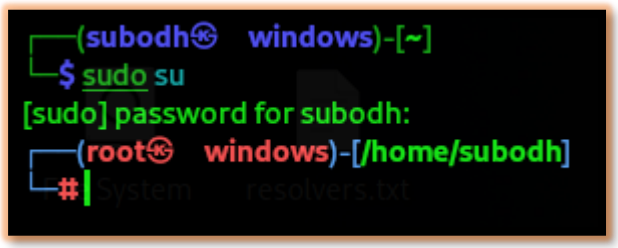
PENETRATION TESTING REPORT

METASPLOITABLE 2

Subodh Bagde

PENETRATION TESTING TOOLS AND METHODS

1. Environment Setup



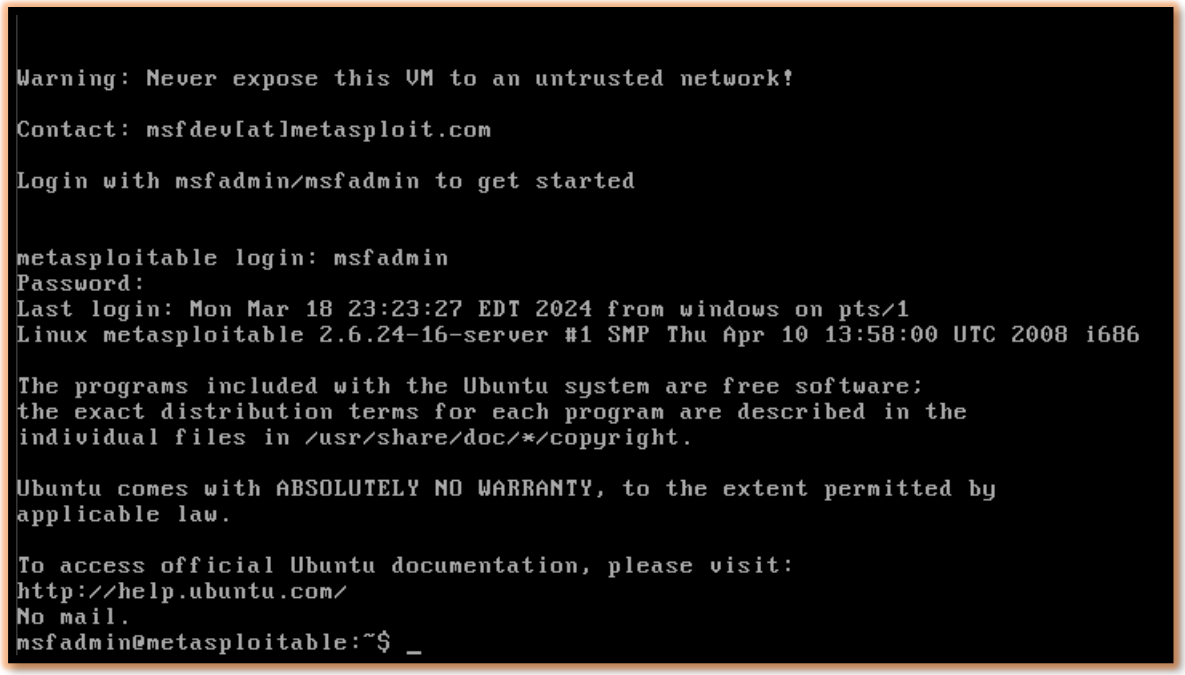


Figure 1. Penetration Testing Environment

Kali Linux was set up as the attacking machine and metasploitable2 as the target machine.

1.1 Metasploitable 2

Metasploitable is a virtual machine created by the Metasploit group, which consists of an Ubuntu 8.04 system image deliberately containing services with insecure configurations and vulnerabilities, which can be exploited using Metasploit Framework. This server was created with the aim of allowing practice with several of the options that Metasploit offers, being of

great help to learn about tests of penetration in a real environment.

2. Information Gathering

Ipconfig command was used in identification of the IP address of Metasploitable2. The IP address was identified as 192.168.1.3

Figure 2. Identification of IP address

A Ping command was used to identify if the attacking machine could communicate to the target machine and as shown below it was communicating.

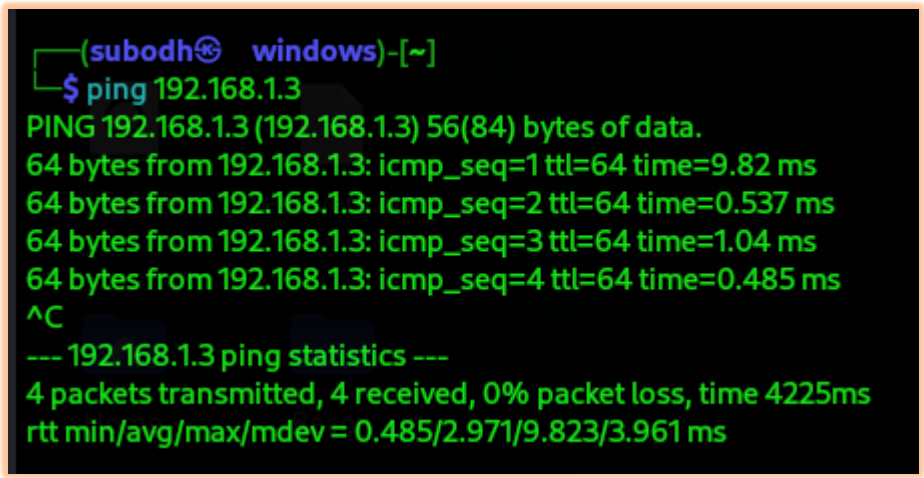


Figure 3. To check if the host is Up

2.2 Network Discovery

To discover the IP address of the Metasploitable2 virtual machine, once inside from the Metasploit Framework console, the ifconfig command was used, since that the IP address of the subnet is 192.168.1.0 with mask 255.255.255.0. The whole subnet was scanned and the IP address of Metasploitable was identified as 192.168.1.3 as shown below.

