

Introduction

Over the past years as the Internet has started making progressive changes for the world, there has been a new crime that occurs digitally that is known as **phishing**. A report from *Defending against phishing attacks: taxonomy of methods, current issues and future directions* provides a clear definition, stating that it is a lucrative identity theft crime that uses social-engineering tactics to manipulate victims to give up sensitive details such as bank login credentials and email passwords [1]. The attackers known as phishers would generate fake emails disguising themselves as staff members or a person of authority and urging their victims to click on the clone website that the phishers had designed to trick their victims into entering their personal credentials. A survey by Gartner had shown that approximately 3.6 million clients in the US alone had lost money to phishing attacks and total losses had reached approximately US\$ 3.2 billion Dollar. The number of victims increased from 2.3 million in 2006 to 3.6 million in 2007, an increase of 56.5%. Among all complaints received by the Federal Trade Commission in 2009 from Internet users, identity theft attributed to phishing email ranked first. It accounted for 21% of the complaints and cost consumers over 1.7 billion US dollars [2].

This digital crime has only continued growing exponentially and affecting more victims globally. It is essential for Online Users such as ourselves to learn how to protect ourselves from this rampant scam. By doing so, we would require to understand the threat and the solutions to prepare ourselves in the events that we encounter a phishing scam. This report will simulate a phishing attack using **GoPhish** and evaluate the effectiveness of the security tool **ClamAV** in detecting and mitigating these attacks within a **Kali** environment.

Tool Selection

Attacker tool: GoPhish is an open-source phishing framework that allows users to create, send, and monitor phishing campaigns. It's widely used for educational and organizational training purposes to test users' ability to identify phishing attempts. It provides beneficial features for new phishing users such as a user-friendly interface that provides a web-based dashboard for setting up phishing campaigns, managing targets and tracking results; providing users to design email templates, landing pages and schedule emails and providing detailed analytics like tracking the number of emails that open, clicks and data entered by recipients.

There are other widely known phishing tools such as **PhishSim** and **King Phisher** however GoPhish was the most suitable option as GoPhish is simple and direct to setup on the Linux virtual box compared to PhishSim that requires organization deployment and King Phisher requires server setup on Linux. Besides that, customization on phishing campaigns is simpler compared to PhishSim. In addition, GoPhish is able to scale well for both small and large tests without needing more technical setup unlike King Phisher. Overall, GoPhish is ideal for its ease of use, powerful analytics and open-source accessibility.

Defender tool: ClamAV is an open-source antivirus engine designed to detect malware, viruses, and other malicious threats across various platforms, including Windows, Linux and macOS. This tool is used for malware detection as it scans emails for malicious links and phishing URLs based on a defined database that often receives updates regarding new phishing techniques or URLs. It also has scheduled scans available to verify if the user's device had been infected.

There were other defender tools that are known for fighting phishing attacks such as Microsoft Defender and Proofpoint however ClamAV was the best option as it was a simple setup on the Linux virtual box compared to Microsoft Defender where it is required to have a Windows setup and Proofpoint requires enterprise-level deployment which isn't convenient for a test setup. Besides that, the user interface is lightweight compared to Microsoft Defender. To summarise the reasoning of choosing this tool, ClamAV is ideal for a lightweight, open-source alternative and able to setup on a Linux platform.

Virtual Environment: Kali Linux is the virtual environment where the attacking and defending will take place. Kali Linux is designed for professionals and students in cybersecurity, it provides a robust environment to conduct controlled tests like phishing simulations, malware analysis and network security assessments.

The reason of choosing this virtual box over other alternatives is because kali provides a broad selection of tools that allow users to conduct multiple types of security analyses without needing to add extra utilities. Furthermore, compared to BlackArch, Kali is user-friendly and it is accessible to those newer to cybersecurity without needing effectiveness for more experienced users. Documentation is particularly robust which provides faster troubleshooting and access to resources for both general and complex scenarios. Overall, Kali Linux is an optimal choice for a virtualized environment as it offers an extensive toolkit and an excellent platform for testing phishing and defensive tools like ClamAV within a controlled, security-focused environment.

Testing proposal

Overview: Phishing, especially in the form of workplace-themed emails, is a major security threat to organizations globally. Commonly, attackers impersonate HR departments, IT teams or executives, asking employees to verify credentials, change passwords, or logging into new accounts. These emails often mimic the look and feel of legitimate corporate communications, making them highly effective and hard to detect.

Studies show that phishing scams with workplace themes are among the most effective, as they tap into employee's natural inclination to comply with workplace directives. To reference *Verizon's Data Breach Investigations Report*, it highlights that 36% of data breaches involve phishing.

This testing proposal displays a simulation of a phishing attack using GoPhish and assessing the effectiveness of ClamAV as a defence mechanism. The goal is to determine whether ClamAV, a popular open-source antivirus tool, can detect and mitigate phishing URLs or attachments embedded in phishing emails.

Testing Objectives: ClamAV's capabilities will be assessed in detecting phishing content and the limitations of ClamAV detecting zero-day phishing threats will be analysed.

Metrics for success: ClamAV is able to scan and detect the email with the malicious link and/or able to analyse zero-day phishing attacks.

Mitre TTPS

Phishing (T1566.002): In this case, an email with a malicious link is sent to the victim, enticing them to click and enter credentials on a fake website.

Procedure: An email purporting to be from the company's HR department welcomes the recipient as a new employee and prompts them to click on a link to access their "new work account". The link directs the victim to a page mimicking an official company login page, capturing credentials upon entry.

Detection measures: The defence tool ClamAV could scan incoming emails for known malicious URLs or attachments, although it may struggle with detecting zero-day phishing links.

User Execution (T1204.001): Users click on a link in a phishing email that initiates a browser session to a fake website.

Procedure: The email contains a convincing link to what appears to be a work-related portal. Once clicked, the link could download malware or open a page designed to harvest login credentials.

Detection measures: Implementing URL filtering, sandboxing, or advanced email filtering on corporate email servers can help detect malicious links before they reach end users.

Credential Dumping (T1071.001): An attacker collects entered credentials directly from the phishing site.

