INSIDER THREAT AT YAHOO AND KEYSTROKE TOOL

A REPORT

Submitted by

V.SATYA SAI [RA2111030010170]

Under the Guidance of

Dr. D. Deepika

Assistant Professor, Department of Networking and Communications

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE ENGINEERING

with specialization in CYBER SECURITY

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR – 603203

APRIL 2024

COLLEGE OF ENGINEERING & TECHNOLOGY
SRM INSTITUTE OF SCIENCE & TECHNOLOGY
S.R.M. NAGAR, KATTANKULATHUR – 603203

BONAFIDE CERTIFICATE

Certified that this project report **"INSIDER THREAT AT YAHOO AND KEYSTROKE TOOL"** is the bonafide work of "V.SATYA SAI" of III Year/VI Sem B. Tech (CSE) who carried out the mini project work under my supervision for the course 18CSE386T PENETRATION TESTING AND VULNERABILITY ASSESSMENT in SRM Institute of Science and Technology during the academic year 2023- 2024(Even sem).

SIGNATURE	SIGNATURE
Dr. D. Deepika	Dr. Annapurani Panaiyappan K
Assistant Professor	Professor and Head
Networking and Communications	Networking and Communications

CASE STUDY ON "INSIDER THREAT AT YAHOO"

EVEN Semester (2023-2024)

Course Code & Course Name: 18CSE386T – Penetration Testing and Vulnerability Assessment

Year & Semester : III/VI

Report Title : INSIDER THREAT AT YAHOO AND KEYSTROKE TOOL

Course Faculty : Dr. D. Deepika

Student Name : V.SATYA SAI [RA2111030010170]

Evaluation:

S. No	Parameter	Marks
1	Problem Investigation & Methodology Used	
2	Tool used for investigation	
3	Demo of investigation	
4	Uploaded in GitHub	
5	Viva	
6	Report	
	Total	

Date:

Staff Name:

Signature:

TABLE OF CONTENTS

INTRODUCTION

The 2014 Yahoo insider threat incident served as a wake-up call, underscoring the urgent necessity for robust security protocols within organizations. It exposed the grave repercussions of internal vulnerabilities when a former employee exploited their access to pilfer sensitive user data from millions of Yahoo accounts. This event shed light on the looming danger posed by insiders harboring malicious intentions.As organizations intensify their efforts to fortify cybersecurity measures, the strategic deployment of penetration testing (pentesting) tools emerges as a linchpin in preemptively identifying and shoring up vulnerabilities against both internal and external threats. Insider threats stand as a formidable adversary across industries and company sizes. Unlike external threats, which typically stem from cybercriminals breaching perimeter defenses, insider threats originate from individuals with legitimate access to sensitive systems and data. These insiders can range from current and former employees to contractors and business associates, knowingly or unknowingly exploiting their privileges to compromise security and undermine organizational integrityTo mitigate the risks associated with insider threats, organizations adopt a multifaceted defensive strategy that encompasses both technological solutions and proactive security measures. While pentesting tools traditionally focus on evaluating and reinforcing external defenses, their adaptability extends to uncovering vulnerabilities within internal infrastructure. By simulating real-world attack scenarios, pentesting tools empower security teams to pinpoint potential points of exploitation that insiders might exploit to cause harm.

SCOPE

Understanding the scope of this incident is crucial for comprehending its impact and implementing effective measures to prevent similar occurrences in the future. In defining the scope of the insider threat at Yahoo.

Understanding the scope of this incident is crucial for comprehending its impact and implementing effective measures to prevent similar occurrences in the future. In defining the scope of the insider threat at Yahoo.

Understanding the Insider Threat:

- Pinpoint the individuals involved in the insider threat incident and their roles within the organization.
- Uncover the motives driving the insider's actions, whether stemming from financial incentives, personal vendettas, or other factors.

Impacted Data and Systems:

- Identify the nature of compromised data, such as user credentials, personal details, or proprietary assets.
- Determine the sources from which data was accessed or removed, including email servers, databases, or cloud storage.
- Assess the potential repercussions of the breach on individuals, businesses, and partners, including financial losses and damage to reputation.

