INSIDER THREAT AT YAHOO AND KEYSTROKE TOOL

A REPORT

Submitted by

N S S S RAJA RAM PULAVARTHI[RA2111030010146]

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 "N S S S RAJA RAM PULAVARTHI" 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 :N S S S RAJA RAM PULAVARTHI[RA2111030010146]

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 insider threat incident at Yahoo in 2014 brought to light the critical need for robust security measures to safeguard against internal risks within organizations. In this case, a former employee exploited their access to steal sensitive data from millions of Yahoo users, highlighting the potential dangers posed by insiders with malicious intent. As organizations strive to bolster their cybersecurity posture, the utilization of penetration testing (pentesting) tools plays a pivotal role in proactively identifying vulnerabilities and fortifying defenses against both internal and external threats. insider threats represent a formidable challenge for organizations of all sizes and industries. Unlike external threats, which often involve cybercriminals targeting vulnerabilities from outside the organization's perimeter, insider threats originate from individuals with legitimate access to sensitive systems and data. These insiders may include current or former employees, contractors, or business partners who intentionally or unintentionally misuse their privileges to compromise security and undermine organizational integrity.To mitigate the risks associated with insider threats, organizations deploy a multifaceted approach that encompasses both technical solutions and proactive security measures. While pentesting tools are primarily designed to assess and strengthen external defenses, they can also be adapted to identify vulnerabilities and weaknesses within an organization's internal infrastructure. By simulating realistic attack scenarios, pentesting tools enable security teams to uncover potential avenues of exploitation that could be leveraged by insiders seeking to inflict harm.Understanding the tools used in pentesting to prevent insider threats is crucial for organizations looking to bolster their defenses and safeguard against internal risks.

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.

Nature of the Insider Threat:

Identify the individual(s) involved in the insider threat incident and their roles within the organization.
Determine the motives behind the insider's actions, whether driven by financial gain, revenge, or other factors.

Affected Data and Systems:

- Identify the types of data compromised in the insider threat incident, such as user credentials, personal information, or proprietary assets.
- Determine the systems or platforms from which the data was accessed or exfiltrated, including email servers, databases, or cloud storage repositories.
- Assess the potential impact of the data breach on affected individuals, businesses, and partners, including financial losses, reputational damage.

Detection and Response Mechanisms:

- Evaluate the effectiveness of existing security controls and monitoring mechanisms in detecting the insider threat incident.
- Identify any gaps or weaknesses in the organization's detection and response capabilities, such as inadequate logging, insufficient access controls, or lack of user behavior analytics.
- Analyze the timeline of events leading up to the discovery of the insider threat and the subsequent response actions taken by the organization, including incident response protocols and coordination with law enforcement agencies .

Organizational Impact and Lessons Learned :

Assess the broader impact of the insider threat incident on Yahoo's business operations, brand reputation, and customer trust.

- Identify lessons learned from the incident and opportunities for improving security practices, employee training, and risk management strategies.
- Evaluate the effectiveness of post-incident remediation efforts, including security enhancements, policy revisions, and employee.

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

About the tool and the application chosen

KEYSTROKE

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.

Protect Yourself From Keylogging

Recognize these six pointers to protect yourself from malicious keyloggers.

Enable two-factor authentication

Don't download unknown files

Consider a virtual keyboard

Use a password manager

Install antivirus software

Consider voice-to-text conversion software

Steps of ethical hacking that you have done on your application using the chosen tool

KEYSTROKE on yahoo application:

Authorization: Yahoo would first authorize ethical hackers or a security consulting firm to conduct penetration testing or security assessments on its systems, networks, and applications.

Scope Definition: Yahoo and the ethical hacking team would define the scope of the assessment, including the specific systems, applications, and networks to be tested, as well as any limitations or constraints on the testing activities.

