**Name: Samarth Jain**

**USN: 4SU20CS081**

**Course: Cybersecurity**

**Trainer: Bharath Kumar**

**Date: 25/08/2023**

**Assignment Details**

Assigned Date: 24/08/2023

Due Date: 25/08/2023

Topic: Manual Exploitation (Gaining Access)

**Introduction**

Exploitation using Metasploit in Kali Linux is a pivotal technique in ethical hacking and penetration testing. Metasploit, a powerful open-source framework, empowers security professionals to identify vulnerabilities within systems and networks. By crafting and deploying exploit modules, analysts can assess an organization's defence mechanisms, aiding in the fortification of digital infrastructures. This introduction offers a glimpse into the dynamic realm of Metasploit-driven exploitation, enabling experts to proactively safeguard against potential cyber threats.

**Content**

**Exploitation Steps/Phases**

1. Find the vulnerabilities and record Vuln Name, Vuln Port Number, Vuln Code
2. Start & Initialize the Metasploit
3. Search & Import the Exploit script
4. Configure the script as per your target
5. Verify the details & execute

**Steps to exploit the target machine and gain access**

1. Description:

Port scanning is performed to find the open ports in the Target Machine (in this case Metasploitable). The command is an aggressive one to get Service Version, OS and Keys.

Command: nmap -T4 -A 10.0.2.5

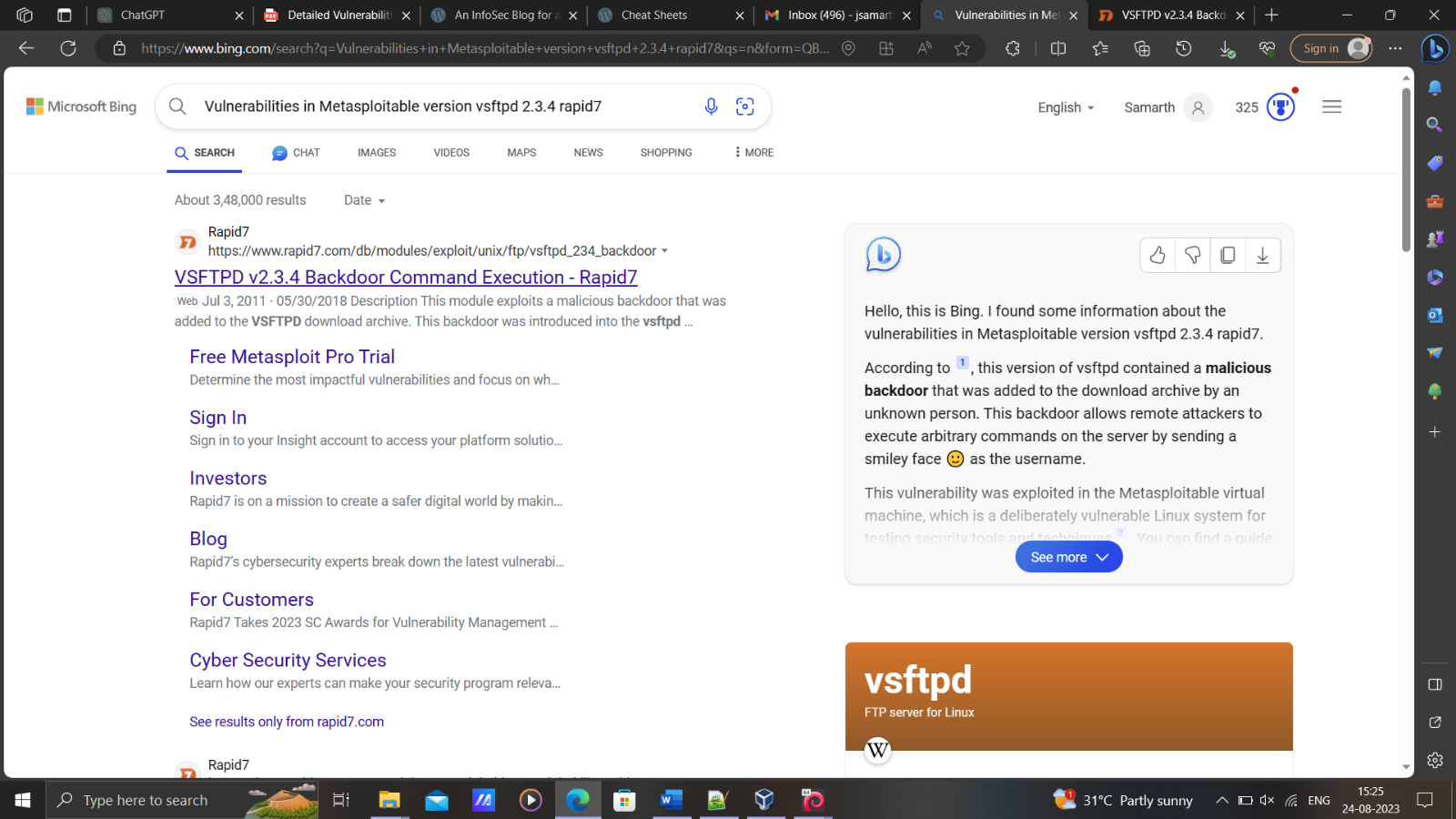
Syntax: #nmap -T4 -A <Target IP address>