Detection and Response Strategies:

- Assess the effectiveness of existing security measures and monitoring systems in identifying insider threats.
- Identify any shortcomings in the organization's ability to detect and respond to such incidents, such as insufficient logging or access controls.
- Analyze the timeline leading to the detection of the insider threat and subsequent response actions, including engagement with law enforcement.

Organizational Fallout and Key Takeaways:

- Evaluate the broader impact of the incident on Yahoo's operations, brand image, and customer trust.
- Extract lessons from the incident to enhance security practices, employee training, and risk management strategies.

OBJECTIVE

Investigate the Insider Threat Incident:

- Conduct a thorough investigation into the insider threat incident at Yahoo, including the identification of individuals involved, their motives, and the methods employed to compromise security.
- Gather forensic evidence and analyze digital artifacts to reconstruct the timeline of events leading up to the data breach and uncover any accomplices or collaborators.

Enhance Insider Threat Detection and Prevention Mechanisms:

- Identify gaps or weaknesses in existing security controls and monitoring mechanisms that allowed the insider threat incident to occur undetected.
- Implement measures to strengthen insider threat detection and prevention capabilities, such as enhanced user behavior analytics, real-time monitoring of privileged access, and improved access controls for sensitive data and systems.

Assess the Impact on Data Security:

- Evaluate the extent of data compromise resulting from the insider threat incident, including the types of data accessed or exfiltrated, the number of affected individuals or accounts, and the potential implications for privacy and confidentiality.
- Determine the financial, reputational, and regulatory consequences of the data breach for Yahoo and its stakeholders, including customers, partners, and shareholders

TOOL DISCRIPTION

KEYSTROKE A keystroke tool, or keystroke logger, is a software or hardware device used to monitor and record the keystrokes typed on a computer keyboard. It can be used for various purposes

KeyFeatures:

Security: Keystroke loggers are sometimes used by organizations to monitor the activities of employees and ensure compliance with security policies.

Forensics: Law enforcement agencies and forensic investigators may use keystroke loggers to gather evidence in criminal cases.

Parental Control: Parents may use keystroke loggers to monitor their children's online activities and ensure they are not engaging in inappropriate behavior or accessing harmful content.

Personal Use: Individuals may use keystroke loggers to keep track of their own typing activity, for example, to analyze their productivity or improve their typing skills.

Advantages of using KEYSTROKE :

While keystroke logging tools can have legitimate uses in certain contexts, such as employee monitoring with proper consent, it's important to recognize the potential ethical and legal implications. However, here are some hypothetical advantages of using keystroke logging tools:

Employee Monitoring: In a professional setting, keystroke logging tools can be used to monitor employee productivity, identify areas for improvement, and ensure compliance with company policies. This can help businesses optimize workflows and enhance overall efficiency.

Security: Keystroke logging can assist in detecting unauthorized access to sensitive information or systems. By recording keystrokes, organizations can identify suspicious behavior and potential security breaches, enabling them to take appropriate action to mitigate risks and protect their assets.

Parental Control: Parents may use keystroke logging tools to monitor their children's online activities and ensure their safety. By tracking keystrokes, parents can identify potential risks such as cyberbullying, online predators, or exposure to inappropriate content, allowing them to intervene as necessary.

Training and Education: Keystroke logging tools can be used in educational settings to analyze students' typing proficiency, track their progress, and provide personalized feedback. This can help students improve their typing skills.

Tool working procedure

How Keyloggers Work:

- Keyloggers are spread in different ways, but all have the same purpose.
- They all record information entered on a device and report the information to a recipient. Let's take a look at a few examples showing how keyloggers can spread by being installed on devices.

• **Web page scripts.** Hackers can insert malicious code on a web page. When you click an infected link or visit a malicious website, the keylogger automatically downloads on your device.

• **Phishing:** Hackers can use phishing emails, which are fraudulent messages designed to look legitimate. When you click an infected link or open a malicious attachment, the keylogger downloads on your device.

• **Social engineering:** Phishing is a type of social engineering, which is a strategy designed to trick victims into divulging confidential information. Cybercriminals might pretend to be a trusted contact to convince the recipient to open an attachment and download malware.