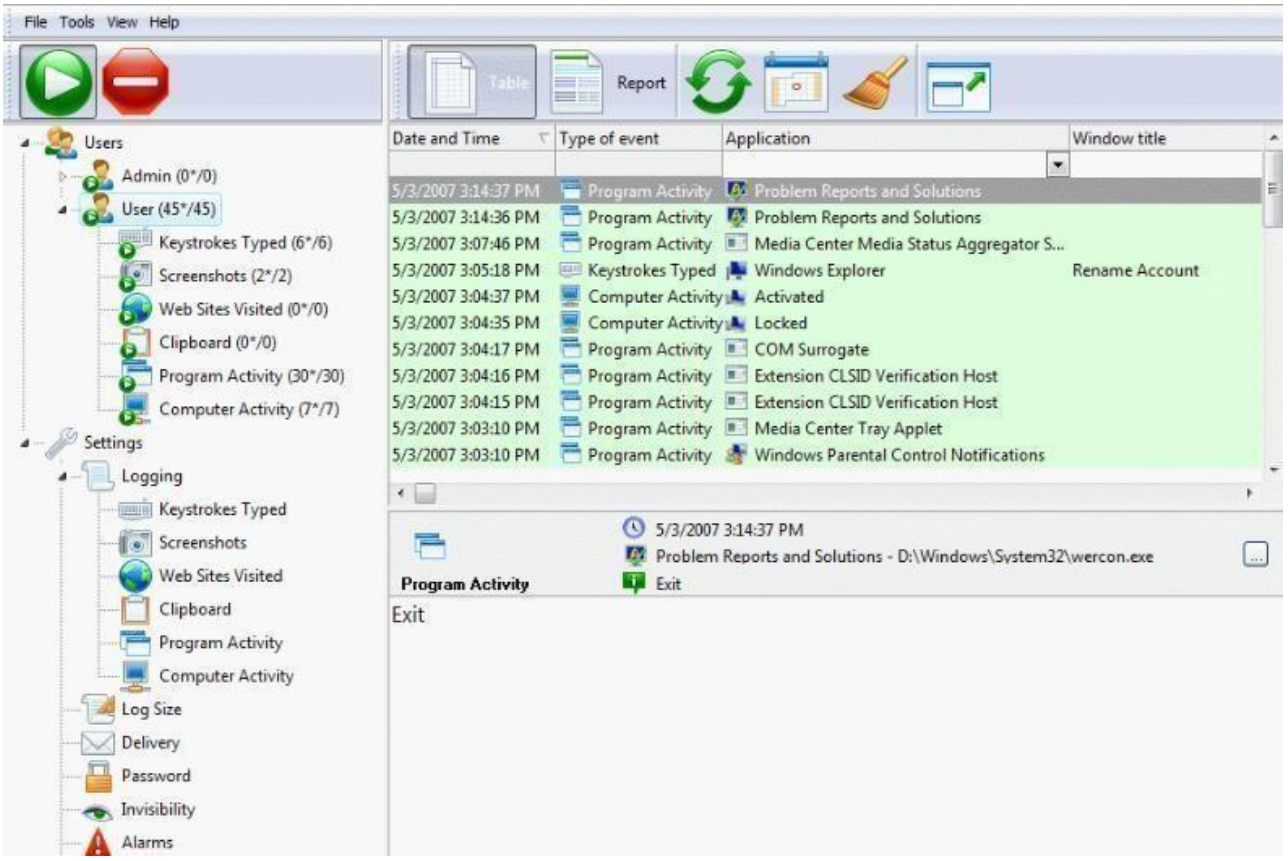
Information Gathering: Ethical hackers would gather information about Yahoo's infrastructure, including its network architecture, system applications, and security controls, to identify potential entry points and attack surfaces.