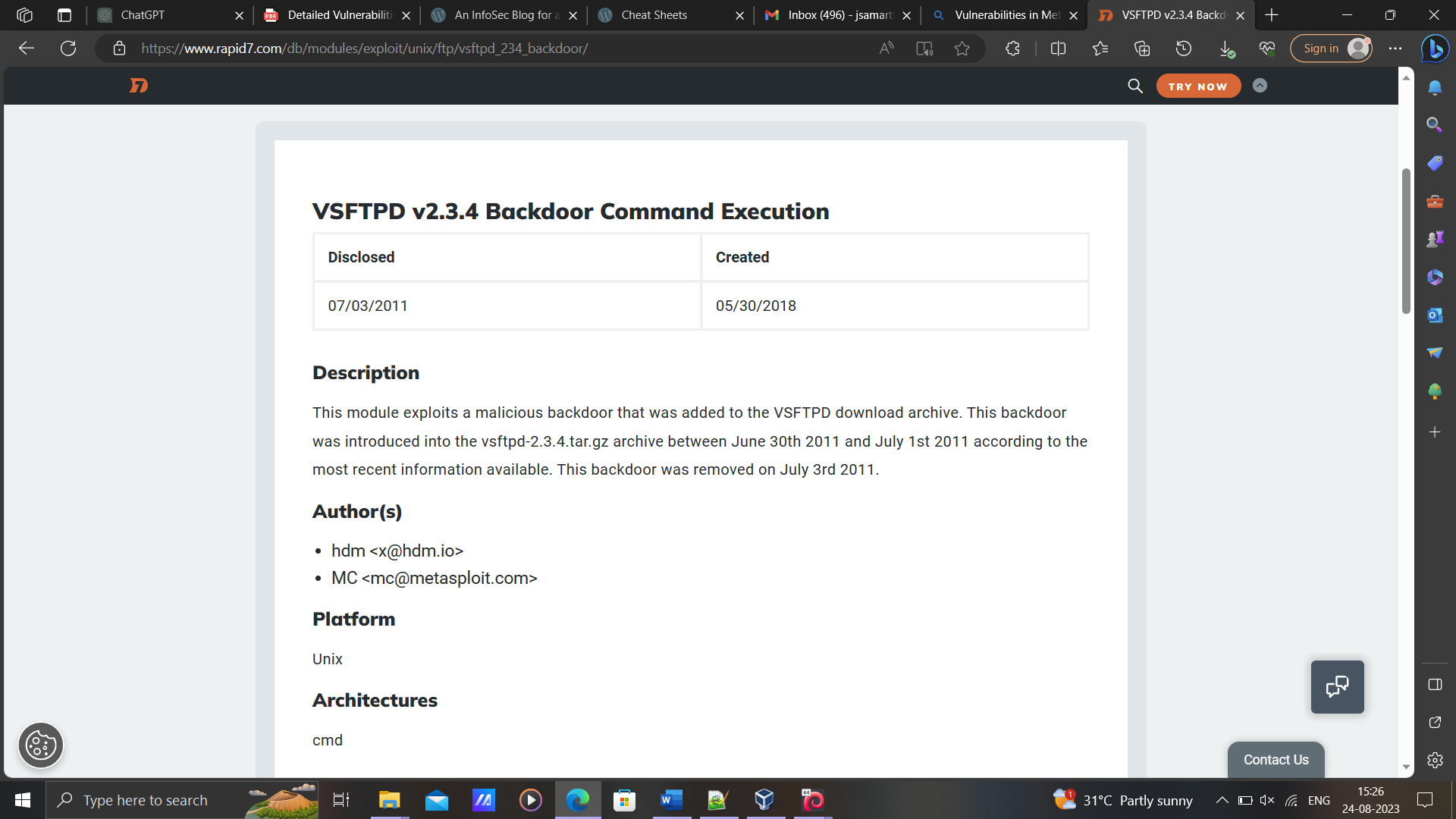


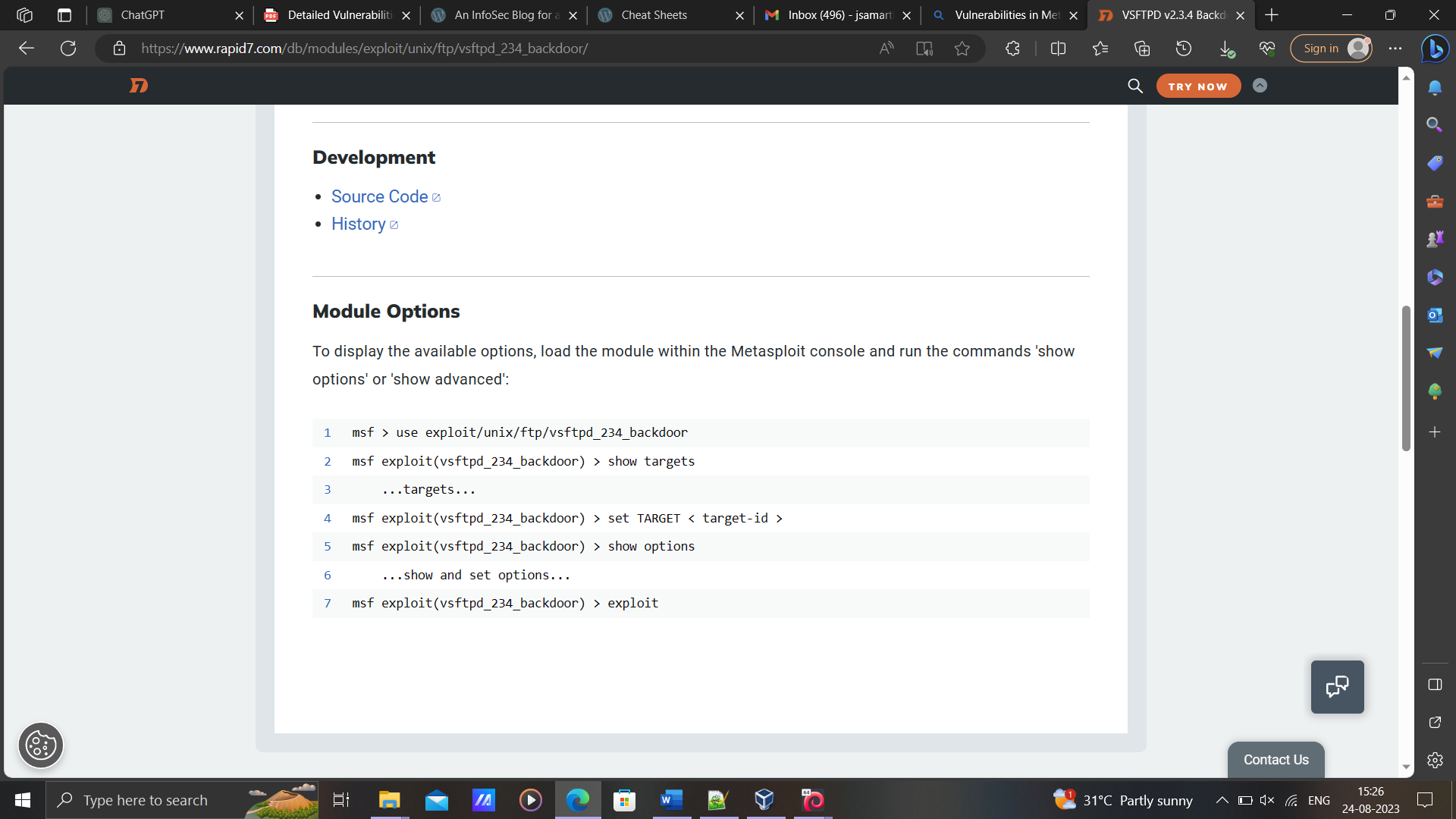
1. Description:

Perform a Manual Vulnerability Scan on the open port displayed in the port scan (in this case port 21). Search Google with a Vulnerability version (in this case vsftpd 2.3.4).

Google Prompt: Vulnerabilities in Metasploitable version vsfpd 2.3.4







From Rapid7 Database we can see that there is a vulnerability vsftpd v2.3.4 which we can exploit.

