**Name:** Viraj Punjani

**Student id:** 20625630

**Assignment-2 3002**

**Answer 1:**

**Key components:**

**OSINT Analysis:**

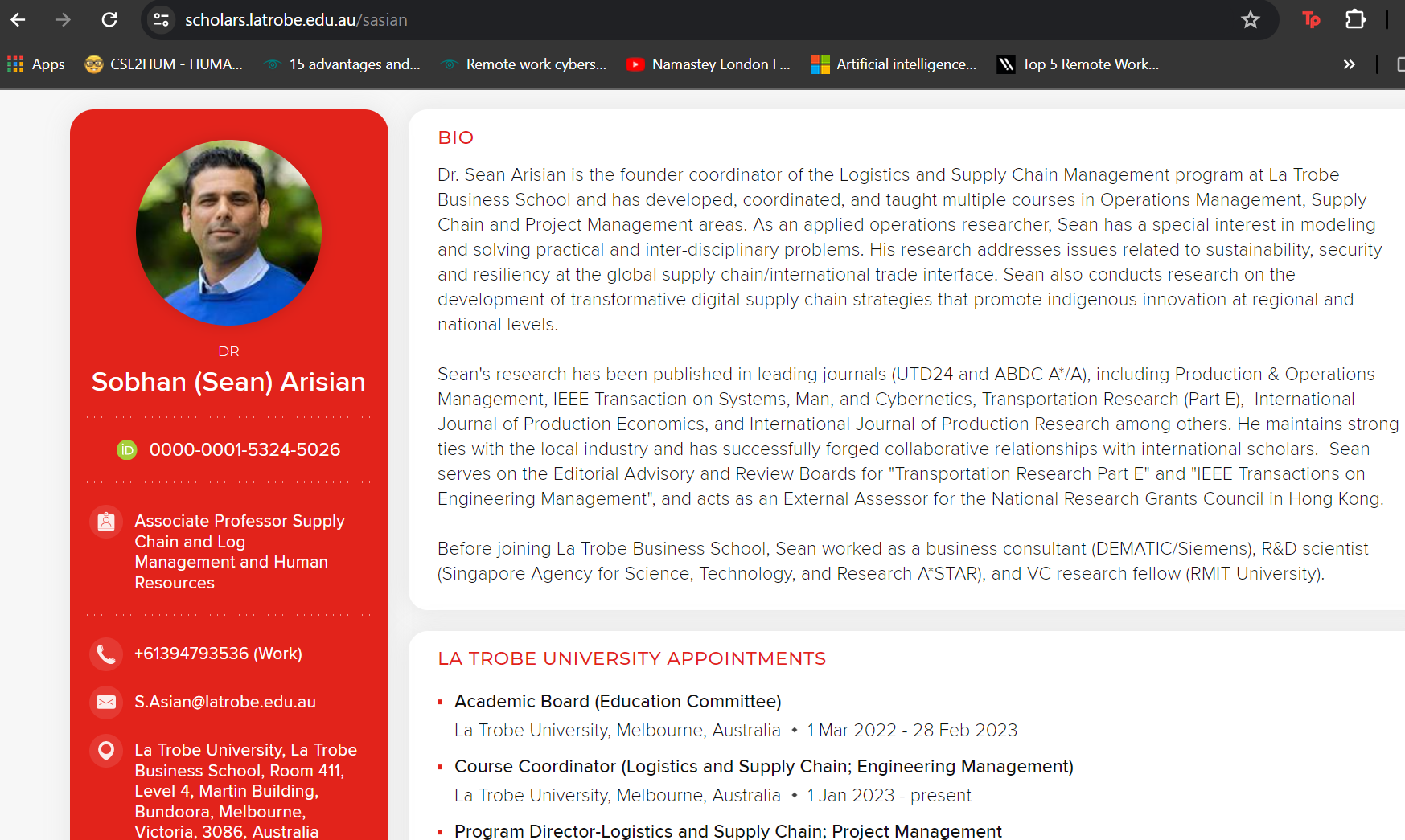
**Reddit scan:**

After multiple search attempts, I didn’t find any sensitive or disclosed information on reddit of Latrobe.

A screenshot of a computer

Description automatically generated

With the use of google Dorking I used various search operators. I found many professors private information such as Mobile Phone Numbers, Email Addresses and Home Address which is accessible publicly it can be misused by hackers if used unethically.

