AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.6, NO. 2 (2026)

CONTROLLED EMAIL SPOOFING AND PHISHING SIMULATION USING SMTP RELAY

[1]Dr B.Ravi kumar, [2] S Abdulla Ahmed,[3] K Sunitha, [4] K Sanjana,[5] V Sudhip
[1]AssistantProfessor, [2345]Students
Department of Cyber Security
Siddhartha Institute of Technology & Sciences, Narapally
dr.brkou@siddhartha.org.in, 24TQ1A6221@siddhartha.co.in, 24TQ1A6207@siddhartha.co.in, 24TQ1A6210@siddhartha.co.in, 24TQ1A6232@siddhartha.co.in

Abstract

The modern digital ecosystem relies heavily on email communication; however, its underlying protocols still contain vulnerabilities that are actively exploited by cyber attackers. Email phishing and sender spoofing remain among the most common and dangerous attack vectors, enabling threats such as malware delivery, credential theft, and unauthorized data access. As traditional security systems improve, attackers increasingly leverage trusted third-party platforms to bypass detection and make malicious emails appear legitimate, shifting the burden of security awareness to end-users.

This project, titled "Controlled Email Spoofing and Phishing Simulation Using SMTP Relay," presents a practical and ethical demonstration of how attackers exploit legitimate infrastructure to deceive users and extract sensitive information. In this simulation, the Brevo platform was used as an SMTP relay to spoof sender identities, taking advantage of its trusted reputation. The experiment was conducted in the Kali Linux environment, where the OSINT tool Hound was utilized to create a phishing payload. The payload was securely hosted using a Cloudflare tunnel to make it accessible over the internet.

A targeted spoofed email, designed with social engineering techniques, was sent using a command-line utility. When the recipient interacted with the malicious link, the system captured sensitive information such as device details, operating system data, IP address, and precise geographical location (GPS coordinates). This experiment highlights how easily attackers can exploit user trust and technological gaps.

I. Introduction

In the modern digital and corporate environment, electronic mail remains a fundamental medium for communication, supporting activities such as identity verification, financial transactions, official correspondence, and enterprise operations. Despite the emergence of secure messaging platforms, email continues to be widely trusted. However, the underlying protocol that governs email transmission, Simple Mail Transfer Protocol, was designed in an era where trust among network systems was assumed, rather than enforced through strong security mechanisms. As a result, SMTP lacks built-in authentication features to verify the actual sender of an email, making it vulnerable to manipulation.

This inherent weakness allows attackers to modify email headers and impersonate legitimate senders, a technique known as email spoofing. By exploiting SMTP, malicious actors can forge sender identities and trick recipients into believing that

Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 11-06-2026

messages originate from trusted sources such as banks, organizations, or company executives. This has contributed to the rise of phishing attacks and Business Email Compromise (BEC), which cause significant financial and data losses globally.

The problem has evolved further with attackers leveraging trusted third-party platforms to bypass traditional security measures. Instead of using suspicious or blacklisted servers, attackers now utilize legitimate SMTP relay services such as Brevo, which maintain high-reputation IP addresses. Emails sent through such platforms appear authentic and are more likely to bypass spam filters, reaching the recipient's primary inbox. This makes detection significantly more difficult and increases the success rate of phishing campaigns.

II. Literature Survey

2.1 Introduction

The landscape of digital communication is built upon protocols that were originally designed with a focus on reliability and connectivity rather than security and authentication. Over time, this design limitation has created opportunities for cyber threats such as email spoofing and phishing. As organizations increasingly adopt cloud-based services, traditional network boundaries have diminished, placing greater responsibility on end-users for security. Therefore, modern research emphasizes not only the technical vulnerabilities in email systems but also the role of social engineering in exploiting human behavior. Understanding both aspects is essential to analyze current cybersecurity threats effectively.

2.2 The Architectural Flaws of SMTP

The foundation of email communication lies in the Simple Mail Transfer Protocol, which was initially defined in RFC 821 and later updated in RFC 5321. SMTP was designed to transfer messages efficiently between servers but does not include built-in mechanisms to verify the authenticity of the sender. This limitation allows attackers to manipulate email headers and forge sender identities by specifying arbitrary addresses in the "MAIL FROM" command or "From" field. Early cybersecurity research identifies this as a fundamental weakness of email infrastructure, enabling widespread spam, phishing, and impersonation attacks. This inherent flaw continues to be exploited in modern cyberattacks.

2.3 Evolution of Sender Authentication Frameworks

To address the limitations of SMTP, several authentication mechanisms have been developed. The Sender Policy Framework allows domain owners to specify authorized sending servers through DNS records. This was followed by DomainKeys Identified Mail, which uses cryptographic signatures to ensure message integrity. Later, Domain-based Message Authentication Reporting and Conformance combined SPF and DKIM to enforce strict policies for handling unauthenticated emails.