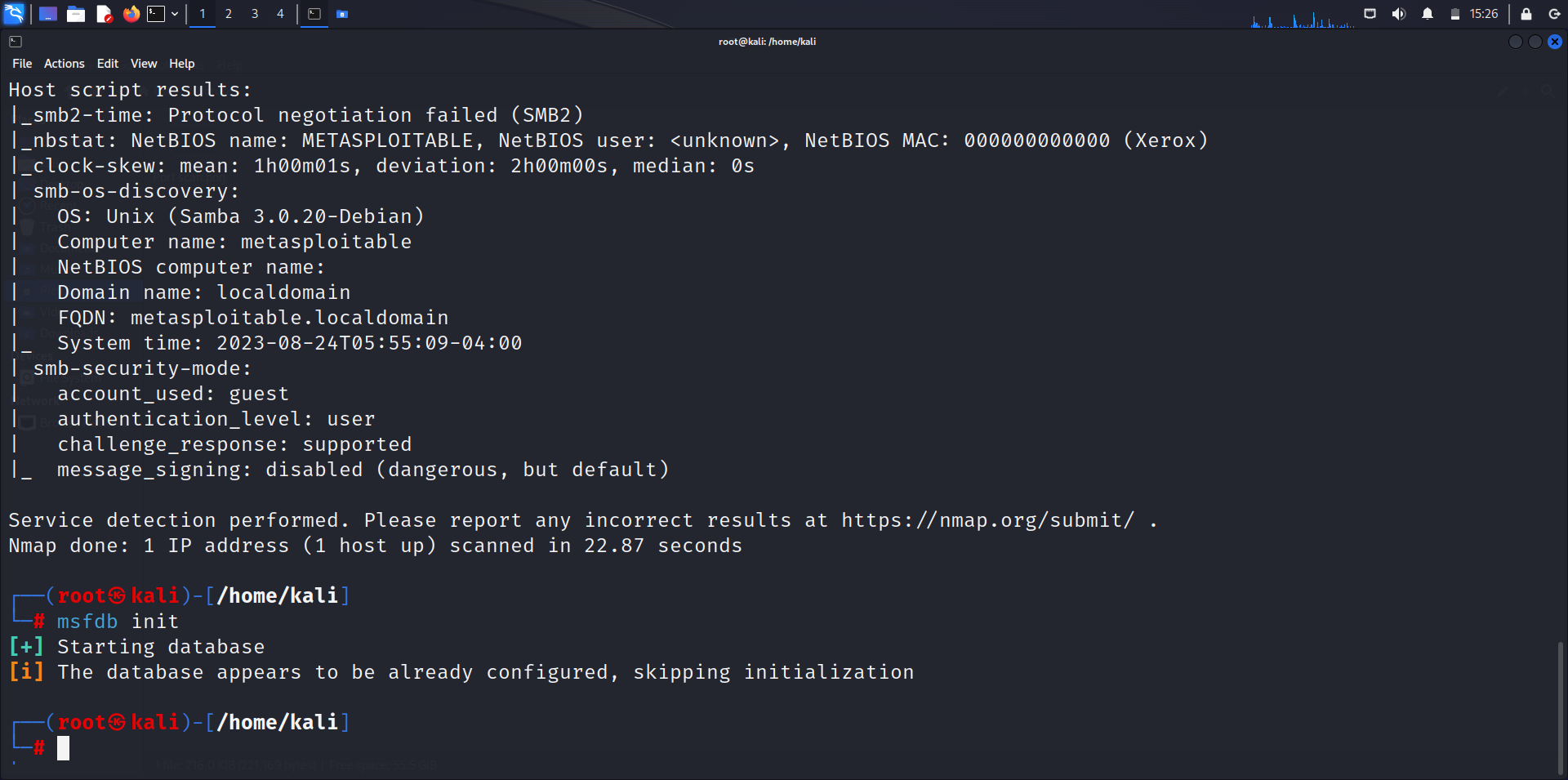
The type of vulnerability found is a **Backdoor**.

The Metasploit module path is “exploit/unix/ftp/vsftpd\_234\_backdoor”

1. Command: #msfdb init

Description:

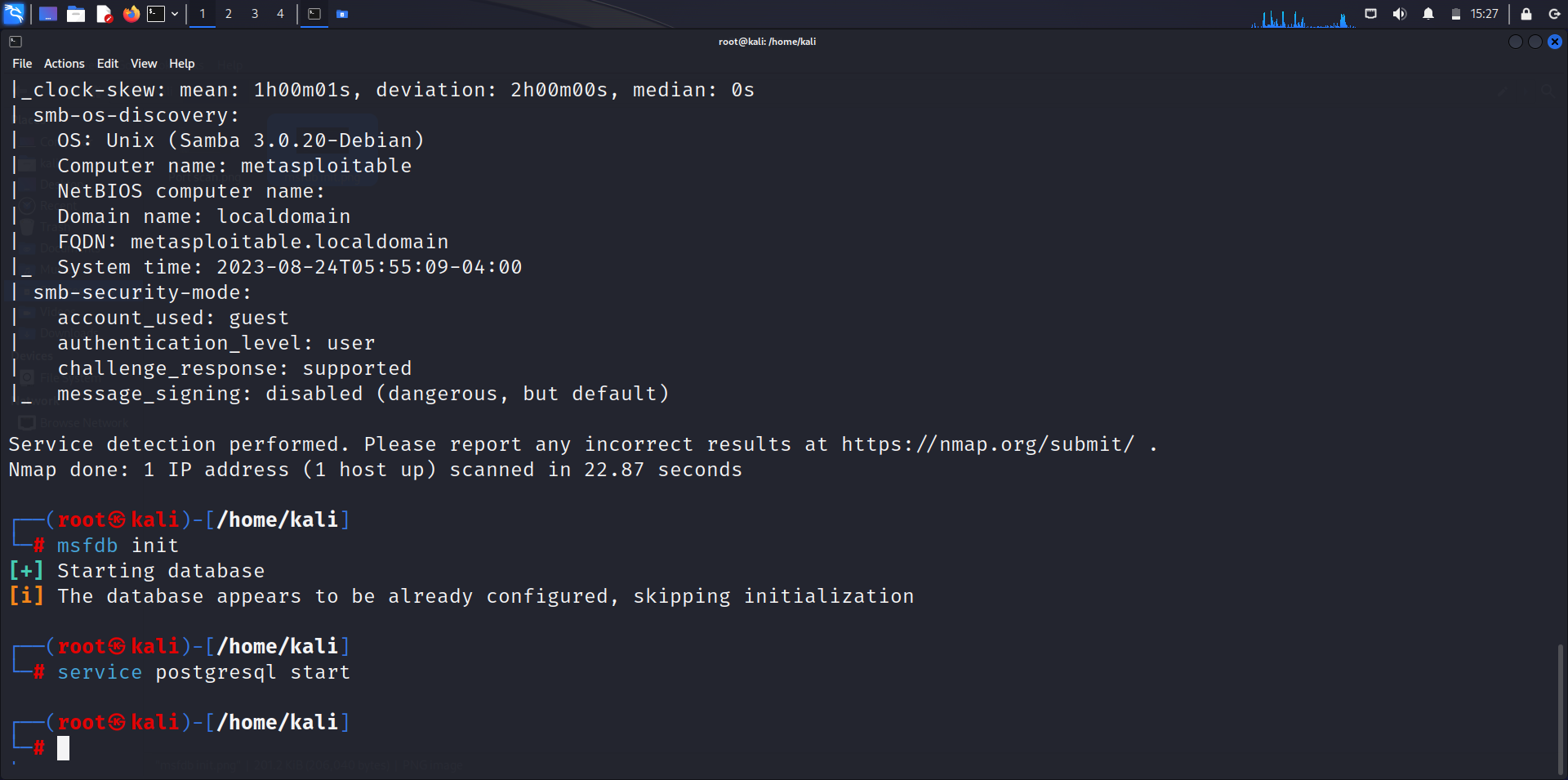
This is the **Second phase of Exploitation**, that is Initialize the Metasploit database (Only written once)