1. site:latrobe.edu.au
2. cache: latrobe.edu.au

When I have searched using the keywords cache: latrobe.edu.au operator on <https://webcache.googleusercontent.com/search?q=cache:latrobe.edu.au&sca_esv=e472bba1732e8ddb&sca_upv=1&rlz=1C1UEAD_en-GBAU1101AU1101&strip=0&vwsrc=0>

**A screenshot of a computer screen

Description automatically generated**I was able to open the source code of the cached web page, if hacker get access to session id and some user password then they can exploit it severely. They can also run few queries with code to see if page pops up something.

**Shodan:**

I found various insecure Ip address and open ports on Shodan when I searched with key word Latrobe university: port 21.

A computer error message

Description automatically generated

A screenshot of a computer

Description automatically generated

Vulnerabilities assessment:

I did vulnerability assessment using nmap and Nessus risk assessment tool to scan latrobe domain**.**

**Nmap:**

nmap --script dns-brute [www.latrobe.com](http://www.latrobe.com)  
I did brute force on Latrobe server and found these ports open. By doing these I found various domains and sub domains related to latrobe which can be used unethically by attacker.

**A computer screen shot of a program

Description automatically generated**

**A screenshot of a computer program

Description automatically generated**

**latrobe.edu.au port:21,22, 80 and 443 ports** are open when I tried to login with Anonymous account it allowed me to login through kali. But later, restriction apply so I didn’t exploit it further.

A screenshot of a computer program

Description automatically generated

**Nessus:**

After deploying a scan with the help of Nessus on the website of the University ([www.latrobe.com.au](http://www.latrobe.com.au)) to conduct a vulnerability assessment, and following are the results of the Scan:

A screenshot of a computer

Description automatically generatedSince, I have detected 14 vulnerabilities in this scan assessment, all of these Vulnerabilities are listed and categorized as follows:

A screenshot of a computer

Description automatically generated

Out of the 14 vulnerabilities that stood out in network scan that multiple half-open SYN ports were detected, suggesting potential external reconnaissance:

A screenshot of a computer

Description automatically generated

21/tcp www.latrobe.com.au

80/tcp www.latrobe.com.au

443/tcp www.latrobe.com.au

1723/tcp www.latrobe.com.au

These ports may(tend-to) expose the network to unauthorized probing and resource strain, risking service disruption.

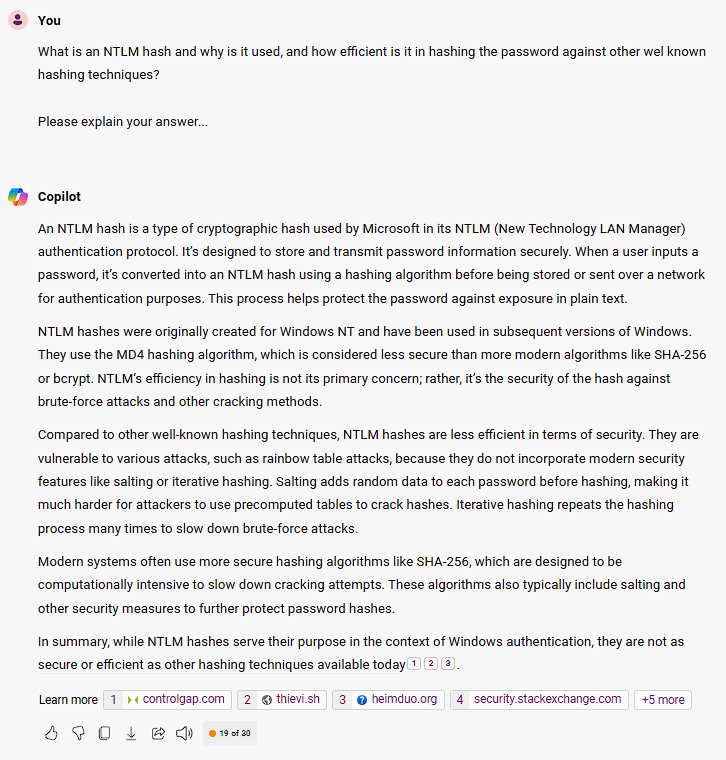
We should Evaluate the necessity of these ports. Close non-essential ones and enforce strict monitoring on required ports to bolster security.