Procedure: After clicking the link, users are taken to a fake login page where their work credentials are entered and sent back to the attacker's server.

Detection measures: Endpoint monitoring or security awareness training for employees can reduce phishing attacks.

Testing Scenario

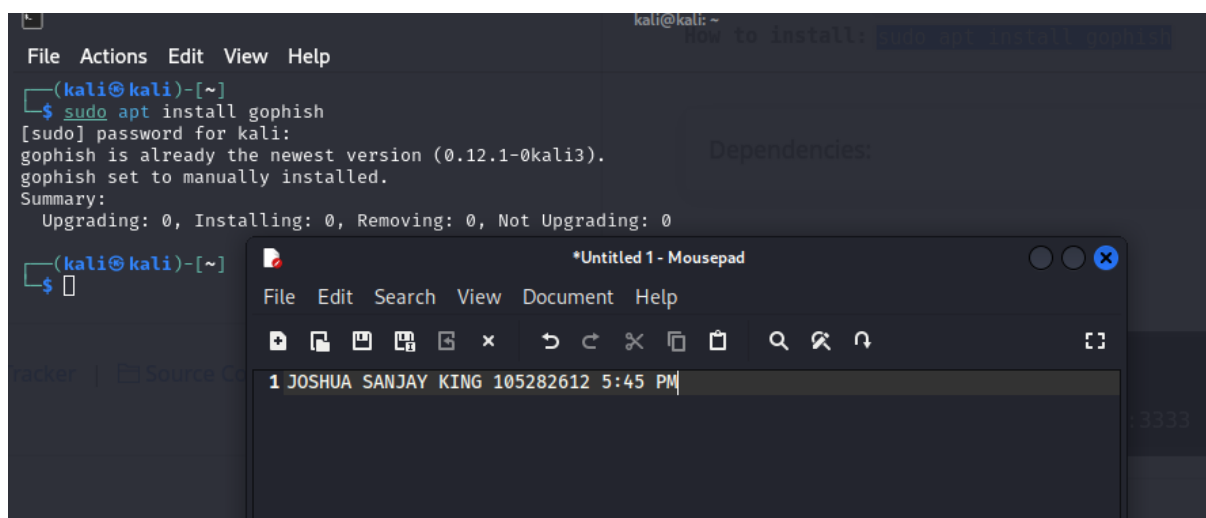
Phase 1: Attacking Phase

Attacker tool – GoPhish

Step 1: Downloading GoPhish on Kali

GoPhish has to be downloaded in Kali terminal with following command:

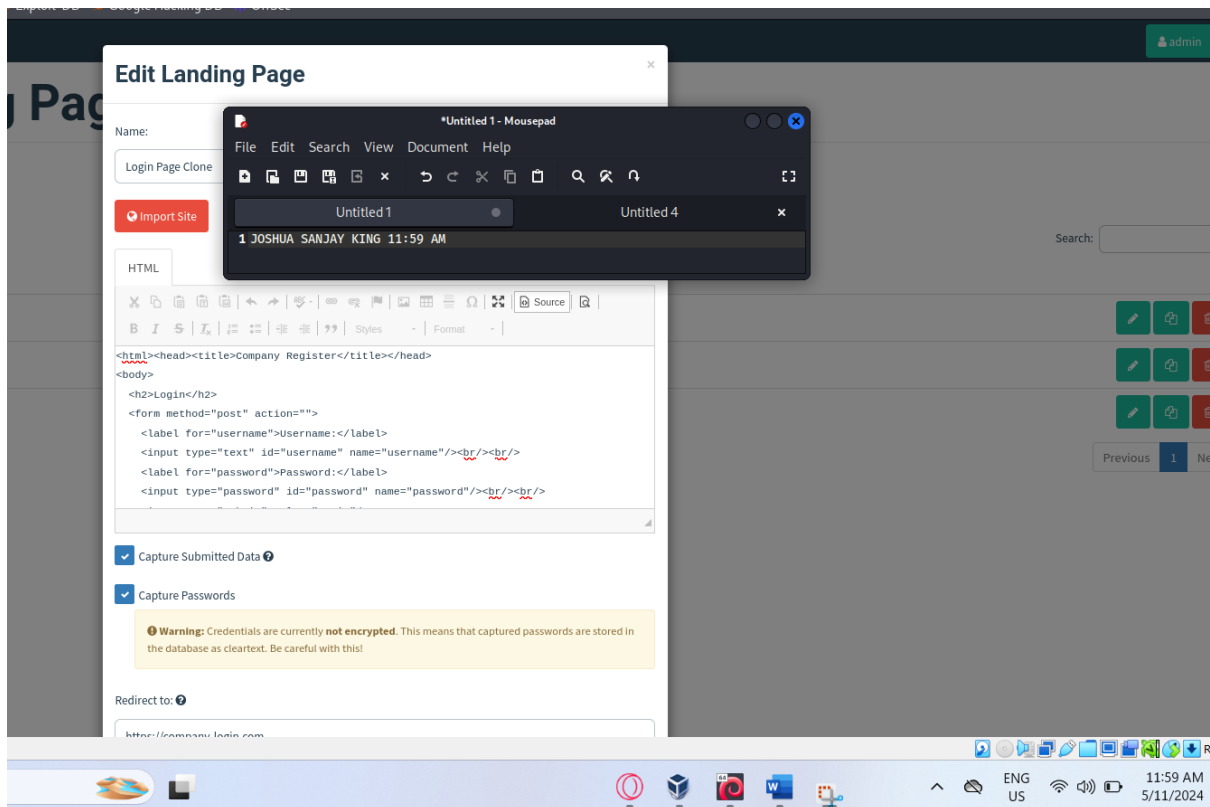
`"sudo apt install gophish"`



The screenshot shows a Kali Linux terminal window with the command `sudo apt install gophish` being executed. The terminal output indicates that gophish is already the newest version (0.12.1-0kali3) and is set to be manually installed. A summary line shows: `Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0`. Overlaid on the terminal is a Mousepad window titled `*Untitled 1 - Mousepad`. The Mousepad window contains a single line of text: `1 JOSHUA SANJAY KING 105282612 5:45 PM`. The terminal window also shows a menu bar with `File Actions Edit View Help` and a status bar at the bottom with `kali@kali: ~`.