1. Command: #service postresql start

Description:

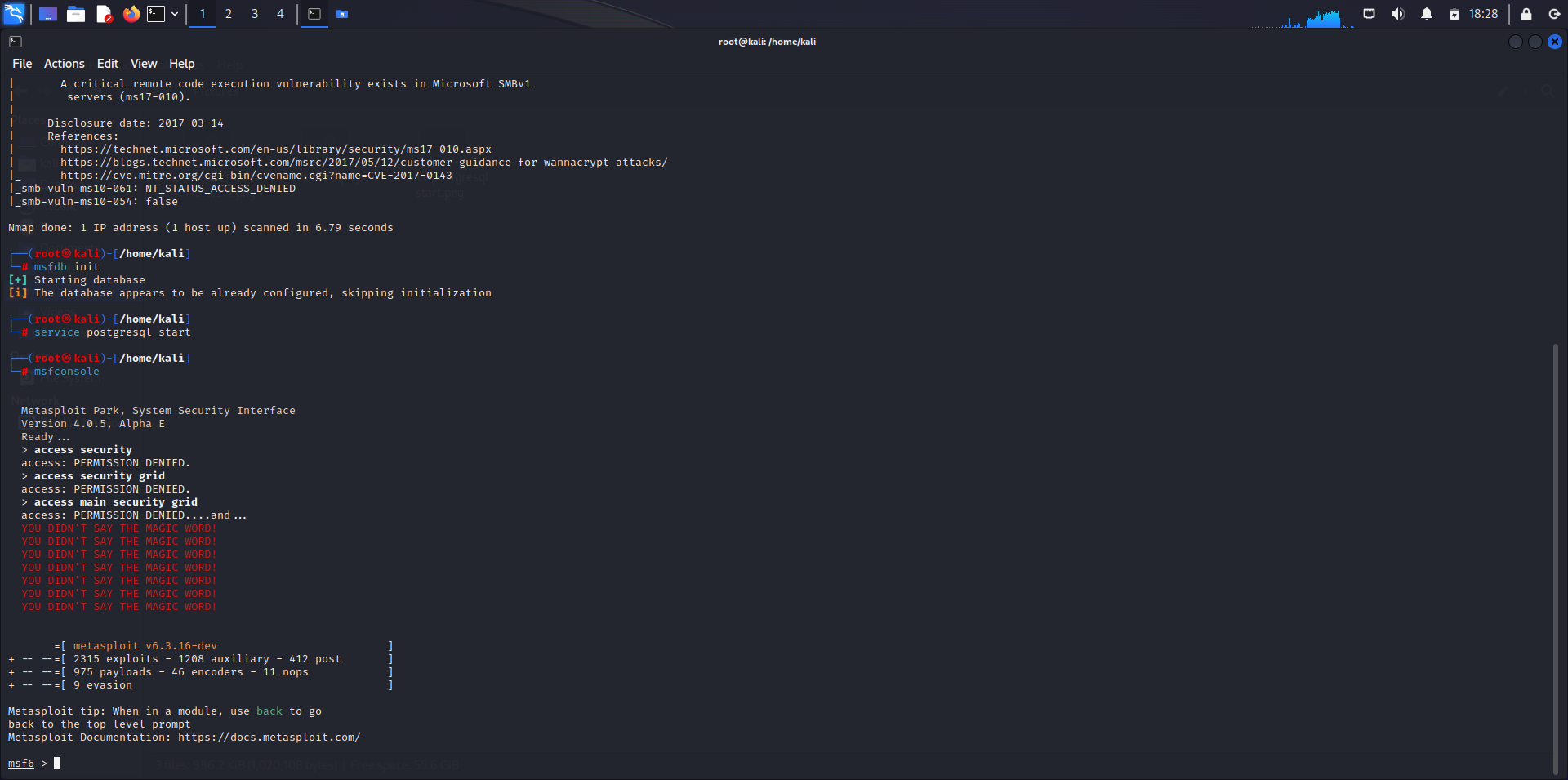
PostgreSQL database server on a Linux-based system. PostgreSQL is a popular open-source relational database management system. To start the backend of the Metasploit.



1. Command: #msfconsole

Description:

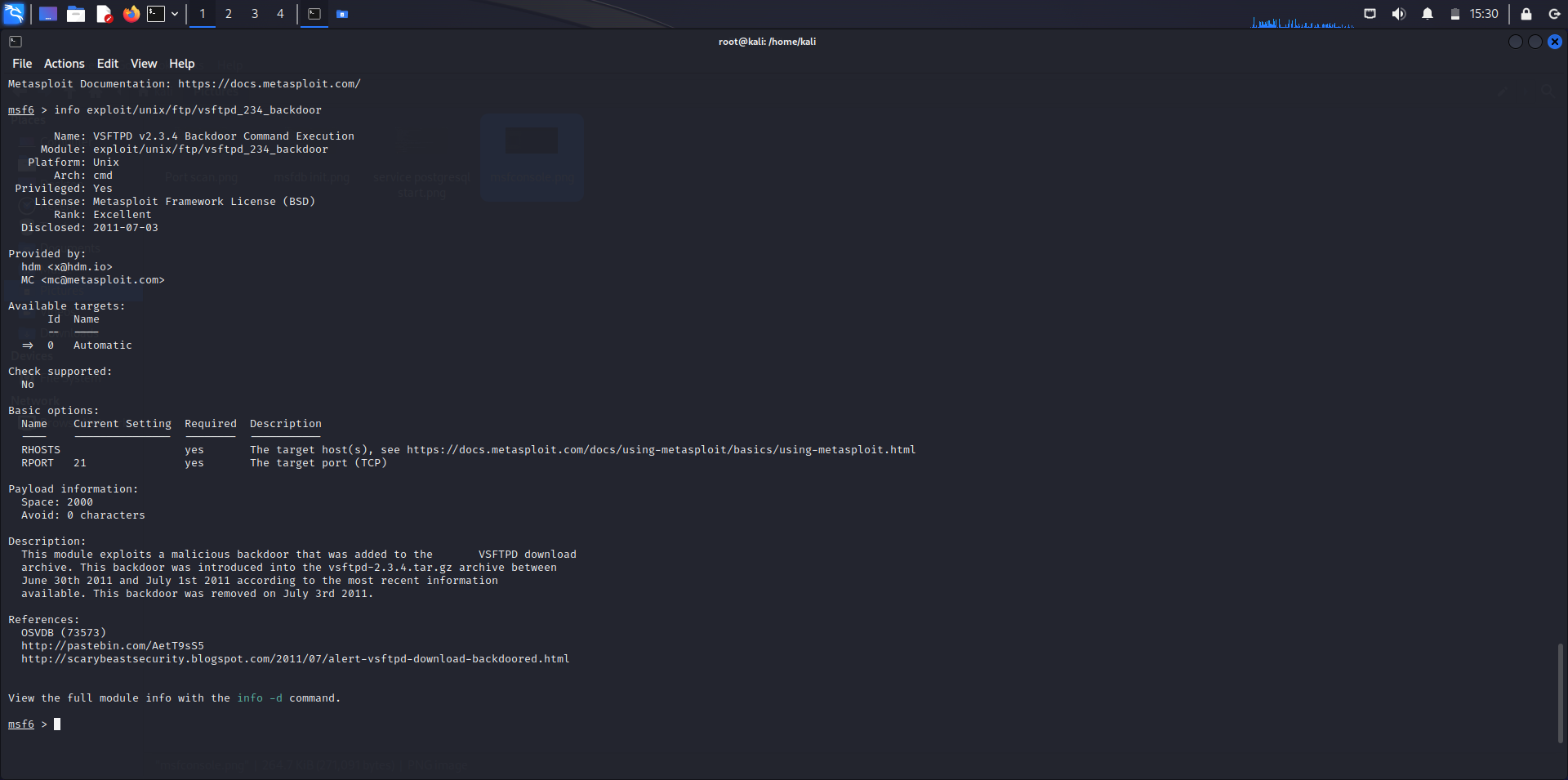
Start Metasploit framework console, you'll access the command-line interface of the Metasploit Framework, which provides a variety of tools and modules for performing security assessments, vulnerability exploitation, and more.



