Attack Simulation Dashboard

Mr. G. Ram Sundar1, Kavin Krishna. S S2, Babu Prasad. S T3
[1] Assistant Professor, Sri Ramakrishna Engineering College, Coimbatore, India
[2] UG Scholar, Sri Ramakrishna Engineering College, Coimbatore, India
[3] UG Scholar, Sri Ramakrishna Engineering College, Coimbatore, India

Abstract- With cyber threats becoming more frequent and sophisticated, it's more important than ever to understand how attacks work and how to respond effectively. This project introduces an Attack Simulation Dashboard—a user-friendly, modular platform designed to help security professionals, educators, and students simulate and study different types of cyberattacks in a safe, controlled setting. The dashboard brings together several offensive tools—like keyloggers, screenshot takers, webcam access scripts, and data exfiltration utilities—into a single, easy-to-use interface that replicates real-world attack scenarios. Built using React.js, it's crafted especially for training and awareness, giving users live feedback, clear attack paths, and insights into system impact. Through a detailed literature review, we identified the limitations of existing solutions and addressed them by building a flexible, lightweight, and interactive tool. The platform not only supports practical, hands-on learning but also helps users better understand how to detect and respond to threats. Testing shows that the dashboard effectively simulates common attacks and encourages deeper learning of cybersecurity defense techniques—without risking any real-world damage

Keywords — Cybersecurity, Attack Simulation, Security Dashboard, Offensive Security Tools, React.js, Threat Visualization, Cyberattack Analysis, Hands-on Training, Blue Team Awareness, Cyber Threat Simulation, Keylogger, Screenshot Capture, Webcam Monitoring, System Information Exfiltration, Real-time Feedback.

1. INTRODUCTION

In today's digital world, cyberattacks have become part of our everyday reality. From phishing emails to spyware and data breaches, threats are constantly evolving—and unfortunately, so are the risks. Reports show that thousands of cyber incidents happen every single day, and yet, many students, researchers, and even professionals don't have a safe, practical way to understand how these attacks actually work. Most learning environments still rely heavily on theory, with limited hands-on exposure. But just like you can't learn to drive by only reading the manual, you can't become truly prepared for real-world cyber threats without experiencing them—even if in a simulated space. That's where the gap lies. To help close this gap, we built the Attack Simulation Dashboard—an interactive tool that brings common cyberattacks to life in a controlled, visual, and easy-to-use platform. It lets users simulate different attack methods, see how they operate in real time, and understand the impact they can have. Whether you're a student getting started or a blue team defender brushing up your skills, this dashboard offers a safe environment to learn, experiment, and grow more confident in tackling cyber threats.

2. LITERATURE REVIEW

John W. Haines, Lincoln M. Rossey, Richard P. Lippmann, Robert K. Cunningham [1] The authors introduce a cyberattack simulation platform for evaluating intrusion detection systems (IDS) by generating realistic network traffic. The framework includes a series of scripted attacks replayed in controlled environments, enabling researchers to assess detection accuracy under varied scenarios. Their work laid the foundation for reproducible testing by simulating complex attack patterns within consistent baselines. The simulated traffic proved effective in benchmarking IDS performance, contributing to the development of more robust defensive systems. This structured testing method supports reproducibility and scalability in cybersecurity experimentation.

Sung Hong, Kyungmin Kim, Taekyoung Kim [2] This study presents a simulated threat generator based on the MITRE ATT&CK framework for cyber warfare training. The generator mimics real-world attacker behaviors across multiple tactics, enabling defenders to test their detection and response capabilities. The tool supports various attack scenarios like privilege escalation and data exfiltration, each mapped to ATT&CK techniques. The authors demonstrated that using simulated threats enhanced both red team training and blue team preparedness, achieving significant improvement in response accuracy. The framework's adaptability and ATT&CK alignment make it a valuable resource for building attack simulation dashboards.

F. Skopik, G. Settanni, R. Fiedler, I. Friedberg [3] The authors explore cyber threat intelligence (CTI) platforms and their role in proactive defense mechanisms. They evaluate several CTI exchange models that allow the integration of threat data into existing dashboards and SIEM systems. The paper highlights the need for automated processing of threat intelligence for faster incident response. It emphasizes the value of simulation in testing CTI-driven detections, pointing to a gap that attack simulation dashboards can fill. The study concludes that coupling CTI with simulation tools enhances situational awareness and cyber resilience.