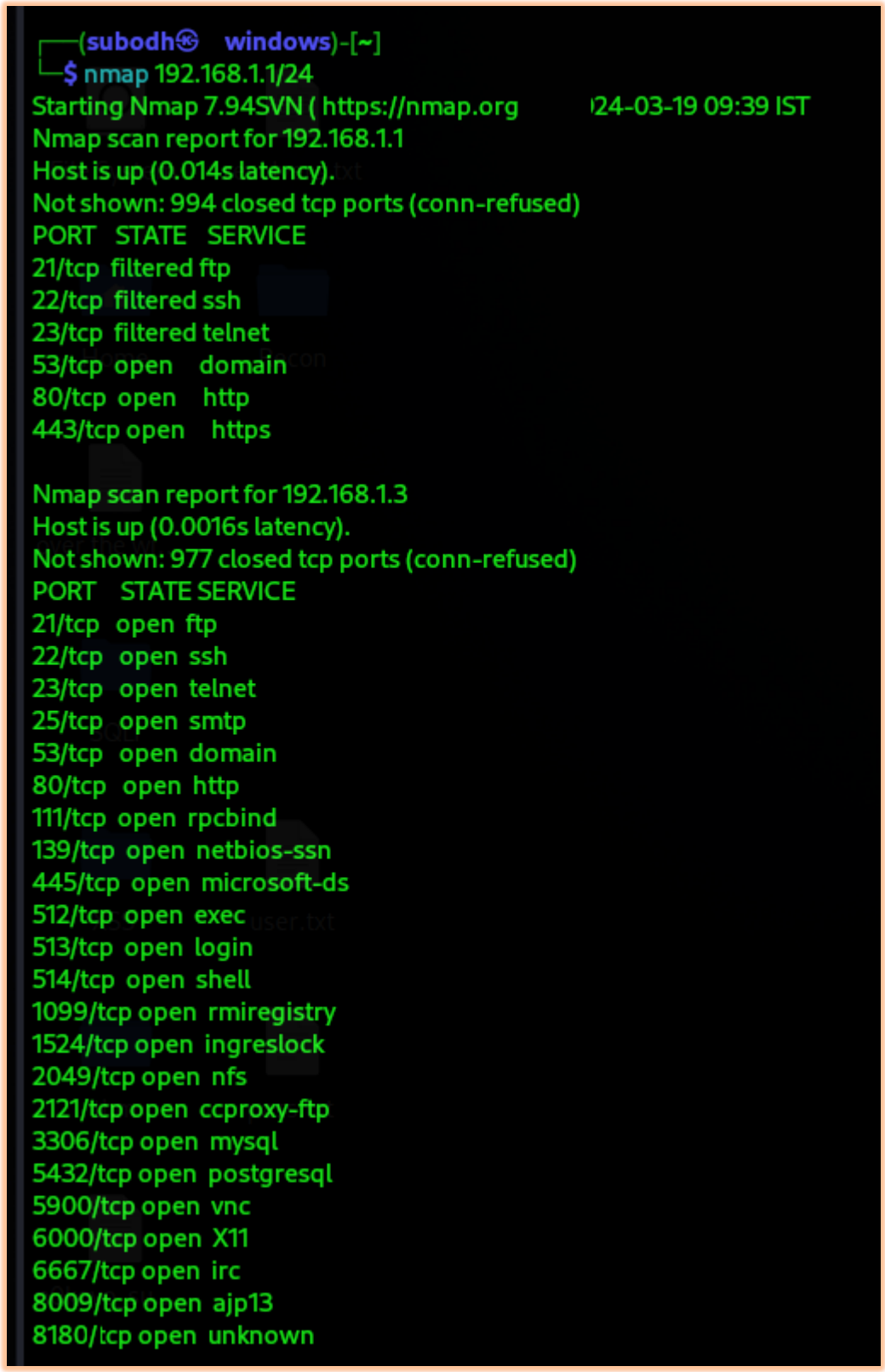


Figure 4. Identification of open ports

2.3 Operating System Identification

It was identified that Metsaploitable2 was running on Linux 2.6.9 - 2.6.33 as shown in Figure 5 below.

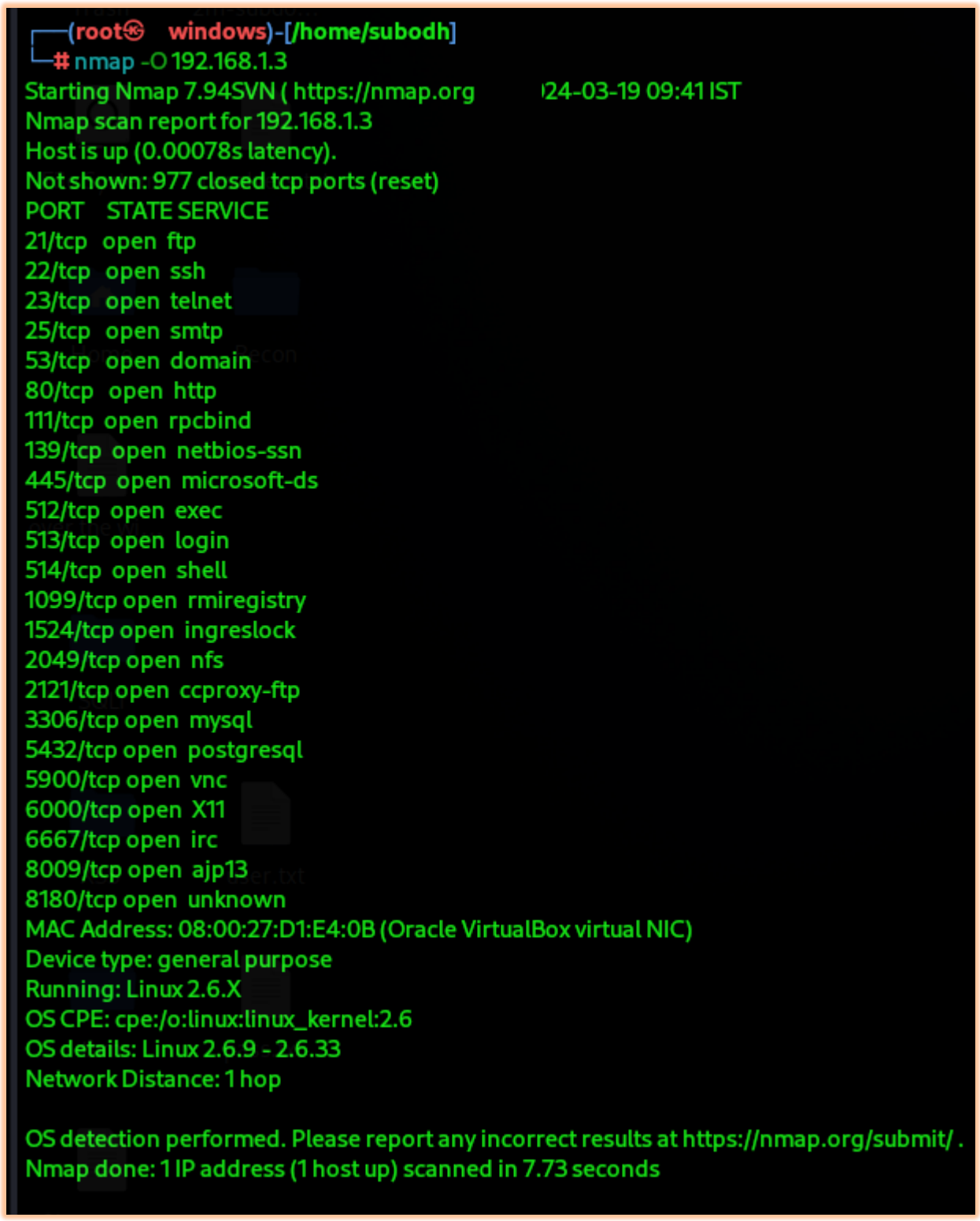


Figure 5. Identification of Operating System

3. Exploitation

After we have discovered the vulnerabilities on the target hosts or network, it is time to try exploit them. The exploitation phase sometimes ends the Penetration Testing process, but this depends on the contract, as there are situations where you must enter deeper into the target network, this with the purpose of expanding the attack throughout the network and winning all possible privileges.

3.1 Metasploit Framework

Metasploit Framework, is one of the most used tools currently for the realization Penetration testing of computer networks. This allows you to discover the different security vulnerabilities present in them and enables the application of security measures. security, so that an attacker cannot exploit these vulnerabilities in order to compromise the system in question.