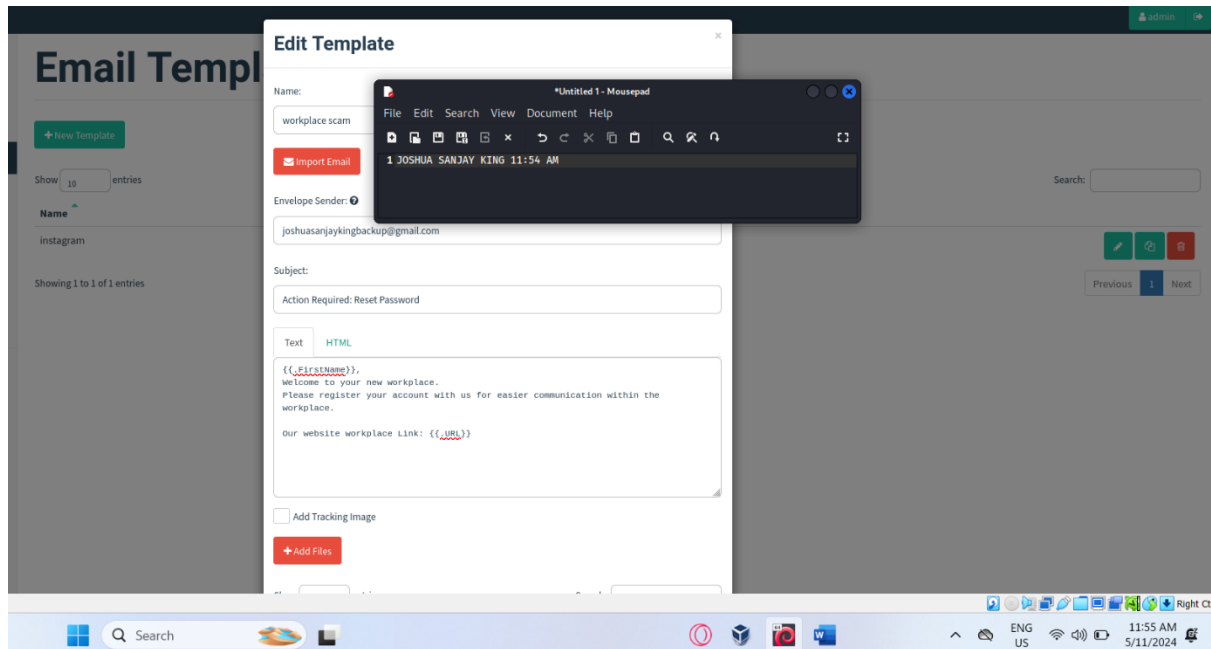
Step 2: Creating a landing page

Once setup is complete, it's time to start creating the webpage where the phishing attacks will take place. GoPhish provides user friendly interface that allows customization processes simple. I have used a general HTML page that request users to enter their username and password.



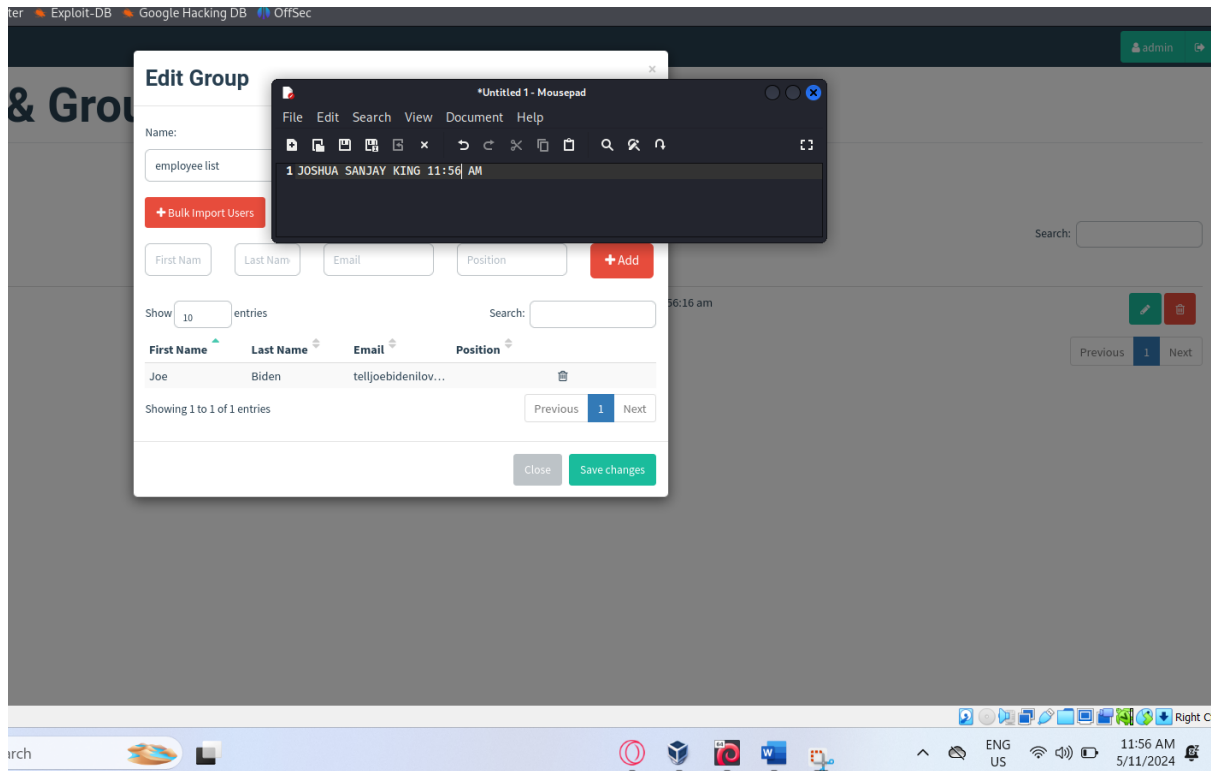
Step 3: Creating Email template

Once the landing page is complete, an email template is necessary in order to communicate with the victims. As seen in the screenshot, “`{{.FirstName}}`”, is a code that will return the first name of the recipient’s email address. This adds a personalised element to the email, enticing receivers to engage with the email rather than a generic message to all. A sense of urgency is also added as the email persuades the recipient to click on the URL for communications within the workplace.



