Framework will be used to exploit four open ports from Metasploitable2. Finally, a summary section is included to analyse the tools and listed down the advantages and limitation of each tool.

# VULNERABILITY ANALYSIS

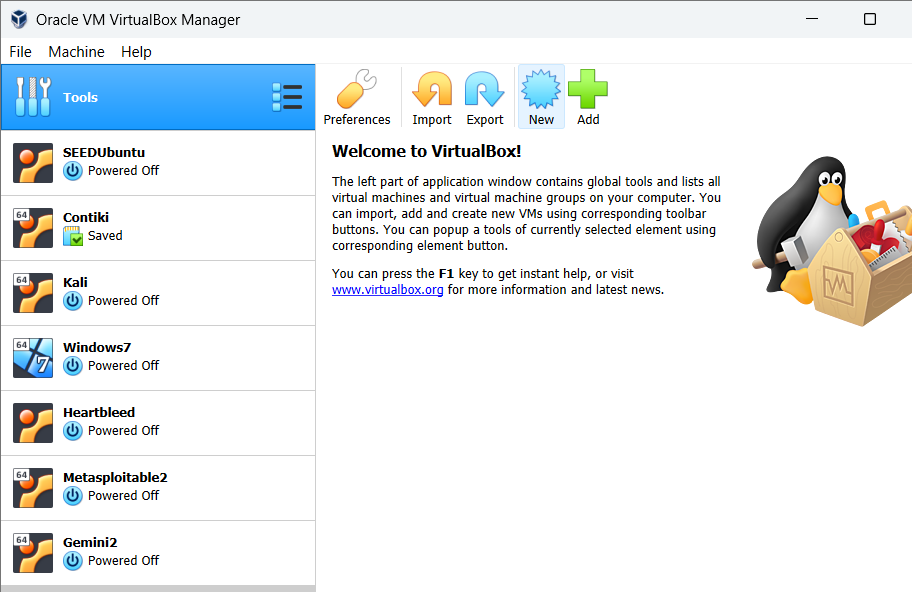
Metasploit Framework is a built-in testing platform of Kali Linux. Accessing Metasploit Framework is done by running the code ‘msfconsole’ in the prompt bar of a terminal in Kali Linux.



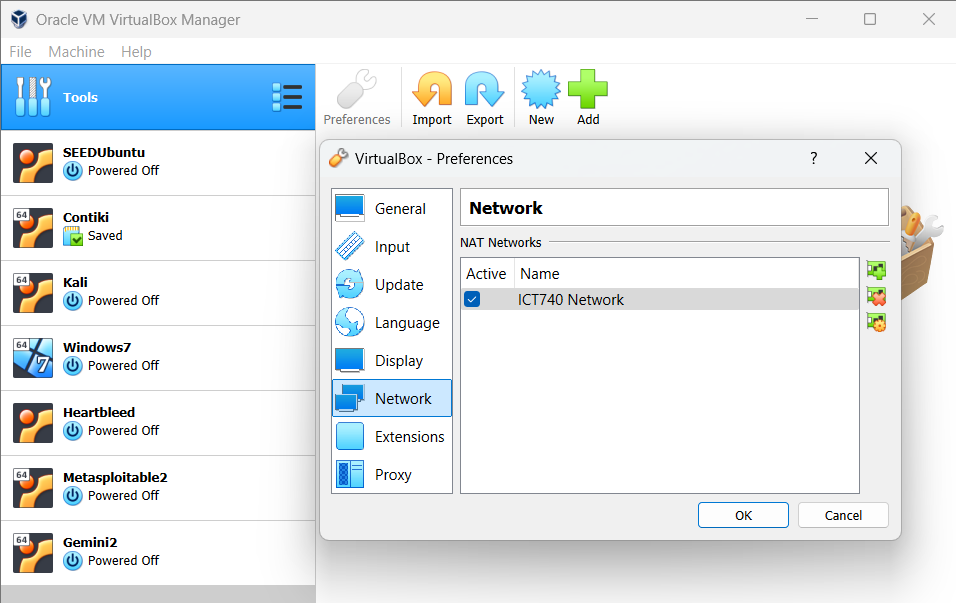
Metasploitable2 is a virtual machine that can be installed in vulnhub.com. To get started in Metasploitable2, I typed ‘msfadmin’ in the metasploitable login, and entered ‘msfadmin’ in the Password.



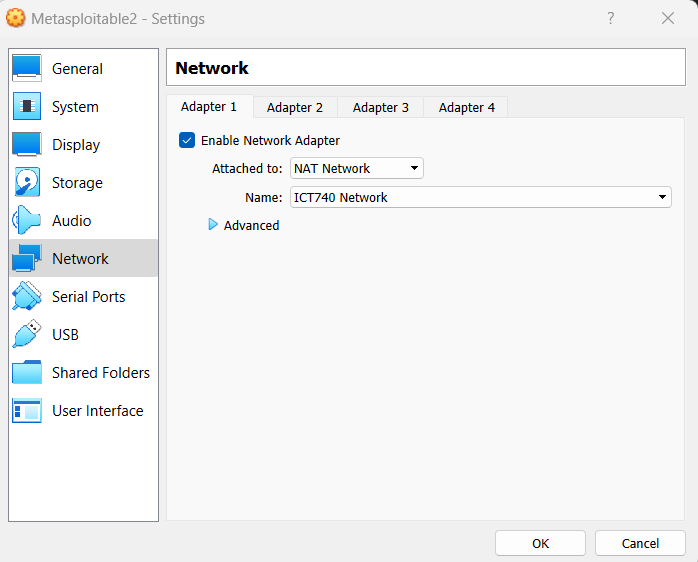
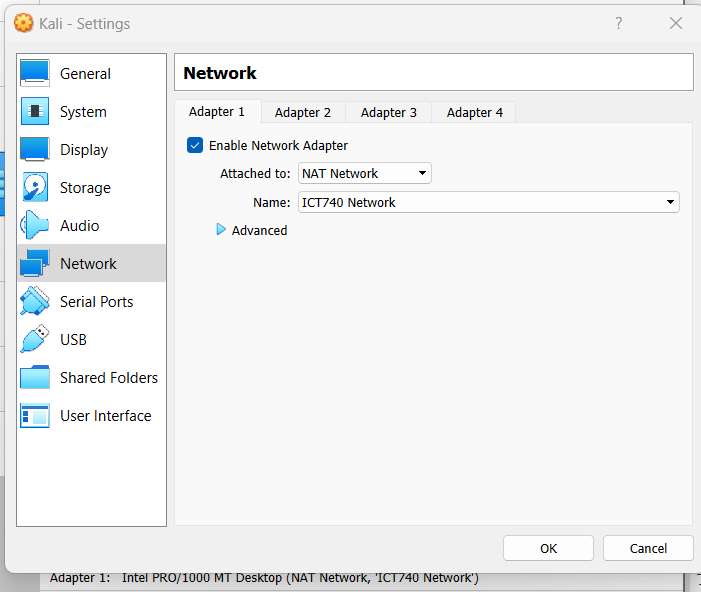
Before I start to exploit the vulnerabilities of Metasploitable2, I had to make sure that my Kali Linux and Metasploitable2 are connected to one network. To do this, I had to go to Tools, then pressed Preferences.



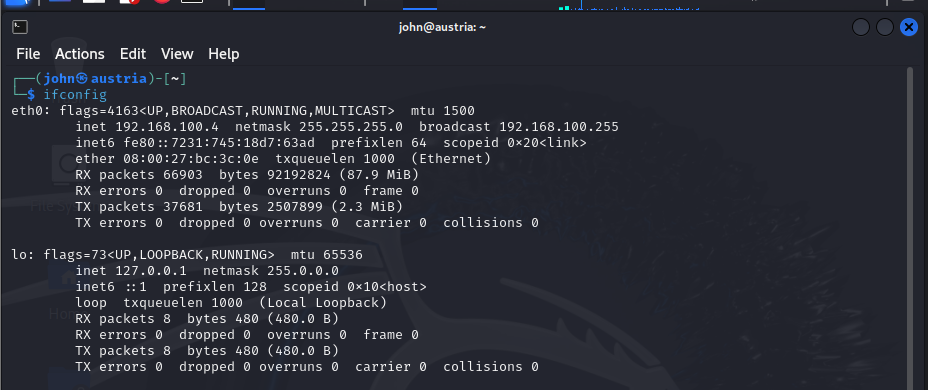
Then, I went to Network tab of Preferences, created a new Nat Network, named the Nat Network “ICT740 Network”, the pressed ‘OK’.

