

UNMASKING UNAUTHORIZED ACCESS TRICKS

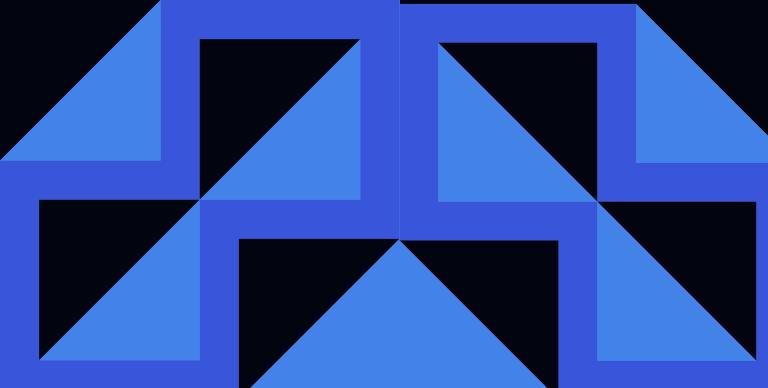


Batch 8 Members :

1. V. Srimanth Teja 2451-20-733-164
2. K. Akhilesh 2451-20-733-176
3. D. Sri Sai Sathwik 2452-20-733-018

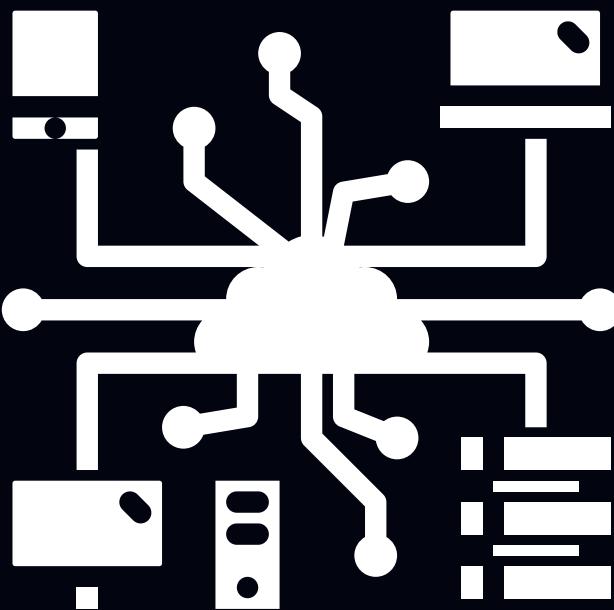
Guide : Dr. Y. Madhulika
Associate Professor, CSED





Problem Definition

It involves the evolving risks of unauthorized access within computer networks.



Tool designed for threat of unauthorized access to android devices.



Tool designed for web security assessment, penetration testing, and vulnerability detection.



The overarching objective is to contribute to the development of effective protective security measures, raising awareness .



SCOPE OF THE PROJECT

A thorough examination of unauthorized access techniques within computer networks. It will not only deep dive into the technical aspects but also consider user awareness and education as crucial components.



Accessing
1. Webcam
2. Microphone
3. Location
of android devices

Vulnerability detection

SQL injection testing

Protective Measures

User Awareness and Education

ABSTRACT



Diving deep into the realm of computer networks, it illuminates weaknesses and potential dangers across diverse computing platforms. First, it investigates the art of threat to unauthorized access to android devices by accessing the webcam, microphone and location through a designed tool.

Subsequently, the project delves into the technologies detection, wordpress scan, google dorking, subdomain enumeration, endpoints enumeration, SQL injection (SQLi) testing, security headers analysis, DNS enumeration, open ports scan, service scan (FTP, SMB, Telnet) of the websites through the designed tool.