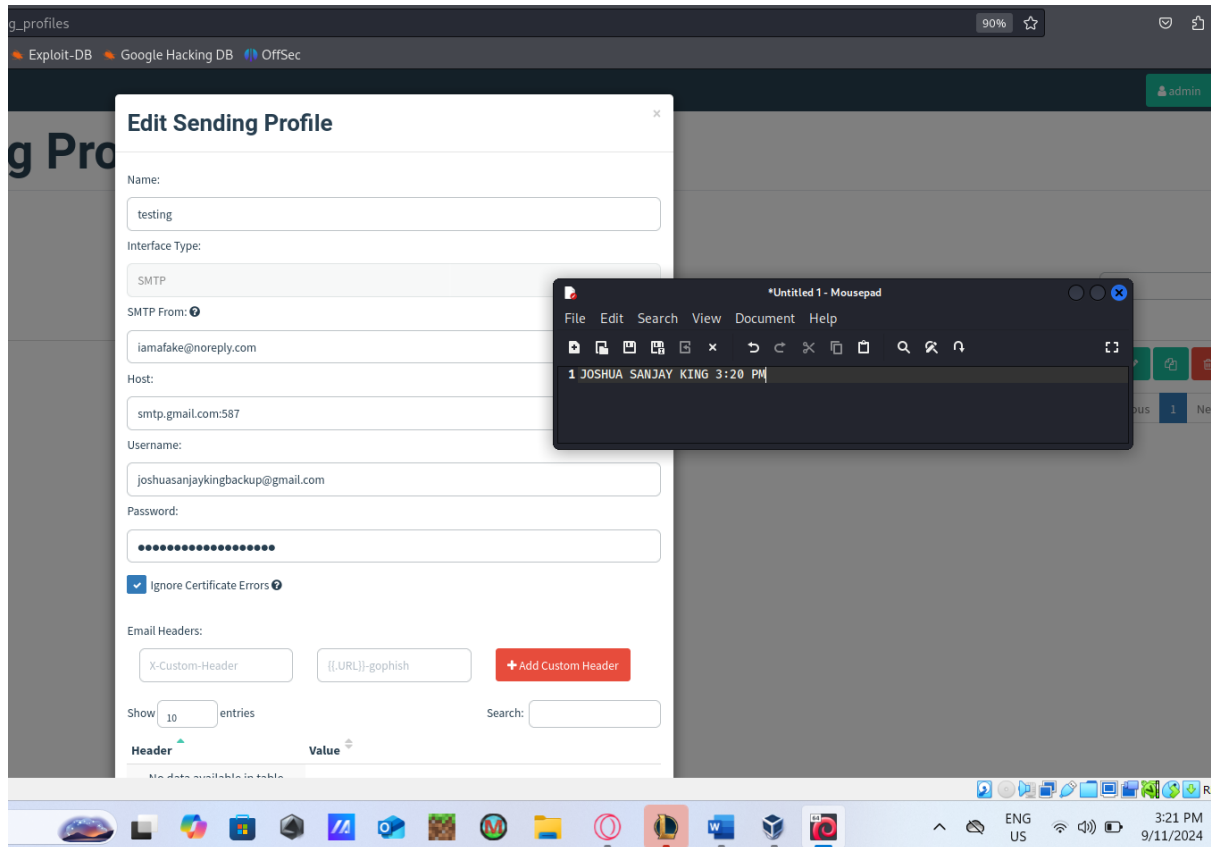
Step 4: Creating Users & Group

This step is deciding which recipient would receive the email. GoPhish allows numerous recipients to be added to the list and will send the email to every intended recipient. For testing purposes, we would only focus on sending the phishing email to one recipient with the name “Joe Biden”.



