Index

TEAM 8.1:

B Venkata Mounish Reddy(VIT- VELLORE,20BSD0149)

Codavali Praveen Jahnavi(VIT-AP,20BCB7072)

Gantegampu Akshitha(VIT-AP, 20BCB7065)

Rayudu Gayatri(VIT-AP,20BCB7058)

TOPIC: Security Awareness Training: Developing and delivering security awareness training programs to educate employees about potential threats, safe practices, and the importance of cybersecurity.

1. Introduction:

1.1 Overview

Security awareness training is an important component of an organization's cybersecurity strategy. It entails training personnel and users about potential security dangers, best practises, and appropriate behaviours to adopt in order to safeguard sensitive data and prevent security breaches.

ABOUT THE ATTACKS

Phishing and Social Engineering:

Percentage: Phishing attacks account for a significant portion of cybercrimes, estimated to be around 80% of all cyberattacks.

Types of Attacks: Email phishing, spear phishing, pharming, vishing (voice phishing), and smishing (SMS phishing).

Hackers: Phishing attacks are typically carried out by individuals or organized groups who employ social engineering tactics to deceive and manipulate victims into disclosing sensitive information.

Ransomware Attacks:

Frequency: Ransomware attacks have seen a significant rise in recent years and account for a substantial portion of cybercrimes.

Types of Attacks: Encrypting ransomware, where files or systems are locked until a ransom is paid; leakware, where stolen data is threatened to be made public; and doxware, which combines encryption and data exfiltration.

Hackers: Ransomware attacks are often conducted by specialized criminal organizations or hacking groups that develop and distribute ransomware software, such as REvil, DarkSide, or Maze.

Data Breaches:

Frequency: Data breaches are prevalent and have affected numerous organizations across various industries, but exact percentages are difficult to quantify.

Types of Attacks: Network intrusions, SQL injections, stolen credentials, unpatched vulnerabilities, insider threats, and third-party breaches.

Hackers: Data breaches can be carried out by different threat actors, including nation-state-sponsored hackers, criminal syndicates, hacktivist groups, or even insiders with malicious intent.

Identity Theft:

Frequency: Identity theft is a widespread issue, affecting a significant number of individuals globally, but it is challenging to assign an exact percentage.

Types of Attacks: Phishing, malware, data breaches, social engineering, and online scams.

Hackers: Identity theft can involve a range of actors, including individual hackers, organized criminal networks, and even state-sponsored entities seeking personal information for intelligence purposes or financial gain.

Online Fraud:

Frequency: Online fraud encompasses various fraudulent activities, making it challenging to provide an exact percentage breakdown.

Types of Attacks: Business email compromise (BEC), credit card fraud, investment scams, romance scams, and fake online marketplaces.

Hackers: Online fraud perpetrators range from individual fraudsters to organized criminal networks that employ sophisticated techniques to deceive victims and illicitly obtain funds or sensitive information.

DDoS Attacks:

Frequency: DDoS attacks account for a smaller portion of cybercrimes but can still cause significant disruption to targeted entities.

Types of Attacks: Volumetric attacks, such as UDP floods or ICMP floods; application layer attacks, such as HTTP floods or SYN floods; and reflective amplification attacks.

Hackers: DDoS attacks can be carried out by various actors, including hacktivist groups, criminal organizations offering DDoS-for-hire services, or individuals seeking to cause disruption or extortion.

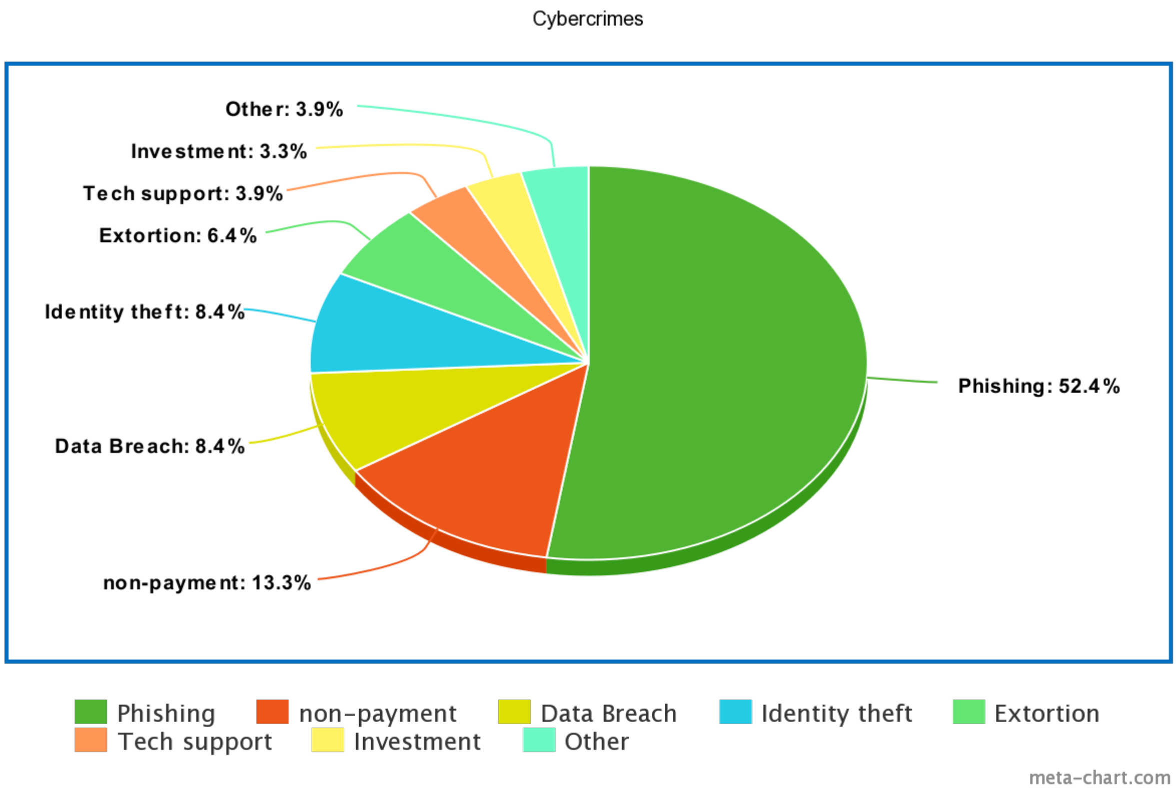
Cyber Espionage:

Frequency: Cyber espionage incidents are typically more targeted and less prevalent compared to other cybercrimes, making it challenging to assign a specific percentage.

Types of Attacks: Advanced Persistent Threats (APTs), spear phishing, zero-day exploits, supply chain attacks, and targeted malware.

Hackers: Cyber espionage activities are often attributed to nation-state-sponsored hacking groups seeking political, economic, or military advantages. Examples include APT28 (Fancy Bear), APT29 (Cozy Bear), and Equation Group.

Statistics of cybercrimes in 2021:



1.2 Purpose

Important features of security awareness training:

1. Threat Awareness: Training sessions are designed to increase awareness of various cybersecurity risks like as phishing emails, social engineering, malware, and ransomware, as well as the need of being diligent in recognising and reporting suspicious activity.

2. Password Security: Employees are trained on the importance of creating strong, unique passwords as well as the importance of frequently updating and not sharing passwords.

3. Phishing Awareness: Employees are taught to be careful of suspicious emails, attachments, or URLs that may lead to the compromise of sensitive information in order to recognise and avoid phishing attacks.

4. Data Protection: Emphasis is placed on the significance of securing sensitive data and adhering to data protection policies, such as secure file handling, encryption, and secure disposal of sensitive information.

5. Device Security: Best practises for safeguarding devices are highlighted, including setting password protection, encrypting data, and exercising caution while using public Wi-Fi networks.

6. Social Engineering Awareness: Employees are trained on the social engineering techniques used by attackers to trick them into disclosing personal information, emphasising the importance of verifying identities and being wary of unexpected demands.

7. Incident Reporting: Employees are encouraged to report any security incidents, suspicious actions, or potential breaches to the proper organisational channels as soon as possible.