• **Unidentified software downloaded from the internet:** Malicious users can embed keyloggers in software downloaded from the internet. Along with the software you want to download, you unknowingly download keylogging software.

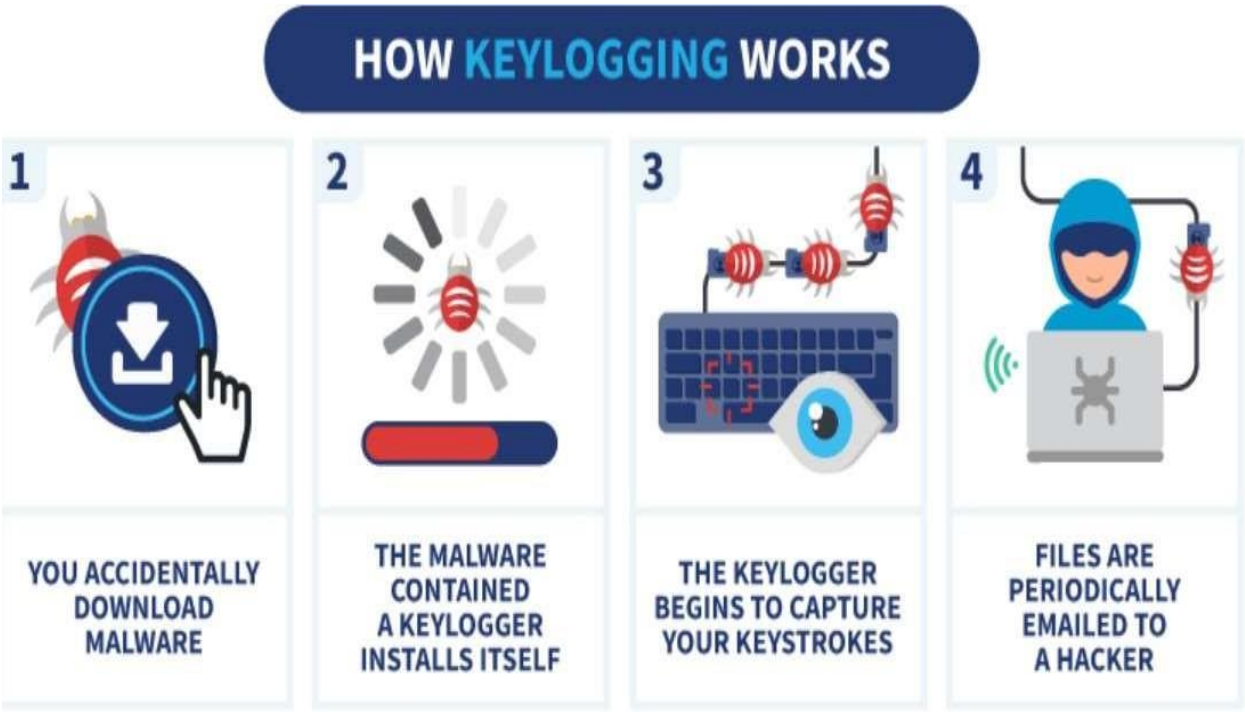
How to Protect Yourself Against Keylogging Attacks on Personal Devices

The best protection against keylogging attacks is education about how the attacks occur. Consider the following precautions you can take to avoid becoming a victim:

- **Verify that emails are sent from legitimate sources.** Check for unusual email addresses and consider whether requests are legitimate. For example, question whether your bank would ask you to reset your password in an email. When in doubt, avoid clicking the link. You can still perform the requested action, such as resetting your password, directly from your bank's portal.

- **Verify that websites are legitimate.** Cybercriminals often create convincing fake versions of popular websites. Before entering personal information, such as a social security number, check that the website has a digital certificate to validate its security.

- **Use a unique and strong password.** It's important to use unique passwords so that cybercriminals don't have access to all your accounts if a password is compromised.



HOW KEYLOGGING WORKS:

- **Capture Input:** Keylogging software or hardware is installed on a computer or device to capture keystrokes. This can be done at different levels of the system, such as at the keyboard driver level, operating system level, or application level.