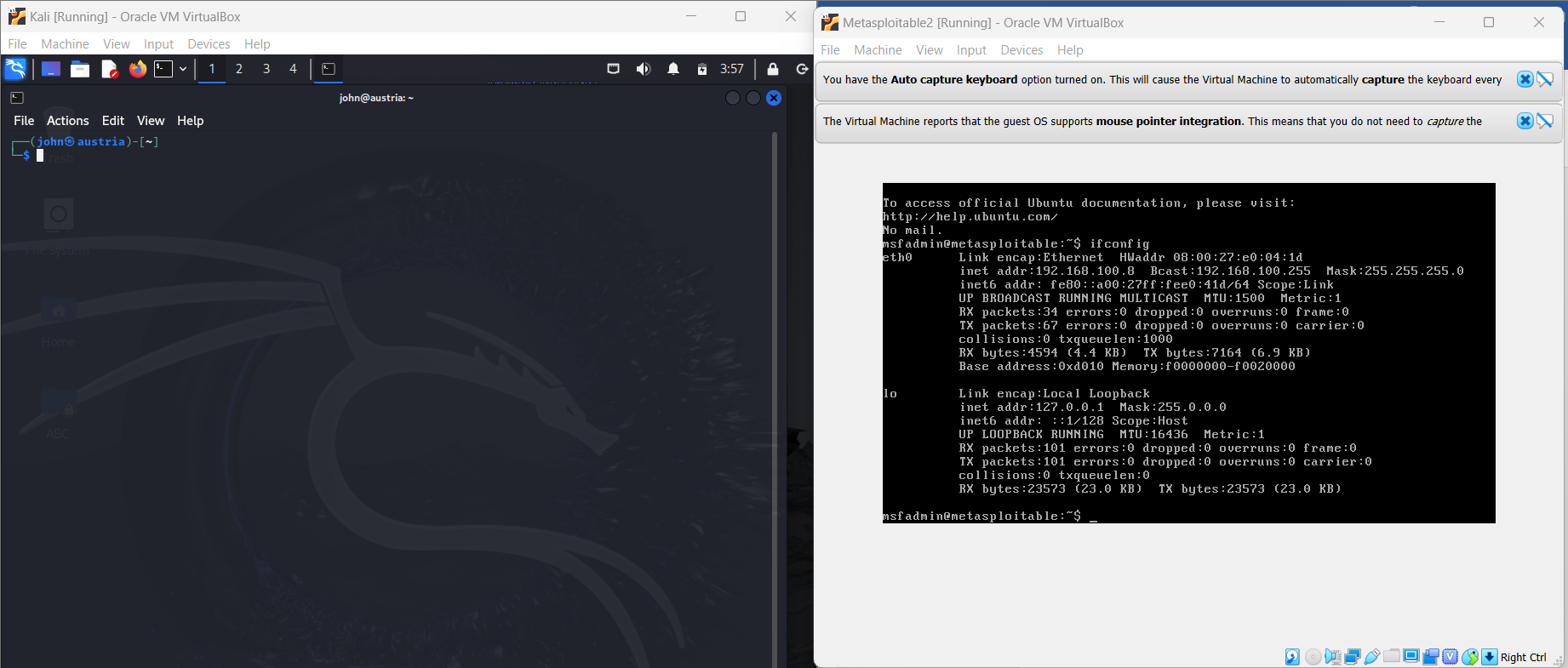


After making a new Nat Network, I had to go to the settings of Kali and Metasploitable2 to make sure that the Adapter 1 is attached to Nat Network of ICT740 Network. After having this done, both of the virtual machines are connected to one network.



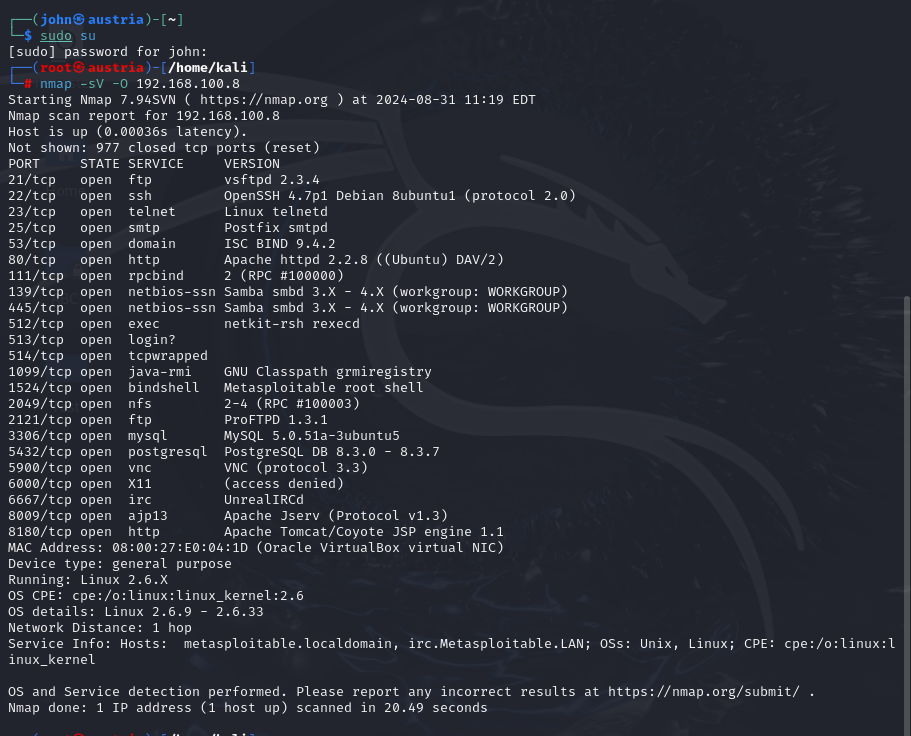
To test whether the two virtual machines are connected to one another, I entered ‘ifconfig’ to the terminal of Kali Linux and Metasploitable2.





The results in ifconfig shows that Kali has the IP address of 192.168.100.4 while Metasploitable2 has the IP address of 192.168.100.8. Both of the IP addresses indicates that they are connected to one network as most of the address has the same numbers and only differs on the last digit.

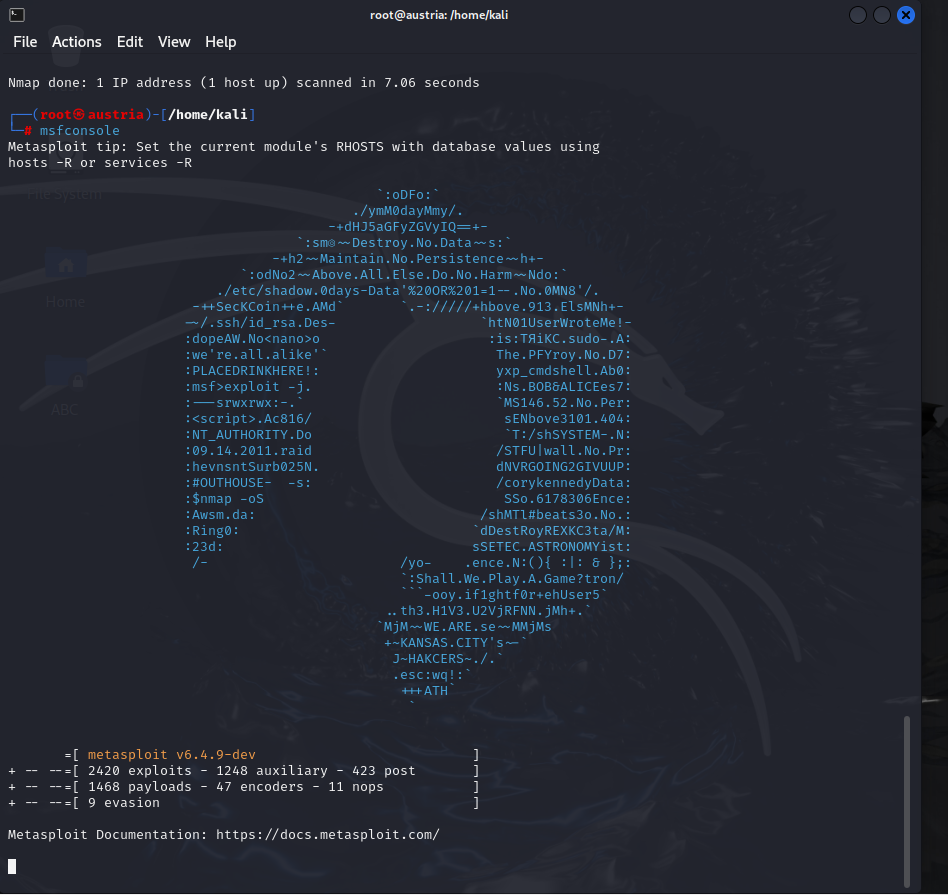
Before I use Metasploit to exploit the vulnerabilities, I have used the help of nmap to help me identify the open ports of Metasploitable2. I typed “nmap -sV -O 192.168.100.8” to determine the open ports and the type of service version running in Metasploitable2.