This tool was created by H. D. Moore, using the programming language of Perl scripting, although it has now been fully upgraded to the scripting language. Ruby programming (Cuadra Pacheco, 2012), and has versions for Windows and Linux systems.

3.2 Threats or Vulnerabilities in Metasploitable 2

Threat 1 - Netcat Blindshell / Metasploitable root shell

Port: 1524

Description: Netcat is a networking utility that can read and write data across network connections, using the TCP or UDP protocols. In this context, a "Blind shell" typically refers to a remote shell (command-line interface) that is opened by an attacker using Netcat without the victim's knowledge. It allows the attacker to execute commands on the victim's machine remotely, potentially leading to unauthorized access or further exploitation.

Operation & Impact:

Figure 6. Netcat Login

Recommendation: To mitigate the risk posed by Netcat Blind shell, ensure that unnecessary services are not running on your system. Additionally, monitor network traffic for any suspicious activity and restrict network access to trusted sources. Regular security audits and updates are also crucial to protect against known vulnerabilities.

Threat 2 - vsftpd 2.3.4 - Backdoor FTP

Port: 21

Description: vsftpd (Very Secure FTP Daemon) is an FTP (File Transfer Protocol) server software for Unix-like systems. It is designed to be fast, stable, and secure, and is commonly used to transfer files over a network.

Operation & Impact:

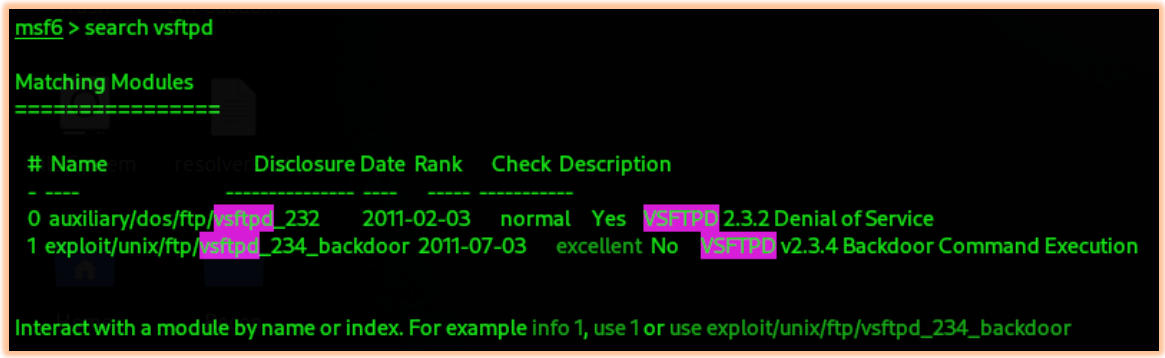


Figure 7. Searching VSFTPD threat

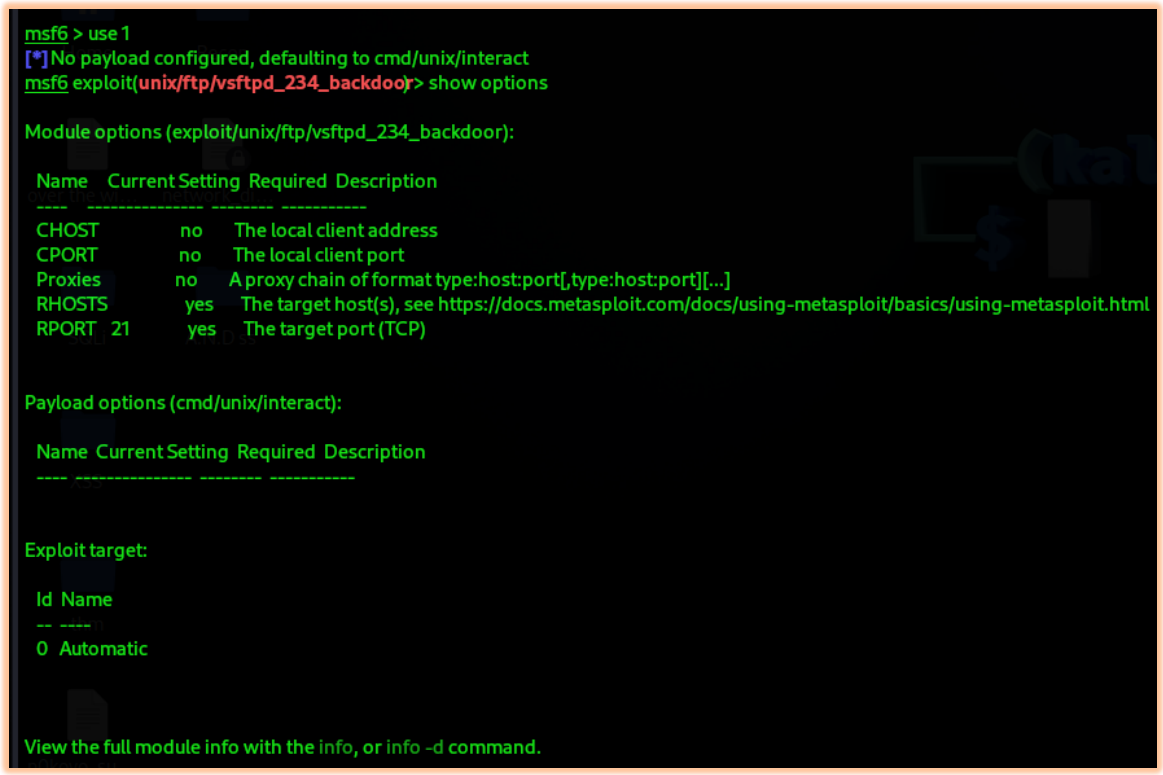


Figure 8. Module options for VSFTPD vulnerability

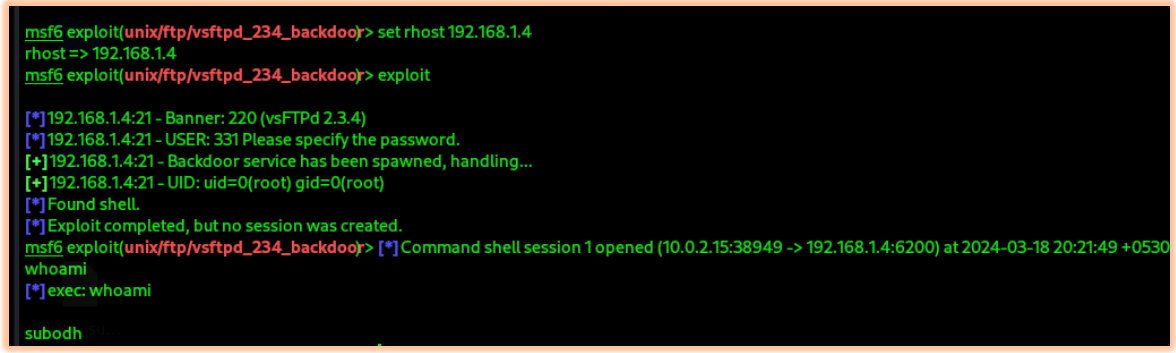


Figure 9. Exploiting VSFTPD vulnerability

Recommendation: To mitigate the risk associated with vsftpd, ensure that the software is kept up to date with the latest security patches. Additionally, use strong authentication mechanisms such as SSH keys or encrypted passwords, and limit access to the FTP server to only those who need it.