Literature Survey

Ref no	PAPER TITLE	AUTHOR	PUBLISHED BY	PUBLISHED ON	DESCRIPTION
1]	A Study on Exploring the Level of Awareness of Privacy Concerns and Risks.	Tommy Nguyen, Garnet Yeates, Tony Ly and Umar Albalawi	MDPI	14 DEC 2023	With the recent increase in phishing attacks and other kinds of malicious activities, increasing the awareness of security and privacy awareness is arguably one of the best proven ways of preventing these kinds of threats. It is hypothesized that people are genuinely unaware of what rights they are giving up, especially since they are signing the terms of service without reading the fine print.
2]	An Overview of Social Engineering: The Role of Cognitive Biases Towards Social Engineering Based Cyber Attacks, Impacts and Countermeasures.	Udochukwu Godswill David and Ayomide Bode-Asa	RESEARCH GATE	12 DEC 2023	It focuses on the contributions of cognitive biases towards successful social engineering attacks. It further clarified the various tactics used by attackers and the stages the attack strategies conform with to achieve the attacker's goals.

Literature Survey

Ref no	PAPER TITLE	AUTHOR	PUBLISHED BY	PUBLISHED ON	DESCRIPTION
3]	Mitigation strategies against the phishing attacks: A systematic literature review.	Bilal Naqvi, Ksenia Perova, Ali Farooq, Imran Makhdoom, Shola Oyedeleji and Jari Porras	SCIENCE DIRECT	09 JULY 2023	Phishing attacks are among the most prevalent attack mechanisms employed by attackers. The consequences of successful phishing include financial losses, impact on reputation and identity theft. The existing mitigation strategies against phishing attacks, and the underlying technologies considered in the development of these strategies.
4]	Social Engineering Attacks Prevention: A systematic literature review	Wenni Syafitri, Zarina Shukur, Umi Asma Mokhtar, Rossilawati Sulaiman, and Muhammad Azwan Ibrahim	IEEE ACCESS	28 MAR 2022	Social engineering is an attack on information security for accessing systems or networks. The attacks occur when victims do not recognize methods, models, and frameworks to prevent them. The current research explains user studies, constructs, evaluation, concepts, frameworks, models, and methods to prevent social engineering attacks. Current prevention methods, models, and frameworks of social engineering attacks include health campaigns, human as security sensor frameworks, user-centric frameworks, and user vulnerability models.

Literature Survey

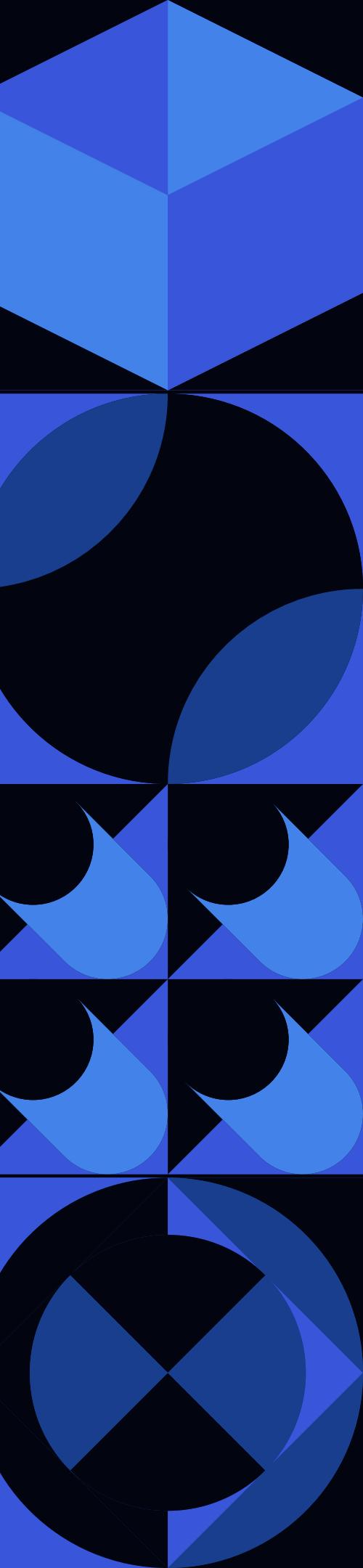
Ref no	PAPER TITLE	AUTHOR	PUBLISHED BY	PUBLISHED ON	DESCRIPTION
5]	Virtuous Human Hacking : The Ethics of Social Engineering in Cybersecurity.	M.Joseph Hatfield, Ph.D	ELSEVIER	23 FEB 2019	<p>It offers a virtue ethics analysis of social engineering in penetration testing. It articulates the core tenets of virtue ethics and applies them to an analysis of white hat social engineering. A virtue ethics analysis requires that individuals and the firms that initiate the penetration test be placed within a larger communal context which obligates individuals who are potential human hacking victims to participate in the constitution and flourishing of larger communities. Finally, penetration- testing firms must be able to demonstrate that a robust ethical training program governs its use of social engineering.</p>