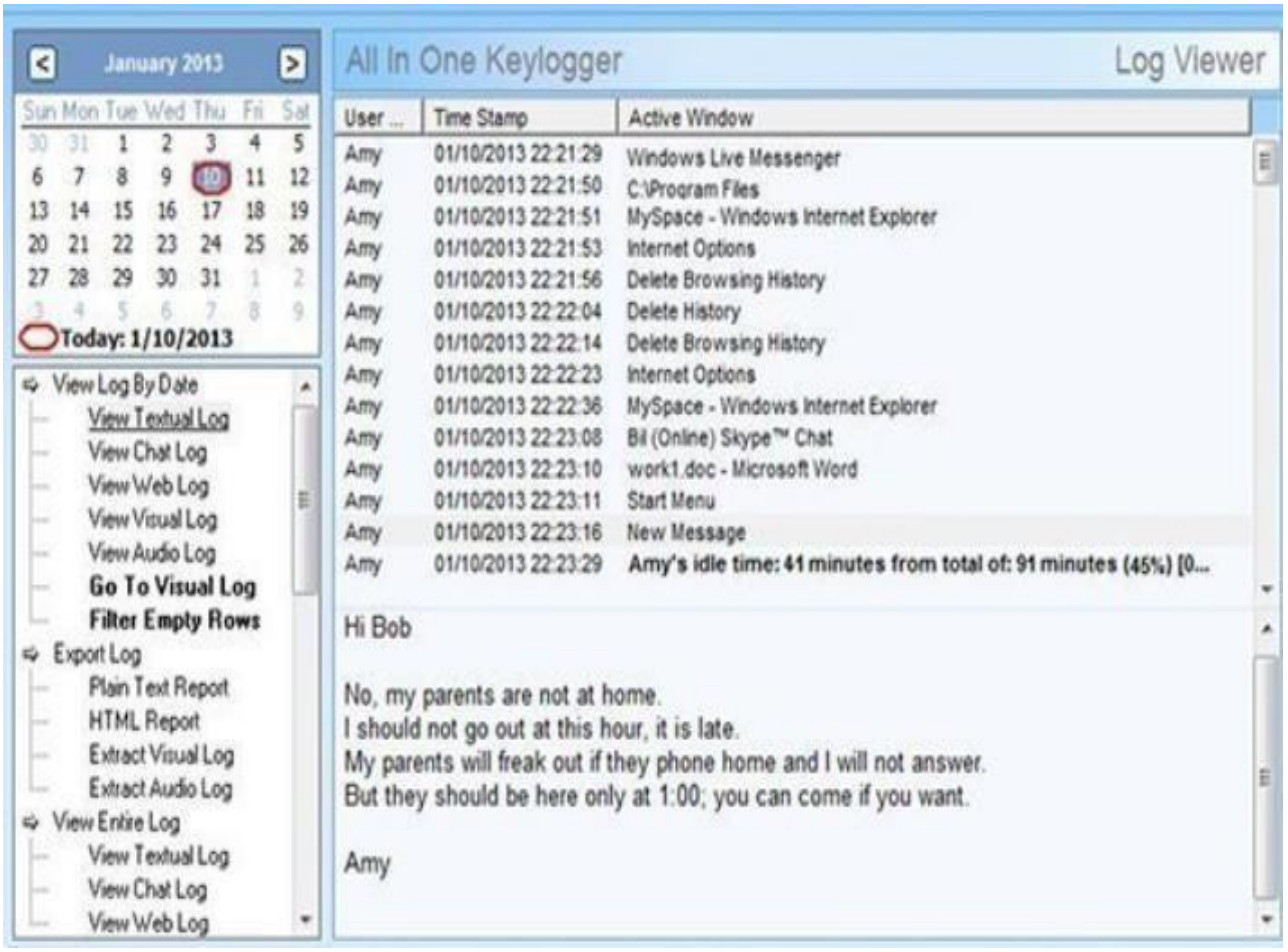
Vulnerability Assessment: Using a variety of tools and techniques, ethical hackers would scan Yahoo's systems and networks for known vulnerabilities, misconfigurations, and weaknesses that could be exploited by attackers.