Threat 3 - SSH Login

Port: 22

Description: SSH is a cryptographic network protocol for operating network services securely over an unsecured network. It is commonly used for

remote login to systems and for executing commands on a remote machine.

Operation & Impact:

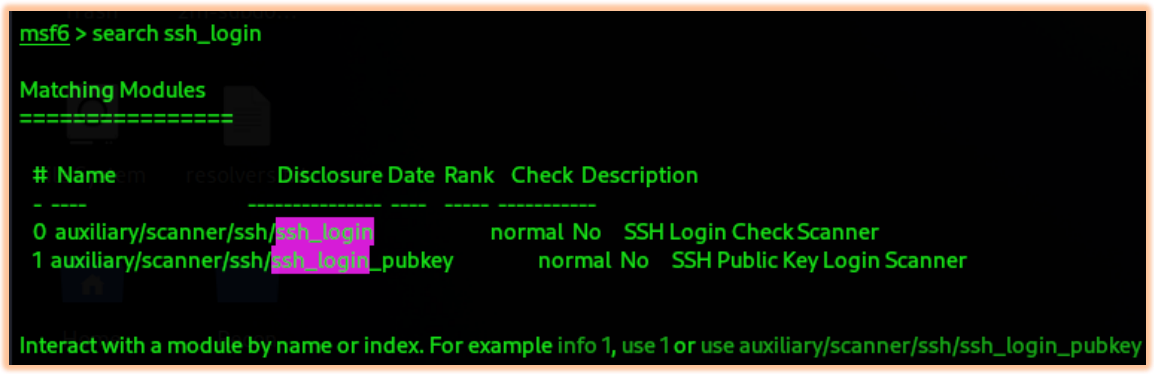


Figure 10. Searching for SSH Login module

Figure 11. Module options for SSH Login

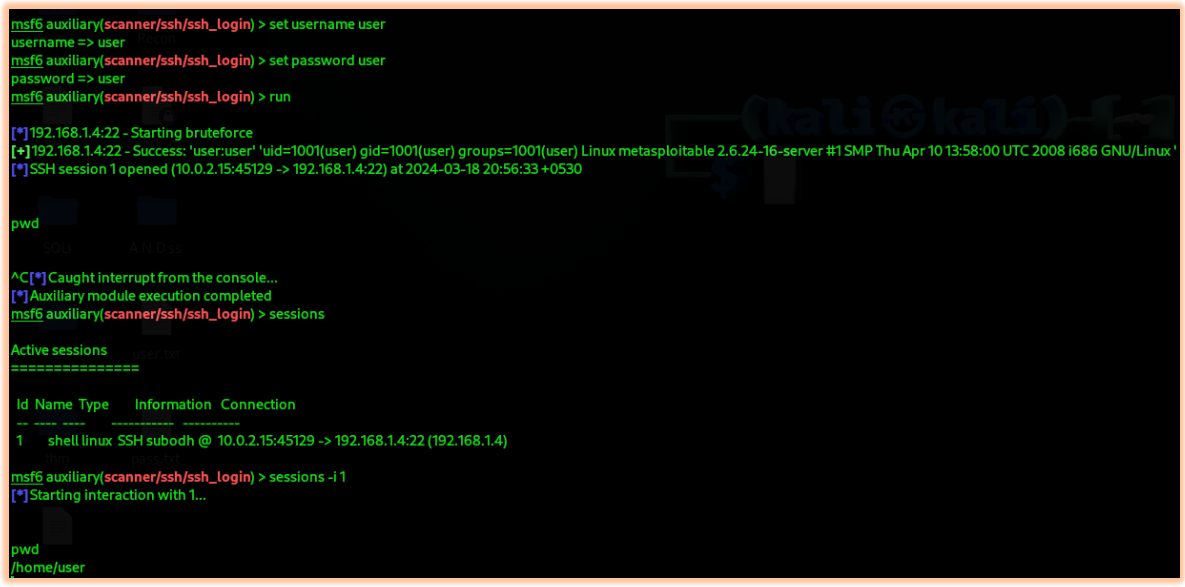


Figure 12. Exploiting SSH Login vulnerability

Recommendation: To mitigate the risks associated with SSH login, ensure that strong authentication mechanisms such as SSH keys or multi-factor authentication (MFA) are used. Disable password-based authentication if possible and regularly update the SSH server to the latest version to patch known vulnerabilities.

Threat 4 - Telnet Login

Port: 23

Description: Telnet is a network protocol used for remote login to a computer system. It allows a user to establish a connection to a remote system and interact with it as if they were physically present at the system's console.

Operations & Impact:

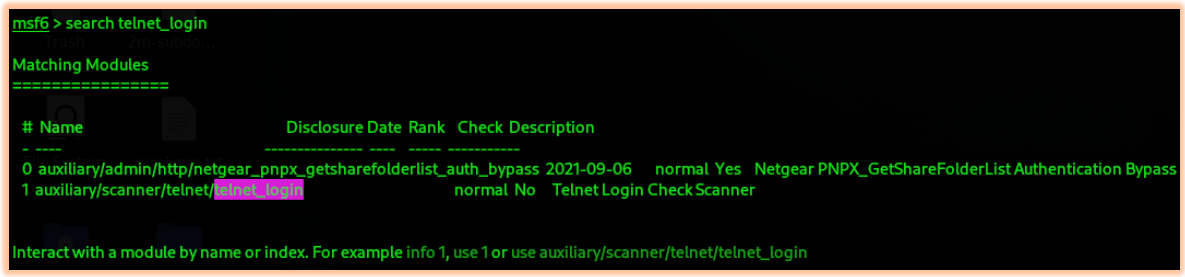


Figure 13. Searching for Telnet Login modules

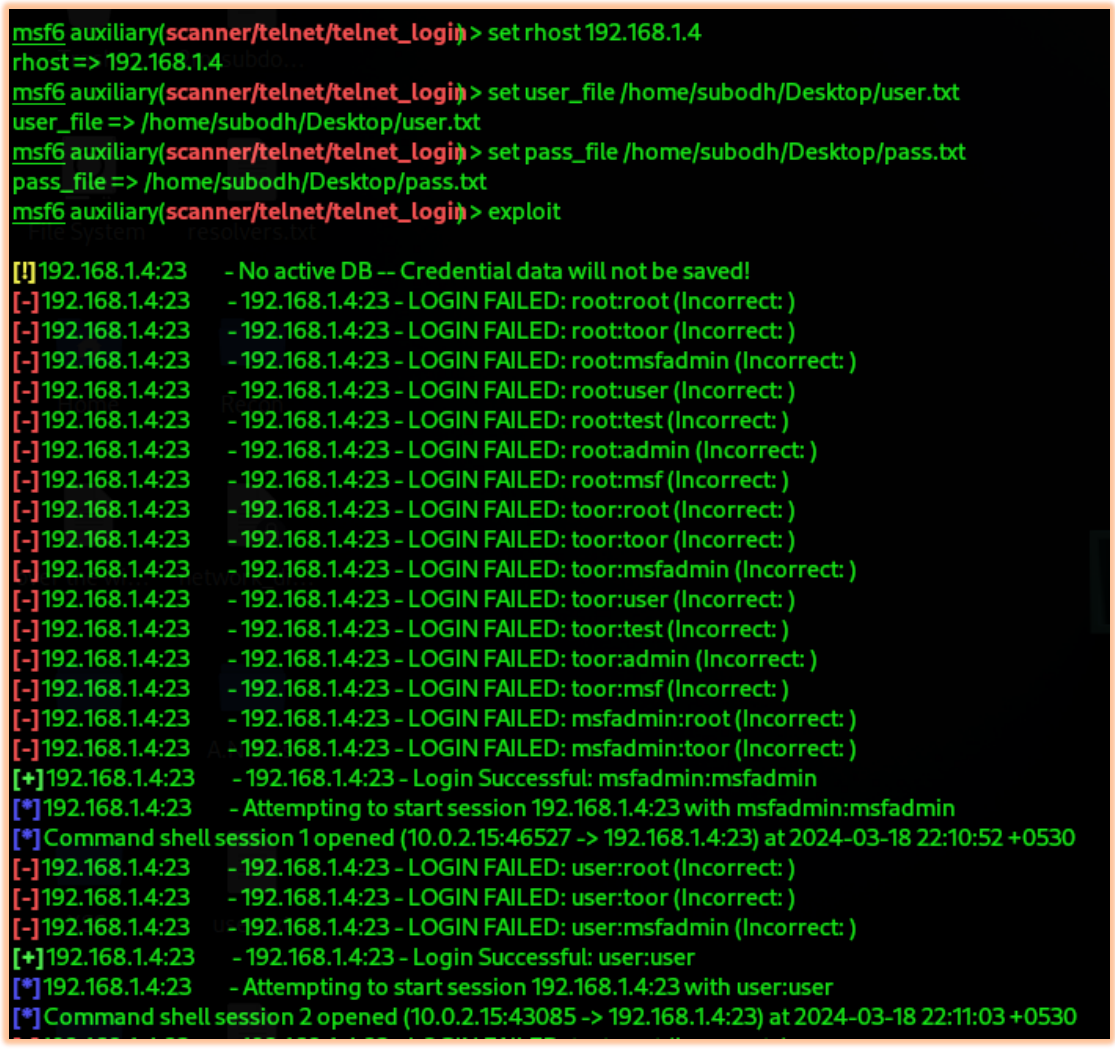


Figure 14. Exploiting Telnet Login vulnerability

Figure 15. Accessing active sessions using Telnet Login

Recommendation: To mitigate the risks associated with Telnet, it is recommended to use more secure alternatives such as SSH (Secure Shell) for remote access. Regularly monitor Telnet logs for any unauthorized access attempts and disable Telnet services when not needed.

Threat 5 - http / PHP-cgi

Port: 80

Description: HTTP (Hypertext Transfer Protocol) is the foundation of data communication on the World Wide Web. It is used to request and transmit web pages and other resources from web servers to web browsers. PHP-CGI is a Common Gateway Interface (CGI) executable used for running PHP scripts on a web server. It allows web servers to process PHP code and generate dynamic web content.

Operations & Impact:

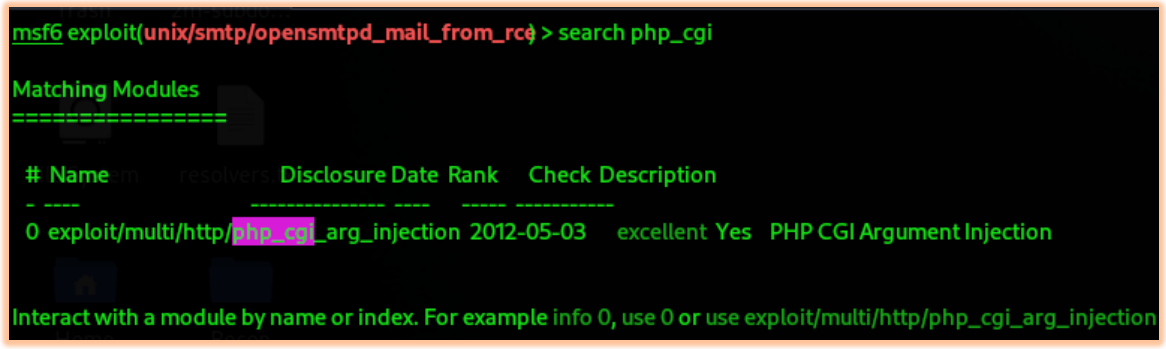


Figure 16. Searching for php_cgi module

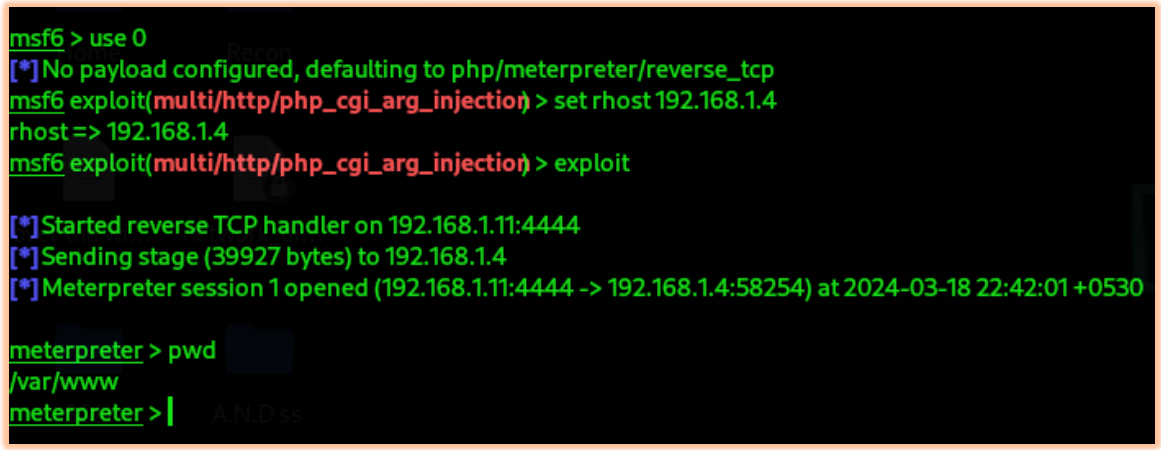


Figure 17. Exploiting php_cgi and gaining meterpreter access

Recommendation: To mitigate the risks associated with HTTP/PHP-CGI, ensure that web servers are kept up to date with the latest security patches.

Threat 6 - Netbios-ssn - Samba smbd 3.X - 4.X

Port: 139/445

Description: Samba is an open-source software suite that provides file and print services for Windows clients. The smbd (Server Message Block Daemon) is a component of Samba that implements the SMB (Server Message Block) protocol, which is used for sharing files, printers, and other resources between Windows and Unix-like systems.