However, literature highlights that the adoption of DMARC is often incomplete or misconfigured, leaving many domains vulnerable. Additionally, modern attackers have adapted by exploiting legitimate SMTP relay platforms such as Brevo, SendGrid,

Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 11-06-2026

and Mailchimp. By using these trusted services, attackers can bypass traditional spam filters and deliver spoofed emails with high credibility.

2.4 Open Source Intelligence (OSINT) and Active Reconnaissance

Recent research also focuses on advancements in reconnaissance techniques used in phishing attacks. Traditionally, gathering sensitive user data required complex malware or direct network access. However, modern approaches leverage standard web technologies to collect information. For instance, the HTML5 Geolocation API can be exploited through social engineering techniques to obtain a user's location data.

Tools like Hound demonstrate how attackers can use lightweight scripts to gather detailed information such as IP address, device specifications, browser details, and GPS coordinates. By hosting malicious payloads through secure tunnels and delivering them via spoofed emails, attackers can extract sensitive data without triggering traditional security systems. This shift highlights the growing importance of understanding browser-based data exposure and user interaction in cybersecurity.

III. System Analysis

System analysis focuses on understanding how email communication systems can be exploited due to weaknesses in underlying protocols and human factors. In this project, the analysis examines how attackers manipulate the Simple Mail Transfer Protocol to spoof sender identities and deliver phishing emails. It studies how legitimate SMTP relay platforms such as Brevo can be misused to bypass spam filters due to their high reputation. The system also analyzes how phishing links are used to collect sensitive user data through browser-based technologies. By evaluating both technical vulnerabilities and social engineering techniques, the system provides a comprehensive understanding of modern email-based cyber threats.

Existing System

The existing email communication system is primarily based on SMTP, which lacks strong built-in authentication mechanisms. While additional security frameworks such as SPF, DKIM, and DMARC have been introduced, their implementation is often incomplete or misconfigured. Traditional security measures rely on spam filters, IP blacklisting, and heuristic analysis to detect malicious emails.

However, these systems are not fully effective against modern attacks. Attackers can use trusted SMTP relay services to send spoofed emails that bypass spam filters. Additionally, current systems depend heavily on user awareness to identify phishing emails, which increases the risk of human error. As a result, email systems remain vulnerable to spoofing and phishing attacks.

Disadvantages of Existing System

- Lack of inherent authentication in SMTP
- Misconfigured or weak SPF, DKIM, and DMARC policies
- Over-reliance on spam filters and blacklisting
- Easy spoofing of sender email addresses

Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 11-06-2026

- High dependency on user awareness
- Inability to detect advanced phishing attacks
- Abuse of trusted SMTP relay services
- Difficulty in analyzing complex email headers
- Increased risk of credential theft and data breaches

Proposed System

The proposed system demonstrates a controlled and ethical simulation of email spoofing and phishing using SMTP relay services. It utilizes Brevo as a trusted SMTP relay to send spoofed emails and analyze how such messages bypass traditional security mechanisms.

The system also incorporates the Kali Linux environment and tools like Hound to create and deploy phishing payloads. These payloads are hosted securely and used to demonstrate how attackers collect sensitive information such as IP address, device details, and location data.

The project emphasizes understanding both attack techniques and defense strategies, including secure email authentication, user awareness, and improved detection mechanisms.

Advantages of Proposed System

- Provides practical understanding of email spoofing and phishing
- Demonstrates real-world attack scenarios in a safe environment
- Helps identify weaknesses in existing email security systems
- Enhances awareness of social engineering techniques
- Shows how attackers bypass spam filters using trusted platforms
- Improves knowledge of SMTP and email authentication protocols
- Useful for cybersecurity learning and research
- Encourages implementation of strong security practices
- Helps in detecting and preventing phishing attacks
- Strengthens overall email security awareness