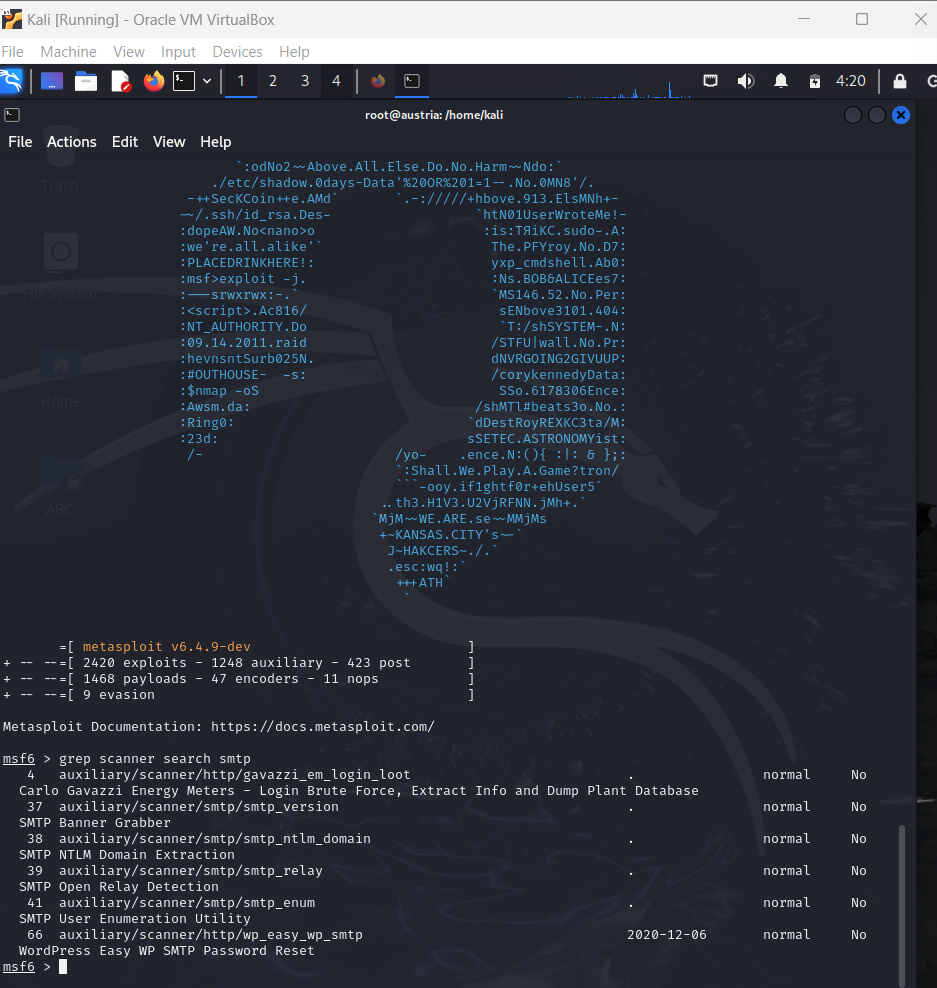
From the results above, there are 23 open ports running in Metasploitable2. The Metasploitable2 is running on Linux 2.6.X and the Operating System Version is Linux 2.6.9 – 2.6.33. We’re going to focus on 4 open ports and exploit them by using Metasploit Framework.

## Port 25: SMTP

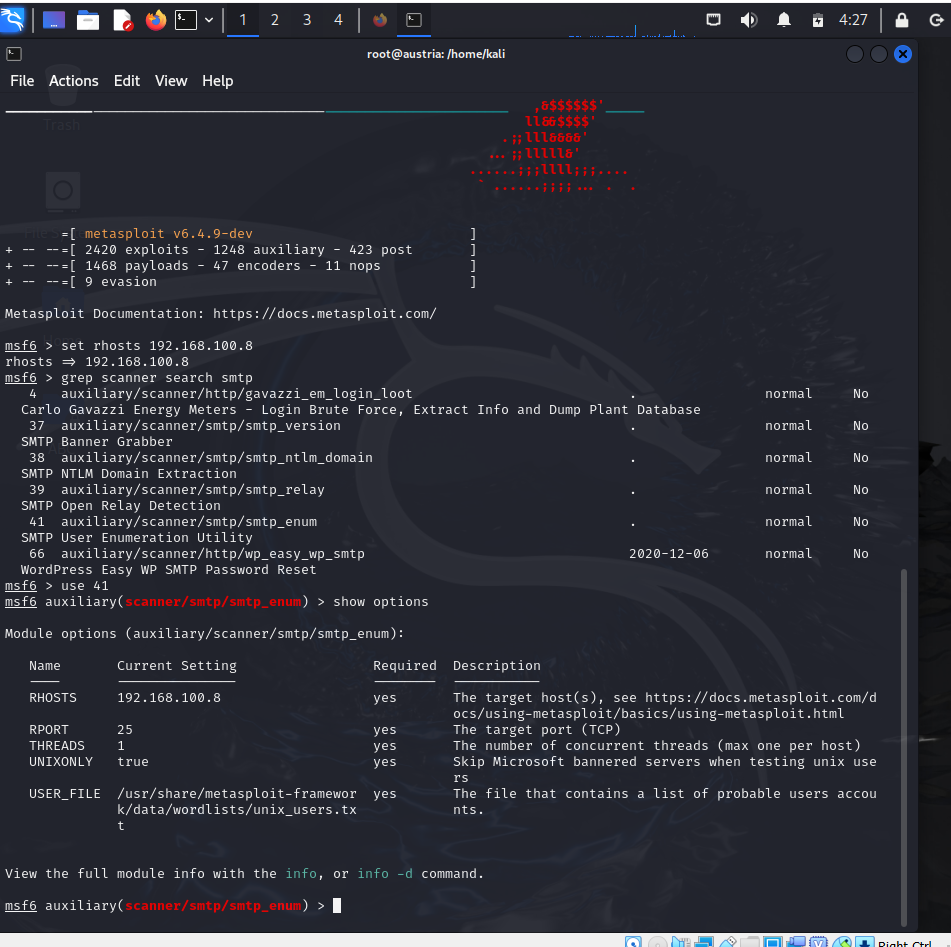
I chose to exploit Port 25: SMTP first. SMTP (Simple Mail Transfer Protocol) is a common language used to communicate between servers and clients through the internet by sending emails (Abnormal, 2024). To begin exploiting the port, I opened Metasploit by typing ‘msfconsole’ in the prompt bar.



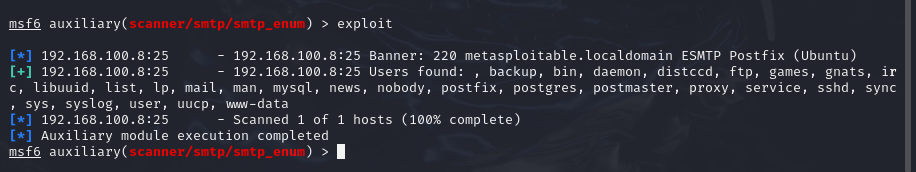
After Metasploit has been opened, I typed ‘grep scanner search smtp’ in the prompt bar.



From the choices above, I chose ‘41’ to determine which type of SMTP is running in Metasploitable2. I also set the Rhosts to ‘192.168.100.8’ to make sure that we are going to exploit Metasploitable2.



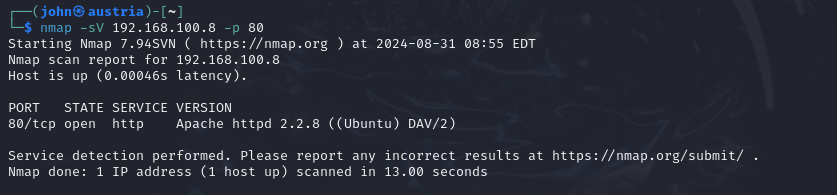
Then I typed, ‘exploit’ in the prompt bar to exploit the smtp port of Metasploitable2. From the image below, there are plenty of users found in smtp of Metasploitable2. These shows which type of languages are used to send emails using the virtual machine. Users must be alarmed when port25 is opened for it can help the hacker hack to your email services.