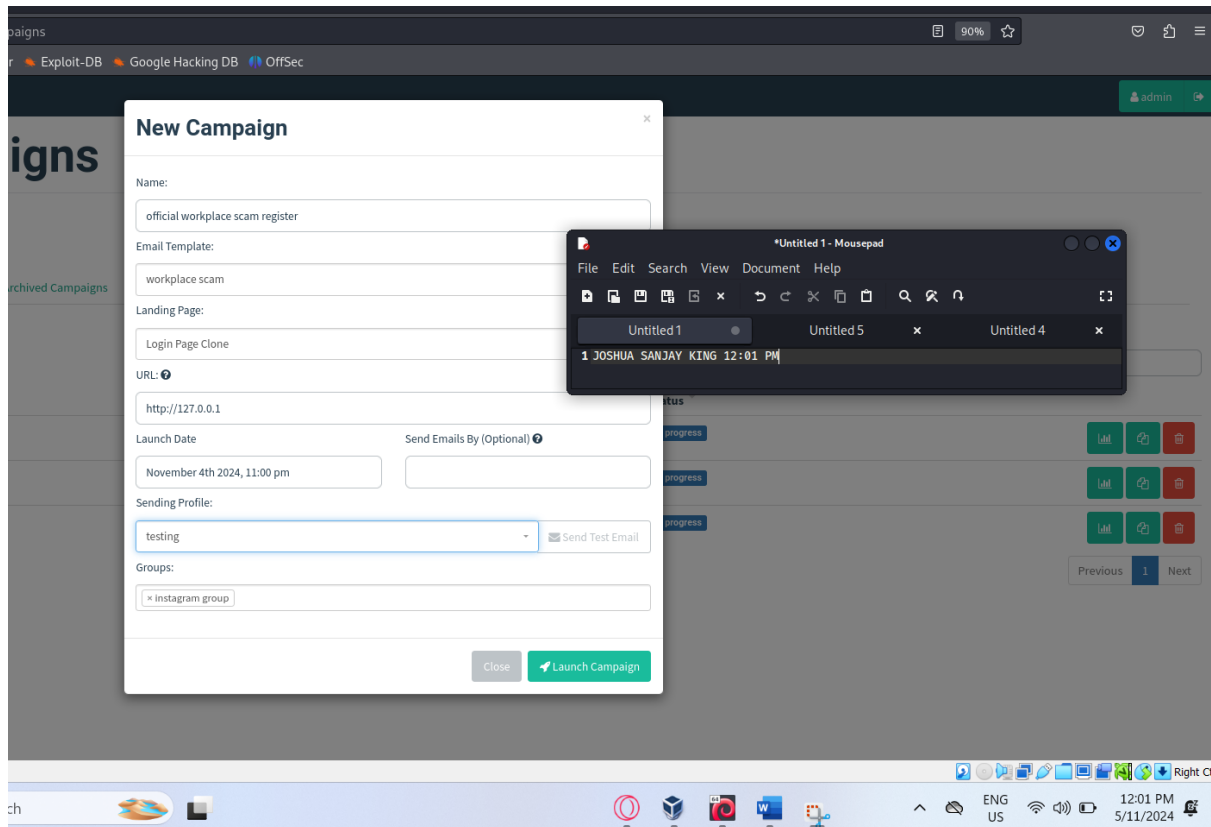
Step 5: Creating sending profiles

The purpose of this step is to create a sender profile that the recipient's would notice. Since our test account "Joe Biden" is using a Gmail account, the sending profile will have to use the same host email server "smtp.gmail.com:587"



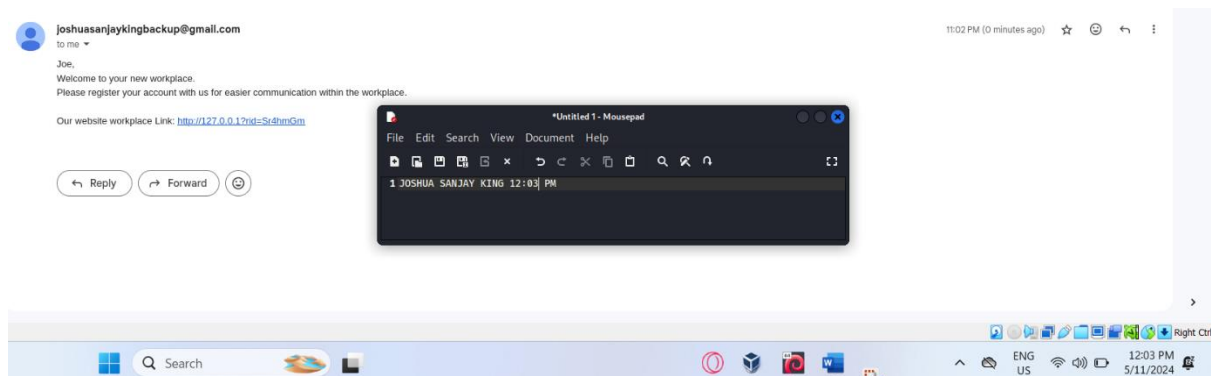
Step 6: Creating the campaign

This is the final step for making a phishing campaign. GoPhish provides customization options to change sending profiles and the groups of recipients.

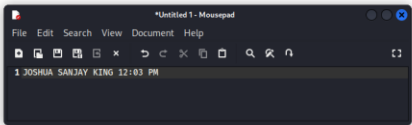
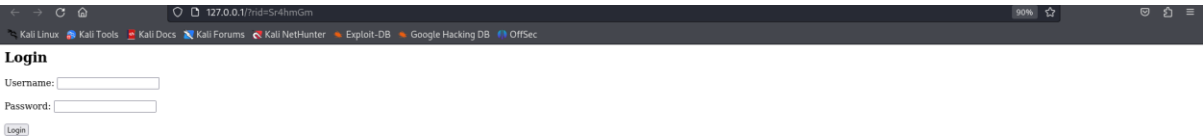


Results of the Campaign

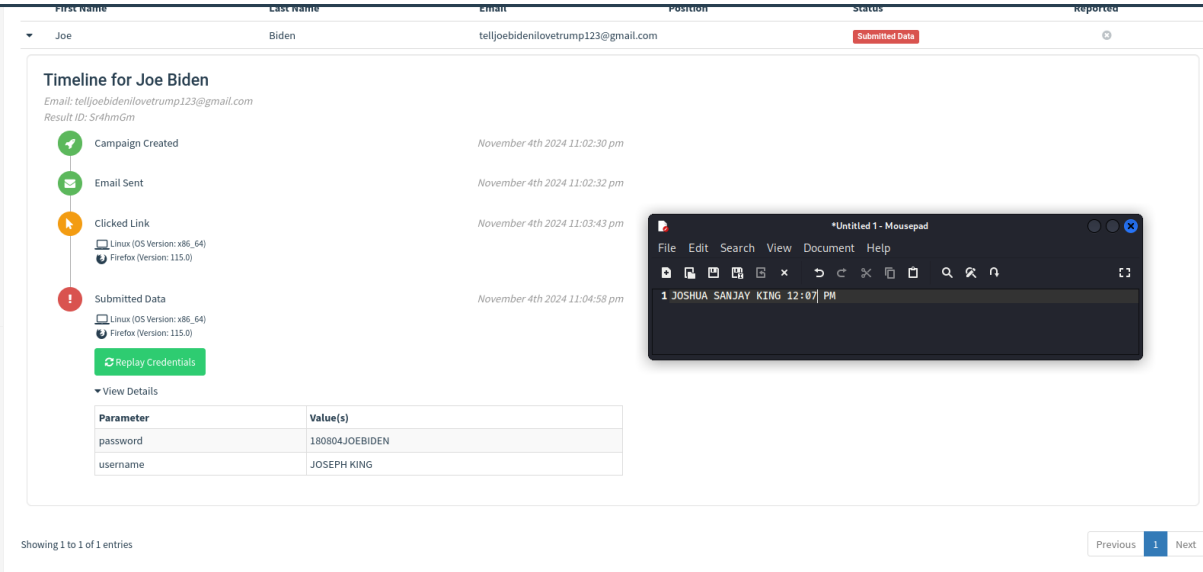
Result 1: This is the email that victims would receive. Notice that in the starting line is the name of the recipient "Joe". A working link with a blue underline would entice victims to click on it.