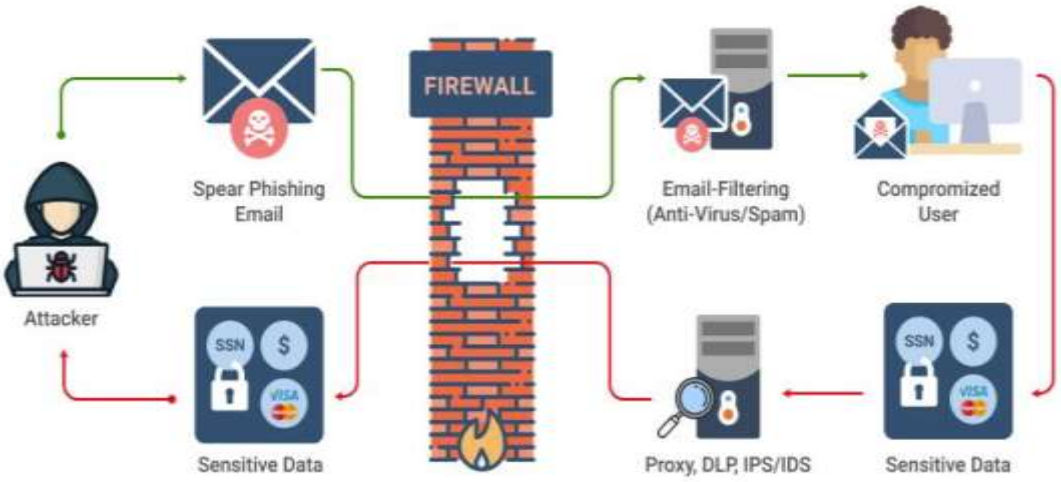
IV. Methodology

The methodology of this project involves conducting a controlled simulation of email spoofing and phishing attacks using SMTP relay services. Initially, the working of the Simple Mail Transfer Protocol is studied to understand how email transmission occurs and how sender information can be manipulated. A spoofed email is then created using a trusted SMTP relay platform such as Brevo to bypass spam filters. The phishing payload is generated using tools available in the Kali Linux environment, particularly Hound. The payload is hosted securely and shared through a malicious link embedded in the email. When the target interacts with the link, sensitive data such as IP address, device information, and location details are collected. The results are analyzed to understand the effectiveness of the attack and to identify preventive measures. The entire process is conducted ethically to ensure safe learning and analysis.

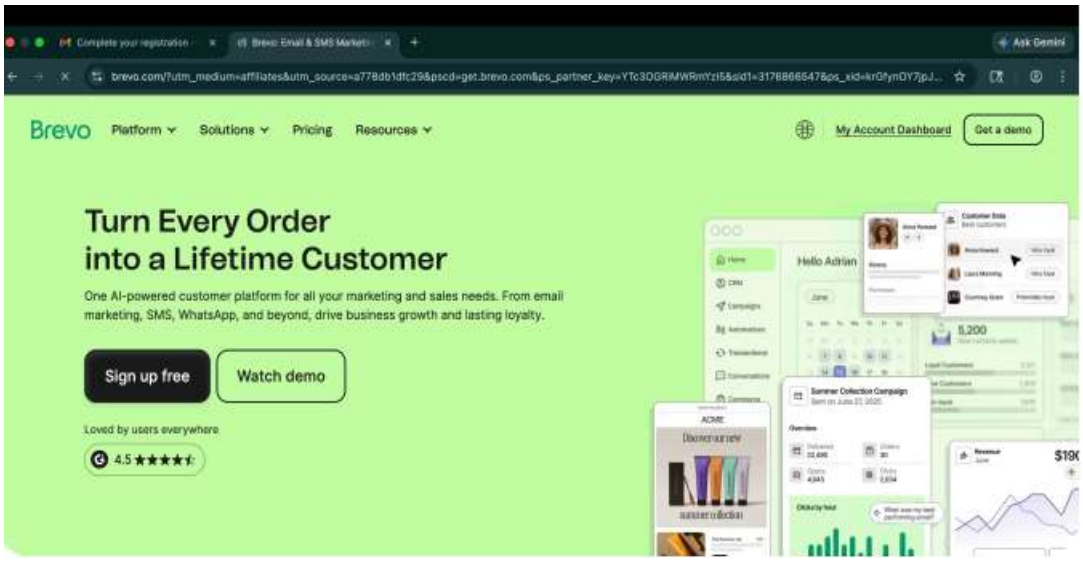
Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 11-06-2026

System Architecture

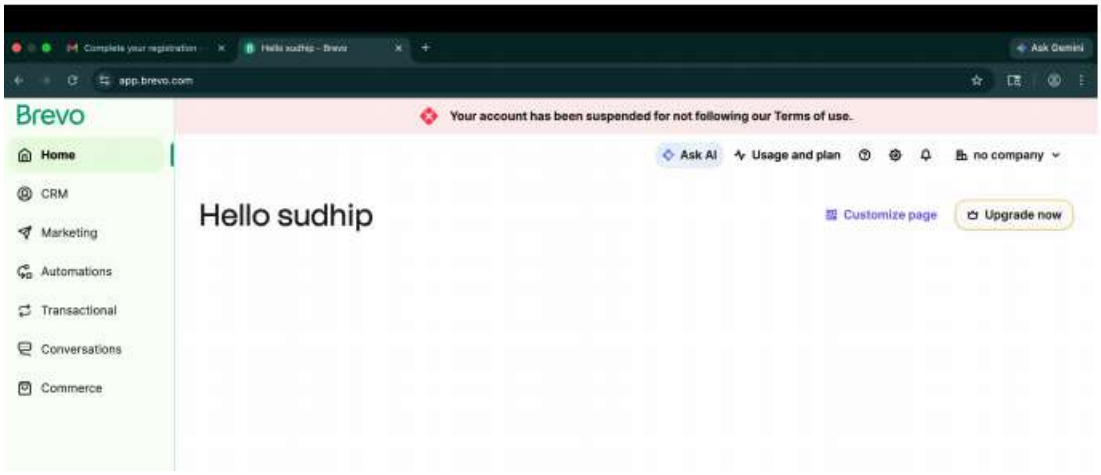
The system architecture of this project consists of multiple components working together to simulate email spoofing and phishing attacks. The user (attacker) initiates the process by creating a spoofed email using an SMTP relay service like Brevo. The email is transmitted through the SMTP protocol, allowing it to reach the target user's inbox while appearing legitimate. The email contains a phishing link generated using tools from the Kali Linux environment. This link is connected to a hosted payload created using Hound. When the target user clicks the link, the payload collects sensitive information such as IP address, device details, and location data. This information is then sent back to the attacker for analysis. The architecture demonstrates the flow of data from email creation to data exfiltration, highlighting how vulnerabilities in email systems and user behavior can be exploited.