3. MODEL SPECIFICATION

1. System Architecture

The dashboard follows a three-tier architecture comprising:

Frontend (Presentation Layer):

- Built using HTML & CSS for a responsive and dynamic user interface.
- Integrates animations and tool cards for better visualization of attack scenarios.

Backend (Logic Layer):

- Developed in Python (Flask) to handle API requests, run attack scripts, and manage communication between frontend and backend.
- Each offensive tool (e.g., keylogger, screenshot capture, webcam access, system info exfiltration) is triggered via specific endpoints.
- Uses Ngrok to create secure tunnels for testing and receiving payload data from remote systems.

Database (Storage Layer):

- Uses SQLite or MongoDB for storing attack logs, user actions, payload results, and metadata related to simulations.
- Maintains timestamps, user IDs, tool- specific logs, and session states for traceability.

2.Tools Integrated in the Dashboard

The platform includes the following modules:

- Keylogger Tool: Captures keystrokes and displays them in a log file.
- Screenshot Capture Tool: Takes screenshots of the victim system and sends them to the dashboard.
- Webcam Spy Tool: Accesses the webcam and streams or captures images remotely.
- System Information Exfiltrator: Collects data like OS version, IP address, CPU info, and more.
- Payload Dispatcher: Sends crafted payloads to the target system to initiate attacks.
- Live Trace Viewer: Displays logs of current activities and results from each attack tool in real-time.

3. Key Features

- Real-time Visualization: Users can see the effects of attacks as they unfold through visual cues and dashboards.
- Safe Testing Environment: All attacks are simulated in a sandboxed environment or on a test system, ensuring no real harm.
- Educational Focus: Descriptive pop-ups and module-based walkthroughs help beginners understand each attack vector and its impact.
- Customizability: Users can enable/disable tools, adjust payload settings, and set runtime parameters.
- Cross-Platform Support: The dashboard runs in any modern browser and supports Linux/Windows for backend testing.

4. DEPLOYMENT

- Development Stack: React.js (Frontend), Python Flask (Backend), SQLite/MongoDB (Database)
- Runtime Environment: Localhost or cloud deployment with Ngrok tunneling for payload testing
- Testing Devices: Secondary test machine or virtual environment (e.g., VirtualBox, VMware)

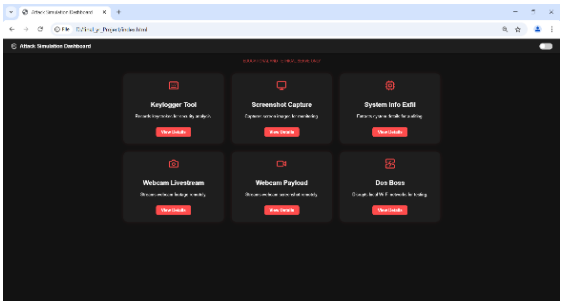


Fig 1.Home page

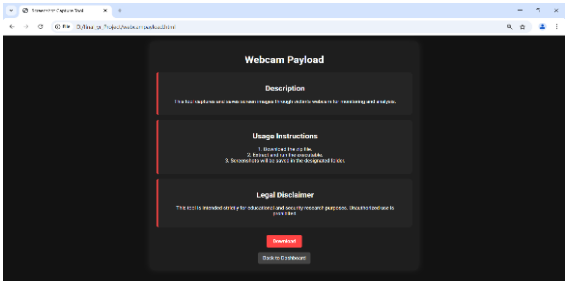


Fig 2. Navigated to Keylogger Tool Screen.

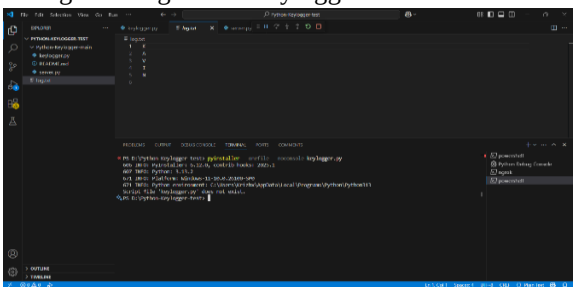


Fig 3. Output of Keylogger Tool.

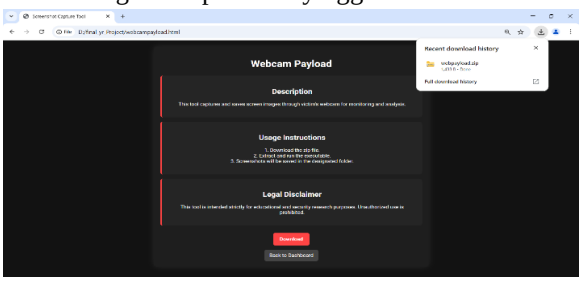


Fig 4. Output of Tool being Downloaded.