Result 2: This is HTML page that users would be led to after clicking. It is a very general login page without nothing else to go on or making new employees think twice before proceeding to enter their credentials.



Result 3: Once the victims had entered their credentials, the page will go blank and display a message saying the page had been interrupted. The credentials are then sent back to GoPhish website where a detailed report of events such as the time of when the email was sent, when the link was clicked and the victim's credentials that were stolen.



Being able to capture the credentials of the victims concludes the attacking phase and is regarded as a success on behalf of the attacking phase. The following step would be the defence phase.

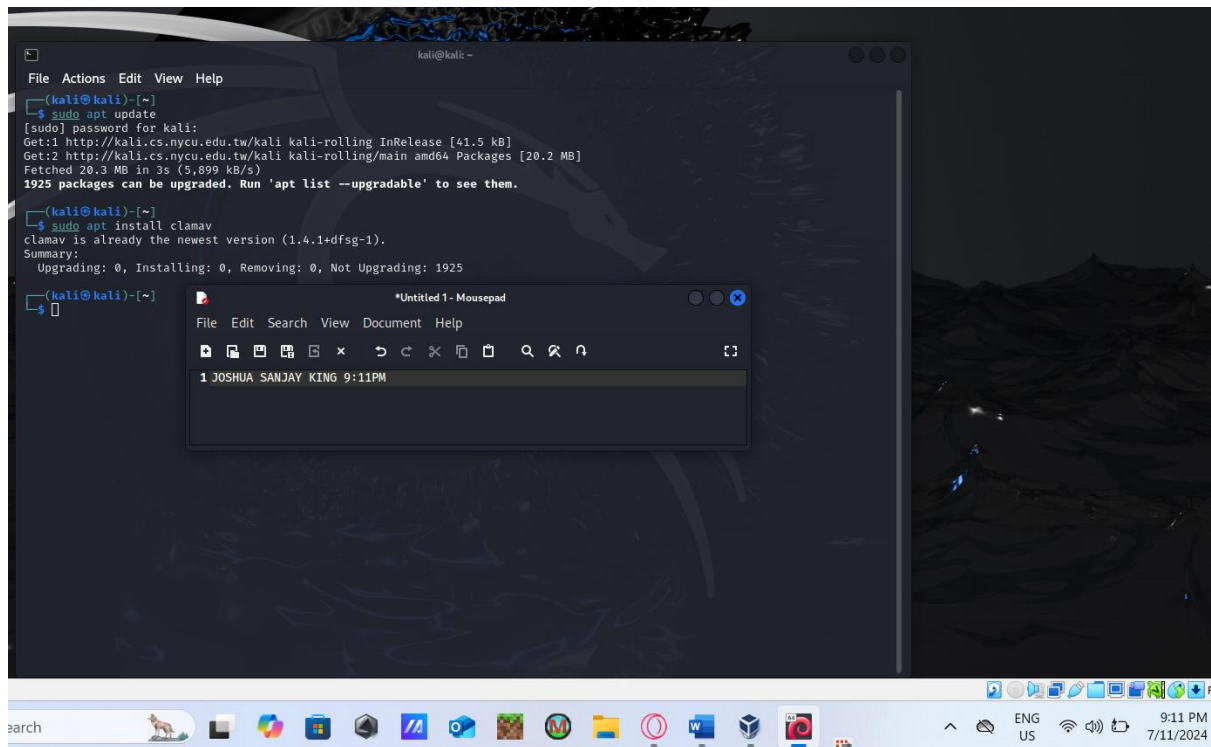
Phase 2: Defending Phase

Defending Tool - ClamAV

Step 1: Downloading ClamAV

ClamAV would be downloaded on the Kali Linux with the following command

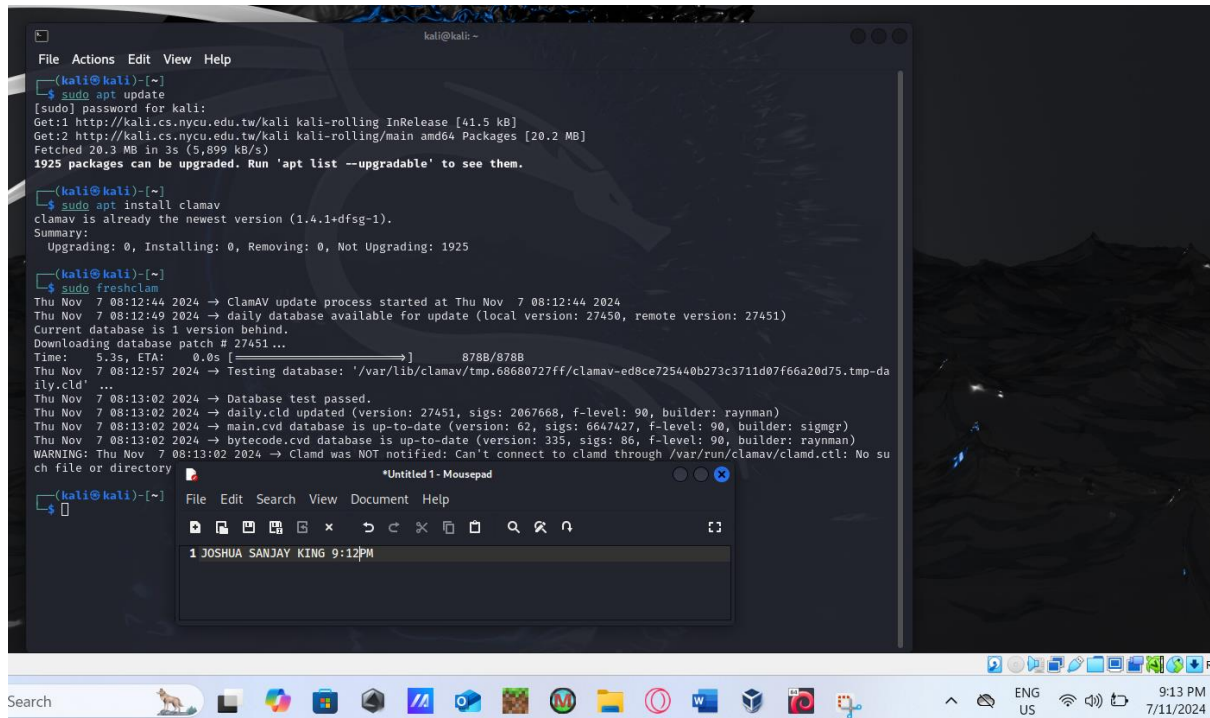
“`sudo apt install clamav`”