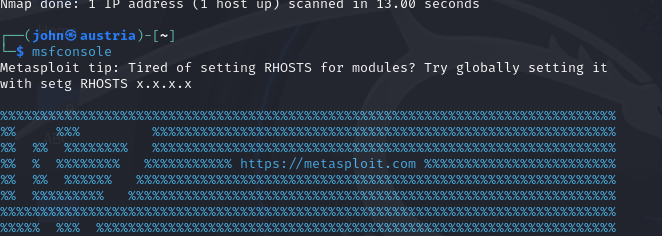
## Port 80: HTTP

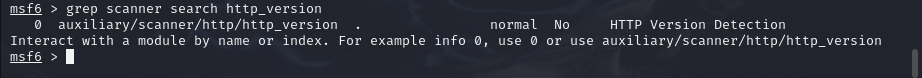
Port 80: http is the port responsible for transmitting data in the web between the web servers and client. Port 80 is mostly used in HTTP and not in HTTPS. Nowadays, transmission of data in web is done through port 443 because it has more security than port 80. Port 80 transmits web data through the internet insecurely.

To test if I can exploit port 80 of Metasploitable2. I have first checked the port 80 in nmap by typing ‘nmap -sV 192.168.100.8 -p 80’ to check if port 80 is open currently in the virtual machine. As the process is performed, nmap has detected that port 80 is currently open and active.

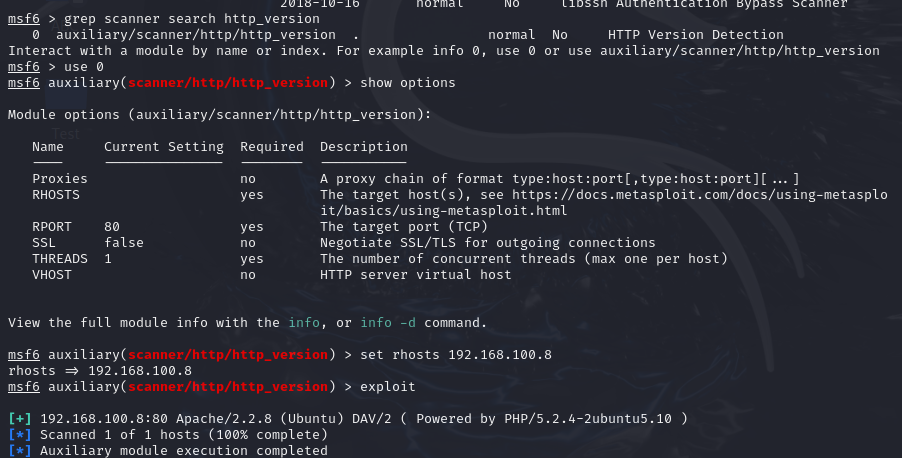


After checking that port 80 is opened, I opened Metasploit Framework again by typing ‘msfconsole’ in the prompt bar. After Metasploit has loaded, I entered ‘grep scanner search http\_version’ in the prompt bar.





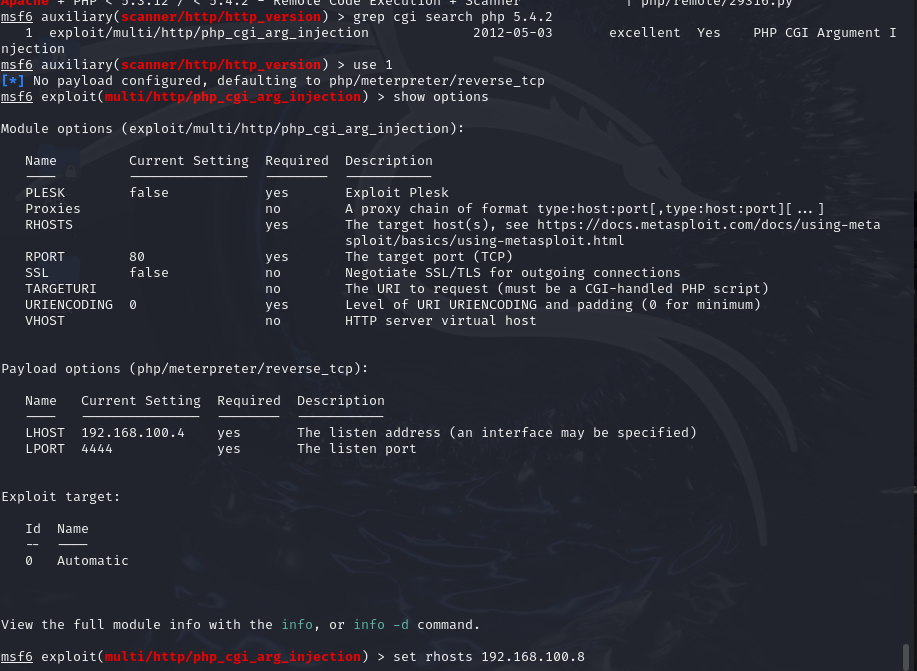
Once Metasploit has scanned and search for the options of http\_version, I chose 0 because it is the only option to detect the version of http running in the virtual machine. Then, I set the rhosts to the IP address of Metasploitable2 which is 192.168.100.8 then entered ‘exploit’ in the prompt bar. The exploit shows the version of Apache which is version 2.2.8 and powered by PHP version 5.2.4.



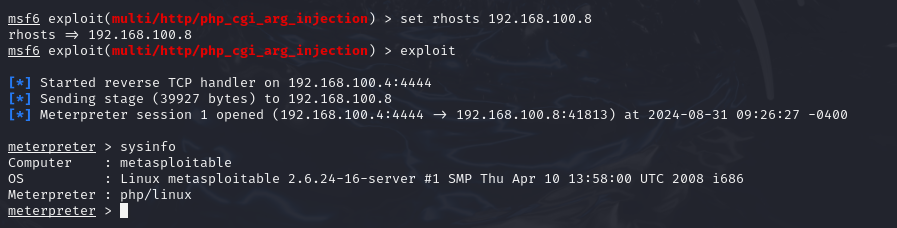
To fully detect which vulnerabilities are happening in apache 2.2.8, I typed ‘searchsploit apache 2.2.8 | grep php’ to the prompt bar. As seen in the image below, there are two vulnerabilities detected in the version of Apache 2.2.8 running in Php 5.4.2.



Digging further in the vulnerabilities, I chose the first vulnerability to exploit. I typed ‘grep cgi search php 5.4.2’, chose ‘1’ as it is the only option in the cgi search and then entered ‘show options’. From the options, we could see that there is LHOST and LPORT. This is a huge red flag because hackers can identify which IP address is to use to retrieve message between the receiver and the sender.