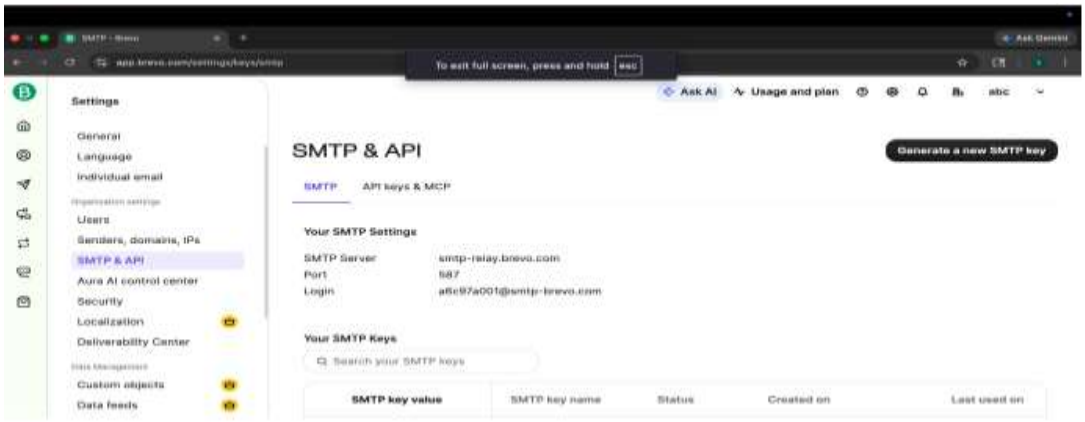


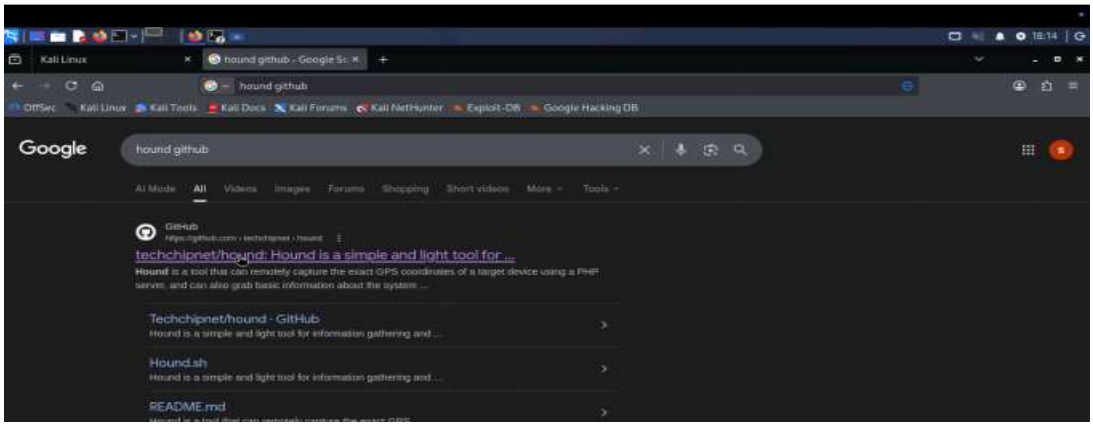
V. Result and Output

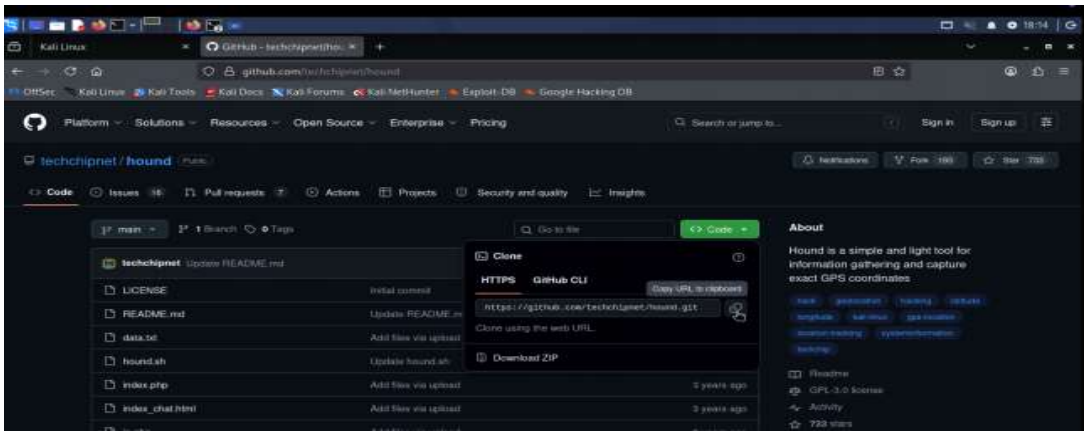


Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 11-06-2026


Brevo
Your account has been suspended for not following our Terms of use.
Home
CRM
Marketing
Automations
Transactional
Conversations
Commerce
Ask AI
Usage and plan
no company
Hello sudhip
Customize page
Upgrade now


Settings
General
Language
Individual email
Users