**Threats Mitigation:**

As per the findings from our research and scanning for vulnerabilities, following are the steps that should be taken into consideration for threat mitigation purposes:

1. Close Non-Essential Ports: Ports 21/tcp, 80/tcp, 443/tcp, and 1723/tcp must be closed if they are not essential to prevent unauthorized access.
2. Update and Patch Systems: Security patches must be applied promptly to all services running on essential ports to protect against known vulnerabilities.
3. Deploy Intrusion Detection System (IDS): An IDS must be implemented to monitor network traffic for signs of reconnaissance or attacks actively.
4. Establish Strict Firewall Rules: Firewalls must be configured to control traffic strictly, allowing only necessary communications based on the principle of least privilege.
5. Implement Access Control Lists (ACLs): ACLs must be used to restrict network access to authorized personnel only, minimizing the risk of unauthorized resource exploitation.
6. Robust Incident Response Plans: Detailed plans must be developed for a quick and effective response to security incidents involving unauthorized access attempts.

These steps are crucial in enhancing the defense against potential cyber threats to the university’s network infrastructure. Regular reviews and updates to these measures are essential to maintain a strong security posture.

**Answer 2:**

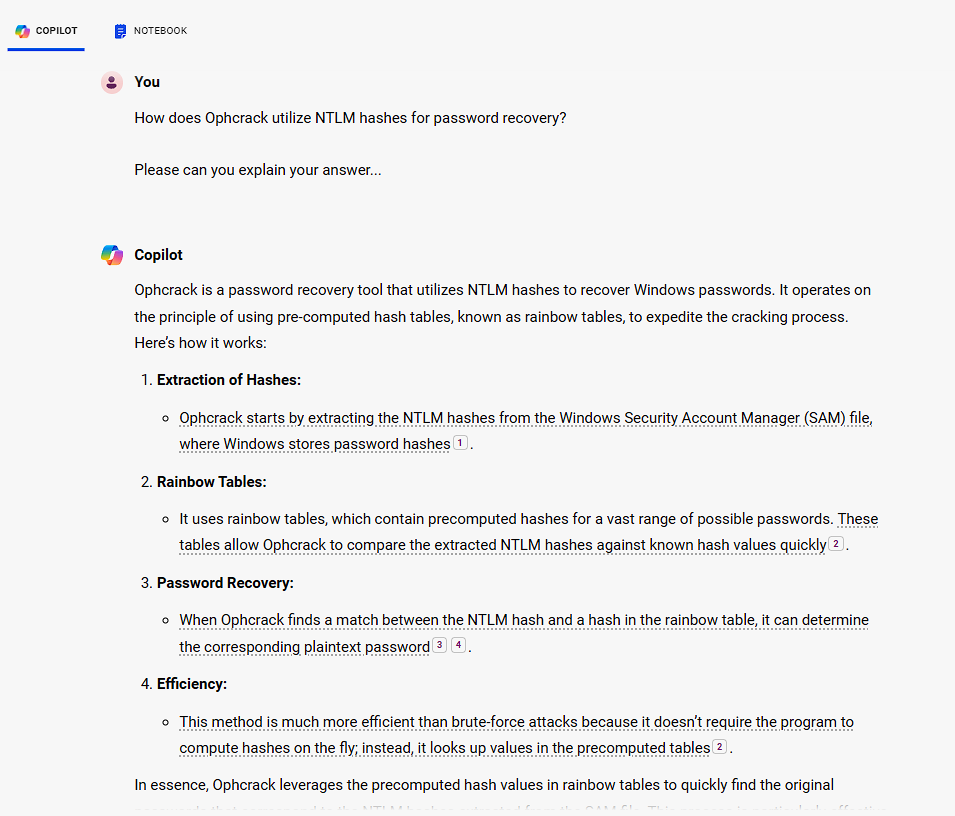
**Cracking Passwords using Ophcrack and Generative AI**

The use of Generative AI to research about the NTLM Hashing and Ophcrack:

Following is the sequence of the communication with Microsoft’s Copilot, to research about NTLM Hashing:

* Here I have learned that NTLM hashes are a way to store passwords securely in Windows systems. They use an older hashing algorithm called MD4, which isn’t as strong as newer methods. I found out that NTLM hashes don’t use extra security features like salting or repeating the hashing process, which makes them easier to crack than other types of hashes. Modern hashing techniques, like SHA-256, are better because they’re harder to break and they add random data to passwords for extra protection. So, NTLM hashes do the job, but there are safer options available today.