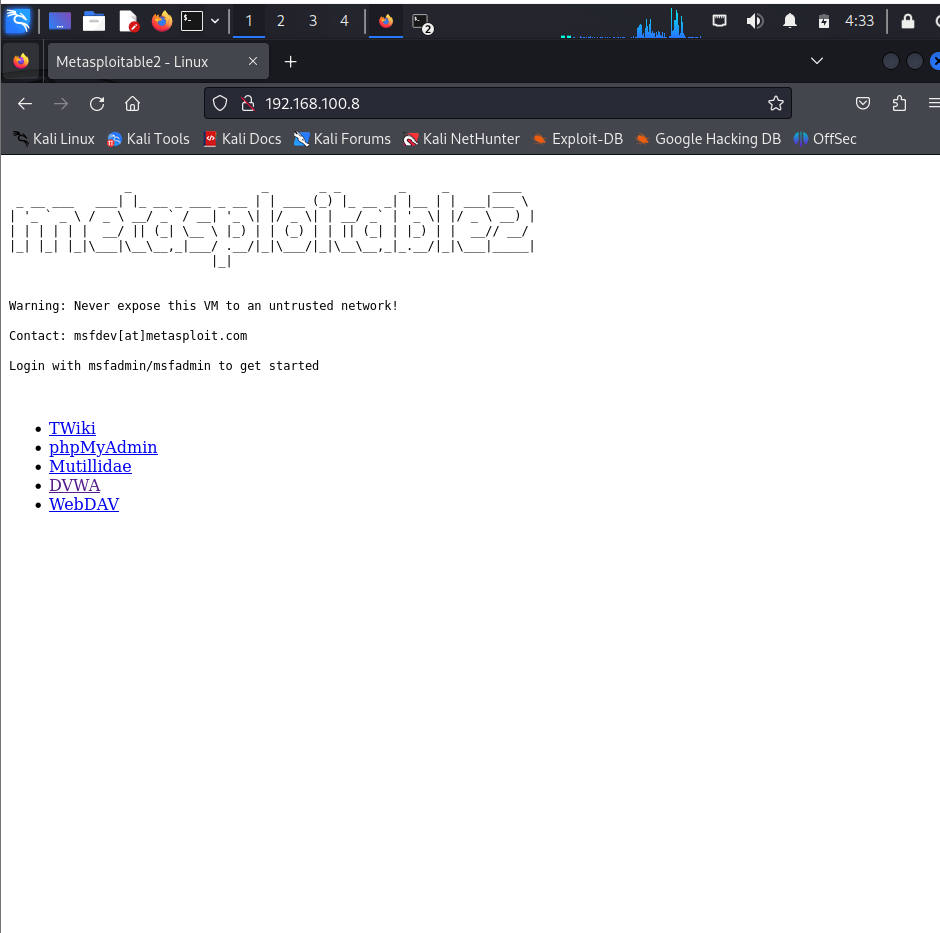


I noticed that there is no Rhosts yet from the options, so I typed ‘set rhosts 192.168.100.8’, then entered ‘exploit’ in the prompt bar. After exploiting the cgi injection, we could see that a Meterpreter session 1 is opened. This is from the LHost of 192.168.100.4, the listen address, sending data to our virtual machine. A prompt bar of meterpreter appeared, I typed ‘sysinfo’, then it showed me which type of OS and the version of OS is the port 80 is running from and also the programming language.

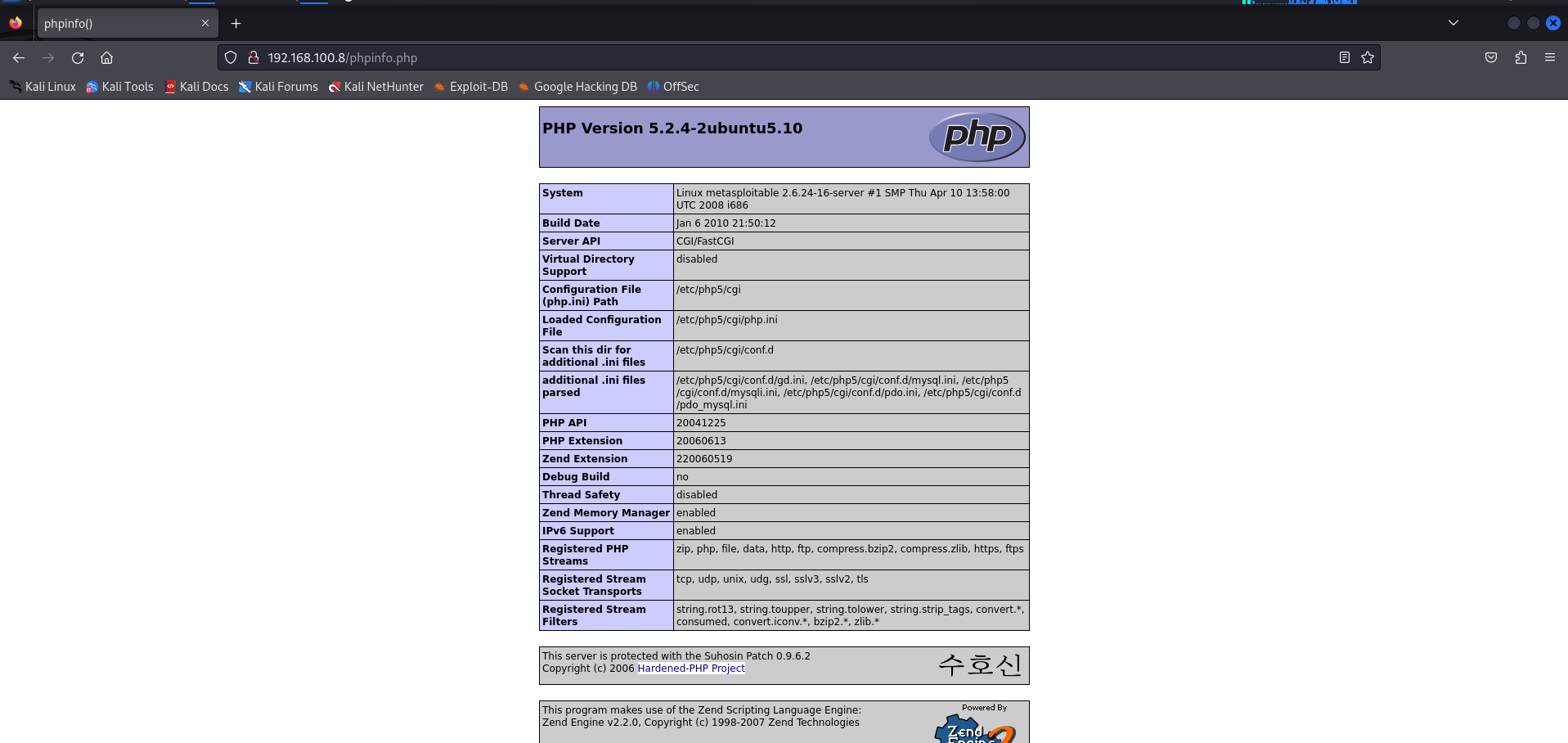


### Browser Version

Another great way of exploiting the vulnerabilities of Port 80 is by opening a browser and typing the IP address of the Metasploitable2 in the search bar.