8. Compliance and Regulations: Employees are educated on industry-specific compliance regulations such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act) to ensure they understand their responsibilities while managing sensitive data.

Security awareness training should be done on a regular basis and reinforced via interactive sessions, simulations, quizzes, and continuous communication channels. It contributes to the development of a security-conscious culture within the organisation and lowers the chance of successful cyber assaults caused by human error or negligence.

Information gathering:

Information gathering is a crucial step in various domains, such as cybersecurity, intelligence gathering, marketing research, and competitive analysis. It involves collecting relevant data and insights to understand a target, make informed decisions, or gain a competitive advantage

DNS Info Gathering:

- DNS info gathering involves collecting information about a target's domain name system (DNS) infrastructure. This includes discovering the target's registered domain names, IP addresses, subdomains, and mail servers. Attackers can use various techniques to gather this information, such as DNS zone transfers, DNS enumeration, or DNS reconnaissance tools.

- By analyzing DNS records, an attacker can gain insights into the target's infrastructure and potentially identify vulnerabilities or points of entry. For example, misconfigured DNS settings or outdated software versions could be exploited to gain unauthorized access. Additionally, DNS info gathering can help identify potential targets for social engineering or phishing attacks.

Email Footprinting:

- Email footprinting focuses on gathering information about an individual or organization through their email communications. This can involve analyzing email headers, email addresses, and email content. Email footprinting techniques include email header analysis, email address enumeration, and searching for publicly available email addresses associated with the target.

- By analyzing email footprints, an attacker can gather information such as organizational structure, email server configurations, or potential targets for spear phishing attacks. It can also provide insights into relationships, communication patterns, and potential vulnerabilities within the target organization.

Social Engineering:

- Social engineering is a technique that exploits human psychology to manipulate individuals into revealing sensitive information or taking specific actions. It can involve impersonating someone, creating a sense of urgency or trust, or exploiting psychological biases.

- Social engineering attacks can take various forms, such as phishing emails, phone calls, or physical interactions. Attackers may attempt to gather information like usernames, passwords, or confidential data through these methods. Social engineering attacks rely on manipulating human behavior rather than technical vulnerabilities to achieve their goals.

- Common social engineering techniques include pretexting (creating a false scenario), baiting (offering something enticing), or phishing (sending fraudulent emails). The success of social engineering attacks relies heavily on the attacker's ability to gather and use relevant information about the target.

Web Scraping:

- Web scraping involves automatically extracting data from websites. It can be used for legitimate purposes, such as market research, competitor analysis, or data aggregation. However, it can also be employed for malicious activities if used to gather sensitive or proprietary information without permission.

- Web scraping techniques involve writing scripts or using specialized tools to navigate websites, parse HTML structures, and extract relevant data. It can involve scraping product details, customer reviews, pricing information, or any other data publicly available on websites.

- While web scraping itself may not involve intrusive methods, scraping websites without proper authorization or in violation of the website's terms of service can be illegal and unethical.

Types of vulnerability paths and parameters:

Input Validation Vulnerabilities:

Input validation vulnerabilities occur when input data is not properly validated, allowing attackers to inject malicious input. Common parameters to consider are user input fields, HTTP request parameters, or command-line arguments. To identify these vulnerabilities, you can perform techniques like fuzz testing (sending malformed or unexpected input), boundary value analysis (testing input at the limits of valid values), or static code analysis (analyzing the code for potential input validation issues).

Authentication and Authorization Vulnerabilities:

Authentication and authorization vulnerabilities involve weaknesses in the mechanisms that verify and control access to systems or resources. Parameters to examine include login forms, session management tokens, or access control policies. Vulnerability identification methods include penetration testing (attempting to bypass authentication mechanisms), security code reviews, or analyzing access control configurations.

Cross-Site Scripting (XSS):

XSS vulnerabilities occur when untrusted data is included in web pages without proper sanitization, allowing attackers to inject and execute malicious scripts. Parameters susceptible to XSS attacks are typically found in user input fields, URL query parameters, or HTTP request headers. To identify XSS vulnerabilities, you can perform manual code reviews, use automated vulnerability scanners, or conduct penetration testing with payloads designed to trigger XSS attacks.

SQL Injection:

SQL injection vulnerabilities arise when untrusted data is included in SQL queries without proper sanitization, enabling attackers to manipulate the queries and potentially gain unauthorized access to databases. Parameters vulnerable to SQL injection attacks include user input fields or URL query parameters used in database queries. Methods to identify SQL injection vulnerabilities involve manual code analysis, input validation testing, and the use of vulnerability scanning tools designed to detect SQL injection patterns.

Buffer Overflows:

Buffer overflow vulnerabilities occur when a program attempts to write data beyond the boundaries of a fixed-size buffer, potentially leading to code execution or crashes. Parameters susceptible to buffer overflows are typically found in functions that accept user input and copy it into buffers without proper bounds checking. Identifying buffer overflow vulnerabilities involves manual code analysis, fuzz testing, or using specialized tools designed to detect buffer overflow conditions.

Misconfiguration:

Misconfiguration vulnerabilities arise from incorrect or insecure configurations of systems, applications, or network devices. Common parameters to consider are security settings, access controls, or network configurations. Methods to identify misconfiguration vulnerabilities include configuration reviews, vulnerability scanning, manual inspection of system configurations, or using automated tools designed to detect misconfigurations.

Methods used to identify vulnerabilities:

Vulnerability Scanning: Vulnerability scanning involves using automated tools to scan systems, networks, or applications for known vulnerabilities. These tools compare the target environment against a database of known vulnerabilities and provide a report highlighting potential weaknesses. Vulnerability scanners can identify issues such as outdated software versions, missing patches, misconfigurations, or common security flaws.

Penetration Testing: Penetration testing, also known as ethical hacking, involves authorized attempts to exploit vulnerabilities in a controlled environment. Skilled security professionals simulate real-world attacks to identify weaknesses in systems, applications, or networks. This method helps identify vulnerabilities that automated scanners may miss, and it provides insights into potential attack vectors and their impact on the target.

Code Review and Static Analysis: Manual code review involves analyzing the source code of applications or software to identify security vulnerabilities. Security professionals examine the code for common coding mistakes, insecure coding practices, or potential logic flaws. Static analysis tools can also be used to automatically analyze the code and detect potential vulnerabilities based on predefined rules or patterns.

Security Audits and Configuration Reviews: Security audits involve assessing the security posture of systems, networks, or applications against established security standards, best practices, or compliance requirements. Configuration reviews focus on examining the settings and configurations of various components to identify misconfigurations, weak security controls, or unnecessary privileges. These reviews can be performed manually or with the help of automated tools.

Web Application Testing: Web application testing involves evaluating the security of web applications and identifying vulnerabilities specific to web technologies. This can include techniques such as input validation testing, cross-site scripting (XSS) testing, SQL injection testing, and session management testing. Automated tools, manual testing, or a combination of both can be used for web application testing.

Security Information and Event Management (SIEM) Solutions: SIEM solutions collect and analyze security logs and events from various systems and applications. By monitoring and correlating these logs, SIEM solutions can help identify patterns or indicators of potential vulnerabilities or attacks. They provide real-time visibility into security incidents and can help detect emerging threats or unusual behavior.

Bug Bounty Programs: Bug bounty programs incentivize individuals or security researchers to identify vulnerabilities in systems or applications by offering rewards. Organizations establish these programs to leverage the expertise of the broader security community in identifying and reporting vulnerabilities. Bug bounty programs can provide an additional layer of vulnerability identification and encourage responsible disclosure.

2. Literary Survey

2.1 Existing problems

Business impact of vulnerabilities:

Data Breaches: Vulnerabilities in a business's cybersecurity infrastructure can lead to data breaches, where sensitive customer information, intellectual property, or financial data is compromised. Data breaches can result in financial losses due to legal penalties, remediation costs, and loss of customer trust. The business may also face reputational damage and a decline in customer loyalty.