SAS_FRAMEWORK :

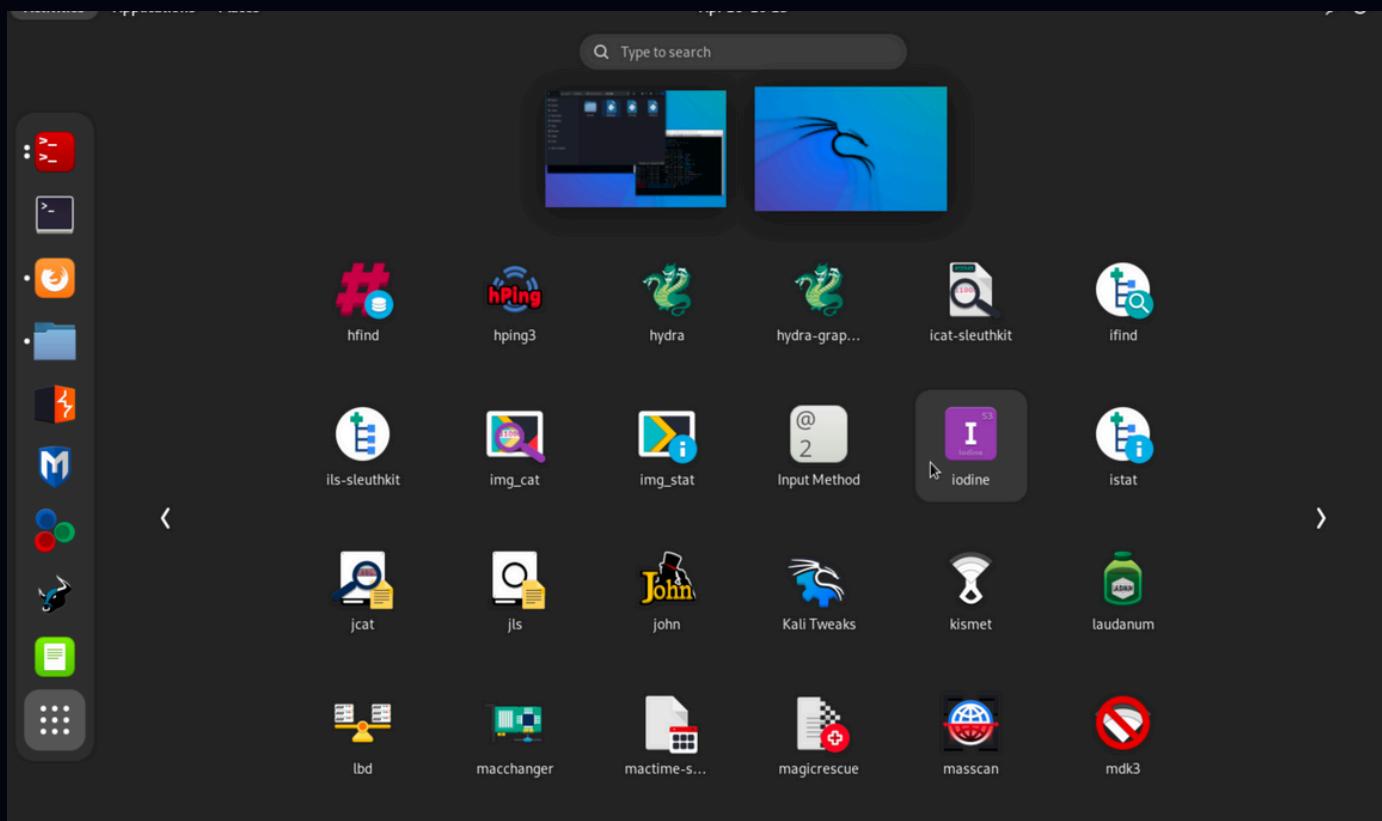