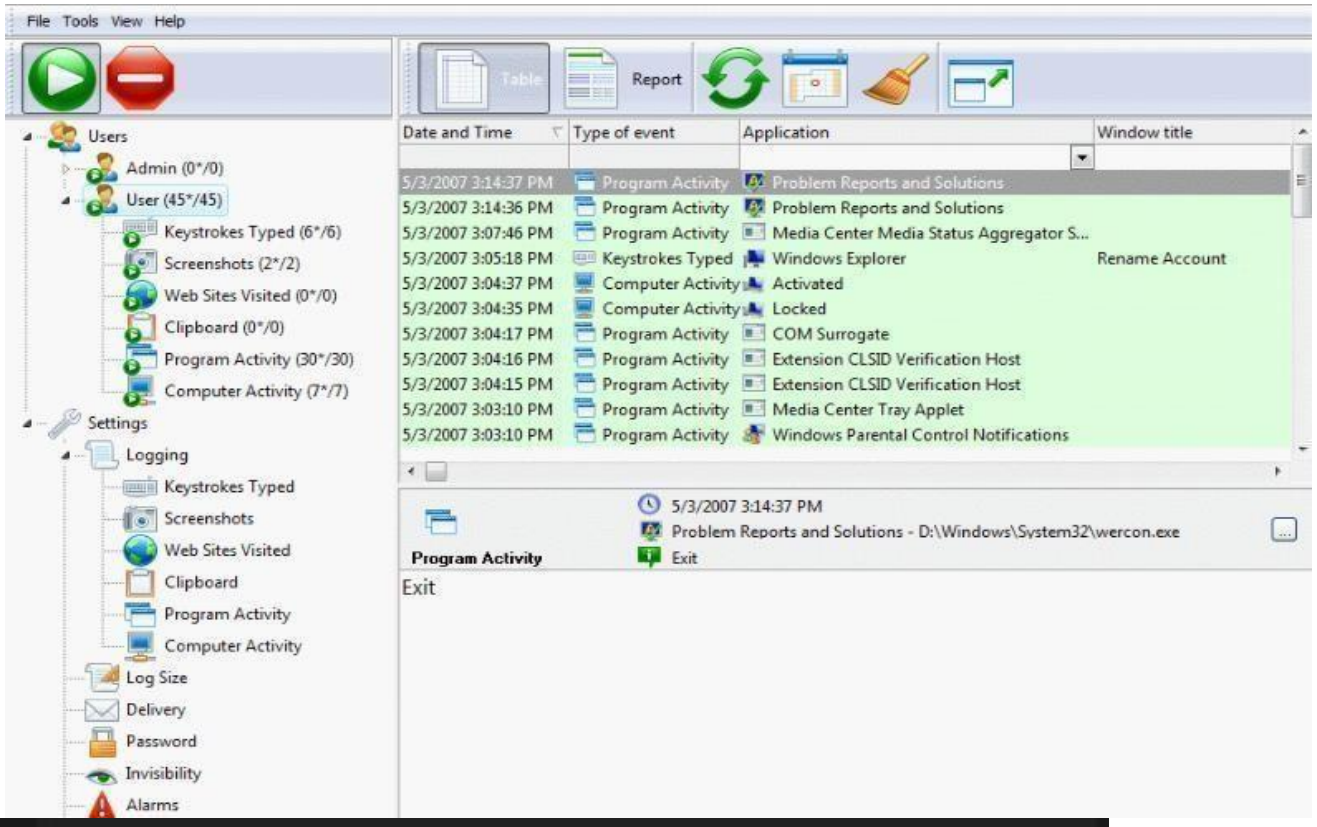
Exploitation: With authorization from Yahoo, ethical hackers would attempt to exploit identified vulnerabilities to demonstrate their impact and potential risk to the organization. This may include exploiting vulnerabilities to gain unauthorized access to systems, escalate privileges, or exfiltrate sensitive data.

Documentation and Reporting: Ethical hackers would document their findings, including details of vulnerabilities discovered, the methods used to exploit them, and recommendations for remediation. They would then provide a comprehensive report to Yahoo, outlining the security risks identified and proposing measures to address them.