**Following is the sequence of the communication with the Microsoft’s Copilot regarding the research about the functioning of the Ophcrack for Password Cracking and Recovery:**

* Here I have learned about Ophcrack, a tool that uses pre-made rainbow tables to match NTLM hashes from Windows with possible passwords. This is faster than guessing passwords one by one because it looks up the answers in a big list. I also learned that NTLM hashes are not very strong compared to newer methods because they don’t mix in random data or hash passwords many times to make them harder to crack. So, Ophcrack works well with NTLM hashes, but it might not work as well with stronger, more modern password protections.

**Steps to Crack the Given password**

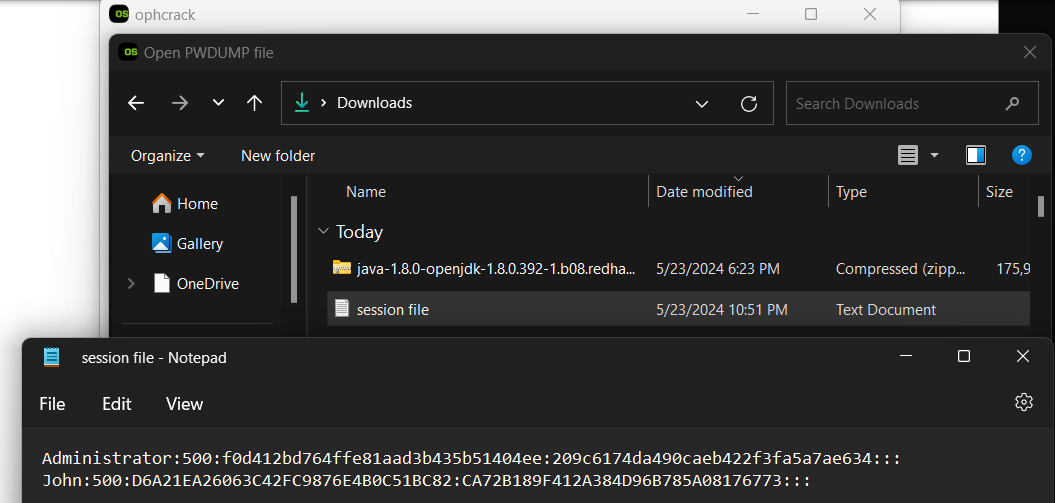
First, I must load the hashed passwords that are given below, as a session file into the Ophcrack:

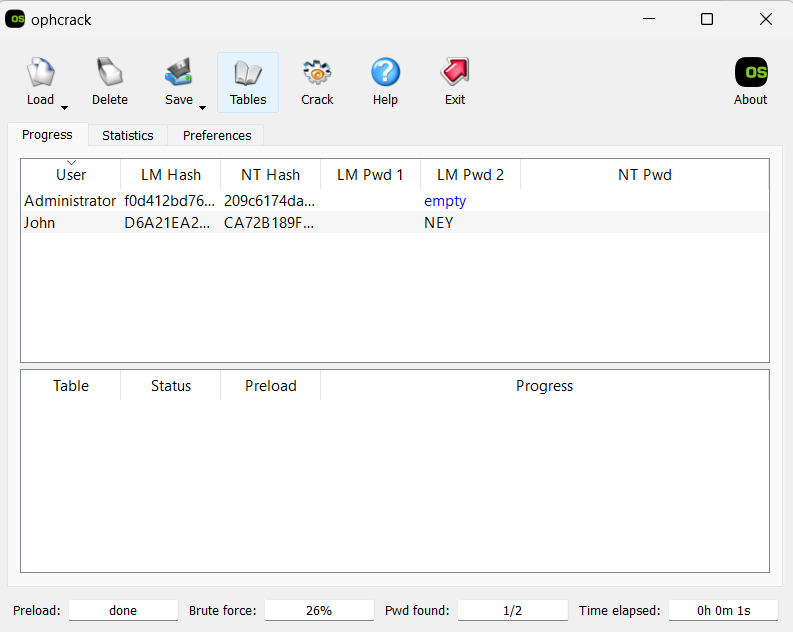
Administrator:500:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634::: John:500:D6A21EA26063C42FC9876E4B0C51BC82:CA72B189F412A384D96B785A08176773:::