- **Recording Keystrokes:** As the user types on the keyboard, the keylogger captures each keystroke, including letters, numbers, symbols, and special keys (like Enter, Shift, Ctrl, etc.).

- **Storage:** The captured keystrokes are typically stored in a log file on the local system. This log file can contain timestamps, the keys pressed, and sometimes additional information such as the application in which the keystrokes were entered.

- **Transmission (if applicable):** In some cases, especially with remote monitoring or malicious keyloggers, the captured keystrokes may be sent over a network to a remote server controlled by an attacker.

- **Analysis:** The logged keystrokes can be analyzed to extract useful information such as passwords, usernames, credit card numbers, messages, or any other sensitive data entered by the user.

IMPLEMENTATION

KEYSTROKE on yahoo application:

- **Download**: Go to the official website of the tool (e.g., PortSwigger's website for Burp Suite) and download the appropriate version for your operating system .

- **Installation:** Once the download is complete, run the installer executable file. Follow the on-screen instructions to install the tool on your system. For Burp Suite, this typically involves selecting installation options (like choosing the installation directory) and confirming the installation process.

- **Configuration:** After installation, launch the tool. For Burp Suite, you may need to configure your proxy settings, especially if you plan to intercept and monitor HTTP/HTTPS traffic. This involves setting up your browser or system to use Burp Suite as a proxy.

- **License Activation (if required):** Some tools, including Burp Suite, may require a license key or activation process for full functionality. Follow the instructions provided by the tool to activate your license or use the free version if applicable.

- **Update:** It's crucial to keep your tools updated to ensure you have the latest features and security patches. Most tools have an update mechanism within the application or provide instructions on how to download and install updates manually.

- **Optional Plugins:** Depending on your testing needs, you may want to install additional plugins or extensions for the tool. For Burp Suite, there are numerous community-developed and official plugins that enhance its capabilities for different types of testing.

- **Practice and Training:** Before using any tool on a live application, it's essential to familiarize yourself with its features, workflows, and best practices. Many tools offer tutorials, documentation, and online courses to help you get started.

INSTALLATION

- **Download:** Go to the official website of the tool (e.g., PortSwigger's website for Burp Suite) and download the appropriate version for your operating system (Windows, macOS, or Linux).

- **Installation:** Once the download is complete, run the installer executable file. Follow the on-screen instructions to install the tool on your system. For Burp Suite, this typically involves selecting installation options (like choosing the installation directory) and confirming the installation process.

- **Configuration:** After installation, launch the tool. For Burp Suite, you may need to configure your proxy settings, especially if you plan to intercept and monitor HTTP/HTTPS traffic. This involves setting up your browser or system to use Burp Suite as a proxy.

- **License Activation (if required):** Some tools, including Burp Suite, may require a license key or activation process for full functionality. Follow the instructions provided by the tool to activate your license or use the free version if applicable.