Senders, domains, IPs
SMTP & API
Aura AI control center
Security
Localization
Deliverability Center
Custom objects
Data feeds
SMTP & API
Generate a new SMTP key
SMTP
API keys & MCP
Your SMTP Settings
SMTP Server
smtp-relay.brevo.com
Port
587
Login
Your SMTP Keys
SMTP key value
SMTP key name
Status
Created on
Last used on

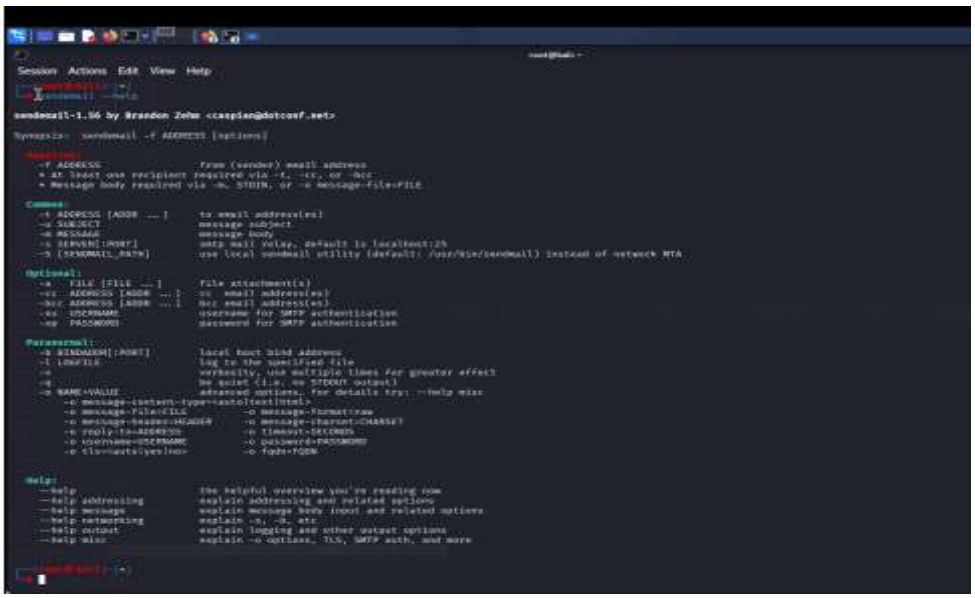

Google
hound github
techchipnet/hound: Hound is a simple and light tool for ...
Techchipnet/hound - GitHub
Hound.sh
README.md

