T.R.
USKUDAR UNIVERSITY
INSTITUTE OF SCIENCE

DEPARTMENT OF CYBER SECURITY

MASTER'SDEGREE PROGRAM OF CYBER SECURITY

MASTER'S DEGREE THESIS

USING STORM-BREAKER, A SOCIAL ENGINEERING TO ANALYZE PENETRATION LEVELS AND DEVELOP ATTACK PREVENTION STRATEGIES FOR ANDROID DEVICES.

Muhammed Nmakatun Umar

Thesis Advisor
Assist. Prof. Dr. Salim Jibrin Danbatta

ISTANBUL-2024

T.R.
USKUDAR UNIVERSITY
INSTITUTE OF SCIENCE

DEPARTMENT OF CYBER SECURITY

MASTER'SDEGREE PROGRAM OF CYBER SECURITY

MASTER'S DEGREE THESIS

USING STORM-BREAKER, A SOCIAL ENGINEERING TO ANALYZE PENETRATION LEVELS AND DEVELOP ATTACK PREVENTION STRATEGIES FOR ANDROID DEVICES.

Muhammed Nmakatun Umar

Thesis Advisor
Assist. Prof. Dr. Salim Jibrin Danbatta

ISTANBUL-2024

ABSTRACT

Using Storm-Breaker, A social Engineering to Analyze Penetration levels and Develop Attack prevention strategies for Android Devices.

The internet has long been an essential component of international communication and is now dominant in people's daily lives all around the world. The internet is now much more usable, accessible, and efficient thanks to technological improvements and lower costs.

On the contrary, social engineering assaults have emerged as a key security concern in both the real and virtual spheres of cyber space, through some malicious programs, individuals are targeted by convincing them to reveal private information or do other activities that compromise security. However, this study involves the use of storm-breaker as a social engineering tool to analyze penetration levels and develop attack prevention strategies for android devices. The experiment was conducted using a complete controlled experimental designed, the data obtained from the stimulation attacks done in an android, iOS device was limited only to tester device so as to ensure data privacy policy. The study was carried out in an environment where the test subject and the attacker were in close access to each other to guarantee that the data acquired was only from the experimental scenario. The study employed identity masquerade techniques in a homelike setting to simulate an online attack. VMWare, Ngrok, Storm-Breaker, Kali Linux, and a social messaging app were among the tools utilized in the study.

The attack was then performed by sending the link into 5 different people through social messaging application, the data was then collected and the analysis was conducted. The data collected from one of the victim's devices, which was running iOS 17.4.1 and had the public IP address 151.135.40.157, the link was accessed via Facebook 458.0.0.34.108. With an eight-core processor, all recorded voice notes are saved in the image folder. The statistical analysis was performed base on the information obtained from the victims and was analyzed in the result discussion. However, simulations performed with all other browsers successfully captured detailed information about the target device. In contrast, the Safari browser demonstrated a reverse attack, capturing and displaying the details and image of the attacker instead of the victim. This behavior is attributed to the unique security architecture implemented in Safari.

Keywords: Cyber-Attack, Cyber security, Social Engineering, Cyber Crime, Cyber Criminal, Storm-Breaker, Ethical Hacking.

ABSTRACT

Using Storm-Breaker, A social Engineering to Analyze Penetration levels and Develop Attack prevention strategies for Android Devices.

The internet has long been an essential component of international communication and is now dominant in people's daily lives all around the world. The internet is now much more usable, accessible, and efficient thanks to technological improvements and lower costs.

On the contrary, social engineering assaults have emerged as a key security concern in both the real and virtual spheres of cyber space, through some malicious programs, individuals are targeted by convincing them to reveal private information or do other activities that compromise security. However, this study involves the use of storm-breaker as a social engineering tool to analyze penetration levels and develop attack prevention strategies for android devices. The experiment was conducted using a complete controlled experimental designed, the data obtained from the stimulation attacks done in an android, iOS device was limited only to tester device so as to ensure data privacy policy. The study was carried out in an environment where the test subject and the attacker were in close access to each other to guarantee that the data acquired was only from the experimental scenario. The study employed identity masquerade techniques in a homelike setting to simulate an online attack. VMWare, Ngrok, Storm-Breaker, Kali Linux, and a social messaging app were among the tools utilized in the study.