1. Command: msf6> info exploit/unix/ftp/vsftpd\_234\_backdoor

Syntax: info <path> or info <id>

Description: Checks whether the script is compatible with the target (Platform, Architecture, Privilege). Finds the Available Targets and provides Basic Options. It used to display detailed information about a specific module. The module can be an exploit, auxiliary module, payload, or any other type of module available in Metasploit's module database.

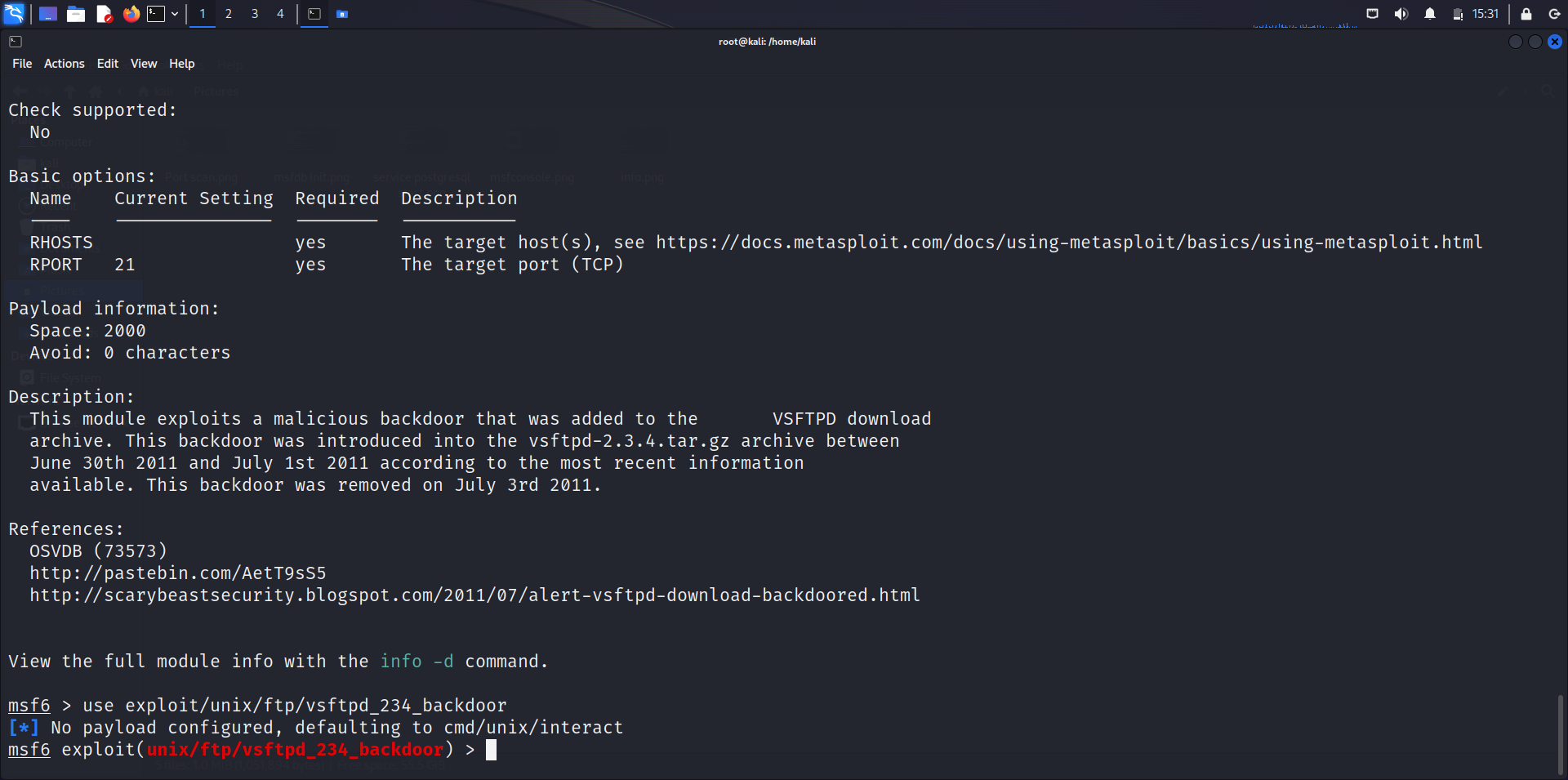


1. Command: msf6> use exploit/unix/ftp/vsftpd\_234\_backdoor

Syntax: use <path> or use <id>

Description:

The use command is used to select a specific module from the Metasploit Framework's module database for further configuration and execution. The module index refers to the position of the module in the list of available modules. However, using just the module index might not be the most accurate way to select a module, as the indexes can change based on the state of the database.