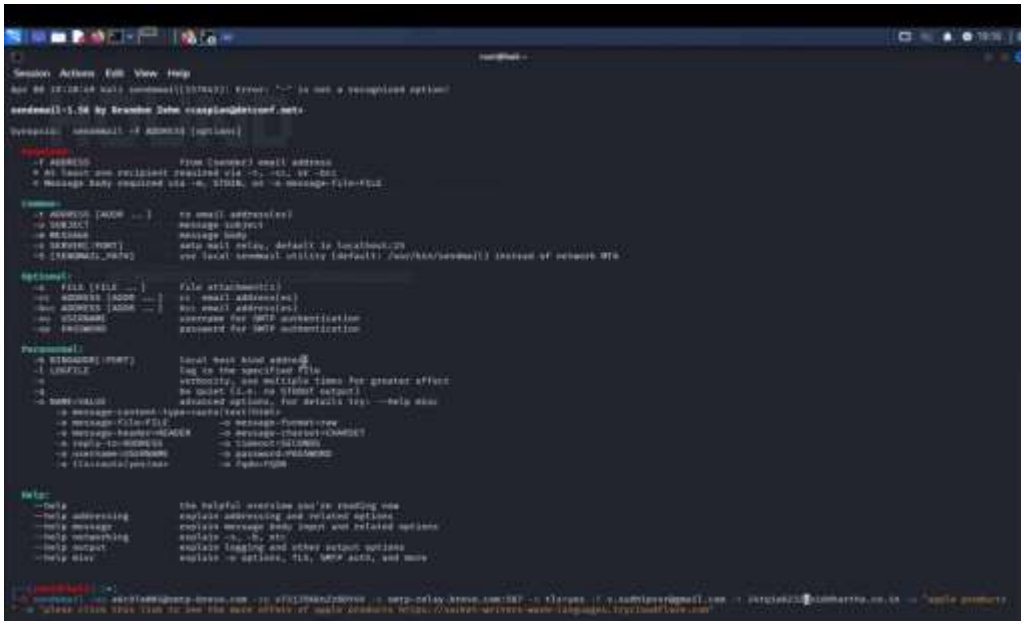

techchipnet / hound
Code
Issues
Pull requests
Actions
Projects
Security and quality
Insights
About
Hound is a simple and light tool for information gathering and capture exact GPS coordinates
Clone
HTTPS
GitHub CLI
Download ZIP

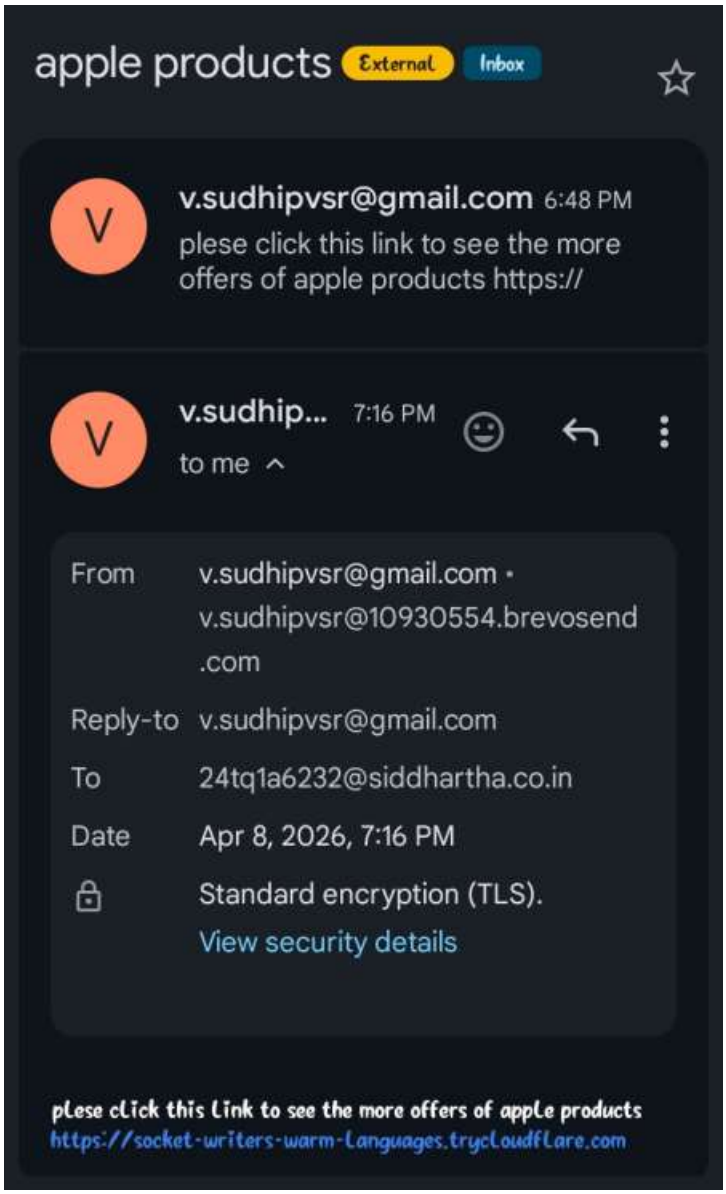

Session Actions Edit View Help
fatal: destination path 'hound' already exists and is not an empty directory.