The attack was then performed by sending the link into 5 different people through social messaging application, the data was then collected and the analysis was conducted. The data collected from one of the victim's devices, which was running iOS 17.4.1 and had the public IP address 151.135.40.157, the link was accessed via Facebook 458.0.0.34.108. With an eight-core processor, all recorded voice notes are saved in the image folder. The statistical analysis was performed base on the information obtained from the victims and was analyzed in the result discussion. However, simulations performed with all other browsers successfully captured detailed information about the target device. In contrast, the Safari browser demonstrated a reverse attack, capturing and displaying the details and image of the attacker instead of the victim. This behavior is attributed to the unique security architecture implemented in Safari.

Keywords: Cyber-Attack, Cyber security, Social Engineering, Cyber Crime, Cyber Criminal, Storm-Breaker, Ethical Hacking.

ACKNOWLEDGEMENT

My supervisor, Dr. Salim Jibrin Danbatta, has my sincere gratitude for his invaluable assistance. Your advice and experience were really beneficial.

I am deeply grateful to my instructors and mentors, especially Dr. Salim Jibrin Danbatta, for their insightful guidance and knowledge.

To my friends and family, your continuous emotional support has helped me get through this journey. I will be eternally grateful to my parents for their unfailing love and support throughout every obstacle. And I can't thank you enough for endlessly correcting my English and punctuation mistakes; your support means everything to me.

I'm also grateful to the numerous resources, references, and publications that have helped me along the journey.

Above all, I praise God Almighty for abundantly gifting me with life, direction, and all that has contributed to my achievement. Thank you for being my helper and sustainer throughout everything.

FORM OF DECLARATION

In this context, I certify that I followed all academic regulations when gathering data and documents for this study, that I presented all written, visual, and auditory data and findings in accordance with scientific ethics, that I did not manipulate any data used, that I cited my sources in accordance with accepted scientific practices, and that, with the exception of the cited instances, I produced my thesis in accordance with the guidelines provided by the Uskudar University Institute of Health Sciences Thesis Writing Guide.

Date:
Muhammed Nmakatun Umar
Signature:

CONTENTS

INDEX OF FIGURES

INDEX OFIMAGERYANDABBREVIATIONS

SET: Social Engineering Tool kits.

CMA CGM: Compagnie Générale Maritime.

HTTPS: Hypertext Transfer Protocol Secure.

URL: Uniform Resource locator.

HTTP: Hypertext Transfer Protocol.

BYOD: Bring your own device.

TLS: Transport Layer Security.

TCP: Transmission control Protocol.

ICICT: International Conference on Information and Computer Technologies.

1. INTRODUCTION

1.1 Introduction

Social engineering assaults have emerged as a key security concern in both the real and virtual spheres of cyber space, through some malicious programs, individuals are targeted by convincing them to reveal private information or do other activities that compromise security. These assaults don't take advantage of security holes; rather, they exploit flaws in people's trust in one another and in themselves. Deception, manipulation, and persuasion are common methods used by the aforementioned people to attain their goals (Abdu’s sobur*etal*., 2023). Over the years, the internet has become an integral part of people's lives all over the world and has played a major role in global communication. The performance, accessibility, and usage of the internet have all significantly increased due to innovations and affordability. There are reportedly three billion users of the internet worldwide (Tan et al., 2021). The global economy receives billions of dollars annually via this extensive network, which has been in place for a long time (Judge et al., 2021). According to Aghajani and Ghadimi (2018), the majority of social, cultural, commercial, political, and economic activities and exchanges nowadays take place online on platforms like Zoom, Microsoft, and social media. This are carried out using gadgets like laptop and phones using mobile applications.