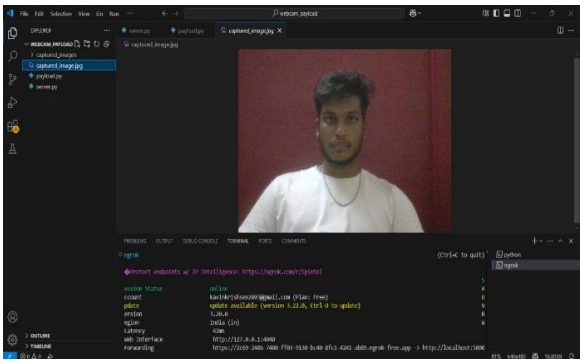
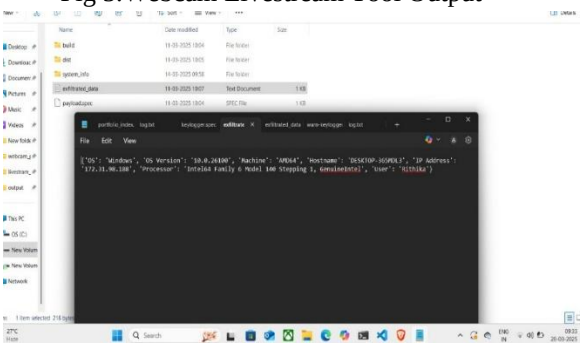


Fig 5.Webcam Livestream Tool Output



6. System Information Tool Output

5.METHEDOLOGY

1. Requirement Gathering & Planning
- Identified the core need for a hands-on cybersecurity training tool that simulates real-world attacks.
- Defined the target users: students, cybersecurity enthusiasts, and blue team professionals.

2. Tool Selection and Tech Stack Setup
- Frontend: Chose React.js for building a dynamic and responsive user interface.
- Backend: Used Python Flask to handle backend logic and manage communication between the user interface and offensive tools.

3. Tool Integration and Module Development
- Connected each tool to the dashboard through secure Flask endpoints, allowing real-time execution and feedback. The tools Integrated are:
- Keylogger to simulate keyboard ta theft.
- Screenshot Capture for visual spying.
- Webcam Livestream to simulate real-time surveillance.
- System Info Exfiltration to demonstrate data leakage.

4. User Interface Design

- Designed a clean and minimalistic UI using HTML, CSS, and React.
- Incorporated animations and icons to make the interface more engaging.
- Included real-time status updates and visual indicators to show the progress and effects of each attack.

5. Security & Ethical Safeguards

- Built all modules to function only in controlled environments
- Avoided storing or logging sensitive data, ensuring the platform is used strictly for learning and demonstration.

6. Testing and Validation

- Conducted functional testing for each tool individually and as part of the integrated system.
- Performed cross-device testing using Ngrok
- Validated tool performance by observing execution accuracy and system impact in various environments.

REFERENCE

[1] L. M. Rossey, R. K. Cunningham, D. J. Fried, J. C. Rabek, and R. P. Lippmann, "LARIAT: Lincoln Adaptable Real-time Information Assurance Testbed," in *Proc. IEEE Aerospace Conf.*, 2022.

[2] T. H. Yu, B. W. Fuller, J. H. Bannick, L. M. Rossey, and R. K. Cunningham, "Visualization for Computer Security: LARIAT," in *Proc. Workshop on Visualization for Computer Security (VizSEC)*, 2020.

[3] J. W. Haines, L. M. Rossey, R. P. Lippmann, and R. K. Cunningham, "Extending the DARPA Off-Line Intrusion Detection Evaluation," in *Proc. DARPA Information Survivability Conference and Exposition II (DISCEX'01)*, 2021.

[4] S. Hong, K. Kim, and T. Kim, "Design and Implementation of an ATT&CK-Based Simulated Threat Generator for Cyber Warfare Training," *Journal of the Korea Institute of Military Science and Technology*, vol. 22, no. 6, pp. 789–797, 2023.

[5] F. Skopik, G. Settanni, R. Fiedler, and I. Friedberg, "A Survey on Threat Intelligence Exchange Platforms," in *Proc. 12th Annual Int. Conf. on Privacy, Security and Trust (PST)*, 2022.