Step 2: Update the phishing database to the latest version

Before running a scan, it is important that the database of the defence tool is updated to be able to combat new and existing phishing attacks. The following command downloads the latest definitions, including phishing URLs and common spam signatures:

“sudo freshclam”



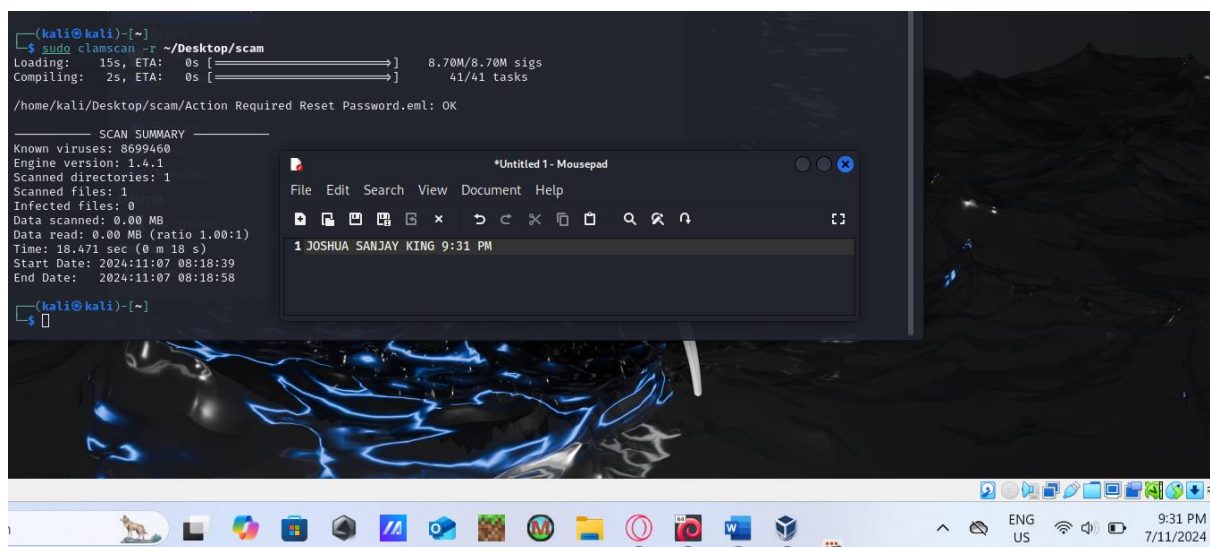
The screenshot shows a Kali Linux desktop environment. In the background, a terminal window displays the output of the 'sudo freshclam' command. The output indicates that the ClamAV update process started at 08:12:44 on Nov 7, 2024. It shows the current database is 1 version behind and that the daily database is being updated to version 27451. The process includes downloading the database patch, testing the database, and updating the main and bytecode databases. A warning message at the bottom states: 'WARNING: Thu Nov 7 08:13:02 2024 -> Clam was NOT notified: Can't connect to clamd through /var/run/clamav/clamd.ctl: No such file or directory'. In the foreground, a mousepad window titled '*Untitled1 - Mousepad' is open, showing the text '1 JOSHUA SANJAY KING 9:12PM'.

Step 3: Scan the email file

Once the tool’s database is updated, the scanning process should be able to be precise and fair. To run the scan, the following command is used:

The general code used is “sudo clamscan -r ~[enter directory path to email file]”

In this case “sudo clamscan -r ~/Desktop/scam”



The screenshot shows a Kali Linux desktop environment. In the background, a terminal window displays the output of the 'sudo clamscan -r ~/Desktop/scam' command. The output shows the scanning process for the file '/home/kali/Desktop/scam/Action Required Reset Password.eml'. It indicates that the file is OK and provides a scan summary. The summary includes: Known viruses: 8699460, Engine version: 1.4.1, Scanned directories: 1, Scanned files: 1, Infected files: 0, Data scanned: 0.00 MB, Data read: 0.00 MB (ratio 1.00:1), Time: 18.471 sec (0 m 18 s), Start Date: 2024:11:07 08:18:39, and End Date: 2024:11:07 08:18:58. In the foreground, a mousepad window titled '*Untitled1 - Mousepad' is open, showing the text '1 JOSHUA SANJAY KING 9:31 PM'.

From the scanning report, the defence tool had concluded that file was safe to use, declaring the defending phase a failure.

Evaluation of the testing phase: The test scenario aimed to assess ClamAV's effectiveness in detecting phishing attempts launched through a simulated campaign using GoPhish. The primary objective was to determine whether ClamAV could detect and mitigate phishing emails containing links to a zero-day phishing website designed to harvest credentials. Despite ClamAV's open-source accessibility and regular updates, the defence tool failed to detect the phishing website due to the zero-day nature of the attack.

ClamAV's effectiveness in detecting phishing threats is highly reliant on its signature-based database, which must be continuously updated with newly identified malicious URLs, phishing sites and patterns. Since zero-day phishing sites are newly crafted and unknown, they are often missing from ClamAV's database. This resulted in ClamAV failing to detect the phishing link, as it could not recognize a threat it hadn't previously encountered. This testing underscored this limitation, as ClamAV lacked heuristic or behavioural analysis capabilities that could have identified unusual patterns indicative of a phishing attempt. As a result of not having advanced techniques, ClamAV was unable to assess the potential risk of the URL embedded within the phishing email.

Although its failure against a zero-day threat revealed a significant gap in its ability to protect users, ClamAV demonstrated good usability and smooth integration, confirming its suitability for environments that prioritize open-source solutions.