Mobile applications are being use consistently in the current century by many people due to rapid evolution and advancement of mobile technologies, many people also use social media on a regular basis without realising the risks involved, including the possibility of theft, unlawful acquisition, and trade of personal data. This risk is always there since social media is such an integral part of our lives (Rafsanjany*etal*., 2018). The British consulting firm ovumone predicted long ago that, billions of people in African countries will have internet access in 2022 (Frizell*etal*., 2018). Over the decades, the method of information delivery has increased since the introduction of internet and social media (Hatice*etal*., 2021). (lewis, 2018) reported that, the prevalence and proliferation of cybercrime have received a global attention, Social engineering in the other hand is particularly a dangerous cyber threat that occurs in the social media domain (Hatice*etal*., 2021). It leverages manipulation tactics to take advantage of human error and gain easy access to the personal data of its victims. Due to its vulnerability, social media is a prime place for these kinds of attacks, which highlights the importance of user understanding in reducing the risks associated with social

engineering (Mohammed *etal*., 2020). This threat is made possible by a number of techniques, such as the monitoring of bank transactions, phoney websites, and email scams designed to steal personal data and money. Increasing awareness and taking preventative action are essential in the fight against social engineering (Abdulateef***et****al*., 2020). Social engineering attacks on social media, particularly phishing, seek to get sensitive information fraudulently through deceptive techniques. Phishing takes the form of deceptive emails posing as legitimate companies, asking users to give personal information such as passwords and credit card details. Account deactivation scenarios, such as in PayPal, are an example of social media phishing, in which attackers claim account compromise and demand confirmation of credit card credentials under the fear of account deactivation. Email phishing uses bogus websites, and stolen credit card information is used for further illegal activity. Furthermore, pretexting involves attackers fabricating lies and appearing as trustworthy persons in order to gain trust and acquire various personal data, such as social security numbers and addresses (Abdulateef*etal*., 2022). Due to the swift advancement of mobile technologies, mobile applications have become indispensable in numerous facets of our existence. On the other hand, hackers use Social Media Posts in these applications to quickly obtain user data, such as phone numbers, browsers, and operating systems. Hackers target social media networks like Facebook, Snapchat, YouTube, and Twitter as susceptible data assets to be stolen and sold due to the growing user base of these apps. The last ten years have seen a tremendous expansion in the methodologies and technology used for information security. Hackers use cunning techniques, disguising themselves as reliable sources, in order to interact with victims, win their trust, and take advantage of data extraction without their knowledge. Spam is when people get unwanted emails or texts that contain dangerous URLs that can damage their devices.

Unsafe URLs are also widely dispersed on social media, which adds another layer of risk. Users are more susceptible to attacks and frequently fall victim to data phishing as a result of their carelessness in inserting URLs in social media posts and accidental link clicking. With the limited resources available online, attackers employ tools such as Social Engineering Tools (SET) to mimic attacks and take advantage of users' unintentional disclosure of personal information, which could jeopardise their security.

1.2 Scope and Limitation

Using the Social Engineering Toolkit (SET), this study will focus on a detailed analysis of simulated attacks on Android and iOS devices, with a special focus on Storm Breaker. The study will also investigate vulnerabilities in Android and iOS devices, examining scenarios of unauthorised access and collecting important information such as device details, online camera photographs, device location, audio, and microphone data. Furthermore, it conducts a thorough investigation of weaknesses in the Android and iOS operating system, browsers, and other important components to provide full insight into potential security concerns.

The research intends to expand its scope beyond identification and analysis, delivering real solutions and recommendations to strengthen Android devices' entire security posture against Social Engineering Toolkits. Tailored recommendations for system administrators, developers, and end users are intended to strengthen defences and provide useful insights to the larger cybersecurity community. The study aims to provide a nuanced understanding of the strategies used by attackers to exploit Social Engineering Toolkits on Android handsets.