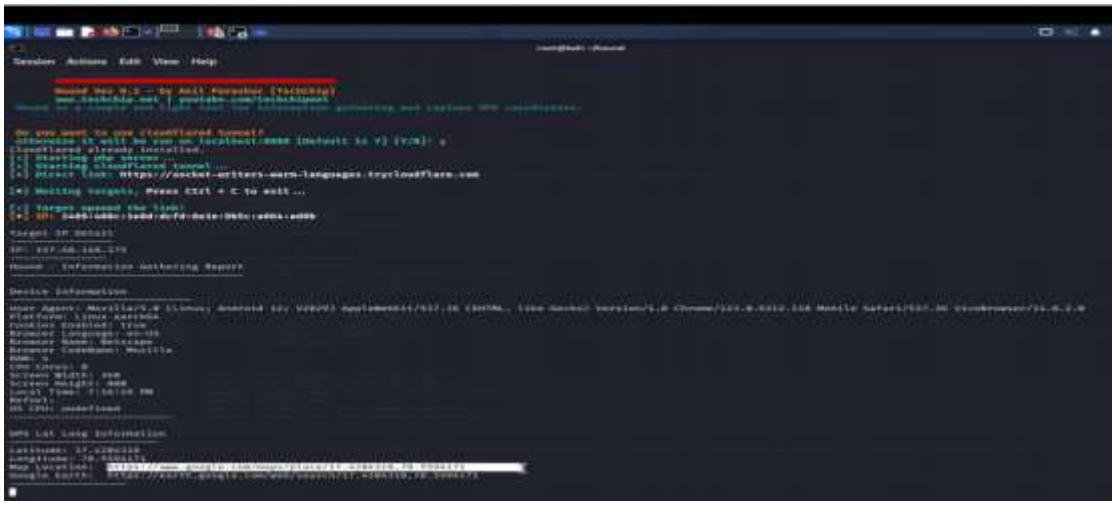

Session Actions Edit View Help
HOUND
Hound Ver 0.2 - by Anil Parashar [TechChip]
www.techchip.net | youtube.com/techchipnet
Hound is a simple and light tool for information gathering and capture GPS coordinates.
Do you want to use cloudflared tunnel?
otherwise it will be run on localhost:8080 [Default is Y] [Y/N]:

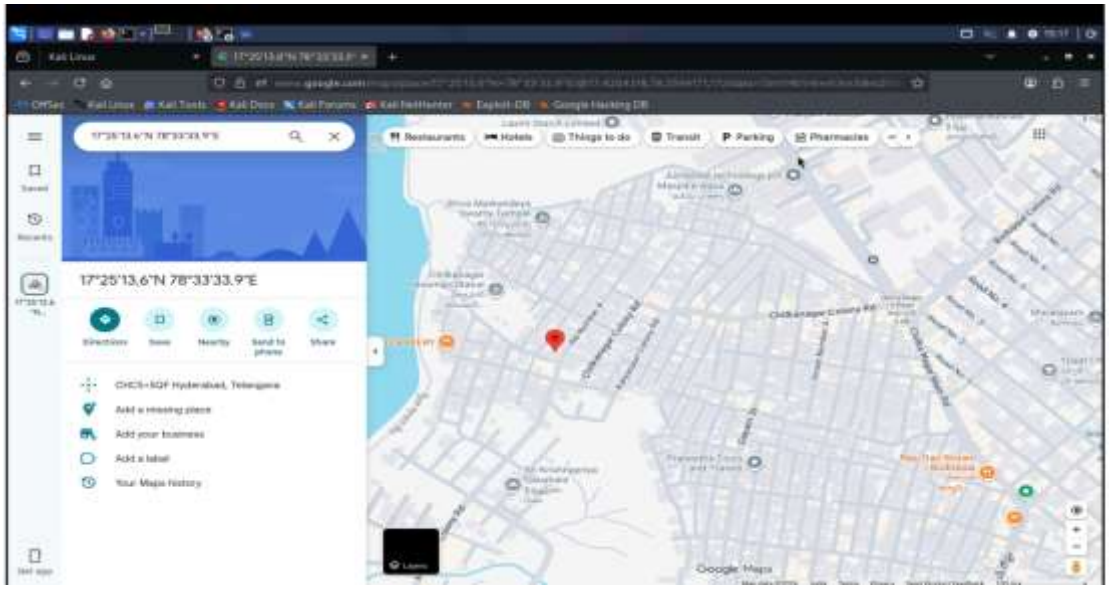

Session Actions Edit View Help
HOUND
Hound Ver 0.2 - by Anil Parashar [TechChip]
www.techchip.net | youtube.com/techchipnet
Hound is a simple and light tool for information gathering and capture GPS coordinates.
Do you want to use cloudflared tunnel?
otherwise it will be run on localhost:8080 [Default is Y] [Y/N]: y
Cloudflared already installed.
[+] Starting php server...
[+] Starting cloudflared tunnel ...
[+] Direct link:
[*] Waiting targets, Press Ctrl + C to exit...