Financial Losses: Vulnerabilities can be exploited by malicious actors to carry out fraud, theft, or financial manipulation. This can result in direct financial losses for the business, such as stolen funds or unauthorized transactions. Additionally, the costs associated with investigating and addressing the vulnerabilities can be significant.

Disruption of Operations: Exploitation of vulnerabilities can lead to the disruption or complete shutdown of critical business operations. For example, a vulnerability in a manufacturing process could cause production delays or product quality issues, leading to financial losses and damage to the business's reputation.

Regulatory Non-Compliance: Many industries have specific regulations and compliance requirements related to data protection, privacy, and security. If a business fails to address vulnerabilities and experiences a data breach or other security incident, it may face legal and regulatory consequences, including fines and penalties.

Loss of Intellectual Property: Vulnerabilities can expose a business's intellectual property, including trade secrets, proprietary information, or research and development data. Competitors or malicious actors may exploit these vulnerabilities to steal or misuse the intellectual property, which can significantly impact the business's competitive advantage and future growth prospects.

Operational Inefficiencies: Vulnerabilities in internal systems or processes can lead to operational inefficiencies. For example, a vulnerability in a supply chain management system could result in inventory inaccuracies, leading to disruptions in the supply chain, delays in fulfilling customer orders, and increased costs.

Damage to Brand Reputation: When a business experiences security breaches or other vulnerabilities, it can damage its brand reputation and erode consumer trust. News of a breach can spread quickly, leading to negative publicity, loss of customers, and difficulty in attracting new customers. Rebuilding trust and repairing a damaged brand can be a time-consuming and expensive process.

RECENT ATTACKS

1. **Microsoft Azure SSRF Vulnerabilities**

Microsoft Azure services were susceptible to server-side request forgery (SSRF) attacks on January 17, 2023, due to four vulnerabilities. Azure Functions, Azure Machine Learning, and Azure Digital Twins were among the services offered. Lidor Ben Shitrit, an Orca researcher, claims that if these SSRF vulnerabilities had gone unpatched, they might have had a substantial effect on Microsoft Azure Services. These vulnerabilities were closed before they could do much harm thanks to Microsoft's quick response.

2. Slack GitHub Account Hack

Slack, one of the most well-liked commercial communication applications, was hacked on December 29, 2022. CyberInt, an Israeli security company, was responsible for the incident. The investigation showed that a small number of employee tokens were taken and used improperly to access a GitHub project that was hosted externally. On December 27, the threat actor had also downloaded private code repositories, although neither the main codebase for Slack nor any client data were contained in those downloads. Slack quickly nullified the stolen tokens and got to work looking into how it might have affected their clients. The threat actor did not gain access to any other parts of Slack's system or client information, it was discovered.

3. Data of 228 Million Deezer Users Stolen

The well-known music streaming service Deezer, which has millions of customers worldwide, revealed a serious data breach that may have impacted millions of Deezer members when a hacker offered information from more than 200 million users for sale on a hacking website. Deezer claims that the data breach occurred in 2019 and that the hackers were successful in acquiring a copy of user data from a third-party service provider, with whom they had not collaborated since 2020.Deezer asserted that it had taken all necessary steps to work with the third-party service provider and ensure that security measures were in place. These steps included obtaining ISO 27001 and SOC 2 certifications, contractual obligations to secure data, GDPR-compliant data protection agreements, and certificates of data destruction at the conclusion of the engagement.

4. Twitter Leaks Data on 200 Million Users

On December 4th, 2023, a data gathering sale including more than 200 million Twitter profiles began. A 59 GB RAR bundle containing the stolen material was made public. The scrapers utilising earlier data collections were able to compromise the vulnerable API. Awareness of targeted phishing scam campaigns is advised for Twitter users. A threat actor on a cyber forum offered a data collection with more than 200 million Twitter profiles for sale on December 4th, 2023, for eight credits, which were finally made accessible for free on November 27, 2022. A second data dossier allegedly containing details on 17 million people was apparently making its way around secretly in November. Threat actors have been selling and sharing enormous data collections of scraped Twitter user accounts since July 22, 2022, on a variety of online hacker forums and markets dedicated to criminality. These accounts featured both personal and work email addresses, usernames, screen names, follower counts, account creation dates, and other publicly available information.

5. Malware Targets 30+ WordPress Plugins

For malicious intents, the Linux Trojan Application takes advantage of out-of-date WordPress plugins and themes. The malicious application has two versions, the second of which is an enhanced version of the first. Even if the plugins are updated, it's possible that the attackers will continue to target WordPress site administrators' accounts. A Linux backdoor worm has been found that can exploit about 30 WordPress plugins in order to insert malicious JavaScript code and send users to fraudulent, phishing websites that the attackers have constructed. Such exploits are possible because outdated plugin and theme versions are present on the susceptible WordPress sites. As a result, the attackers are able to execute these assaults because as soon as a user accesses a WordPress website that has been hacked, they are immediately forwarded to a malicious website

6. Kubernetes Clusters Hacked

Vulnerable images and improperly configured PostgreSQL servers were used as two possible points of attack. The attack's motivation is money-making and cryptocurrency mining. Cluster security for Kubernetes is a laborious task that must be completed. The threat actors behind the Kinsing Crypto Jacking operation have been observed using unprotected and incorrectly configured PostgreSQL servers in order to get early access to Kubernetes systems. Golang, a high level programming language designed to develop cloud native applications, was used to write the malware known as Kinsing. It is put together using Go 1.13.6. Typically, Linux installations are the major targets of this malware for cryptocurrency mining. The objective changes to invading other PCs once the malware has been successfully deployed and is operating successfully on the victim's system. Two attack vectors were used, according to an analysis of the attack by Microsoft security researchers. Establishing and listing the PostgreSQL servers that had setup problems is the first attack path. The "trust authentication" setting, which enables PostgreSQL to assume that any connection made to the server is authorised to gain database access, is one of the most frequent configuration errors that were being abused from there. Additionally, any IP address that the attacker may be using can be utilised to access the server if a security flaw results in a wide range of IP addresses being assigned. The second attack strategy aims to take advantage of a vulnerability in container images.

7. Marriott Data Breach (2018)

Marriott International reported a data breach that exposed personal information of approximately 500 million guests, highlighting the significant impact of cyber attacks on the hospitality industry.

8. Equifax Data Breach (2017)

Equifax, one of the largest credit reporting agencies, experienced a data breach that exposed sensitive personal information of approximately 147 million individuals, including social security numbers and financial data.

9. The Emergence of RaaS Gangs

A number of Ransomware as a Service gangs, ranging from Doppelpaymer and REvil to Vice Society and Nevada, have posed substantial risks to businesses, individuals, and governments all around the world. Some were politically motivated, such as the Conti gang, while others, such as Vice Society, virtually solely target schools and other educational institutions. The advent of RaaS has compelled government agencies to reconsider security.

10. Attack on Tallahassee Memorial

Tallahassee Memorial Hospital provides 772-beds and special care units in 21 counties around North Florida. The hospital's IT systems were damaged by a suspected ransomware attack, forcing it to shut down all online processes for more than a week. All elective surgical procedures have to be rescheduled. Many patients were relocated to other facilities.

11. Attack on VMare ESXi

VMware ESXi is a Hypervisor that allows virtual machines to run. The corporation released a fix for the vulnerable OpenSLP in 2021, however it appears that many servers were not patched. "The ransomware encrypts files with the.vmxf,.vmx,.vmdk,.vmsd, and.nvram extensions on compromised ESXi servers and creates a.args file for each encrypted document"

12. Bank Accounts Hacked in Nepal

The police have arrested eight criminal actors in Kathmandu, Nepal, for hacking into bank accounts. The attackers used WhatsApp to distribute the Android package kit (APK) for a bogus app called Nepali Keti. They then stole money by hacking into the bank accounts of anyone who downloaded the programme.

13. XSS vulnerabilities found in DMS providers

The attack had happened on February 7 2023. Its targets were OnlyOffice, OpenKM, LogicalDOC, Mayan. Four DMS providers were said to have an XSS vulnerability -

CWE - 79. The firms provide both free and freemium services. Rapid7 uncovered the zero-day vulnerabilities during a routine inspection.