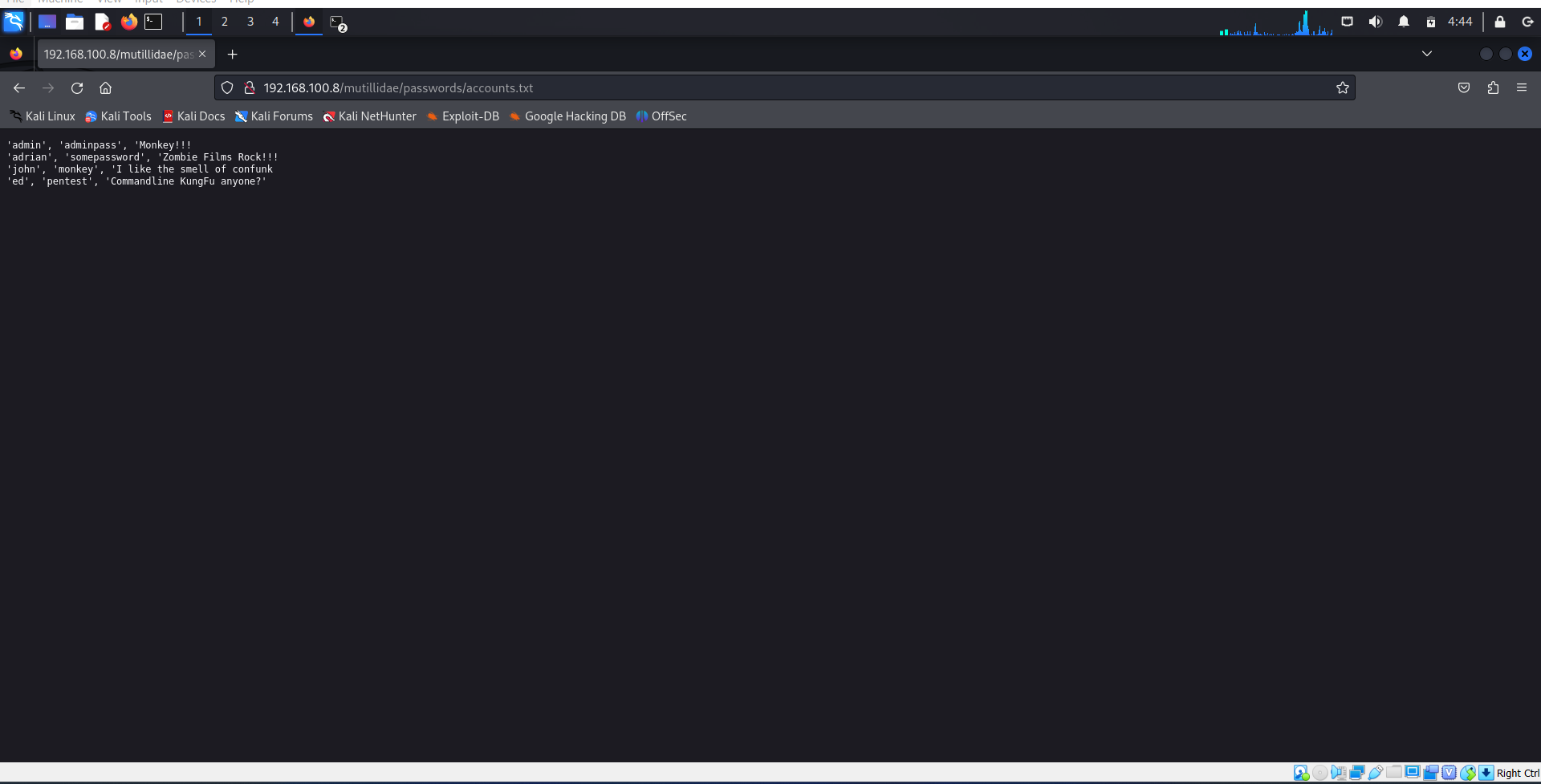
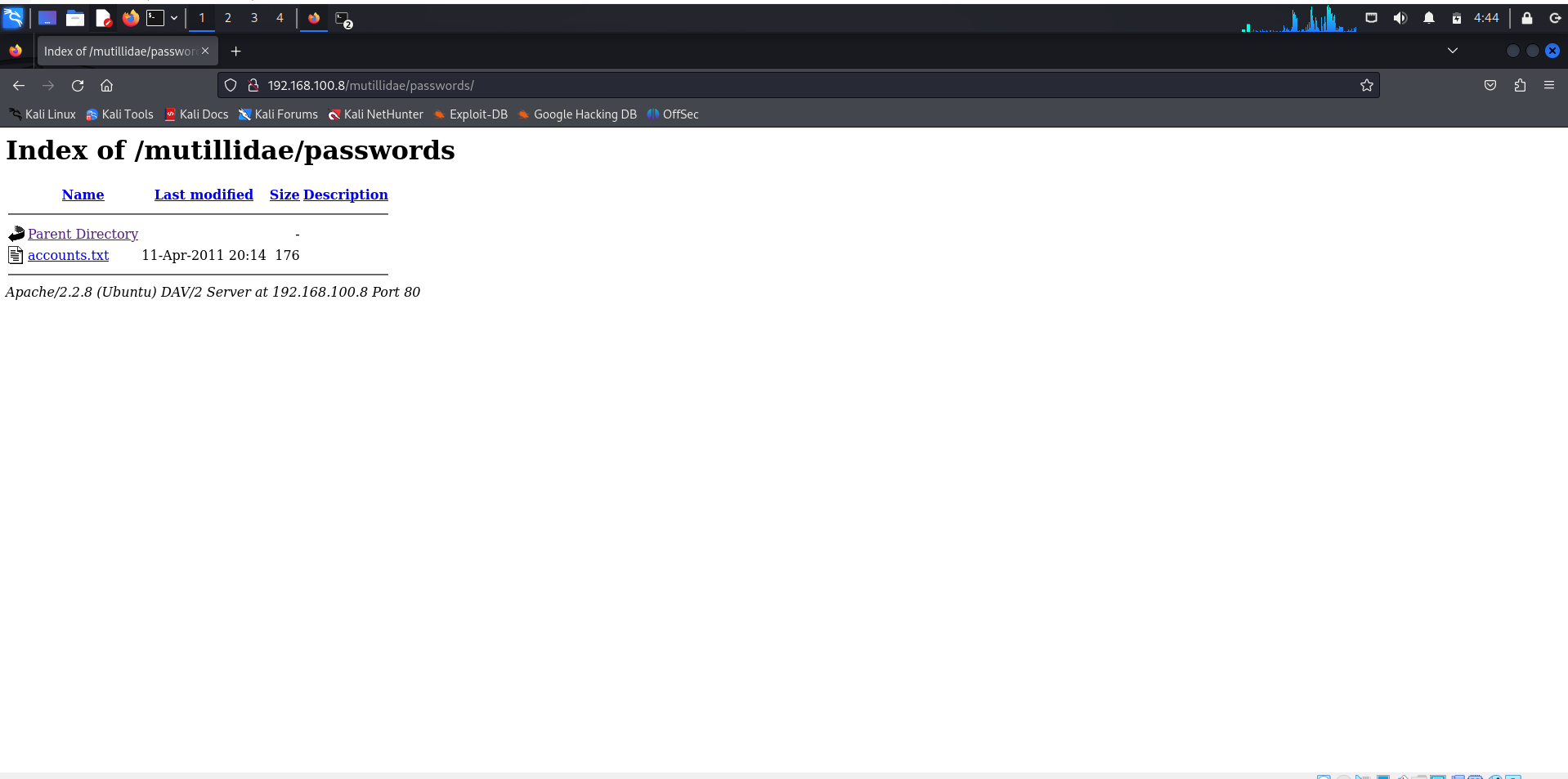
For us to determine which version of php is running in metasploitable2, I typed ‘192.168.100.8/phpinfo.php’, then pressed enter. We could see that the version of PHP is 5.2.4-2ubuntu5.10 which is the same from the exploited information from Metasploit above. Developers should never expose the version of PHP. This could let the hacker know if the PHP is outdated or in updated version. This information should be in a password file directory when exposed to public.



Another incident I found while using the browser, I chose Multillidae, then hacked into the robots setting of the Multillidae. From the image below, we can see that we can access the passwords of the users from the Multillidae. Robots.txt is a good way to do a security audit on a website because it could expose information about hidden directories.



To check the passwords of the users, I typed ‘192.168.100.8/multilladae/passwords/’ in the search bar. An accounts.txt file appeared, I opened it, then the usernames and passwords saved in Multillidae appeared.



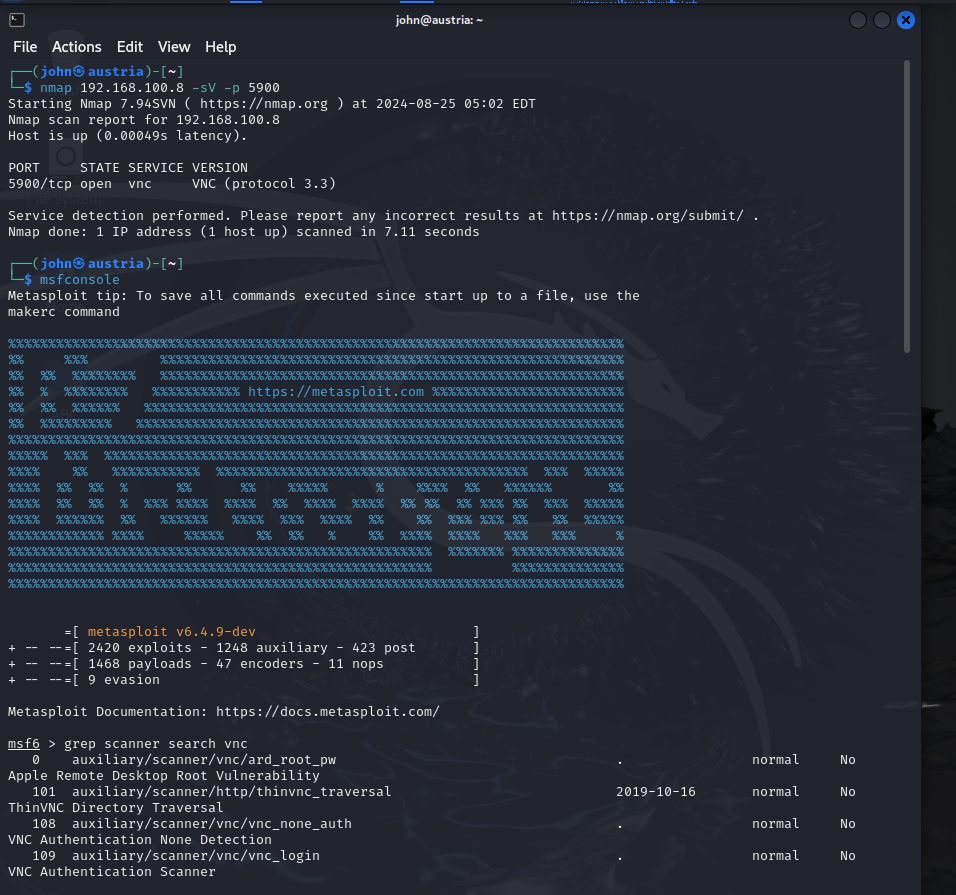
## Port 5900: VNC

Port 5900 according to Ellie (2023) is “commonly used for remote desktop connections using the Remote Frame Buffer (RFB) protocol. It is associated with the Virtual Network Computing (VNC) system, which allows users to control a computer over a network and file transfer remotely.”