Session Actions Edit View Help
sendmail-1.56 by Brandon Zehm <caspian@dotconf.net>




apple products
External
Inbox
v.sudhipvsr@gmail.com 6:48 PM
plese click this link to see the more offers of apple products https://
v.sudhip... 7:16 PM
to me
From v.sudhipvsr@gmail.com • v.sudhipvsr@10930554.brevosend.com
Reply-to v.sudhipvsr@gmail.com
To 24tq1a6232@siddhartha.co.in
Date Apr 8, 2026, 7:16 PM
Standard encryption (TLS).
View security details
plese click this link to see the more offers of apple products
https://socket-writers-warm-languages.trycloudflare.com





VI. Conclusion

The project "Controlled Email Spoofing and Phishing Simulation Using SMTP Relay" successfully demonstrates the critical vulnerabilities present in both email protocol architecture and human interaction with digital systems. By leveraging tools such as Kali Linux, Hound, and trusted SMTP relay platforms like Brevo, the simulation highlights how easily attackers can create convincing spoofing and phishing campaigns.

The experiment clearly shows that even a simple user action—such as clicking on a malicious link—can result in the exposure of highly sensitive information, including device details, IP address, and precise geographical location. This emphasizes the significant role of social engineering in modern cyberattacks and how attackers exploit both technical weaknesses and human trust.

Furthermore, the project reinforces the urgent need for strong security measures such as proper email authentication mechanisms, including Domain-based Message Authentication Reporting and Conformance, along with improved monitoring and

Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 11-06-2026

filtering systems. Equally important is the need to enhance user awareness and develop a culture of cybersecurity vigilance within organizations.

References

[1] Kumar, R. D., Prudhviraj, G., Vijay, K., Kumar, P. S., & Plugmann, P. (2024). Exploring COVID-19 through intensive investigation with supervised machine learning algorithm. In Handbook of Artificial Intelligence and Wearables (pp. 145-158). CRC Press.

[2] Swathi, B., Vijay, K., Sushanth Babu, M., & Dinesh Kumar, R. (2024, November). Machine Learning Techniques in Cloud Based Intrusion Detection. In The International Conference on Artificial Intelligence and Smart Environment (pp. 557-564). Cham: Springer Nature Switzerland.

[3] Sv satyakrishna, shirisha rangu ,bhargavi nalacheruve.(2024) Prospective investigation on colorectal cancer with SMOTE on machine learning Algorithm

[4] Dr.G.Vishnu Murthy, BhargaviNalacheruve 1Professor, Department of computer Science & engineering, Anurag University, TS, India. 2Student, Department of computer Science & engineering, Anurag University, TS, India.

[5] V. N. S. Manaswini, K. K, C. Nigam, S. S. Ali, R. Niranjana, and Suman, "Real-Time Object Detection in Drone Surveillance Using YOLOv5," in Proc. 2025 3rd Int. Conf. IoT, Communication and Automation Technology (ICICAT), Gorakhpur, India, 2025, pp. 1–6, doi: 10.1109/ICICAT68430.2025.11414670.

[6] B. Soundarya, V. N. S. Manaswini, M. Ayyakrishnan, R. D. Kumar, "Contextual Analysis of Big Data Analytics in Intelligent Transportation Frameworks," in Intersection of Artificial Intelligence, Data Science, and Cutting-Edge Technologies: From Concepts to Applications in Smart Environment, Lecture Notes in Networks and Systems, vol. 1353, Cham: Springer, 2025, doi: 10.1007/978-3-031-88304-0_79.

[7] R. D. Kumar, V. N. S.Manaswini, "Applications of blockchain in smart cities: detecting fake documents from land records using blockchain technology," in Blockchain for Smart Cities, Elsevier, 2021, pp. 105–117, doi: 10.1016/B978-0-12-824446-3.00017-X.

[8] Tejavath Veeramma, Badarla Anil, Guguloth Ravinder, "An advanced movie recommender using collaborative filtering and sentiment analysis," International Research Journal of Modernization in Engineering Technology and Science, vol. 7, no. 7, July 2025, doi: 10.56726/IRJMETS81618.

[9] Ravi Kumar Banoth, Ramana Murthy B V, "Automatic crop recommendation system using LightGBM and decision tree machine learning models," Journal of Machine and Computing, vol. 5, no. 1, pp. 343, Jan. 2025, doi: 10.53759/7669/jmc202505026.

[10] Ravi Kumar Banoth, Dr. B.V. Ramana Murthy, "Smart agriculture through IoT and machine learning for analyzing carbon footprints," in Proc. Int. Conf. Computer Science and Communication Engineering (ICCSCE), Apr. 2025.

[11] Ravi Kumar Banoth, B. V. Ramana Murthy, "Soil image classification using transfer learning approach: MobileNetV2 with CNN," SN Computer Science, vol. 5, art. no. 199, 2024, doi: 10.1007/s42979-023-02500-x.

Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 11-06-2026