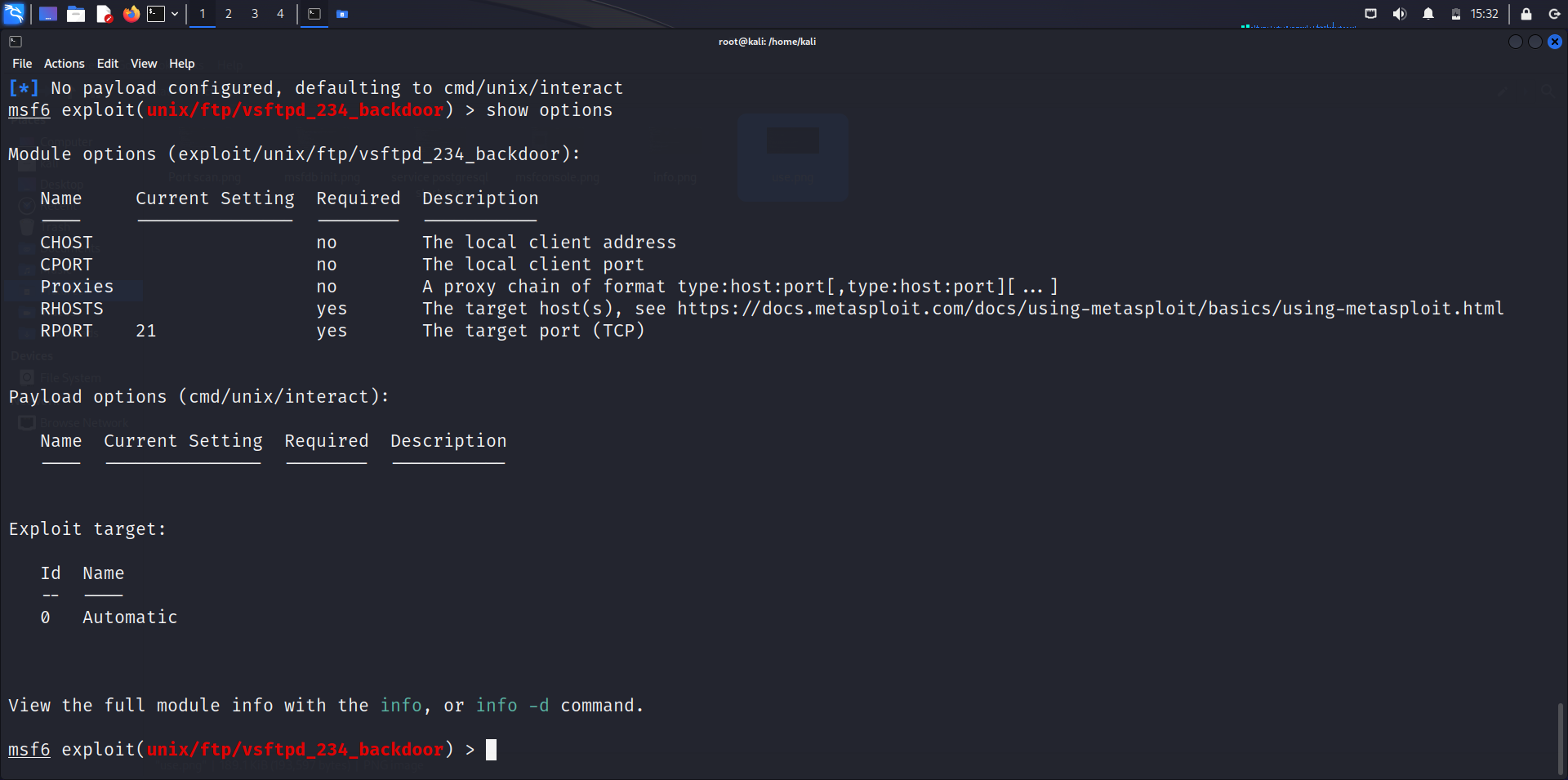


1. Command: msf6 exploit(unix/ftp/vsftpd\_234\_backdoor)> show options

Description:

Checks the mandatory setting (Set Current Setting if Required: yes). The show options command is used to display the available configuration options for the selected module. These options allow you to customize the behavior of the exploit to suit your needs.

Note: The below picture shows the options **BEFORE** setting the values.

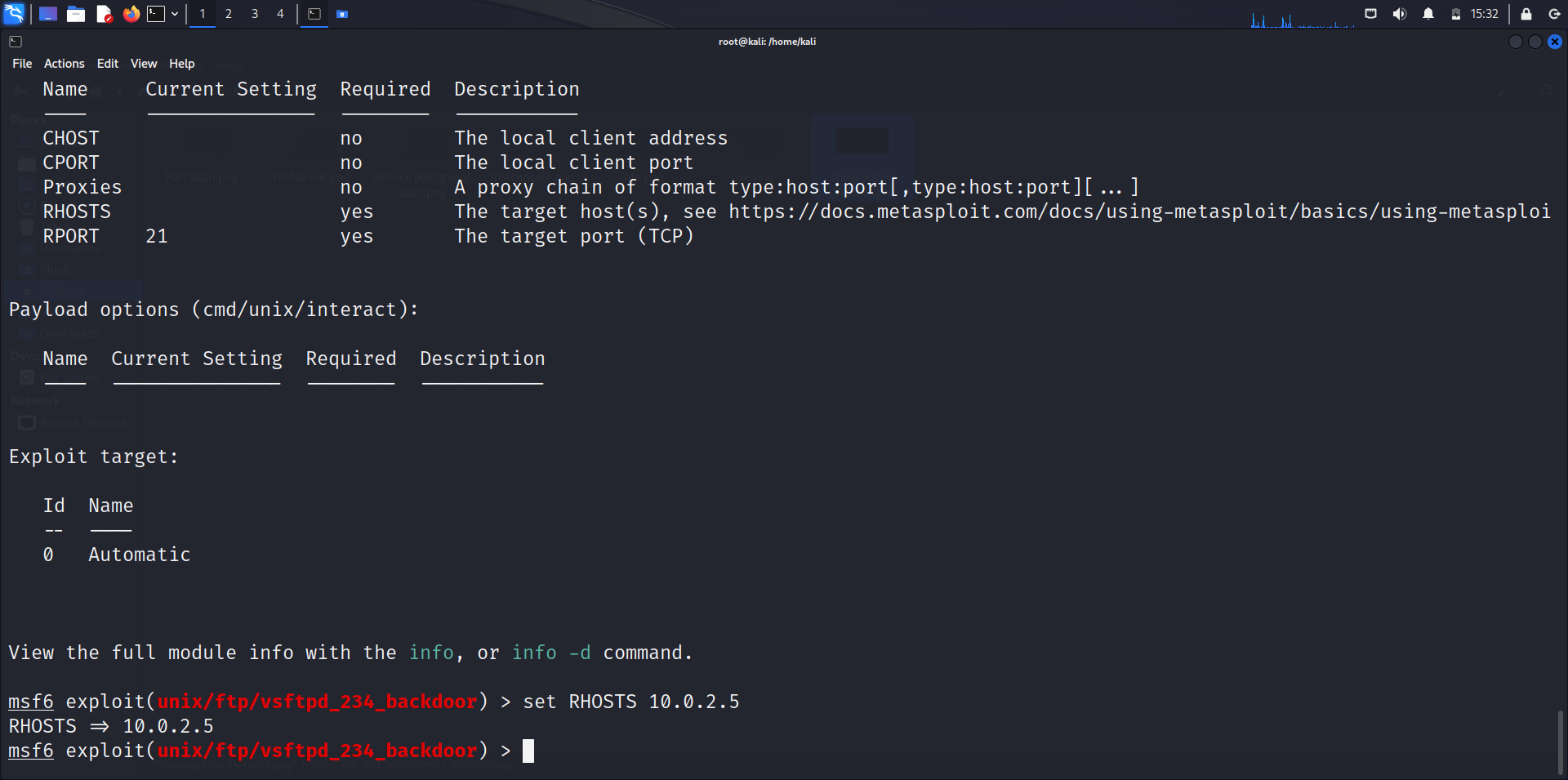


1. Command: msf6 exploit(unix/ftp/vsftpd\_234\_backdoor)> set RHOSTS 10.0.2.4

Syntax: set <option-name> <option-value/Current Setting value>

Description:

In the context of Metasploit, RHOSTS stands for "Remote Hosts," and it is used to specify the IP address or IP range of the target system(s) you intend to exploit.