Operations & Impact:

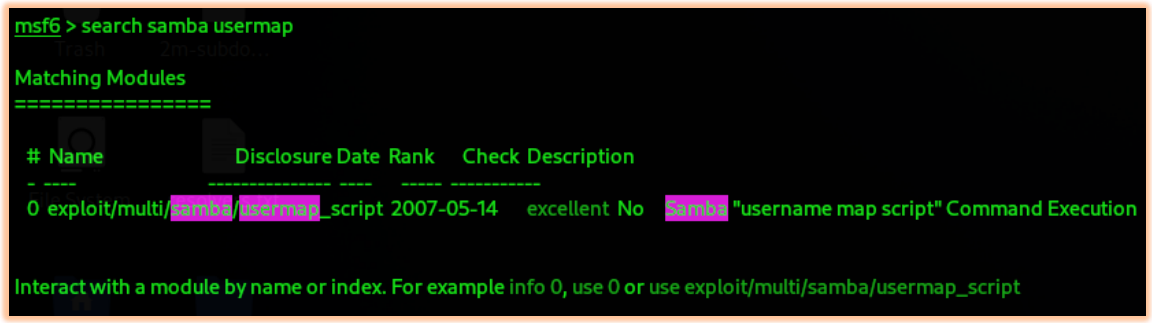


Figure 18. Searching for Samba usermap module

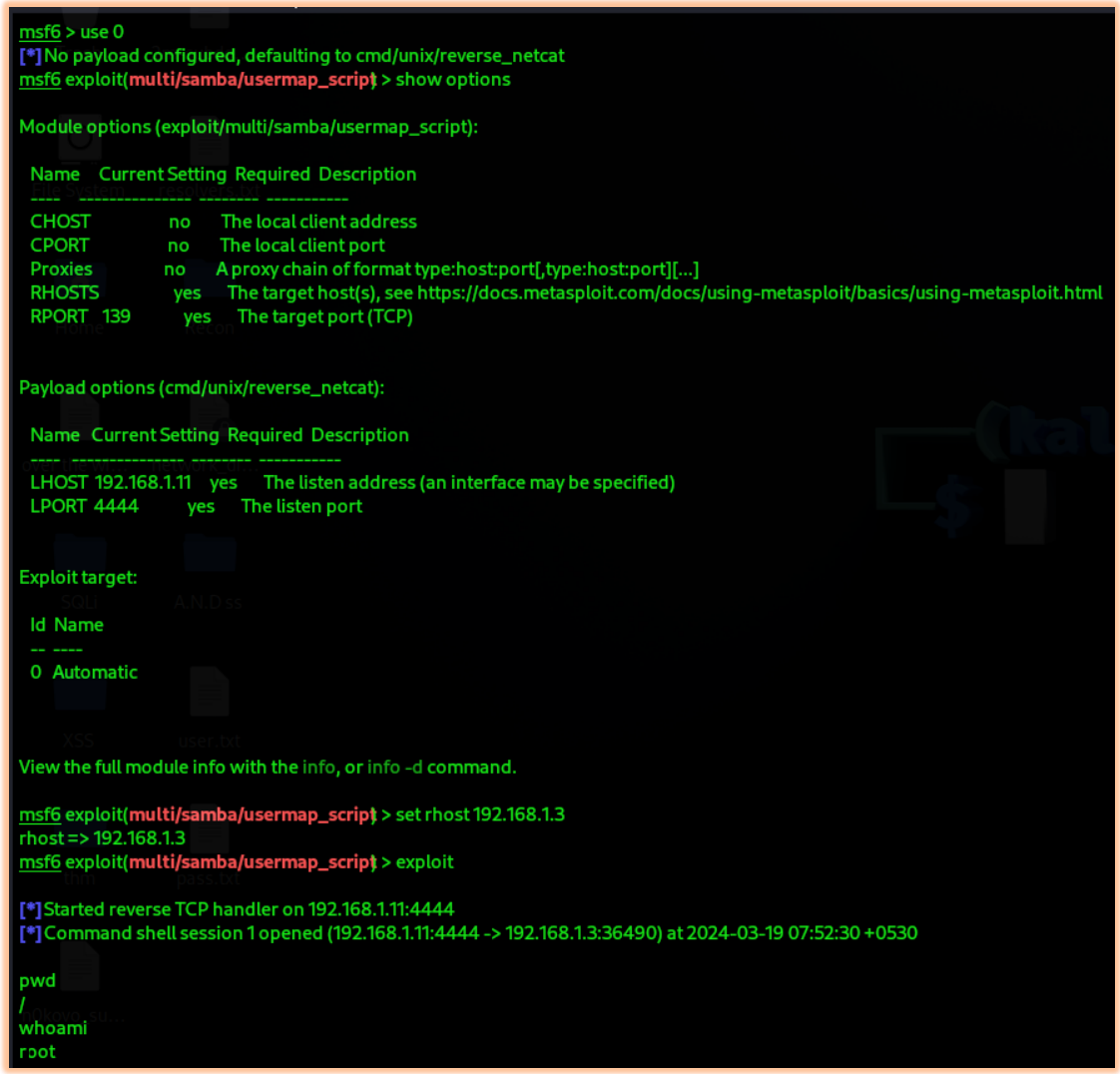


Figure 19. Exploiting samba usermap vulnerability

Recommendation: Keep Samba and the underlying operating system up to date with the latest security patches. Use strong authentication mechanisms such as encrypted passwords or Active Directory integration.

Threat 7 - PostgreSQL DB 8.3.0 - 8.3.7

Port: 5432

Description: PostgreSQL is a powerful, open-source relational database management system (RDBMS) known for its reliability, robustness, and feature set. It is used by many organizations for storing and managing data in a variety of applications.

Operation & Impact:

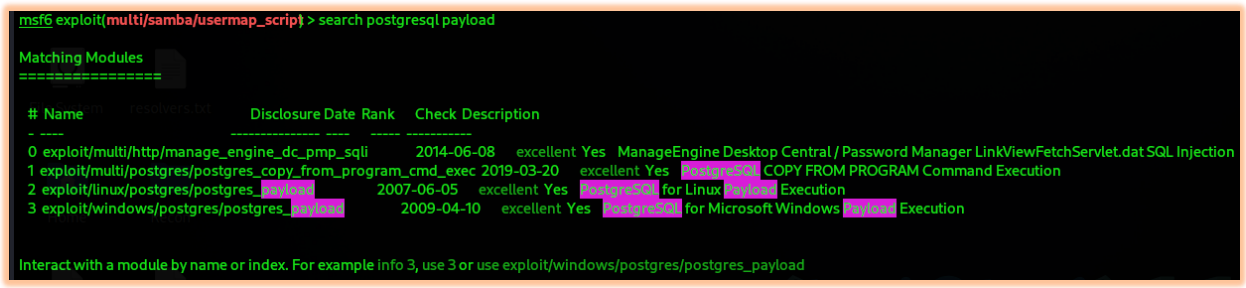


Figure 20. Searching for PostgreSQL payload module

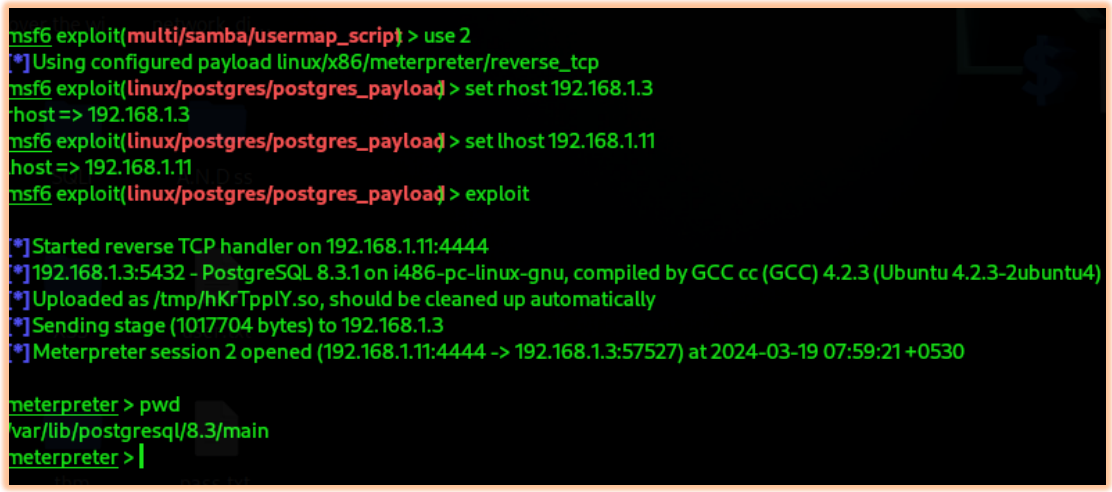


Figure 21. Exploiting PostgreSQL payload vulnerability

Recommendation: To mitigate the risks associated with PostgreSQL, ensure that the database is configured securely, with strong authentication mechanisms in place. Use role-based access control (RBAC) to restrict access to sensitive data and regularly update PostgreSQL to the latest version to patch known vulnerabilities.

Threat 8 - Backdoor IRC / Unreal IRCd

Port: 6667

Description: UnrealIRCd is an open-source Internet Relay Chat (IRC) server software. IRC is a protocol used for real-time text messaging and is commonly used for group communication and chat rooms. UnrealIRCd is known for its flexibility and feature set, making it popular among IRC server operators.

Operations & Impact:

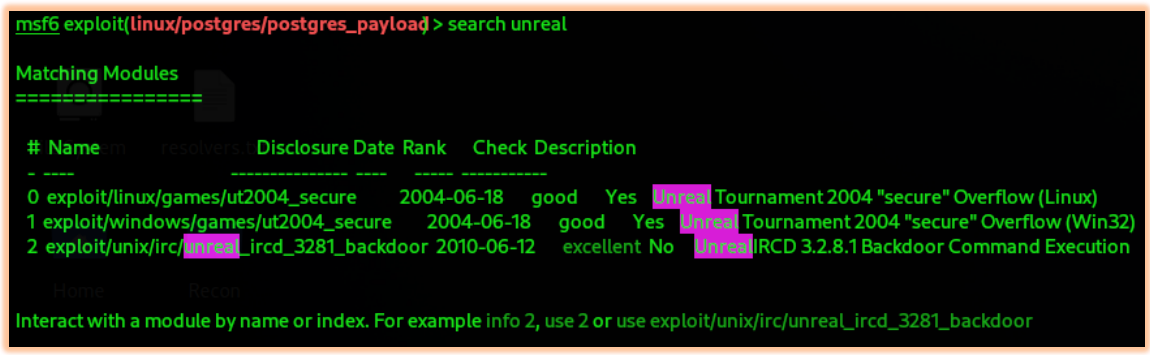


Figure 22. Searching for unreal IRC module

Figure 23. Compatible payloads for unreal IRC module

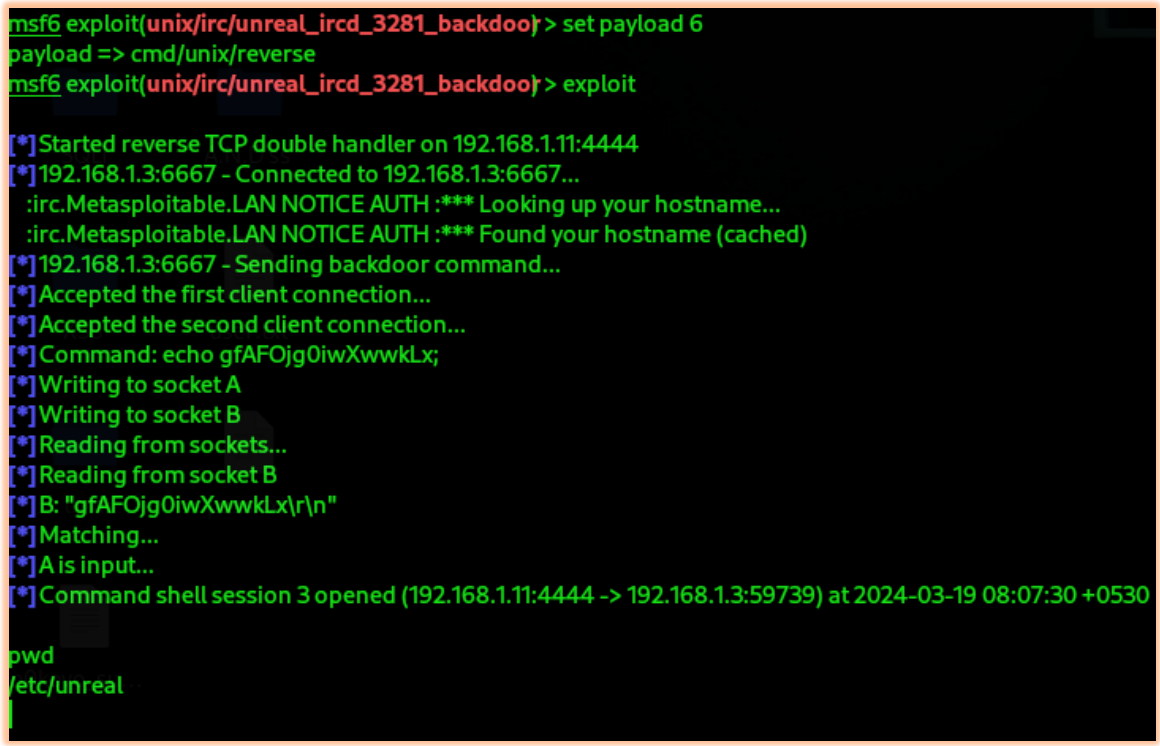


Figure 24. Exploiting unreal IRC module using payload and gaining access

Recommendation: To mitigate the risks associated with UnrealIRCd, ensure that the server is configured securely, with strong authentication mechanisms in place. Regularly update UnrealIRCd to the latest version to patch known vulnerabilities. Monitor IRC server logs for any suspicious activity and consider using a firewall to restrict access to the IRC server from external sources.

Threat 9 - VNC Login

Port: 5900

Description: VNC is a graphical desktop-sharing system that allows users to remotely control another computer. The VNC server runs on the remote machine, while the VNC client runs on the local machine and enables the user to interact with the remote desktop. VNC sessions are not encrypted by default, making them vulnerable to eavesdropping and unauthorized access.