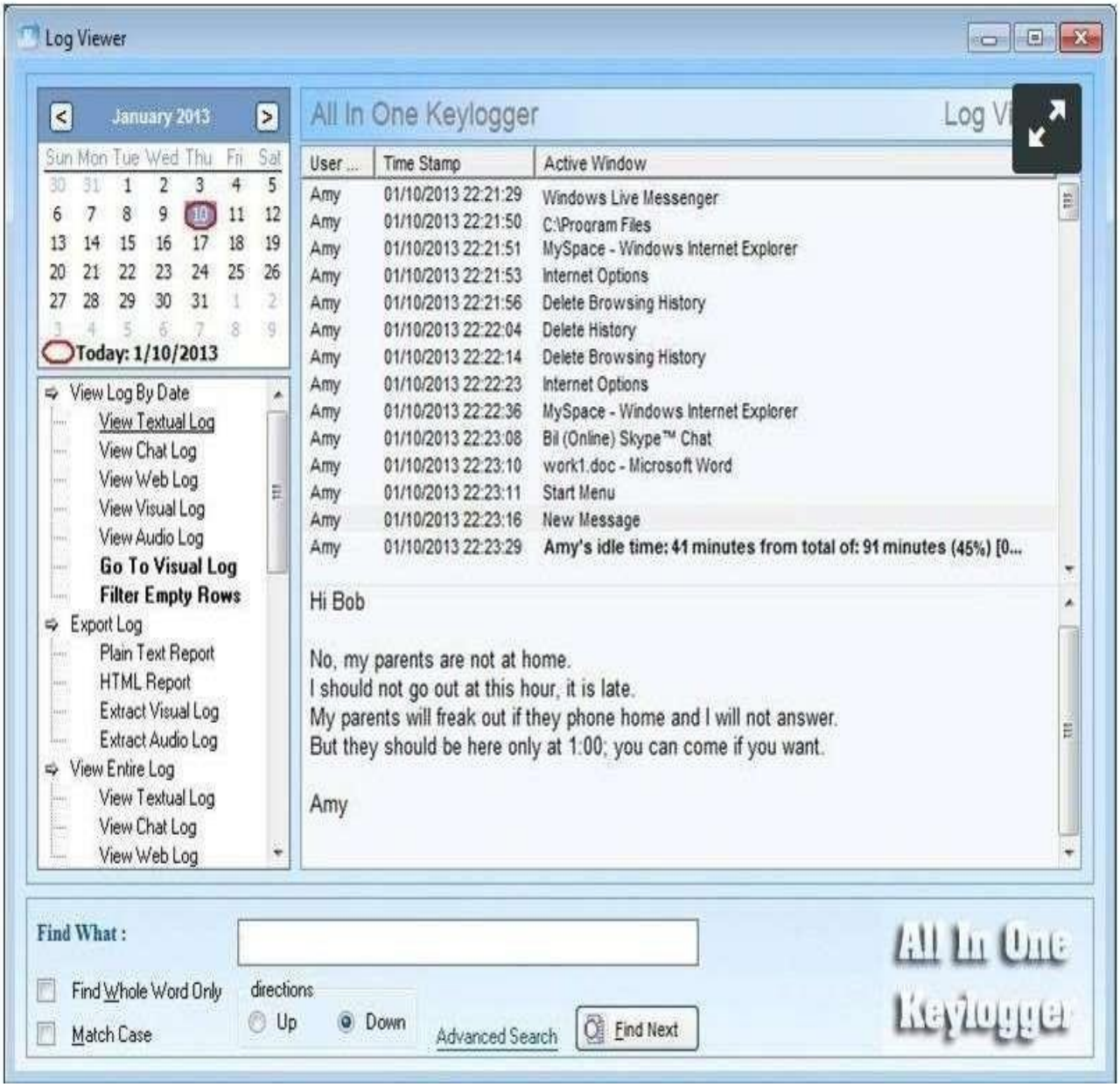
- **Update:** It's crucial to keep your tools updated to ensure you have the latest features and security patches. Most tools have an update mechanism within the application or provide instructions on how to download and install updates manually.

- **Optional Plugins:** Depending on your testing needs, you may want to install additional plugins or extensions for the tool. For Burp Suite, there are numerous community-developed and official plugins that enhance its capabilities for different types of testing.