Checking whether port 5900 is opened in Metasploitable2, I ask the help of nmap, then typed ‘nmap 192.168.100.8 -sV -p 5900’. After nmap scan the IP address, it shows that Port 5900 is currently opened as showed in the image below.



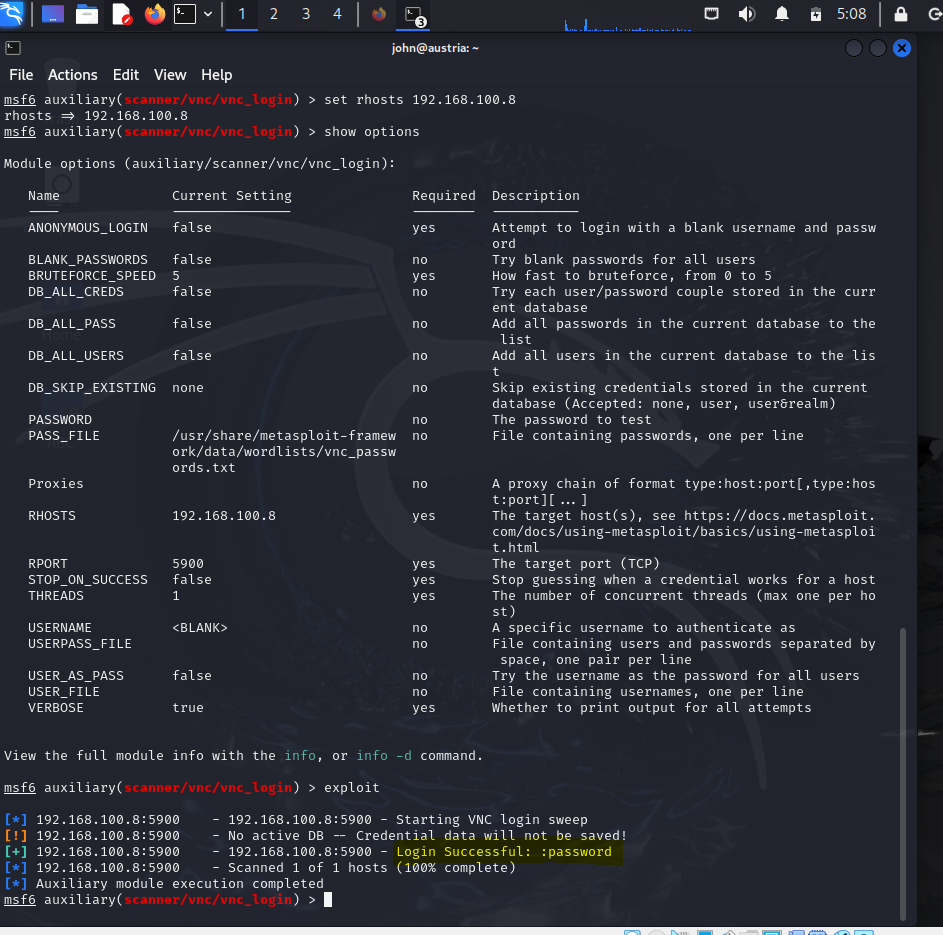
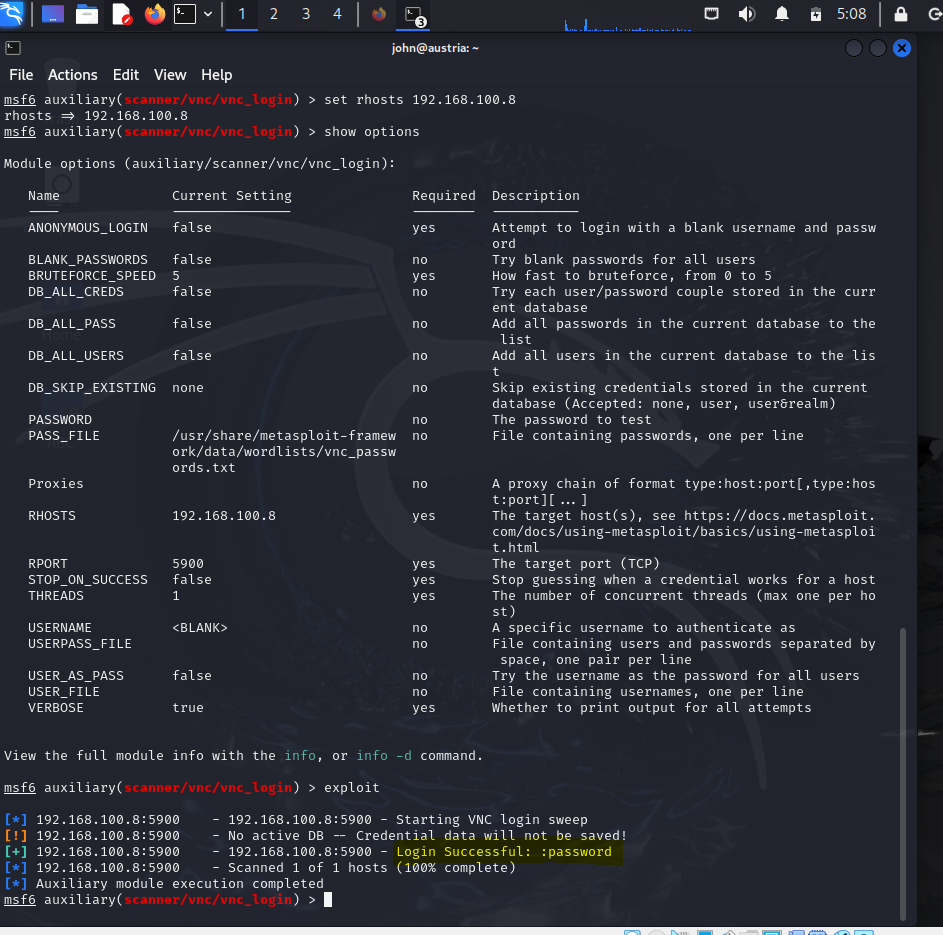
To exploit the port, I opened Metasploit by typing ‘msfconsole’ in the prompt bar.



Once Metasploit has loaded, I entered ‘grep scanner search vnc’. I chose 109 from the options to determine the login and password of the VNC.

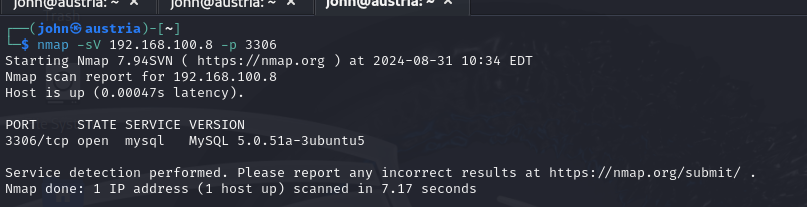


After choosing 109, I set the rhosts to the IP address of Metasploitable 2 which is 192.168.100.8 then entered ‘exploit’ in the prompt bar. From the exploitation, we have determined that the password for the VNC is ‘password’. This indicates that we should use strong passwords in using VNC servers because weak passwords are prone to attacks.