14. 71 million request-per-second HTTP DDoS attack thwarted by CloudFare

Cloudflare thwarted the greatest known DDoS attack on February 14, 2023, with 71 million requests per second. The attack targeted gaming platforms, cryptocurrency organisations, and hosting providers, among others, which utilise Cloudflare to secure their websites. The assault used HTTP/2 and included 30,000 IP addresses.

15. Dish Network faced a data breach

Dish Network, one of the largest television providers in the United States, confirmed that the earlier reported network disruption was caused by a cyber assault. The underlying causes of the intrusion have yet to be discovered. The attack resulted in data theft and a breakdown in internal communication. Some data was extracted and Dish's share fell by 6.5%

16. US Marshals Service faces ransomware attack

The US Marshals Service is in charge of sensitive operations such as federal judge security, fugitive apprehension, and so on. Attackers hacked the standalone USMS system, exposing data connected to USMS investigations.

17. T-Mobile Data Breach

T-Mobile, a wireless telecommunications operator in the United States, disclosed on January 19, 2023, that a bad actor had acquired access to some customer data via a weak API. According to their declaration, the breach exposed sensitive data such as credit card information or social security numbers.

18. Attack on AirFrance and KLM

Two major airlines, AirFrance and KLM, confirmed unauthorised access to consumer data in a recent study. Some personally identifiable information about Flying Blue customers was revealed as a result of the assault. However, no Passport, financial, or social security information was compromised. Flying Blue is a customer loyalty programme operated by several airlines.

19. Windows ALPC Zero Day

According to Microsoft, "A malicious user who successfully exploited this vulnerability could gain SYSTEM privileges." Particularly, on January 10, 2023, Microsoft released 98 updates, including one for the ALPC zero-day vulnerability.

20. Attack on Mailchimp

Mailchimp discovered unauthorised access to several Mailchimp accounts on January 11, 2023. Social engineering was employed by attackers to gain employee credentials for a tool utilised by MailChimp's customer-facing workers. According to Mailchimp's announcement, the hack was restricted to 133 accounts. The impacted accounts were shut down on January 12th and later reactivated.

21. A third-party data breach affected Nissan North America

Nissan North America revealed a data breach that occurred in June 2022 on January 16, 2023. The bad actor targeted a third-party vendor who had limited access to client data for development purposes. Nissan started an inquiry in September 2022, which revealed that the hack took advantage of the vendor's poorly built database.

22. Attack on PayPal customers

Credential stuffing is a cyber-attack in which hackers use automated techniques to submit thousands of stolen user IDs and passwords into consumer input areas. Credential stuffing works because people have a habit of using the same credentials for several accounts. For two days, hackers had full names, dates of birth, social security numbers, postal addresses, and individual tax identification numbers of 34,942 PayPal members.

23. Attack on schools in Tucson, Arizona, and Nantucket

Tucson Unified School District is the largest school district in Southern Arizona. Since their data was encrypted by a ransomware attack on the last weekend of January, the schools were forced to switch to an offline method of education. The hackers have demanded a ransom and threatened to reveal stolen material if payment is not made.

24. Exposition of Yandex source code

Yandex is a significant Russian technology corporation. Recently, 44.7GB of code repositories were uploaded as a Torrent on a hacker forum. According to the poster, the files contain Yandex Git resources. The corporation has denied that it was hacked. It has blamed the theft on a former employee and stated that the leaked source code is no longer in use.

25. Killnet targets US hospitals with DDoS attacks

KillNet is a Russian hacktivist organisation that has actively targeted US healthcare facilities, including Stanford University. The US Department of Health and Human Services has issued a warning about the attacks. KillNet is well-known for assaulting countries who fought back against Russia's invasion of Ukraine. Additionally, in Kaspersky's most recent quarterly report, 57000 DDoS attacks were registered in three months. DDoS attacks increased by 79% in 2022.

26. Attack on ION Group

After launching a ransomware attack against ION Cleared Derivatives, a part of ION Markets, on January 31, the Russian RaaS gang LockBit added ION Group to their data leak site, threatening to reveal sensitive investor data. This had considerable impact on derivative trading in Europe, the United States, and the United Kingdom.

27. Capcom Ransomware Attack (2020)

Gaming company Capcom was targeted by ransomware, resulting in a data breach and theft of sensitive information.

28. Garmin Ransomware Attack (2020)

Garmin, a GPS technology company, experienced a ransomware attack that disrupted their services for several days.

29. Blackbaud Data Breach (2020)

Blackbaud, a cloud software provider for nonprofits, suffered a data breach, potentially exposing personal information of millions of individuals.

30. Twitter Bitcoin Scam (2020)

Hackers compromised high-profile Twitter accounts to promote a Bitcoin scam, tricking users into sending funds to fraudulent addresses.

31. EasyJet Data Breach (2020)

EasyJet, a major airline, experienced a data breach, affecting approximately nine million customers.

32. Maze Ransomware Attacks (2019-2020)

Maze ransomware operators targeted numerous organizations, encrypting their data and demanding ransom payments.

33. Garmin Ransomware Attack (2020)

Garmin, a GPS technology company, experienced a ransomware attack that disrupted their services for several days.

34. Travelex Ransomware Attack (2019)

Foreign exchange company Travelex suffered a ransomware attack, causing their services to be offline for weeks.

35. MGM Resorts Data Breach (2019)

Personal details of more than 10 million guests of MGM Resorts were exposed on a hacking forum.

36. Wawa Data Breach (2019)

Wawa, a convenience store chain, experienced a data breach, compromising payment card information of millions of customers.

37. **Capital One Data Breach (2019)**

A former employee of Capital One gained unauthorized access to their systems, compromising personal information of over 100 million customers.

38. **Marriott Data Breach (2018)**

Marriott International suffered a data breach, exposing personal information of approximately 500 million guests.

39. **British Airways Data Breach (2018)**

British Airways experienced a data breach, compromising personal and financial information of around 380,000 customers.

40. **Facebook-Cambridge Analytica Scandal (2018)**

The personal data of millions of Facebook users were harvested by Cambridge Analytica for political profiling.

41. **SolarWinds Attack (2020)**

Hackers inserted malware into SolarWinds software, compromising numerous organizations, including government agencies and tech companies.

42. **Colonial Pipeline Ransomware Attack (2021)**

A ransomware attack forced the Colonial Pipeline, a major fuel pipeline operator in the US, to shut down operations, causing fuel shortages in several states.

43. **Microsoft Exchange Server Hack (2021)**

State-sponsored hackers exploited vulnerabilities in Microsoft Exchange Servers, compromising thousands of organizations worldwide.

44. **JBS Ransomware Attack (2021)**

JBS, one of the world's largest meat processors, was targeted by a ransomware attack, causing temporary shutdowns in their operations.

45. Kaseya Supply Chain Attack (2021)

Hackers exploited vulnerabilities in Kaseya's software to deploy ransomware on managed service providers' systems, affecting numerous businesses.

46. Accellion FTA Data Breach (2021)

Cybercriminals targeted Accellion's file transfer application, exposing sensitive data from various organizations, including government entities and financial institutions.

47. CD Projekt Red Ransomware Attack (2021)

The game developer CD Projekt Red experienced a ransomware attack that resulted in the theft of source code for their games.

48. Facebook Data Leak (2021)

A massive data leak exposed personal information of over 500 million Facebook users, which was posted on a hacking forum.