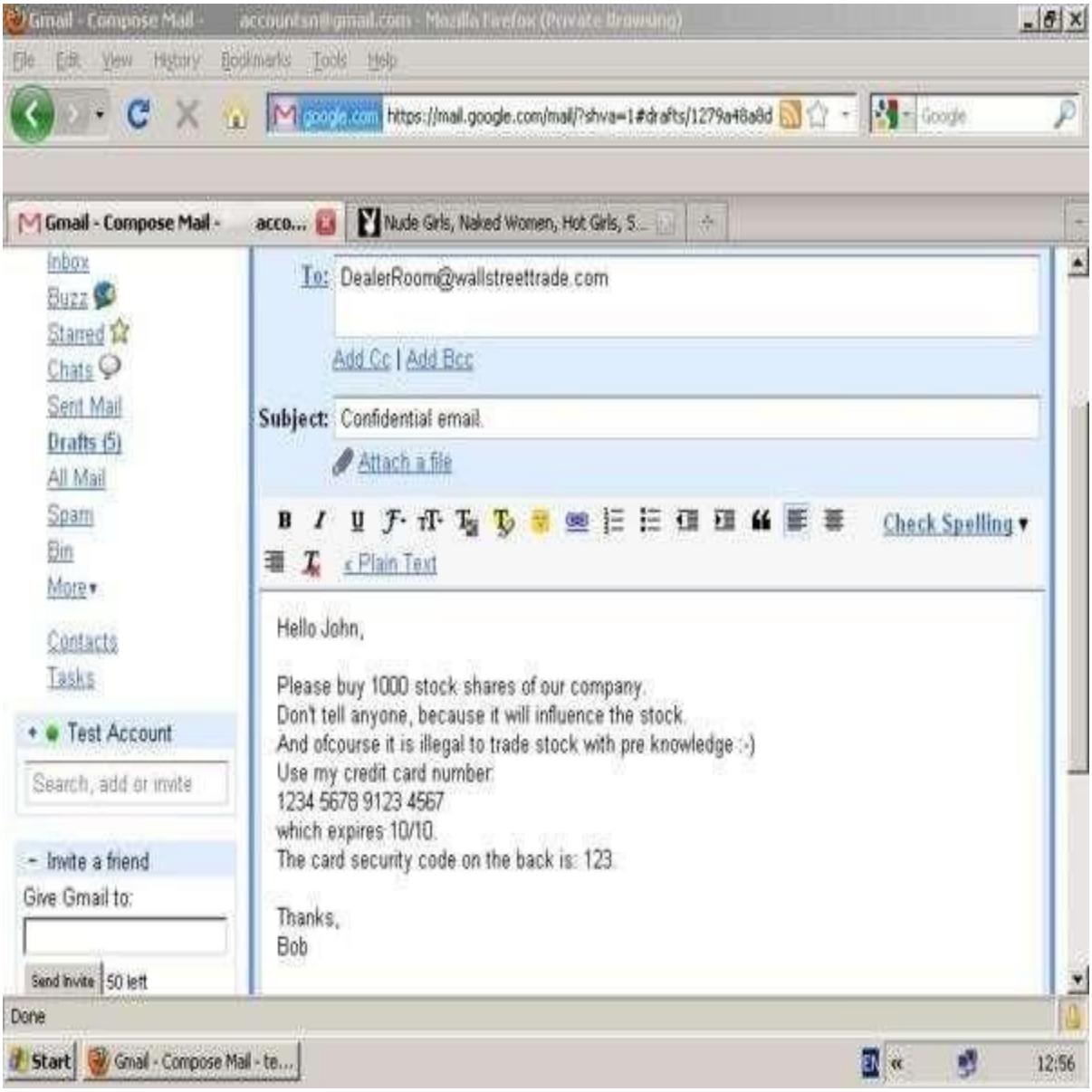
- **Practice and Training:** Before using any tool on a live application, it's essential to familiarize yourself with its features, workflows, and best practices. Many tools offer tutorials, documentation, and online courses to help you get started.