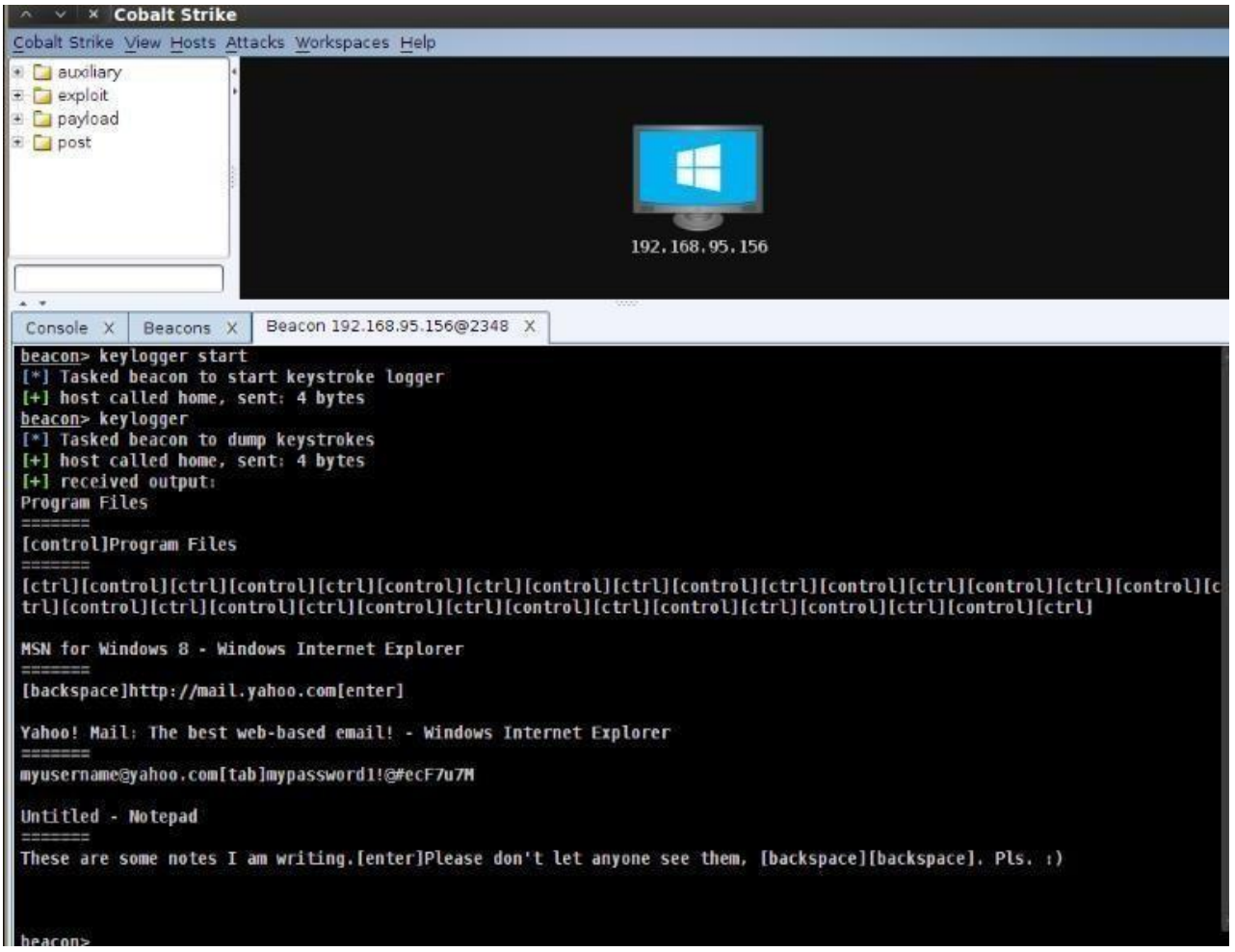
Screenshots of the implementation




January 2013
Sun Mon Tue Wed Thu Fri Sat
30 31 1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31 1 2
3 4 5 6 7 8 9
Today: 1/10/2013
View Log By Date
View Textual Log
View Chat Log
View Web Log
View Visual Log
View Audio Log
Go To Visual Log
Filter Empty Rows
Export Log
Plain Text Report
HTML Report
Extract Visual Log
Extract Audio Log
View Entire Log
View Textual Log
View Chat Log
View Web Log
All In One Keylogger
Log Viewer
User ... Time Stamp Active Window
Amy 01/10/2013 22:21:29 Windows Live Messenger
Amy 01/10/2013 22:21:50 C:\Program Files
Amy 01/10/2013 22:21:51 MySpace - Windows Internet Explorer
Amy 01/10/2013 22:21:53 Internet Options
Amy 01/10/2013 22:21:56 Delete Browsing History
Amy 01/10/2013 22:22:04 Delete History
Amy 01/10/2013 22:22:14 Delete Browsing History
Amy 01/10/2013 22:22:23 Internet Options
Amy 01/10/2013 22:22:36 MySpace - Windows Internet Explorer
Amy 01/10/2013 22:23:08 Bil (Online) Skype™ Chat
Amy 01/10/2013 22:23:10 work1.doc - Microsoft Word
Amy 01/10/2013 22:23:11 Start Menu
Amy 01/10/2013 22:23:16 New Message
Amy 01/10/2013 22:23:29 Amy's idle time: 41 minutes from total of: 91 minutes (45%) [0...
Hi Bob
No, my parents are not at home.
I should not go out at this hour, it is late.
My parents will freak out if they phone home and I will not answer.
But they should be here only at 1:00; you can come if you want.
Amy