49. Capcom Ransomware Attack (2020)

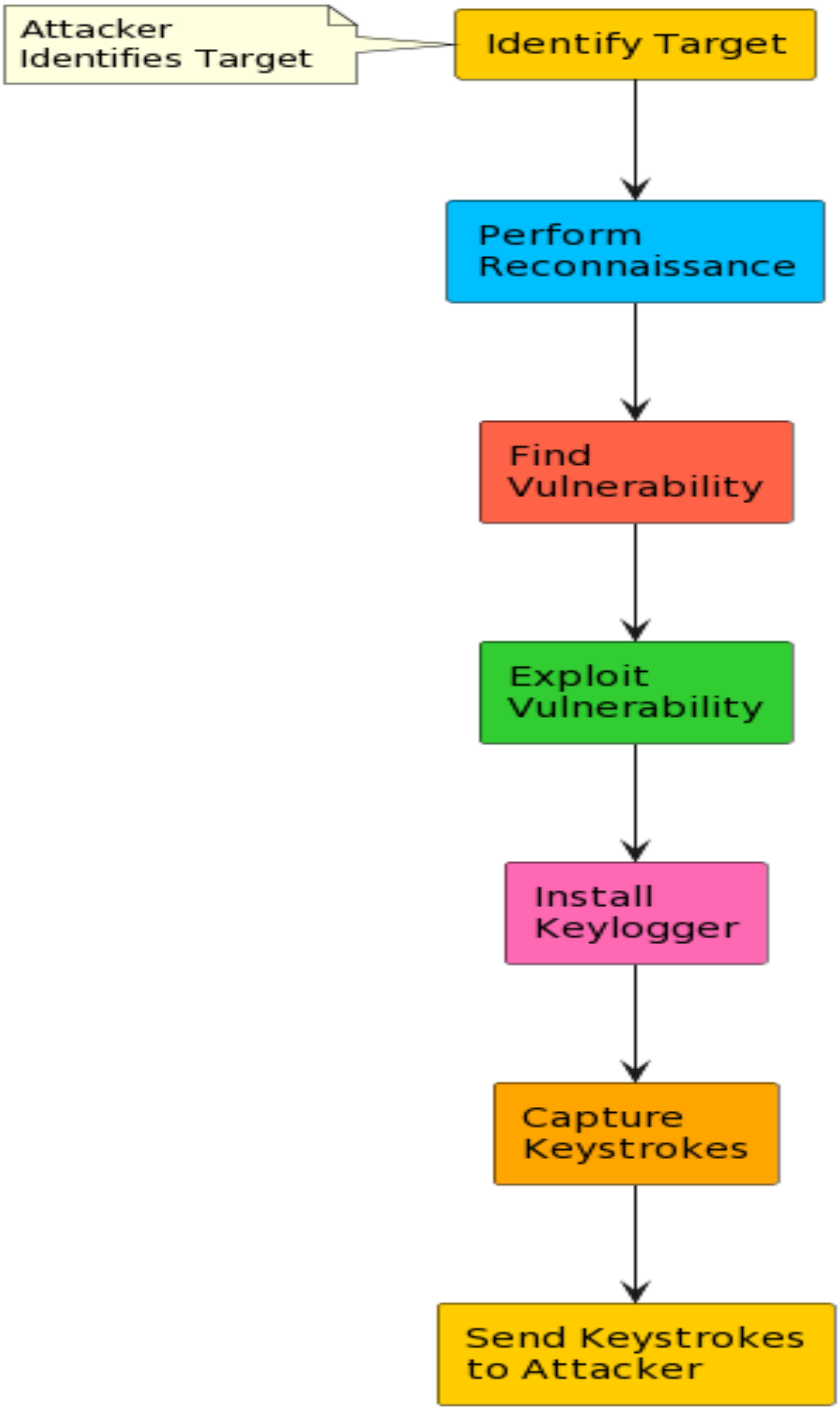
Gaming company Capcom was targeted by ransomware, resulting in a data breach and theft of sensitive information.

50. ASUS Live Update Attack (2019)

Hackers targeted ASUS, a prominent computer hardware manufacturer, by injecting malware into their official software update tool, potentially compromising millions of users.

3. THEORITICAL ANALYSIS

3.1 Block diagram for Keylogger attack:



A keylogger attack is a type of cyber-attack where a malicious actor installs software or hardware on a target system to capture and record keystrokes made by the user. This attack allows the attacker to collect sensitive information such as passwords, credit card numbers, or personal messages.

Theoretical overview of the attack:

1. Delivery: The attacker needs to deliver the keylogger to the target system. This can be done through various means, such as email attachments, malicious downloads, infected websites, or physical access to the target device.
2. Installation: Once the keylogger is delivered to the target system, the attacker needs to install it. This can be achieved through social engineering techniques, exploiting vulnerabilities in the operating system or software, or physical access to the device. The keylogger can be installed as software or as a physical device connected to the system.
3. Execution: After installation, the keylogger starts running in the background, capturing and recording keystrokes made by the user. The keylogger may also capture other information, such as clipboard contents, screenshots, or mouse movements, depending on its capabilities.
4. Data Collection: The captured keystrokes are stored by the keylogger, usually in a hidden file or sent to a remote server controlled by the attacker. The attacker can access the collected data later to extract sensitive information.
5. Persistence: To ensure long-term access to the victim's data, the attacker may configure the keylogger to start automatically with the system or hide its presence to evade detection by antivirus or security software.
6. Exfiltration: Periodically or upon specific triggers, the keylogger may send the collected data to the attacker's command-and-control server. This can be done through various communication channels, such as email, FTP, or a remote server.
7. Exploitation: Once the attacker receives the captured data, they can analyse it to extract valuable information like passwords, login credentials, financial details, or other sensitive data. The attacker can then use this information for various malicious purposes, such as identity theft, financial fraud, or unauthorized access to the victim's accounts.

3.2 Hardware / Software designing Requirements:

A computer system with USB ports for connecting the USB drive.

Python: A programming language used to write the keylogger code.

Python to EXE Library: A library used to convert Python code into an executable file.

Text Editor or Integrated Development Environment (IDE): To write and edit the Python code.

Operating System: Compatible with Python and Python to EXE library.

4. EXPERIMENTAL INVESTIGATIONS

1. Keystroke Logging:
   - The keylogger successfully captures and logs keystrokes entered by the user.
   - Each keystroke is recorded in a log file, typically stored on the attacker's machine or in a predetermined location.

2. Captured Information:
   - The log file contains a record of every keystroke made by the user during the attack.
   - This includes sensitive information such as login credentials, credit card numbers, personal messages, or any other text input made by the user.