1. Command: msf6 exploit(unix/ftp/vsftpd\_234\_backdoor)> show options

Note: The below picture shows the options **AFTER** setting the values.

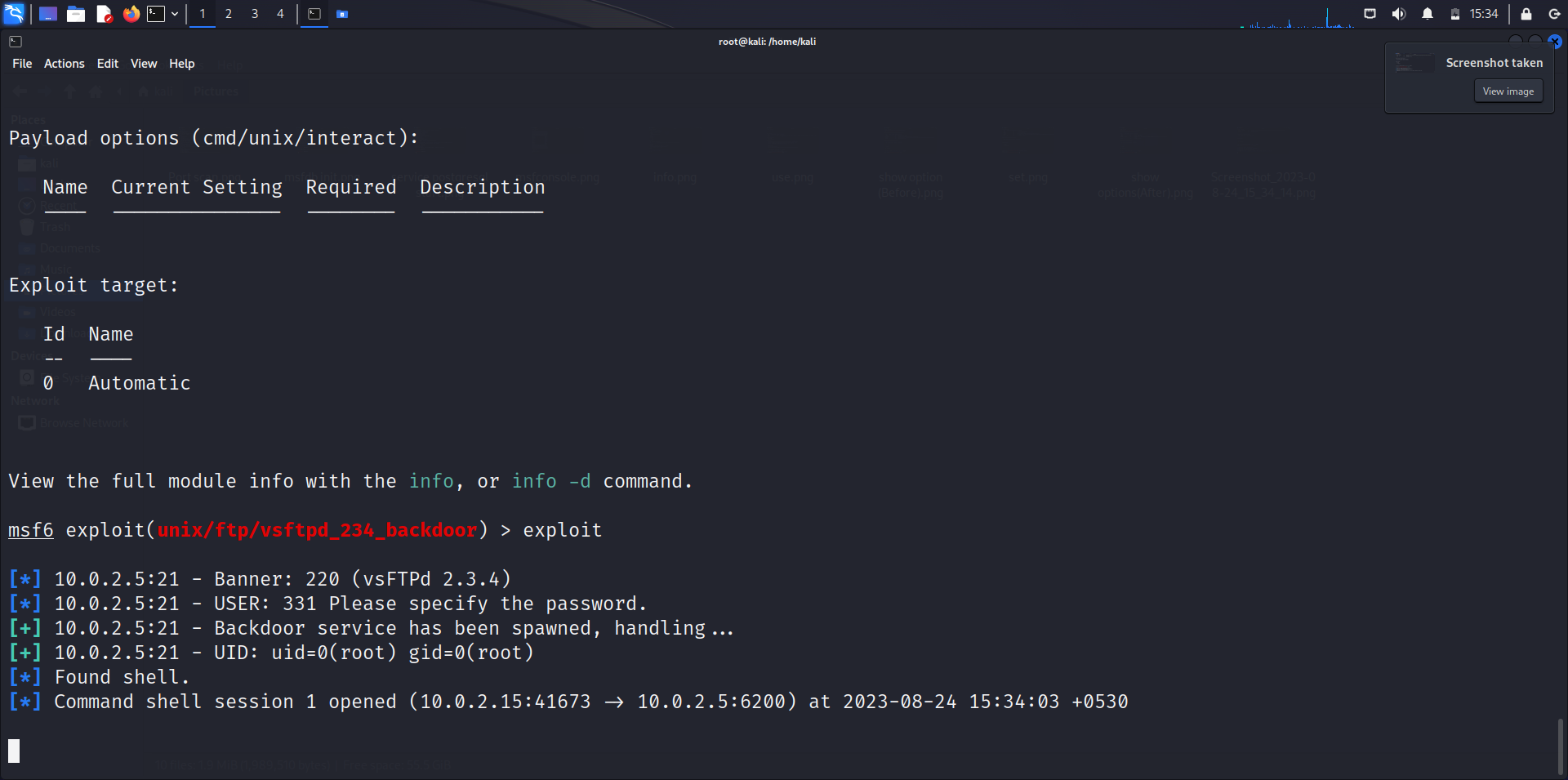


1. Command: msf6 exploit(unix/ftp/vsftpd\_234\_backdoor)> exploit

Description:

This the **Fifth phase of Execution**, that is Verify the Details and Execute the Exploit.

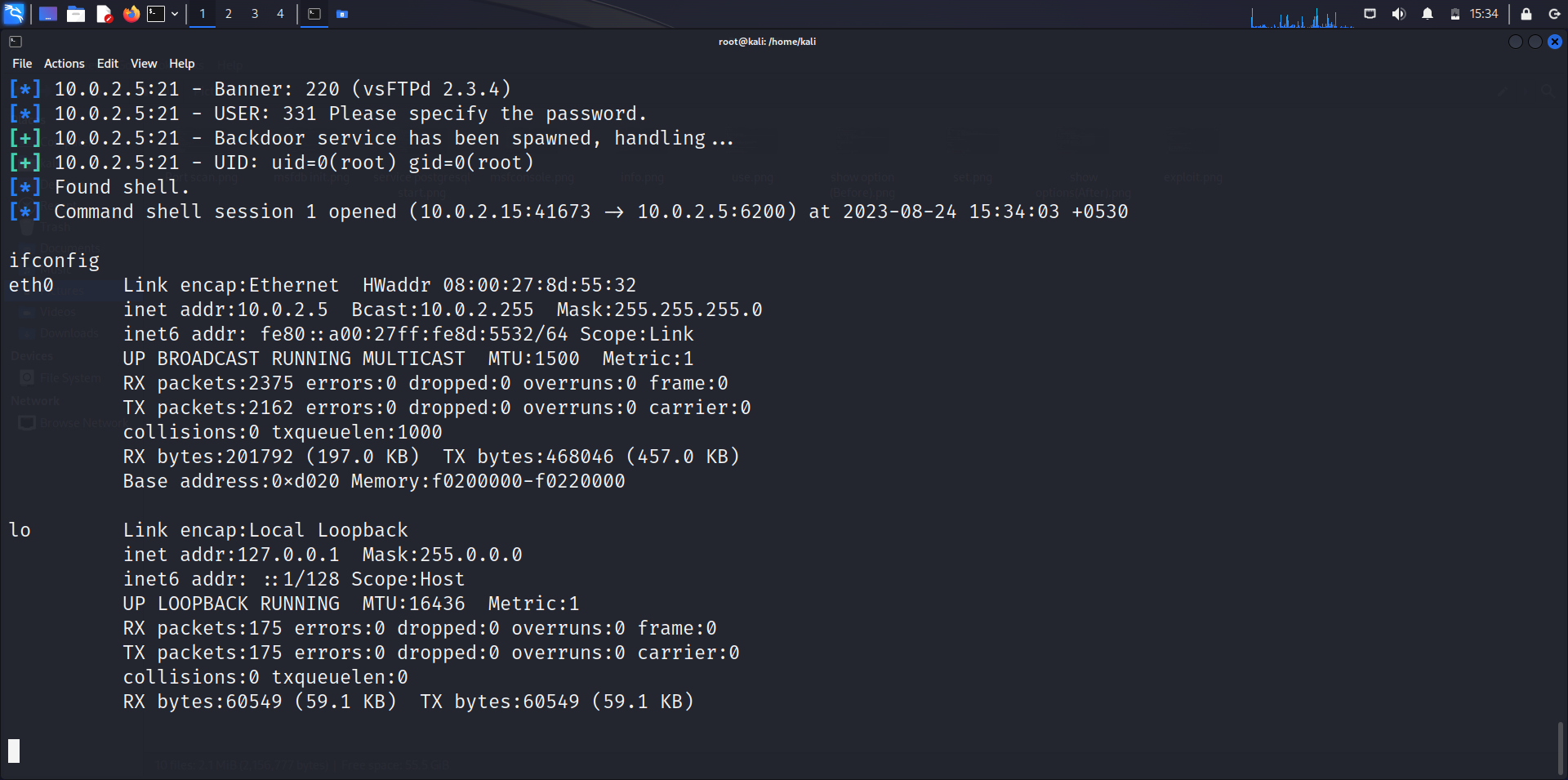
To execute the exploit. Executing the exploit command launches the selected module with the configured options. If the exploit is successful, it may result in gaining unauthorized access to the target system.