>>>

A screenshot of a computer

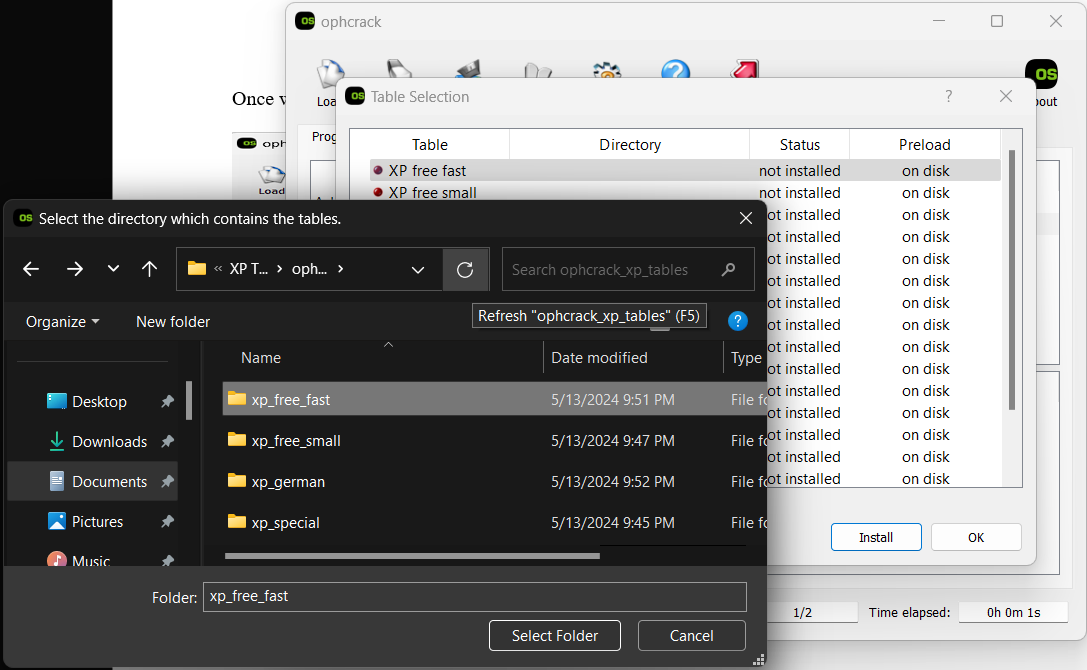
Description automatically generated

>>>

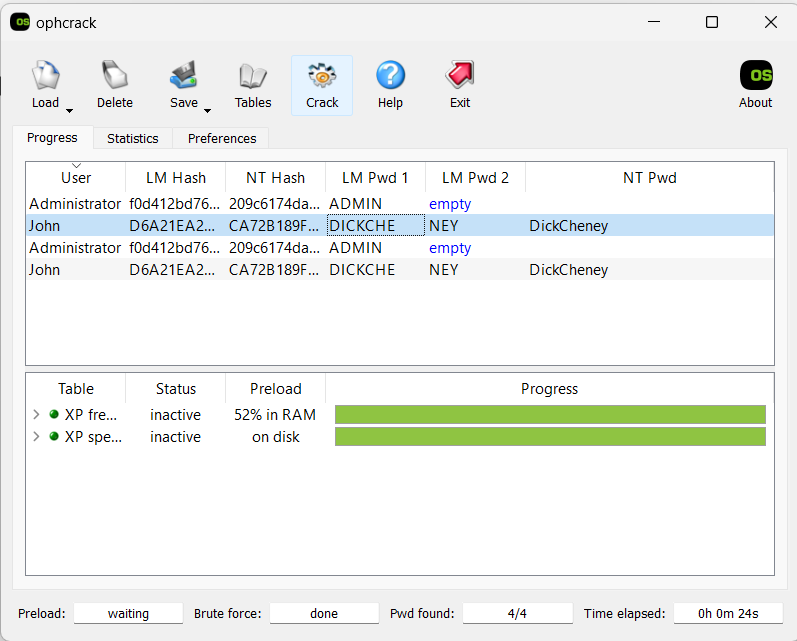
Once I load the Session File into Ophcrack, it should look something like this as follows:  
>>>

After this I have to simply select the tables which I have already downloaded, that I want to use for the cracking the passwords:

>>>



Afterwards, I need to crack the passwords using the selected tables, following are the outputs of the same session file using Different tables as shown in the picture below:

>>>

* So these are the Password Cracked for both of our users which will be as follows

Administrator : **Admin**

John : **DickCheney**

**Answer 3:**

1. Following are the list of services which I found to be running on the Metasploitable Machine:

* FTP: vsftpd 2.3.4
* SSH: OpenSSH 4.7p1
* Telnet: Telnetd
* SMTP: Postfix
* DNS: BIND 9.4.2
* HTTP: Apache 2.2.8
* MySQL: MySQL 5.0.51a
* RPC: Various RPC services
* SMB: Samba 3.0.20
* NFS: Network File System
* VNC: VNC server

Miscellaneous Services: Including telnet, login, domain, and http.