3. Data Transmission:
   - The keylogger may employ various methods to transmit the captured data to the attacker.

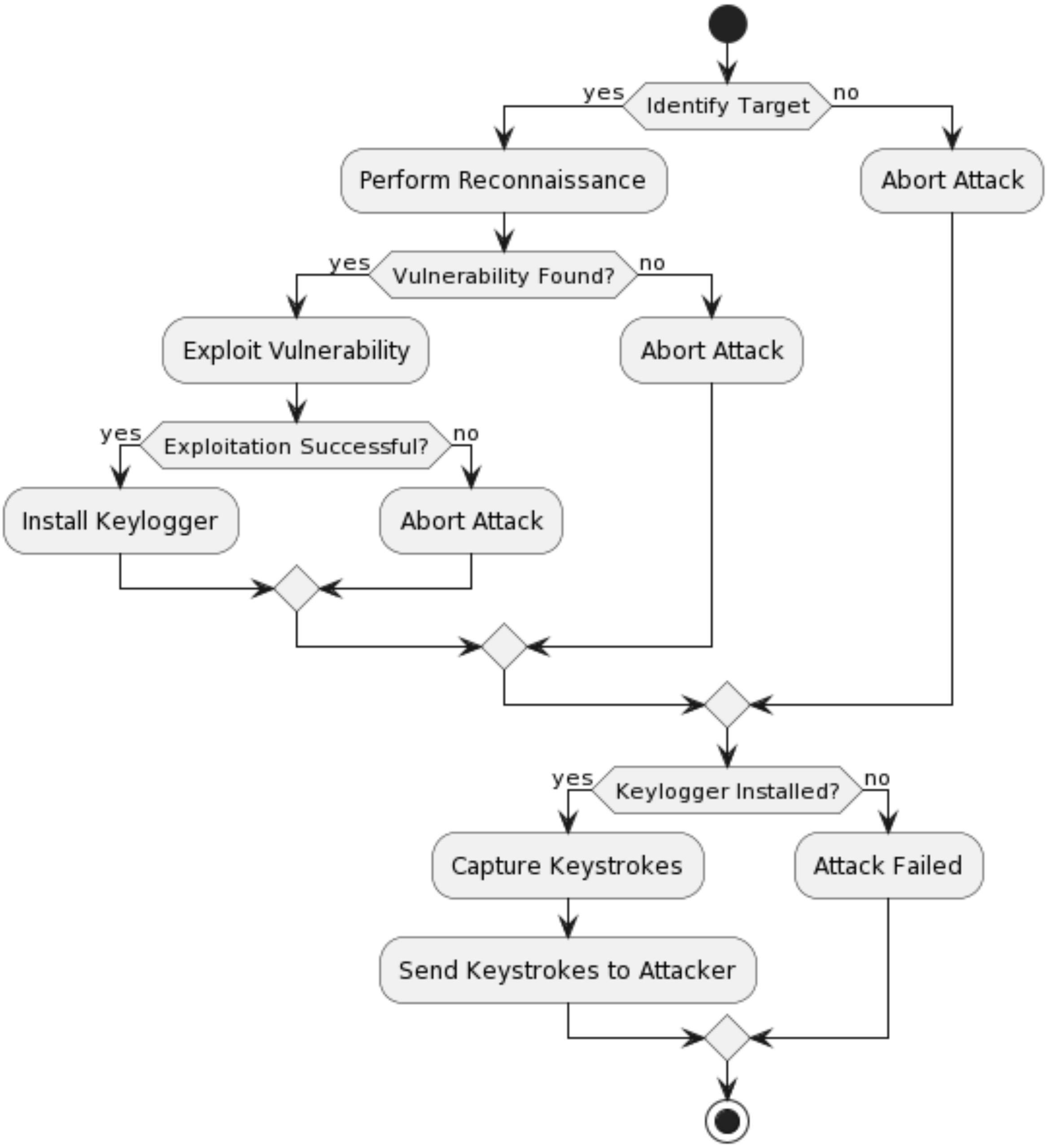
- This could involve sending the log file via email, uploading it to a remote server, or utilizing covert channels for communication.

4. Detection and Evasion:
   - Keyloggers strive to remain undetected to prolong their data collection efforts.
   - They may use techniques like rootkit functionality or camouflage themselves as legitimate processes to evade detection by antivirus software or other security measures.

5. Risks and Consequences:
   - The captured keystrokes pose significant risks to the user's privacy, sensitive information, and online security.
   - The attacker may exploit the captured data for identity theft, financial fraud, or unauthorized access to the user's accounts or systems.

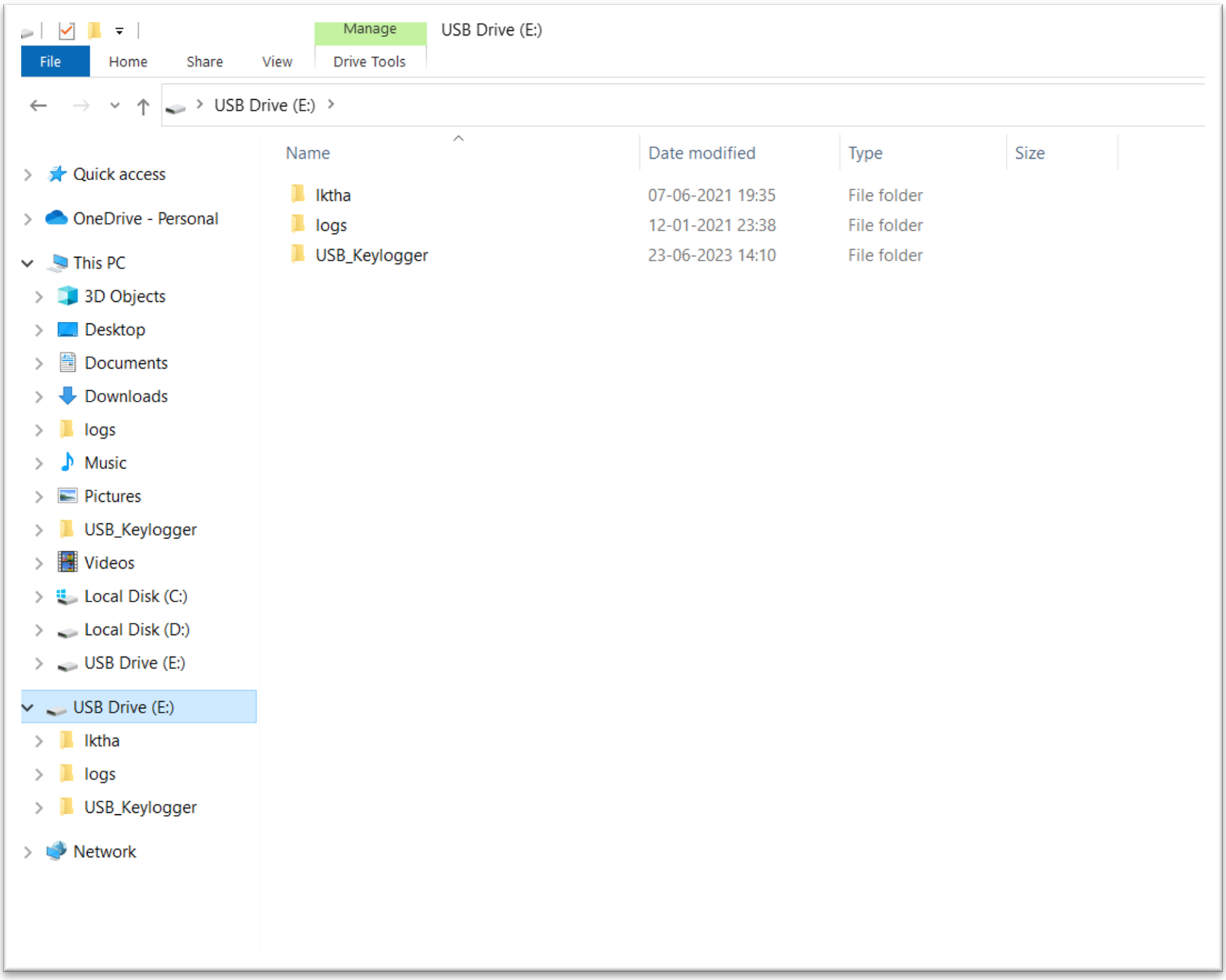
6. Mitigation and Prevention:
   - Users can protect themselves from keylogger attacks by practicing good cybersecurity hygiene.
   - Implementing strong and unique passwords, using two-factor authentication, and keeping software and systems up to date can help mitigate the risks.
   - Employing robust antivirus and anti-malware solutions can also assist in detecting and preventing keylogger infections.

5. FLOWCHART


Identify Target
yes
no
Perform Reconnaissance
Abort Attack
Vulnerability Found?
yes
no
Exploit Vulnerability
Abort Attack
Exploitation Successful?
yes
no
Install Keylogger
Abort Attack
Keylogger Installed?
yes
no
Capture Keystrokes
Attack Failed
Send Keystrokes to Attacker