In conclusion of this testing, ClamAV is a valuable tool for detecting well-documented malware and popular phishing links, its reliance on signature-based detection makes it insufficient as a stand-alone defence against zero-day phishing threats. In real world scenarios, zero-day phishing attacks are increasingly common as attackers constantly develop new techniques to evade detection.

Mitigations Of Phishing Attacks

It is clear that phishing at current times is at a very sophisticated level where many well-known defender tools such as ClamAV not being able detect and prevent victims from proceeding onto the malicious link. The main reason that these kind of defender tools is not able to battle against phishing threats is due to its nature of the attack relying on the vulnerabilities of the human users and not the system vulnerabilities. There are essential mitigation strategies that were provided by the Australian Cyber Security Centre (ACSC), that outline a practical framework for improving resilience against cyber threats.

User awareness remains one of the most effective defences against phishing. Regular training programs that educate employees on identifying phishing attempts help reduce the likelihood of users falling for these schemes. Incorporating phishing simulations allows employees to experience a mock phishing attempt in a safe environment and help them to recognise a phishing tactic.

Many phishing attacks reach their targets through email, making advanced email filtering a vital first line of defence. Implementing filters to detect and block potentially malicious emails before they reach users greatly reduces exposure to phishing threats.

Restricting the execution of unauthorized application, particularly web browsers or email applications, limit opportunities for malware introduced by phishing links to execute. Organisations can create an additional safeguard by allowing only approved applications can reduce the chances of

Regular updating and patching applications minimize vulnerabilities that attackers could exploit through phishing. For example, vulnerabilities in browsers or email clients can provide attackers with entry points through which they can inject malware or exploit unpatched systems.

By disabling risky features in applications (etc. Java, Flash and web ads), user application hardening reduces the likelihood of phishing websites triggering malicious scripts. This also includes disabling macros, which are often exploited through phishing emails with malicious attachments.

Limiting administrative privileges can minimize the impact of phishing attacks. If a user without administrative privileges is compromised, the potential for damage is significantly reduced as attackers would have fewer privileges to access critical systems or data.

Enforcing Multi-Factor Authentication (MFA) accounts especially those with remote access adds an additional layer of protection as even if credentials are stolen through a phishing attack, MFA servers as an effective barrier to unauthorized access.

Ensuring backups are regularly conducted and stored securely helps mitigate the risk of data loss due to phishing attacks that lead to ransomware. In the event of an incident, organisations can restore data and resume operations without needing to pay ransom demands.

Relevance of the testing scenario to the real world

Phishing attacks is highly relevant in the current cybersecurity landscape and remain a top attack vector for threats actors globally. This testing was not merely a theoretical but mirrors real-world tactics commonly used to compromise the privacy of individuals and organisations.

The *Verizon Data Breach Investigations Report* has cited that phishing is the primary tactic in data exfiltration and credential theft, with 36% of data breaches involving phishing. This shows that phishing is a key initial access method used by attacker as they masquerade as a trusted contact and exploit the human vulnerability to bypass technical defences, making phishing one of the most successful social engineering techniques.

Phishing attacks are becoming increasingly sophisticated, with attackers making unique zero-day phishing sites to evade traditional signature-based defences like ClamAV. These zero-day phishing often involve newly registered or modified URLs that are not in the security databases allowing these sites to bypass conventional antivirus tools. Such sites are often taken down after a short period after targeting specific users or organisations, avoiding these detection tools that are reliant on signature-based threat identification. This evolution in phishing tactics highlights the growing need for advanced detection capabilities, such as behaviour-based or machine learning tools which can identify malicious patterns in real time.

Besides credential theft, phishing attacks can escalate gaining access to their victim's internal system. Successful phishing attacks often lead to lateral movement within networks, where attackers pivot to other devices, escalate privileges and access sensitive areas of the infrastructure. From there, they may retrieve confidential data, alter critical files or establish persistent access points to revisit the compromised network at a later time.

Organisations today are more interconnected than ever, and a single compromised account can serve as a gateway for extensive cyber intrusion. This scenario illustrates how phishing remains a critical area of focus within the cybersecurity landscape, demanding a multi-layered defence strategy that combines technological safeguards with user training to mitigate the ever-evolving tactics of phishing.

In summary, this scenario reflects the real-world threat of phishing and underscores the importance of advanced, proactive defences in today's cybersecurity strategies. These new phishing tactics will need to be addressed with a layered and more adaptive security measures would be essential to maintain the security of every organisational data.

Conclusion

Phishing, a digital crime that exploits social-engineering techniques to steal personal information, has become a pervasive threat. Defined as a lucrative identity theft crime, phishing typically involves attackers posing as trustworthy entities to deceive victims into revealing sensitive details like banking or email credentials. This report explores a phishing simulation using GoPhish and evaluates ClamAV's effectiveness as a defence tool within a Kali Linux environment.

GoPhish was chosen for its simplicity in creating, sending and tracking phishing campaigns. Compared to other tools, it is user-friendly and highly customizable, making it ideal for educational and testing scenarios. ClamAV was selected as the defender tool for its Linux compatibility and capacity to detect phishing-related malware.

The test done for the report simulates a phishing attack, mimicking a workplace-themed email urging recipients to enter credentials on a fake login page. ClamAV's ability to detect phishing URL embedded in the email was assessed, with success measured by its detection of malicious links or zero-day phishing threats. However, due to its reliance on a signature-based database, ClamAV may struggle with unknown threats, demonstrating a gap in defences against zero-day attacks.

User education is essential to battle against phishing. Providing training programs and simulated phishing tests help employees identify and avoid phishing attempts. Besides user education, additional layers of defence, such as advanced email filtering, restricted application execution, application hardening, and regular patching, can further strengthen security. Lastly, multi-factor authentication and data backups also serve as protective measures, reducing risk of unauthorised access and data loss.

Phishing remains a significant cybersecurity threat as attackers are increasingly using zero-day phishing sites to evade signature-based defences like ClamAV, underscoring the need for adaptive and multi-layered security approaches to counter this evolving threat.