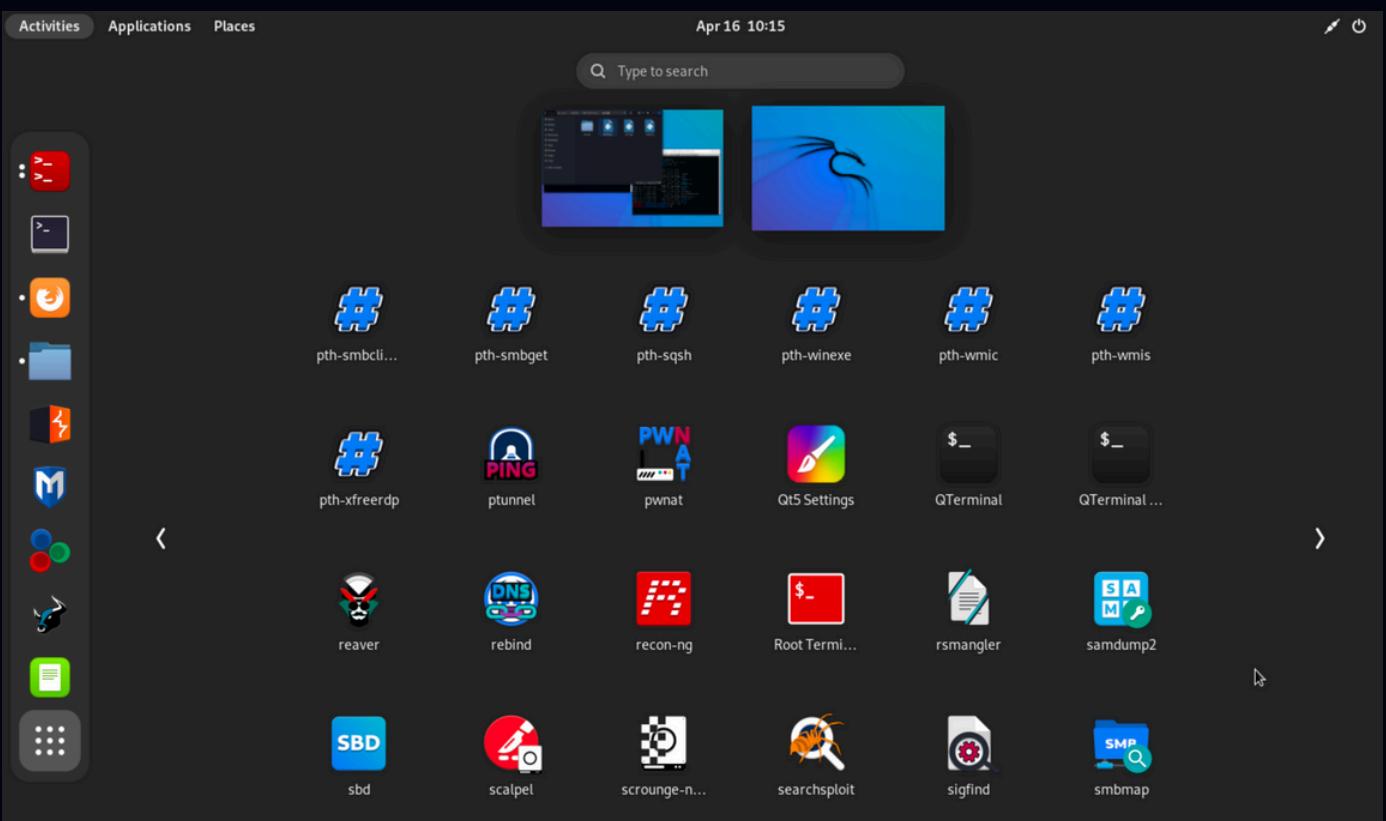
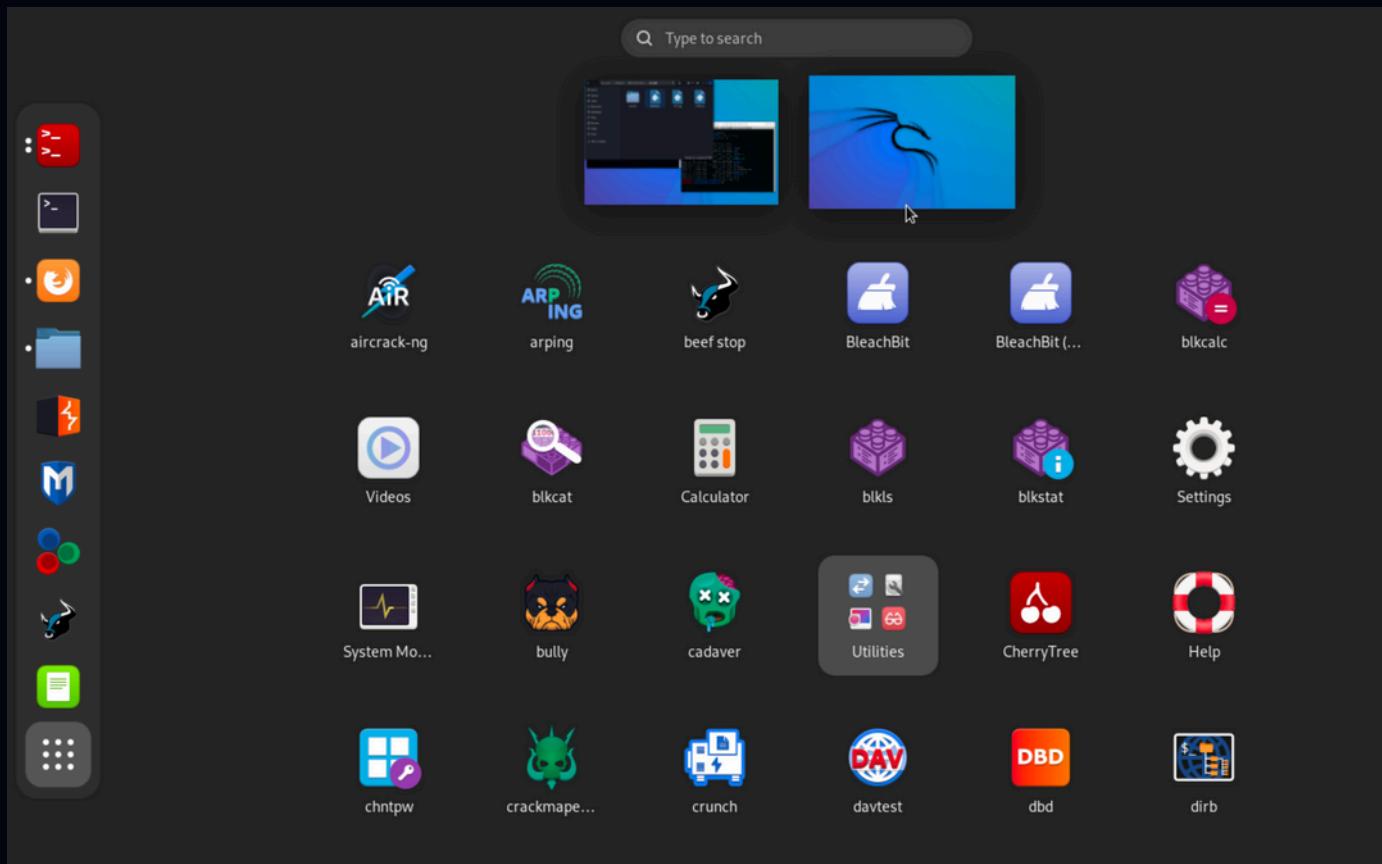