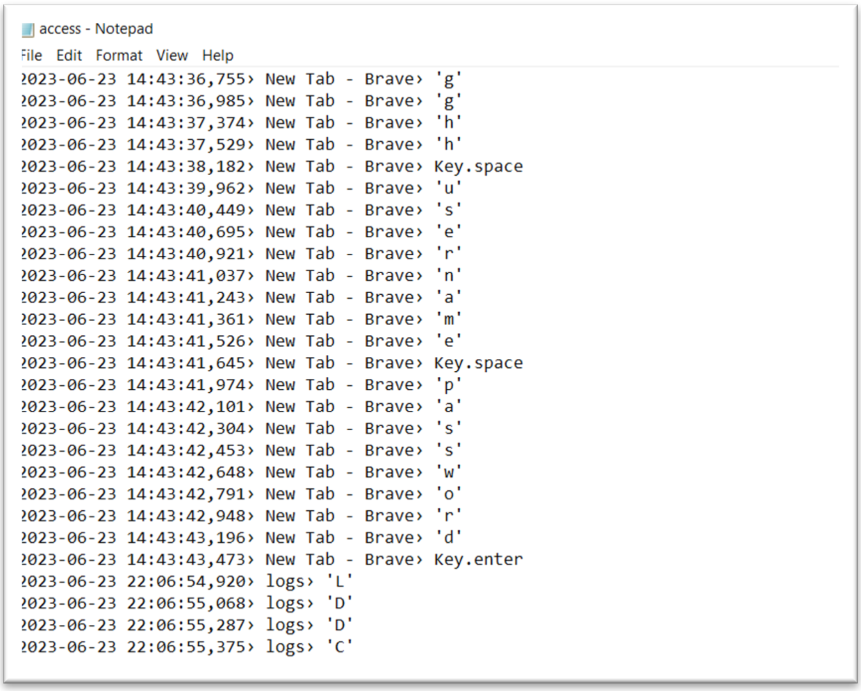
6. RESULT

Insert the USB drive:



Name	Date modified	Type	Size
Iktha	07-06-2021 19:35	File folder	
logs	12-01-2021 23:38	File folder	
USB_Keylogger	23-06-2023 14:10	File folder	

The log file starts capturing the keystrokes:



```
2023-06-23 14:43:36,755› New Tab - Brave› 'g'
2023-06-23 14:43:36,985› New Tab - Brave› 'g'
2023-06-23 14:43:37,374› New Tab - Brave› 'h'
2023-06-23 14:43:37,529› New Tab - Brave› 'h'
2023-06-23 14:43:38,182› New Tab - Brave› Key.space
2023-06-23 14:43:39,962› New Tab - Brave› 'u'
2023-06-23 14:43:40,449› New Tab - Brave› 's'
2023-06-23 14:43:40,695› New Tab - Brave› 'e'
2023-06-23 14:43:40,921› New Tab - Brave› 'r'
2023-06-23 14:43:41,037› New Tab - Brave› 'n'
2023-06-23 14:43:41,243› New Tab - Brave› 'a'
2023-06-23 14:43:41,361› New Tab - Brave› 'm'
2023-06-23 14:43:41,526› New Tab - Brave› 'e'
2023-06-23 14:43:41,645› New Tab - Brave› Key.space
2023-06-23 14:43:41,974› New Tab - Brave› 'p'
2023-06-23 14:43:42,101› New Tab - Brave› 'a'
2023-06-23 14:43:42,304› New Tab - Brave› 's'
2023-06-23 14:43:42,453› New Tab - Brave› 's'
2023-06-23 14:43:42,648› New Tab - Brave› 'w'
2023-06-23 14:43:42,791› New Tab - Brave› 'o'
2023-06-23 14:43:42,948› New Tab - Brave› 'r'
2023-06-23 14:43:43,196› New Tab - Brave› 'd'
2023-06-23 14:43:43,473› New Tab - Brave› Key.enter
2023-06-23 22:06:54,920› logs› 'L'
2023-06-23 22:06:55,068› logs› 'D'
2023-06-23 22:06:55,287› logs› 'D'
2023-06-23 22:06:55,375› logs› 'C'
```

SECURITY BEST PRACTICES

Use tougher security questions

Using more stringent security questions is important to enhance the verification process and prevent imposters from gaining access.

Characteristics of a good security question:

An effective security question should meet the following criteria:

- Safety: It should be difficult for hackers to guess or find the answer through research.
- Stability: The answer should remain consistent over time and not change frequently.
- Memorability: Users should be able to easily remember their chosen security question and its answer.

- Simplicity: The question should be straightforward and precise, making it easy for users to provide accurate responses.

- Variety: The question should have numerous possible answers, ensuring a wide range of valid responses.

Enable multi-factor authentication (MFA)

- Implementing multi-factor authentication (MFA) is crucial for safeguarding sensitive data against unauthorized access.

- By combining various elements such as biometrics, SMS/text messages, emails, and security questions, users can add extra layers of protection to their sign-in process.

- Use additional layers of protection: Text verification, email verification, and time-based security codes can also be employed for enhanced security.

Create a strong password policy

Organizations should establish a robust password policy to protect their networks. This includes implementing practices such as using longer passwords, combining uppercase and lowercase letters, numbers, and symbols, avoiding dictionary words and sequential keyboard paths, regularly changing passwords, and utilizing password managers.

Embrace cybersecurity training

- Conduct regular cybersecurity awareness training for employees to educate them about common threats and best practices.

- Encourage a culture of security consciousness, emphasizing the importance of responsible online behavior.

Create data backups

Creating data backups is another vital measure to ensure the security of personal and business data in the event of a ransomware attack. Continuous backups, preferably stored on remote servers in the cloud, can help restore data in case of a system breach.

Perimeter Security:

- Utilize firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) to monitor and filter incoming and outgoing network traffic.
- Implement strong access controls, such as secure authentication and authorization mechanisms, to protect network boundaries.

Endpoint Protection:

- Deploy robust antivirus/anti-malware solutions on all endpoints (computers, laptops, mobile devices) to detect and mitigate malicious software.

- Apply regular security patches and updates to operating systems and software to address known vulnerabilities.

Secure Network Architecture:

- Implement secure network segmentation to isolate critical systems and data from the rest of the network.

- Use virtual private networks (VPNs) to encrypt data transmission and secure remote access.

Access Control:

- Enforce the principle of least privilege, granting users only the necessary access privileges for their roles.
- Implement strong password policies, including complex passwords, multi-factor authentication (MFA), and password expiration.

Email Security:

- Employ email filtering and anti-spam solutions to block malicious attachments and phishing attempts.

- Train employees on identifying and reporting suspicious emails or phishing attempts.

Data Backup and Recovery:

- Regularly back up critical data and ensure backups are stored securely and offline to protect against ransomware attacks.

- Test data restoration processes periodically to ensure backups are reliable and usable.

Incident Response and Monitoring:

- Implement a robust incident response plan to detect, respond to, and recover from security incidents effectively.
- Use security information and event management (SIEM) systems and intrusion detection systems to monitor and analyze network activity for suspicious behavior.

Vendor and Third-Party Risk Management:

- Assess and monitor the security practices of vendors and third-party service providers to ensure they meet your organization's standards.

- Implement contractual agreements that include specific security requirements and obligations.

Regular Security Assessments and Audits:

- Conduct regular security assessments, penetration testing, and vulnerability scanning to identify and address weaknesses in the system.

- Perform periodic audits to ensure compliance with industry standards and regulatory requirements

7. Advantages and Disadvantages of cybersecurity

Advantages	
Protection against Data Breaches:	Cybersecurity measures help safeguard sensitive data, preventing unauthorized access, data breaches, and data loss. This protects individuals' personal information and helps organizations maintain the trust of their customers.
Mitigation of Financial Loss:	Effective cybersecurity practices can help mitigate financial losses associated with cyberattacks. By preventing unauthorized access, data theft, and system disruptions, organizations can avoid the financial impact of recovering from such incidents.
Safeguarding Intellectual Property:	Cybersecurity measures protect valuable intellectual property and trade secrets from theft or unauthorized disclosure. This is especially crucial for businesses that rely on their intellectual property for competitive advantage and innovation.
Maintenance of Business Continuity:	Cybersecurity helps ensure the continuity of business operations by minimizing disruptions caused by cyber incidents. By implementing robust security measures, organizations can mitigate the risk of system downtime, financial loss, and reputational damage.
Compliance with Regulations:	Many industries and jurisdictions have specific cybersecurity regulations and compliance requirements. By implementing cybersecurity measures, organizations can fulfill their legal obligations and avoid penalties.