File Tools View Help
Table
Report
Users
Admin (0*/0)
User (45*/45)
Keystrokes Typed (6*/6)
Screenshots (2*/2)
Web Sites Visited (0*/0)
Clipboard (0*/0)
Program Activity (30*/30)
Computer Activity (7*/7)
Settings
Logging
Keystrokes Typed
Screenshots
Web Sites Visited
Clipboard
Program Activity
Computer Activity
Log Size
Delivery
Password
Invisibility
Alarms
Date and Time
Type of event
Application
Window title
5/3/2007 3:14:37 PM Program Activity Problem Reports and Solutions
5/3/2007 3:14:36 PM Program Activity Problem Reports and Solutions
5/3/2007 3:07:46 PM Program Activity Media Center Media Status Aggregator S...
5/3/2007 3:05:18 PM Keystrokes Typed Windows Explorer Rename Account
5/3/2007 3:04:37 PM Computer Activity Activated
5/3/2007 3:04:35 PM Computer Activity Locked
5/3/2007 3:04:17 PM Program Activity COM Surrogate
5/3/2007 3:04:16 PM Program Activity Extension CLSID Verification Host
5/3/2007 3:04:15 PM Program Activity Extension CLSID Verification Host
5/3/2007 3:03:10 PM Program Activity Media Center Tray Applet
5/3/2007 3:03:10 PM Program Activity Windows Parental Control Notifications
Program Activity
5/3/2007 3:14:37 PM
Problem Reports and Solutions - D:\Windows\System32\wercon.exe
Exit
Exit


Keystroke Logger
ENABLE KEYBOARD
SET INPUT LANGUAGES
SET INPUT METHOD
START LOGGING
Enabling Keystroke Logger
Keystroke Logger provides a new Android input method. It is disabled by default, and for security reasons Android doesn't allow programs to change input method settings. Please follow the following steps to activate it.


Cobalt Strike
Cobalt Strike View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
192.168.95.156
Console X
Beacons X
Beacon 192.168.95.156@2348 X
beacon> keylogger start
[*] Tasked beacon to start keystroke logger
[+] host called home, sent: 4 bytes
beacon> keylogger
[*] Tasked beacon to dump keystrokes
[+] host called home, sent: 4 bytes
[+] received output:
Program Files
=======
[control]Program Files
=======
[ctrl][control][ctrl][control][ctrl][control][ctrl][control][ctrl][control][ctrl][control][ctrl][control][ctrl][control][c
trl][control][ctrl][control][ctrl][control][ctrl][control][ctrl][control][ctrl][control][ctrl][control][ctrl]
MSN for Windows 8 - Windows Internet Explorer
=======
[backspace]http://mail.yahoo.com[enter]
Yahoo! Mail: The best web-based email! - Windows Internet Explorer
=======
myusername@yahoo.com[tab]mypassword1!@#ecF7u7M
Untitled - Notepad
=======
These are some notes I am writing.[enter]Please don't let anyone see them, [backspace][backspace]. Pls. :)
beacon>

Conclusion

The insider threat at Yahoo, which occurred in 2014, resulted in one of the largest data breaches in history. It was revealed that hackers had gained unauthorized access to Yahoo's network and compromised the personal information of over 500 million users. The breach went undetected for several years before being disclosed by the company in 2016.Investigations into the breach uncovered evidence suggesting that the attack was carried out by state-sponsored actors, although specific attribution remains challenging. The attackers exploited vulnerabilities in Yahoo's systems to steal sensitive information, including names, email addresses, phone numbers, and encrypted passwords.The consequences of the breach were significant for Yahoo and its users. It damaged the company's reputation, led to a decline in user trust, and resulted in legal and regulatory scrutiny. Yahoo faced criticism for its handling of the breach, including delays in disclosure and perceived inadequacies in its security practices.

References

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