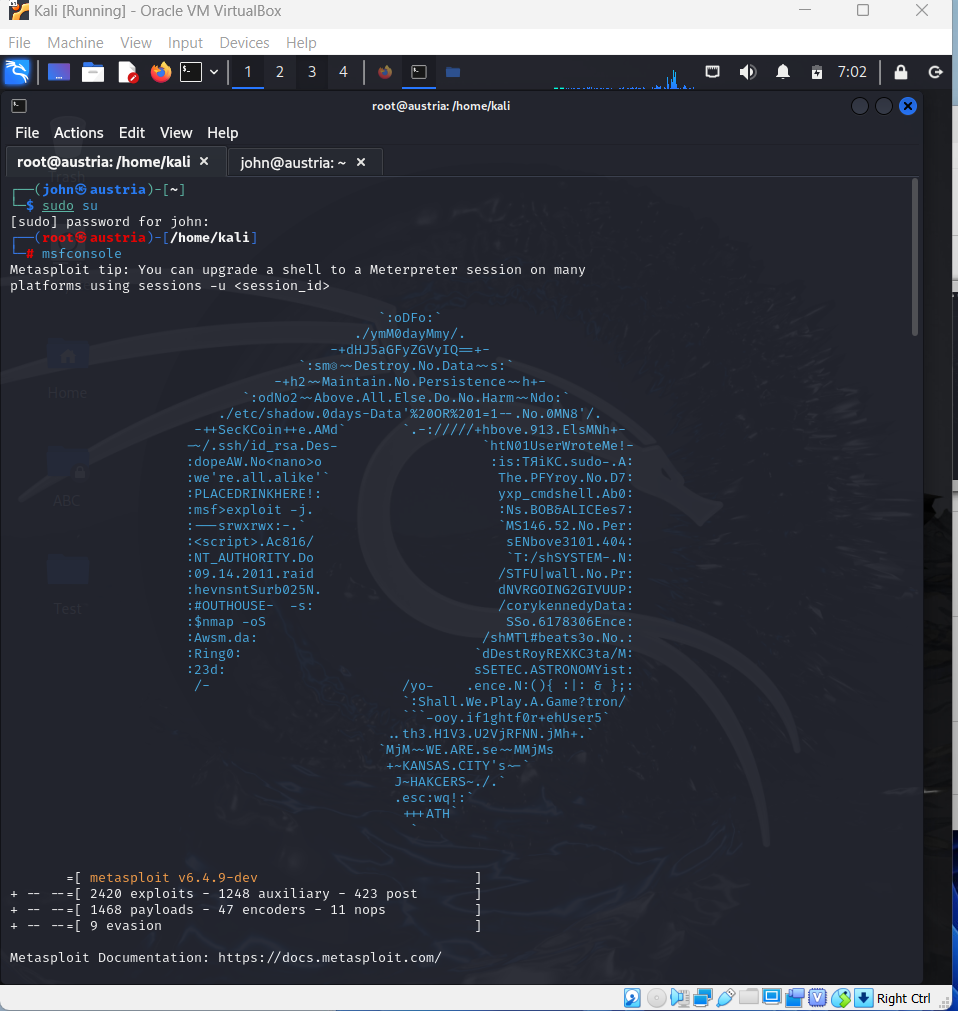


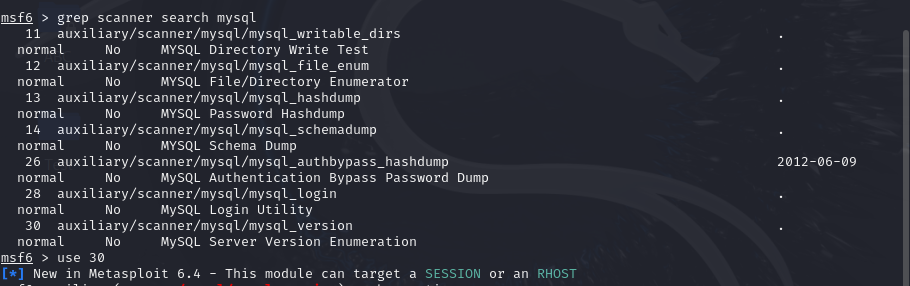
## Port 3306: MySQL

Port 3306 represents the MySQL of the Metasploitable2. This shows the database of the virtual machine. To check whether the port is open in Metasploitable2, I typed ‘nmap -sV 192.168.100.8 -p 3306’. The nmap scan reported that port 3306 is opened.

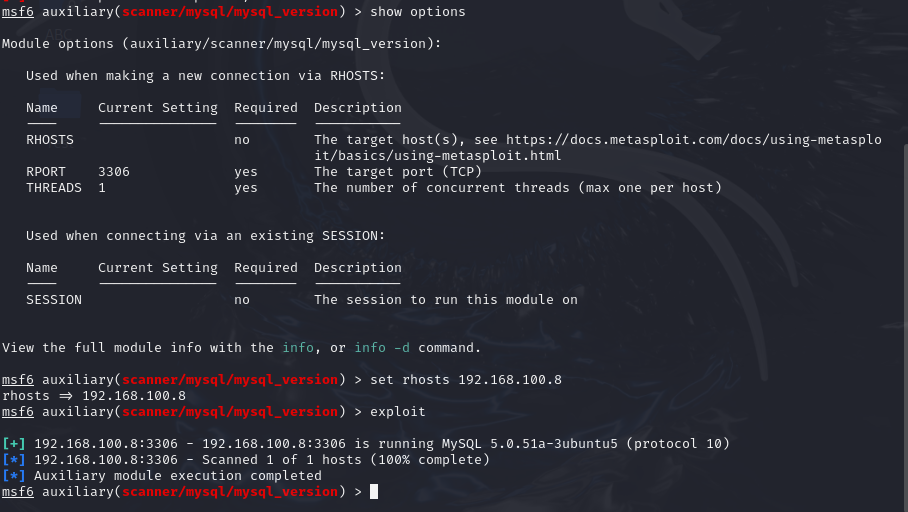


Exploiting the port 3306 will be done by opening Metasploit. Metasploit is opened in the prompt bar by typing ‘msfconsole’. After Metasploit has loaded, I entered ‘grep scanner search mysql’ then use the number 30 option.





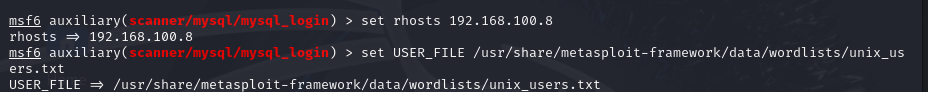
After choosing 30 as my option, I set the Rhosts to ‘192.168.100.8’, then entered ‘exploit’ in the prompt bar. The exploit shows that the version of MySQL running in Metasploitable2 is Version 5.0.51a-3ubuntu5.

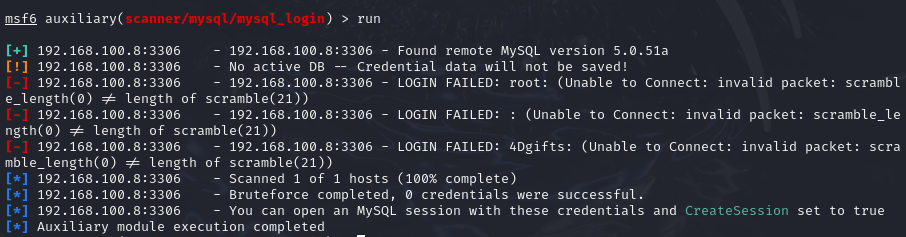


Another version of exploiting the vulnerabilities of MySQL is to choose number 28 which is the MySQL Login Utility.



The same thing I did as option 30, I set the Rhosts to the IP address of Metasploitable2 and set the USER\_FILE to /usr/share/metasploit-framework/data/wordlists/unix\_users.txt. Then I typed ‘run’ in the prompt bar. From the images below, we can see that the scanner is brute forcing to scan the port from any type of database it could find. It has successfully found the version of MySQL but failed logging in for the other profiles.





# SUMMARY

In this assessment, Metasploit Framework from Kali Linux and Metasploitable2 have been utilized to analyse the network between the virtual machines. Potential vulnerabilities and security issues in Metasploitable2 have also been identified through the help of Metasploit Framework. Metasploit Framework is a strong and powerful tool to exploit vulnerabilities. In a single command, we can expose the vulnerabilities lying around the open ports of Metasploitable2.

The code ‘grep scanner search’ is very helpful in Metasploit Framework. By adding keywords such as http, mysql or vnc, Metasploit displayed different options in which the user can exploit the vulnerabilities. Then, setting the rhosts to the IP address of Metasploitable2, and running the code ‘exploit’, Metasploit will already determine which type of programming language and the version of the system in the Metasploitable2.

However, despite the easy usage of Metasploit Framework, one disadvantage I found is that it cannot brute force its way in to the MySQL. I tried running it a couple of times, but it didn’t give me any users found for it has failed in logging in.

Metasploitable2, on the other hand, is designed to be vulnerable. I like how it is easy to use in the virtual machine and in the browser of Kali Linux. It taught me how to look at the red flags of a website and identify which information are needed to be hidden and be stored in a password protected file if it is exposed to the public.

# REFERENCES

Abnormal (2024). *SMTP (Simple Mail Transfer Protocol): How It Works and Why It’s Necessary*. [online] Available at: https://abnormalsecurity.com/glossary/smtp.

Ellie (2023). *Port 5900 - Everything You Want to Know!* [online] AnyViewer. Available at: https://www.anyviewer.com/how-to/port-5900-2578.html.

Kumar, V. (2023). *METASPLOITABLE 2*. [online] Medium. Available at: https://medium.com/@Vishal17/metasploitable-2-33e1495b0a50.

Rapid7 (2022). *Metasploit Framework | Metasploit Documentation*. [online] docs.rapid7.com. Available at: https://docs.rapid7.com/metasploit/msf-overview/.