Disadvantages	
Implementation Challenges:	Implementing and maintaining robust cybersecurity measures can be complex and resource-intensive. It requires specialized knowledge, skilled professionals, and ongoing investments in technology, training, and infrastructure.
False Sense of Security:	While cybersecurity measures are essential, they may create a false sense of security if not implemented comprehensively. Organizations may assume they are adequately protected but overlook vulnerabilities or fail to address emerging threats effectively.
Potential for User Inconvenience:	Strong cybersecurity measures such as complex passwords, multi-factor authentication, and frequent security updates can inconvenience users. Balancing security and usability is a challenge to ensure that security measures do not hinder productivity or frustrate users.
Evolving Nature of Threats:	Cyber threats continually evolve, with attackers finding new vulnerabilities and attack vectors. Cybersecurity measures need to adapt and stay up to date with emerging threats, requiring constant monitoring, threat intelligence, and proactive security measures.
Cost considerations:	Effective cybersecurity can be expensive, particularly for small businesses or organizations with limited resources. Investments in technology, personnel, and ongoing maintenance can strain budgets, making it challenging for some organizations to implement comprehensive cybersecurity measures.

8. APPLICATIONS

Scope of cybersecurity

Information Security:

This includes securing sensitive data, intellectual property, and personally identifiable information (PII) from unauthorized access, theft, or disclosure. It involves implementing measures such as encryption, access controls, and data classification.

Network Security:

Network security focuses on protecting computer networks from unauthorized access, attacks, and disruptions. It involves implementing firewalls, intrusion detection/prevention systems, virtual private networks (VPNs), and network segmentation to secure network infrastructure and prevent unauthorized access.

Application Security:

Application security involves protecting software applications from vulnerabilities and ensuring they are free from security flaws. It includes secure coding practices, secure software development lifecycle (SDLC), and regular security testing (e.g., penetration testing) to identify and mitigate vulnerabilities in applications.

Endpoint Security:

Endpoint security focuses on securing individual devices (endpoints) such as computers, laptops, mobile devices, and IoT devices. It includes measures such as antivirus/anti-malware software, endpoint encryption, and device management to protect against malware, unauthorized access, and data breaches.

Cloud Security:

As organizations increasingly adopt cloud computing, cloud security becomes critical. It involves securing cloud-based infrastructure, platforms, and services. This includes access controls, encryption, data segregation, and monitoring to ensure the security and privacy of cloud-based resources.

Incident Response:

Incident response is the process of handling and responding to security incidents effectively. It includes incident detection, containment, eradication, and recovery, as well as post-incident analysis and learning to improve future incident response capabilities.

Security Governance and Risk Management:

This involves establishing security policies, procedures, and frameworks to manage and mitigate risks effectively. It includes risk assessments, security awareness training, compliance with regulations and standards, and establishing a security culture within organizations.

Security Operations and Monitoring:

Security operations involve continuous monitoring, analysis, and response to security events and threats. It includes security information and event management (SIEM), threat intelligence, log monitoring, and security incident response to detect and respond to security incidents promptly.

Privacy and Data Protection:

Privacy and data protection focus on safeguarding individuals' personal information and complying with privacy regulations. It involves implementing privacy controls, data encryption, consent management, and data breach notification processes.

Emerging Technologies:

With the rapid evolution of technologies such as artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT), cybersecurity needs to adapt and address the unique challenges and risks associated with these technologies.

9. CONCLUSION

Security awareness training is an important component of an organization's entire cybersecurity strategy. Organisations may greatly minimise the risk of security breaches and data compromises by educating staff and users on potential threats, best practises, and right security behaviours.

Employees become more knowledgeable about various cyber dangers, such as phishing, malware, and social engineering, as a result of security awareness training, allowing them to recognise and respond correctly to possible risks. They understand the value of strong passwords, secure data handling, and device security in order to keep critical information safe.

Furthermore, security awareness training promotes an organisational culture of attention and responsibility. Employees are urged to report issues as soon as possible and to adhere to established security processes, which strengthens the organization's overall security posture.

Regular training sessions, interactive simulations, and continuous communication channels are critical for increasing security awareness and adjusting to emerging threats. Employees become an active line of defence against cyber threats by staying aware and updated on cybersecurity best practises, enhancing the organization's overall resilience.

Lastly, security awareness training equips employees with the knowledge they need to make educated decisions, protect sensitive data, and contribute to a secure digital environment. It is a critical investment that assists organisations in reducing the risks connected with cyber threats and protecting their precious assets.

10. FUTURE SCOPE

The future scope our project can include:

1. Personalised Training: As technology progresses, security awareness training can take use of personalised learning methods. This comprises customised training content based on a person's role, level of knowledge, and specific areas of vulnerability. Adaptive learning systems, virtual reality simulations, and AI-driven training modules can all be used to give personalised training.

2. Gamification and Interactive Training: Gamification components like challenges, leaderboards, and awards can be used into security awareness training to boost participation and information retention. Employees can gain hands-on experience by using interactive training modules, simulations, and realistic scenarios.

3. Continuous Training and Microlearning: Given the rapid evolution of cybersecurity threats, security awareness training will progressively shift towards continuous learning. Microlearning modules will provide regular updates and reminders on emerging dangers, new attack strategies, and best practises in compact and easily digestible formats.

4. Behavioural Analytics: Organisations can use behavioural analytics to monitor and analyse user behaviour in order to discover potential security issues or abnormalities. Organisations can spot patterns, detect suspicious activity, and give focused training interventions to address specific areas of concern by collecting and analysing data on user interactions.

5. Phishing Simulations and Red Team Exercises: Organisations will continue to perform phishing simulations and red team exercises to evaluate the efficacy of security awareness training. These exercises imitate real-world circumstances, allowing organisations to measure employee reactions, discover vulnerabilities, and fine-tune training programmes as needed.

6. Mobile and Remote Workforce Training: As remote work and mobile devices become more prevalent, security awareness training will evolve to address the particular problems and hazards that these environments present. To guarantee consistent security practises across multiple work environments, training programmes will focus on secure remote access, secure communication technologies, and safe use of personal devices.

7. Technology Integration: Security awareness training will be integrated with developing technologies like artificial intelligence, machine learning, and natural language processing. Chatbots or virtual assistants powered by AI can provide immediate assistance and direction, while machine learning algorithms can analyse training data to discover trends, personalise training content, and predict future risks.

8. Cultural Shift and Leadership Support: Organisations will recognise the importance of establishing a cybersecurity culture from the top down. Leadership commitment and support for cybersecurity awareness will be critical in creating a secure environment and motivating staff to prioritise security in their daily activities.

Overall, the future of security awareness training will be defined by the use of modern technology, personalised learning methodologies, continuous training, and a comprehensive organisational approach to cybersecurity.

11. BIBILOGRAPHY

Reference

- OWASP (Open Web Application Security Project): https://owasp.org/
- NIST (National Institute of Standards and Technology): https://www.nist.gov/
- SANS Institute: https://www.sans.org/
- CERT (Computer Emergency Response Team) Division: https://www.cert.org/
- Anti-Phishing Working Group (APWG): https://apwg.org/
- United States Federal Trade Commission (FTC): https://www.ftc.gov/
- National Cybersecurity and Communications Integration Center (NCCIC): https://www.us-cert.gov/ncas/tips/ST04-014
- PhishTank: https://www.phishtank.com/
- Microsoft Security: https://www.microsoft.com/security/blog/?f=332.25
- US-CERT (United States Computer Emergency Readiness Team): https://www.us-cert.gov/ncas/tips/ST04-001
- Symantec Security Response: https://www.symantec.com/security-center/writeup/2003-091113-0914-99
- McAfee Blogs: https://www.mcafee.com/blogs/tag/keylogger/
- SANS Institute: https://www.sans.org/security-awareness-training/resources/benefits-cybersecurity
- University of California, Berkeley: https://www.ocf.berkeley.edu/~jamiechang/advdis-sec.html
- Cybersecurity and Infrastructure Security Agency (CISA) Advisories: https://www.cisa.gov/cisa-advisories
- Recorded Future: https://www.recordedfuture.com/
- Kaspersky Threat Intelligence: https://www.kaspersky.com/blog/category/threat-intelligence/
- FireEye Threat Research Blog: https://www.fireeye.com/blog/threat-research.html
- Dark Reading: https://www.darkreading.com/