Operations & Impact:

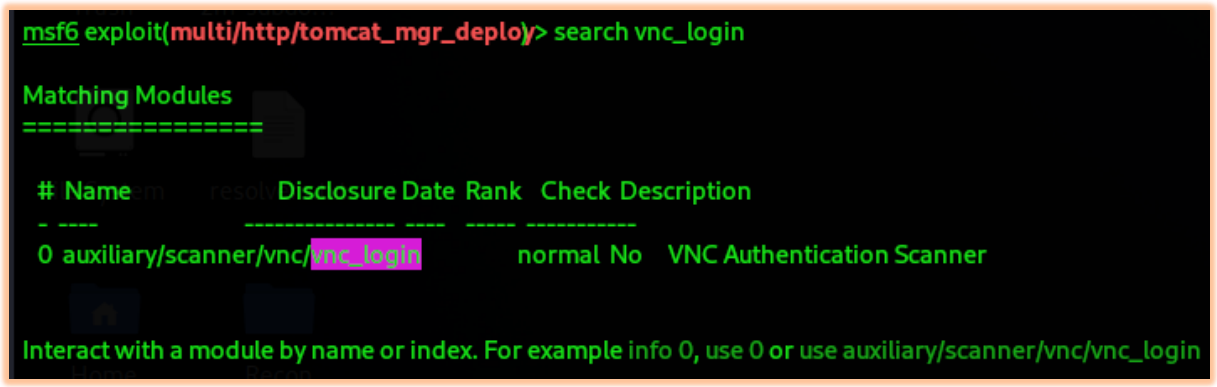


Figure 25. Searching for VNC Login module

```
msf6 auxiliary(scanner/vnc/vnc_login) > set rhost 192.168.1.3
rhost => 192.168.1.3
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.1.3:5900      - 192.168.1.3:5900 - Starting VNC login sweep
[!] 192.168.1.3:5900      - No active DB -- Credential data will not be saved!
[+] 192.168.1.3:5900      - 192.168.1.3:5900 - Login Successful: :password
[*] 192.168.1.3:5900      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

Figure 26. Exploiting VNC Login module

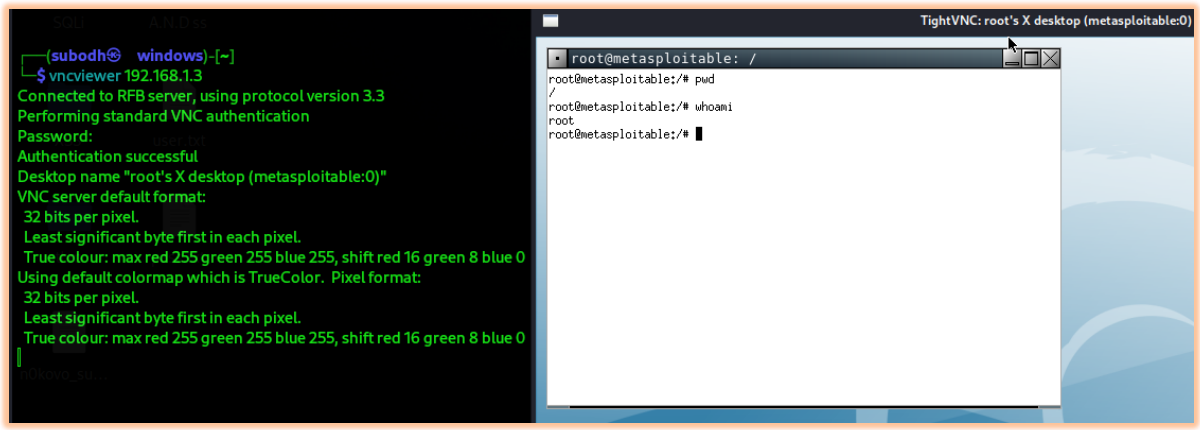


Figure 27. Gaining access using vncviewer

Recommendation: To mitigate the risks associated with VNC login, it is recommended to use encryption technologies such as SSH tunnels or VPNs (Virtual Private Networks) to secure VNC sessions.

Threat 10 - RLogin

Port: 512 (exec), 513 (login), 514 (shell)

Description: R services typically refer to the RSH (Remote Shell) services, which allow users to execute commands on a remote system. These services use the RSH protocol, which is a simple, unencrypted protocol that is insecure and susceptible to eavesdropping and unauthorized access.

Operations & Impact:

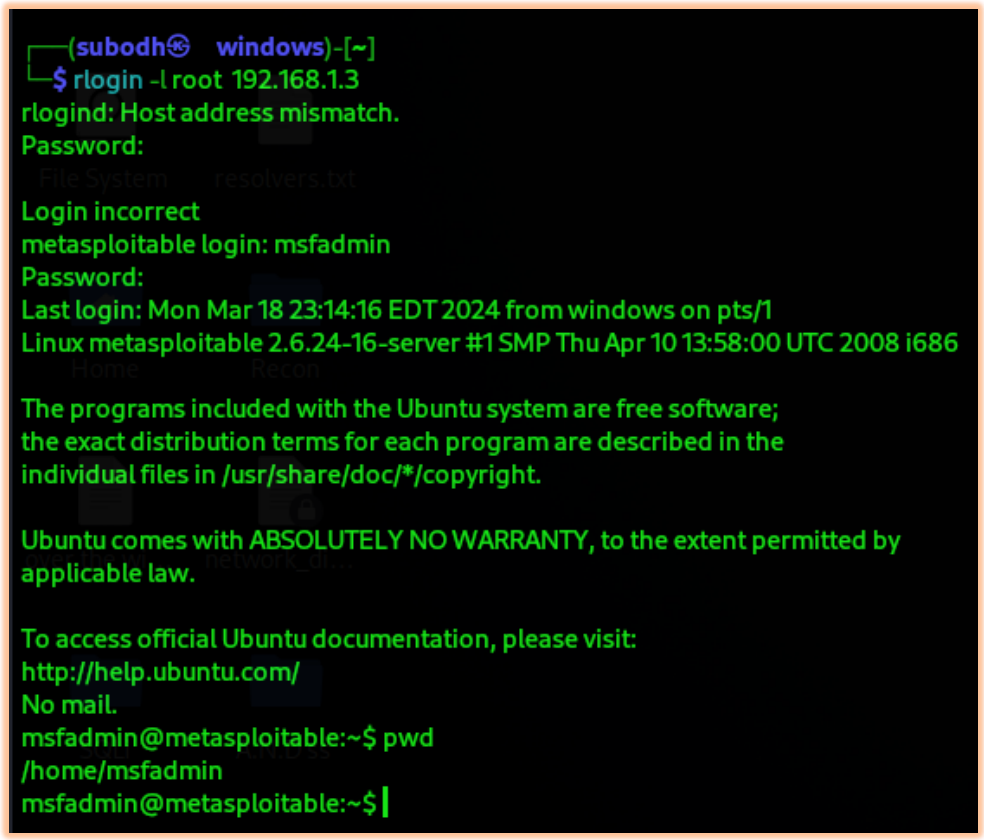


Figure 28. Gaining Shell access

Recommendation: To mitigate the risks associated with R services, it is recommended to disable or block these services, as they are inherently insecure. Instead, use more secure alternatives such as SSH (Secure Shell) for remote access.