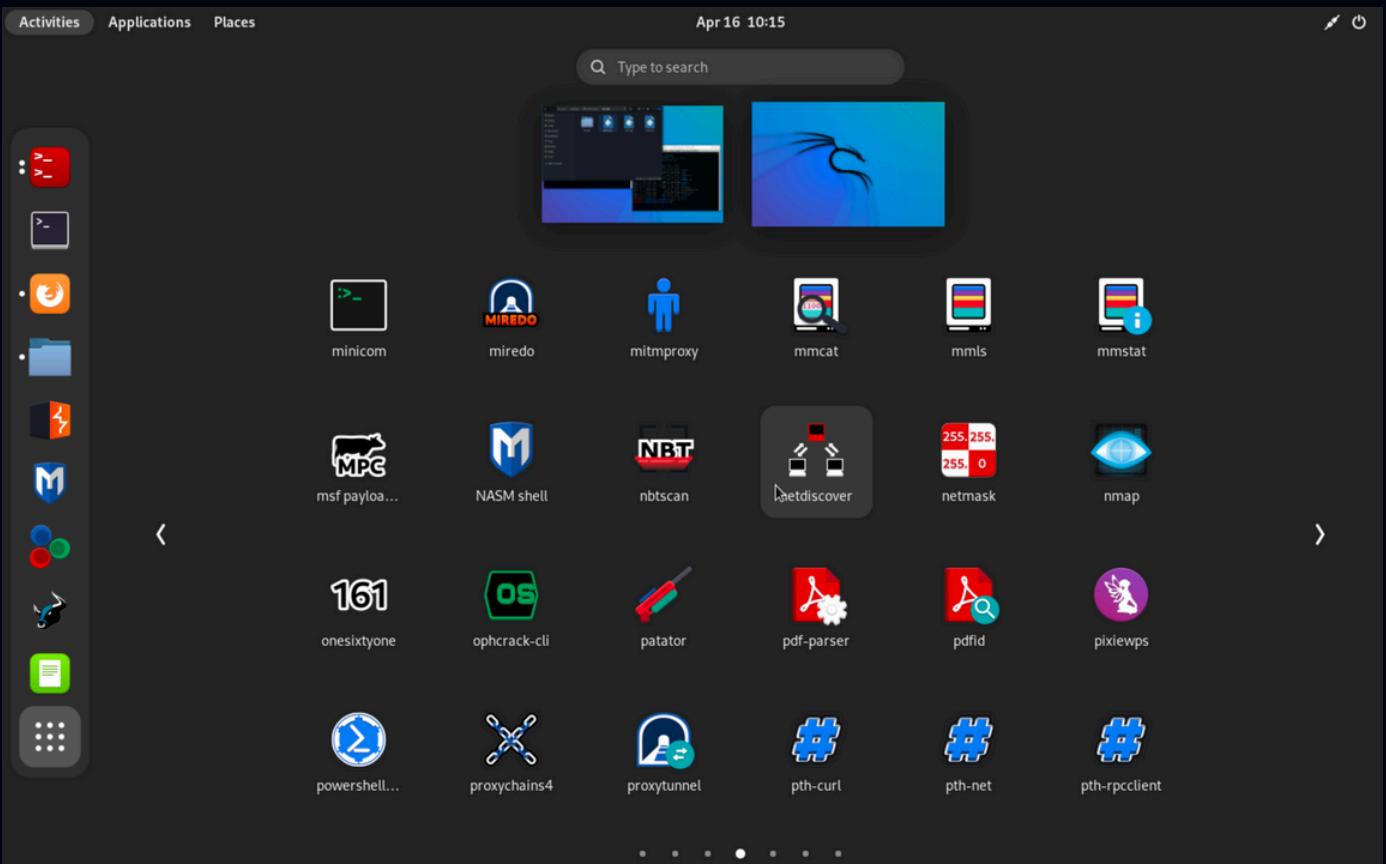
A tool designed for accessing webcam, microphone and location of the android devices.