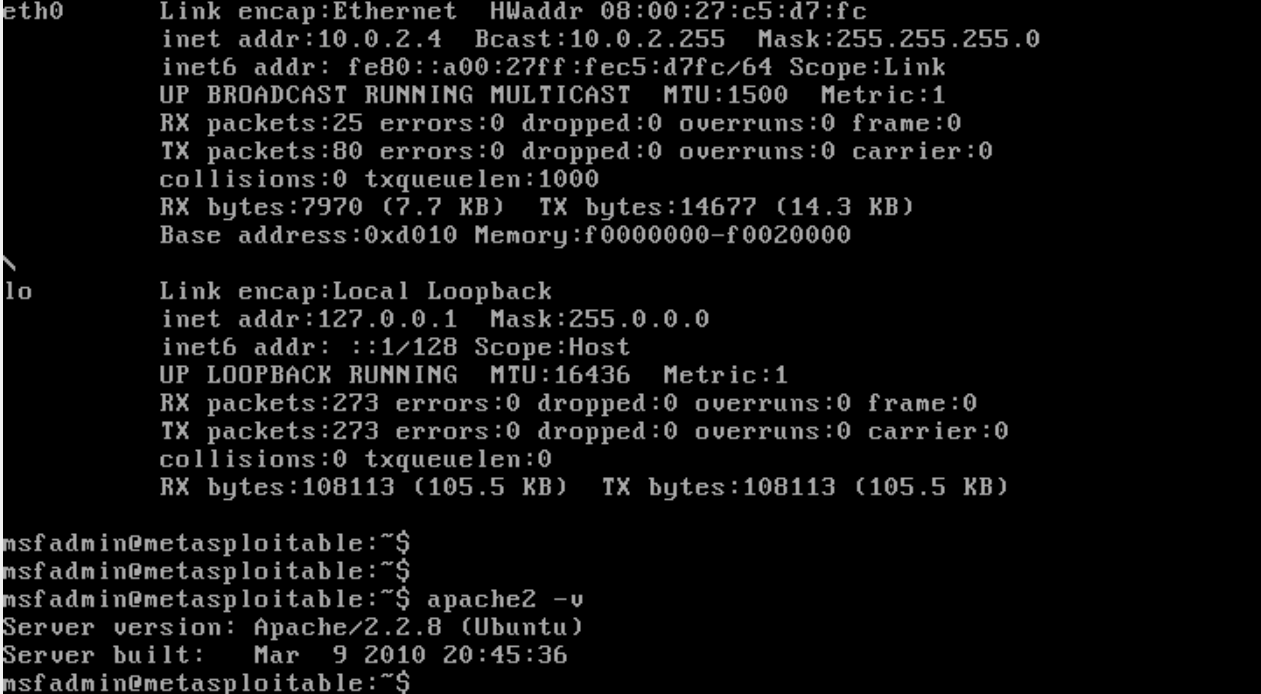
A computer screen shot of a computer program

Description automatically generated

1. Software Name and Version for Web Server

The web server running on the Metasploitable machine is:

* Software Name: Apache
* Version: Apache ubuntu DAV/2, 2.2.8



3.

Exploitation of the Web Service (Apache)

I have use Metasploit Framework to exploit a known vulnerability in Apache.

Step-by-Step Exploitation:

1. HTTP web service Apache exploitation:

In the below figures I am exploiting HTTP web service running on (Apache Server) and I was able to get access to the command prompt of the metasploitable machine from your Kali machine. I went to (http:10.0.2.4/phpinfo.php) website to find the configuration file path cgi which gave me access to exploit injection php\_cgi\_arg\_injectionleading me toshell meterpreter.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

1. **SQL Injection and XSS:**

I have attached the screen recording in the LMS as requested.