Screenshots of the implementation

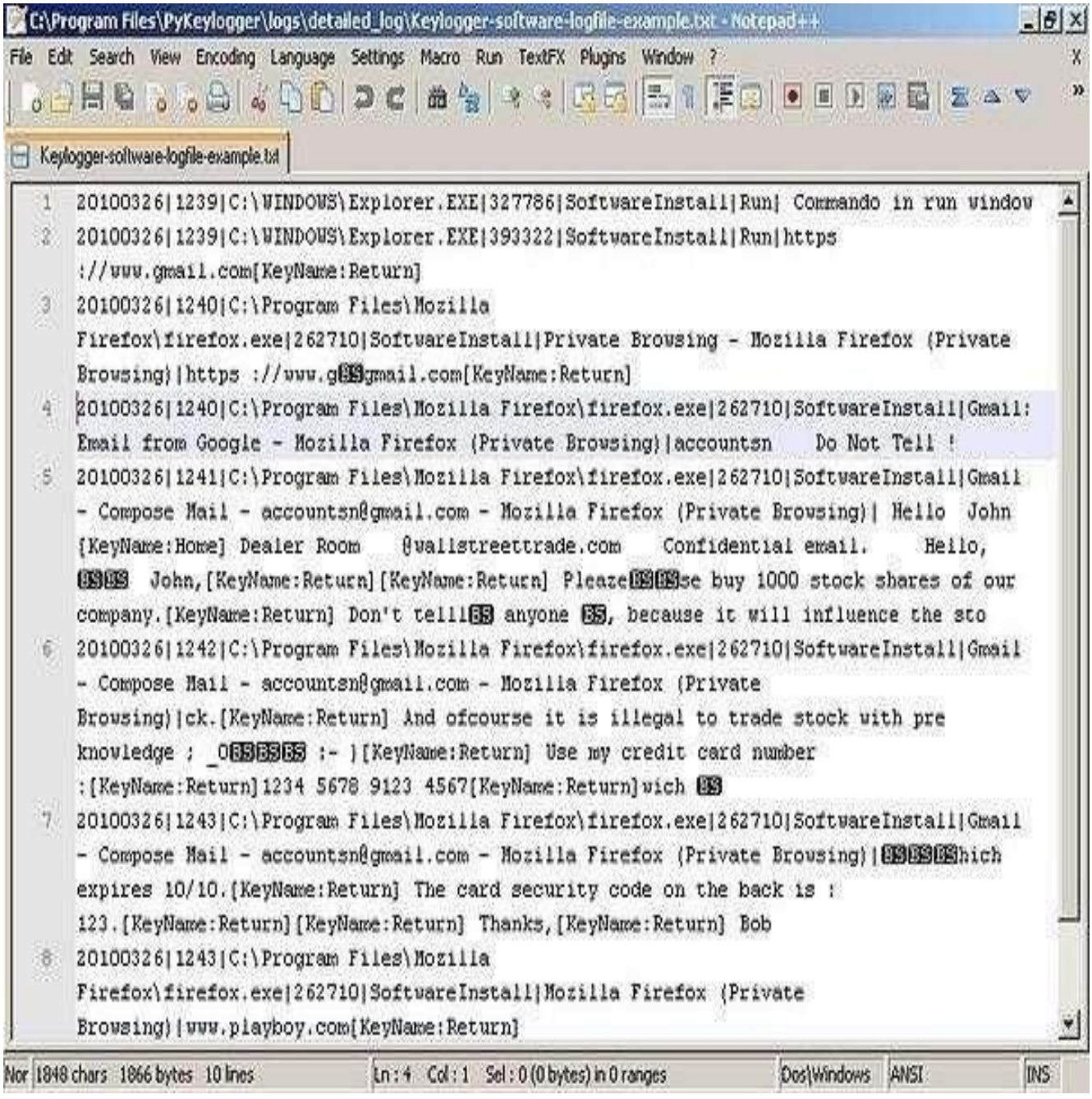
6.1 files in keystroke



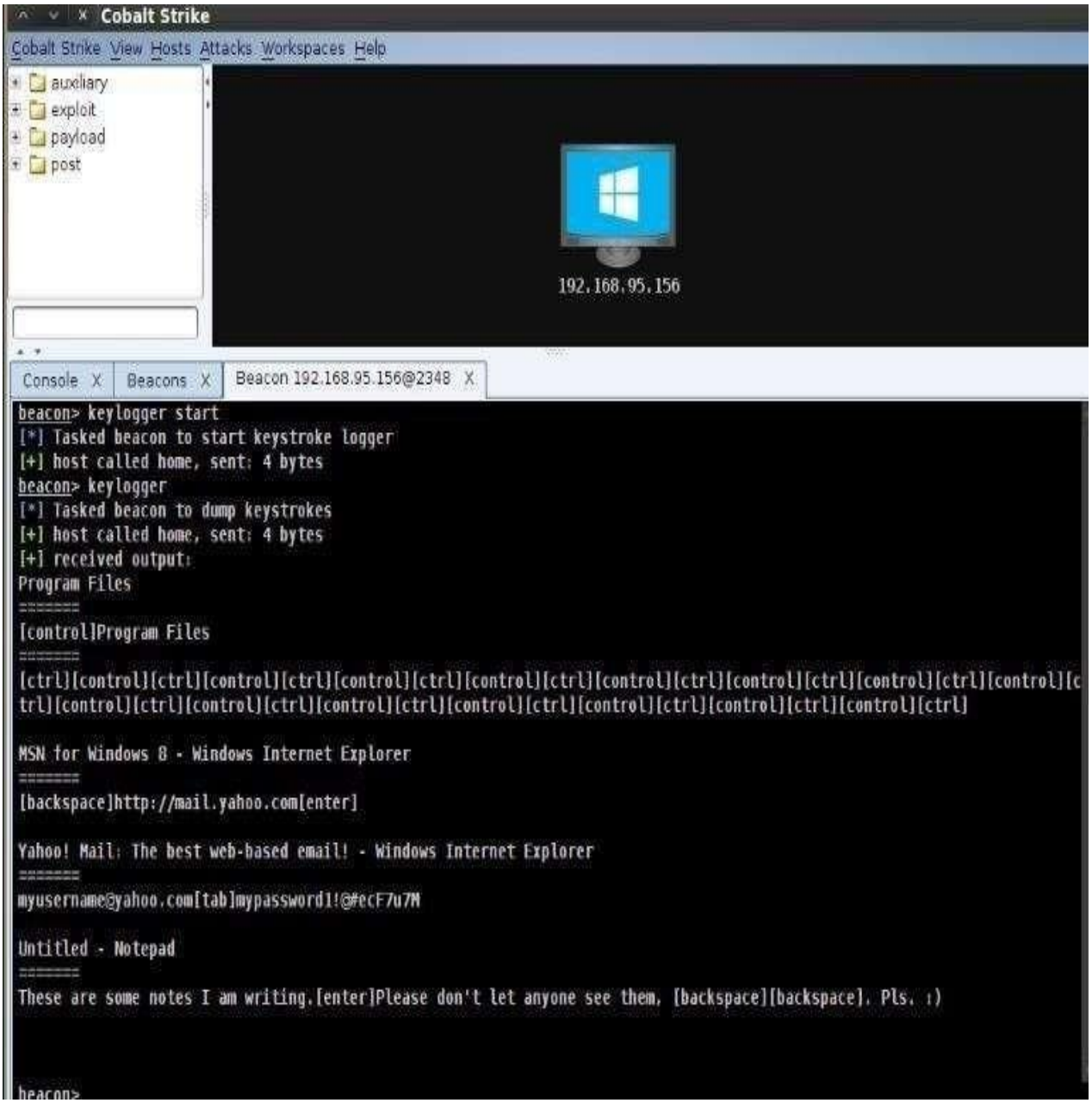
6.2 Mailing process in keystroker



6.3 Keylogger software logfile



6.4 Output of keylogger



CONCLUSION

The 2014 Yahoo insider threat incident stands as a stark reminder of the immense impact and lasting repercussions of data breaches. With over 500 million users affected, it ranks among the largest breaches in history. Despite occurring in 2014, the breach remained concealed for years, shedding light on the challenges of timely detection and disclosure.Investigations revealed indications of state-sponsored involvement, highlighting the sophistication and persistence of the attackers. Exploiting vulnerabilities within Yahoo's systems, they accessed a trove of sensitive user data, ranging from personal details to encrypted passwords.The fallout from the breach reverberated across Yahoo and its user base. It inflicted substantial damage to the company's reputation, eroding user trust and inviting intense scrutiny from both legal and regulatory bodies. Criticism was leveled at Yahoo for its handling of the incident, raising questions about transparency and the adequacy of its security protocols.As organizations grapple with the evolving threat landscape, the Yahoo breach serves as a cautionary tale, emphasizing the critical importance of robust cybersecurity measures, prompt incident response, and transparent communication. It underscores the need for continuous vigilance and investment in defensive strategies to safeguard against future breaches and mitigate their impact on both businesses and individuals.

REFERENCES

https://www.crowdstrike.com/cybersecurity-101/attack-