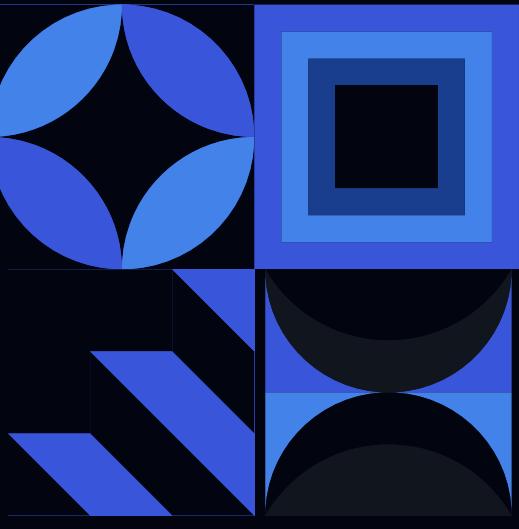
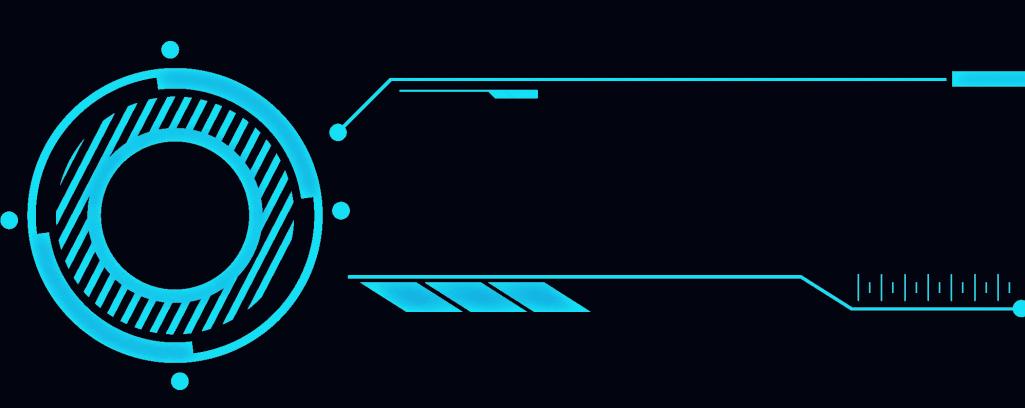
SAS_HELPER :