1. Command: ifconfig

Description:

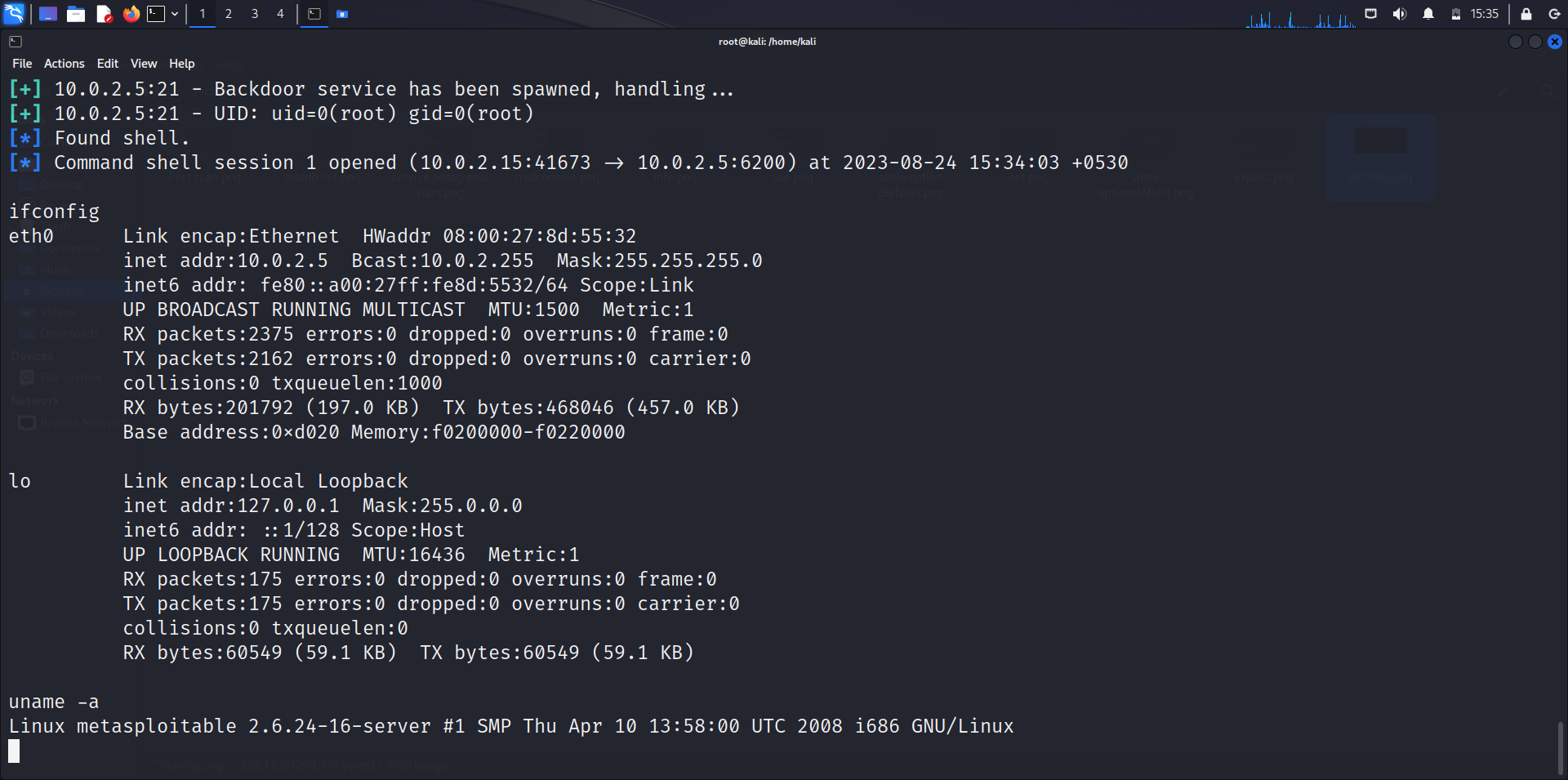
We can see that the shell session 1 has been opened, which means that the vulnerability vsftpd v2.3.4 of the target machine has been exploited. We can perform the ifconfig command in the command shell session, if the IP address of the target machine is displayed then the exploit has been confirmed.



1. Command: uname -a

Description:

Even though there is no visible command line prompt, we are still able to type command on the target machine’s shell. Another command which is the Linux equivalent of ‘sysinfo’ is uname -a. The ‘uname -a’ command is used in Unix-like operating systems to display detailed information about the system's kernel and system architecture. When this command is executed in a terminal or command prompt, it outputs a line of information that includes various details about the system.



**Analysis**

The report outlines the process of manually scanning for vulnerabilities by utilizing internet databases and executing an exploit. By searching comprehensive databases, potential vulnerabilities are identified based on known weaknesses and attack patterns. The subsequent execution of an exploit provides a practical assessment of the system's susceptibility to attacks, shedding light on potential security gaps. This approach offers a real-world perspective on the system's resilience and aids in understanding the urgency and severity of remediation measures.

**Conclusion**

In conclusion, the manual vulnerability scanning process that involves searching internet databases and executing exploits serves as a crucial methodology for assessing a system's security posture. This approach uncovers vulnerabilities that might not be apparent through automated scans and provides a hands-on understanding of potential attack vectors. The combination of database research and exploit execution offers a comprehensive view of a system's weaknesses and aids in making informed decisions about mitigation strategies. As cyber threats continue to evolve, integrating such manual assessments into a holistic security framework is imperative to effectively safeguarding valuable assets.