Tool designed for web security assessment, penetration testing, and vulnerability detection.



Why Kali-Linux ?





TEST RESULTS



Accessing webcam of an android device.

The screenshot shows a mobile application interface with a sidebar containing various icons. The main area displays a list of URLs with copy buttons and a detailed device configuration section.

URLs:

- [Copy](http://5ac2-49-205-122-225.ngrok-free.app/templates/camera_temp/index.html)
- [Copy](http://5ac2-49-205-122-225.ngrok-free.app/templates/microphone/index.html)
- [Copy](http://5ac2-49-205-122-225.ngrok-free.app/templates/nearyou/index.html)
- [Copy](http://5ac2-49-205-122-225.ngrok-free.app/templates/normal_data/index.html)
- [Copy](http://5ac2-49-205-122-225.ngrok-free.app/templates/weather/index.html)

Device Information:

```
ip : 49.205.122.225
os name : Android
Version : 10
Browser Name : Chrome
Get Browser Version : 123.0.0.0
Cpu Name : undefined
Resolution : 412x892
Time Zone : India Standard Time
Language : en-GB
Number Of CPU Core : 8
```

Buttons at the bottom:

- Listener Running / press to stop
- Download Logs
- Clear Logs

Accessing microphone of an android device.

The screenshot shows a web-based interface for a penetration testing or security analysis tool. On the left, there is a vertical sidebar with various icons, likely representing different modules or functions. The main content area displays a list of five URLs, each with a 'Copy' button to its right:

- http://9851-49-205-122-225.ngrok-free.app/templates/camera_temp/index.html Copy
- <http://9851-49-205-122-225.ngrok-free.app/templates/microphone/index.html> Copy
- <http://9851-49-205-122-225.ngrok-free.app/templates/nearyou/index.html> Copy
- http://9851-49-205-122-225.ngrok-free.app/templates/normal_data/index.html Copy
- <http://9851-49-205-122-225.ngrok-free.app/templates/weather/index.html> Copy

Below this list, there is a large text box containing device information:

```
ip : 49.205.122.225
os name : Android
Version : 10
Browser Name : Chrome
Get Browser Version : 123.0.0.0
Cpu Name : undefined
Resolution : 412x892
Time Zone : India Standard Time
Language : en-GB
Number Of CPU Core : 8
```

At the bottom of the interface, there are three buttons:

- Listener Running / press to stop (red background)
- Download Logs (green background)
- Clear Logs (yellow background)

Accessing location of an android device.

A screenshot of a Firefox browser window. The address bar shows the URL <https://0eea-49-205-121-100.ngrok-free.app/>. A modal dialog titled "Google Map Link" is open, displaying the URL <https://google.com/maps/place/17.4224879+78.5188363>. Below the modal, a list of URLs is visible:

- http://0eea-49-205-121-100.ngrok-free.app/templates/camera_temp/index.html
- <http://0eea-49-205-121-100.ngrok-free.app/templates/microphone/index.html>
- <http://0eea-49-205-121-100.ngrok-free.app/templates/nearyou/index.html>
- http://0eea-49-205-121-100.ngrok-free.app/templates/normal_data/index.html
- <http://0eea-49-205-121-100.ngrok-free.app/templates/weather/index.html>

Below the URLs, a panel displays device information:

- ip : 157.47.63.120
- os name : Android
- Version : 10
- Browser Name : Chrome
- Get Browser Version : 125.0.0.0
- Cpu Name : undefined
- Resolution : 412x892
- Time Zone : India Standard Time
- Language : en-GB
- Number Of CPU Core : 8

Google Map Link : <https://google.com/maps/place/17.4224879+78.5188363>

A screenshot of a Firefox browser window showing a Google Maps search result. The address bar shows the URL [https://www.google.com/maps/place/17°25'21.0"N 78°31'07.8"E/@17.2521,78.3107,15z](https://www.google.com/maps/place/17°25'21.0). The map displays a street view image of a residential area with two motorcycles parked in front of a house. The coordinates $17^{\circ}25'21.0"N$ $78^{\circ}31'07.8"E$ are shown at the top of the search results. Below the image, there are five action buttons: Directions, Save, Nearby, Send to phone, and Share. The search results list the following locations:

- 12-10-590/10/3, Indira Nagar, Padmarao Nagar, Secunderabad, Telangana 500061
- CGC9+XGW Secunderabad, Telangana
- Add a missing place
- Add your business
- Add a label

The map interface includes zoom controls (+, -), a layers button, and a scale bar indicating 100 m. The address $17.4224879+78.5188363$ is visible at the bottom right of the map.

THANK YOU

Any Questions ?
Your queries are welcomed !