Despite its objectives, the study has limits. Using simulated environments may reduce the realism of findings, thereby overlooking the complex nature inherent in real-world cybersecurity threats. The sole focus on Storm Breaker inside the Social Engineering Toolkit may limit the findings' application to new tools. Legal and ethical constraints may limit the investigation into specific components of simulated attacks and data extraction. The study's emphasis on Android smartphones may limit its direct relevance to other operating systems or device types. Furthermore, the study's conclusions may be time-sensitive due to the continuously changing nature of cybersecurity environments, potentially ignoring newly emergent threats or remedies discovered after the study. Generalising findings to include all Android devices or diverse user behaviours may provide issues in terms of applicability and relevance. Additionally, Strong security mechanisms prevent attempts to utilize Storm Breaker to obtain device information and photographs on iOS devices, especially through the Safari browser. As a result, the attacker's photo is captured rather than the target victims.

1.3 Significance of the Study

With an emphasis on the Social Engineering Toolkit (SET) and Storm-Breaker, this research significantly advances cybersecurity and technology by thoroughly analyzing simulated attacks on Android and iOS devices.

The fundamental significance is the comprehensive investigation of vulnerabilities within Android devices in order to identify potential points of unauthorised access. The extraction of critical information, ranging from device specifications to audio and microphone data, makes a substantial contribution to a comprehensive understanding and assessment of security concerns in the digital ecosystem.

Beyond just identifying vulnerabilities, the study investigates the inherent faults in Android devices, including the operating system, browsers, and essential components. This extensive analysis reveals particular flaws that make these devices vulnerable to Social Engineering Toolkit assaults, providing useful insights for the creation of more resilient security measures. The study's findings are useful in educating and guiding continuing work to strengthen Android devices' security posture against sophisticated cyber-attacks such as Storm-Breaker.

Furthermore, the study effort extends beyond analysis to offer actionable solutions and recommendations customised to system administrators, developers, and end users. These practical solutions are critical tools for strengthening defences and limiting the dangers associated with sophisticated attacks. The study's broader impact resonates with the cybersecurity community, giving valuable insights into the hidden methodologies, techniques, and procedures used by attackers to exploit Social Engineering Toolkits on Android cell phones. This knowledge provides cybersecurity professionals with the tools they need to proactively defend against evolving threats in the areas of social engineering and device exploitation.

Finally, the study's broader goals of increasing security awareness among Android device users and providing practical suggestions for risk mitigation, particularly in the context of Social Media Platforms, help to promote a safer and more secure digital environment. By providing users with knowledge and meaningful recommendations, the study actively contributes to increasing resilience to possible attacks in the ever-changing cyber security scene.

1.4 Objective of the Study

The main goal of this thesis is to perform an in-depth examination of simulated attacks on Android smart phones using the Social Engineering Toolkit (SET), with a focus on Storm-Breaker. The researchers want to analyse the vulnerability of Android, iOS devices to unauthorised access by extracting essential information from the target device, including the device information, web camp photo, device location, Audio and microphones.

In addition to the simulated assaults, the study plans to examine the vulnerabilities and flaws inherent in Android, iOS devices, particularly those that make them vulnerable to Social Engineering Toolkit attacks. This investigation will include a thorough examination of weaknesses in the Android, iOS operating system, browsers, and other important components, providing light on specific points of vulnerability that attackers may use to get unauthorised access to user data.

Furthermore, the study will look into potential remedies to improve Android, iOS devices' overall security posture against Social Engineering Toolkits such as Storm-Breaker. Recommendations for system administrators, developers, and end-users will be made to strengthen their defences and lessen the danger of falling victim to such attacks.

The study also aims to provide significant insights to the larger cybersecurity community by offering a thorough understanding of the methods, techniques, and procedures used by attackers to exploit Social Engineering Toolkits on Android, iOS devices. This contribution seeks to provide cybersecurity professionals with the knowledge they need to proactively defend against developing threats in the areas of social engineering and device exploitation.

In the end, this research study hopes to raise users of iOS and Android devices' knowledge of security issues. Furthermore, the research aims to provide useful and feasible suggestions for reducing the threats connected with Social Engineering Toolkit attacks, specifically in the context of Social Media Platforms.

1.5 Problem Statement

The increased reliance on mobile applications, particularly social media, has created serious worries about security flaws used by hackers to get access to sensitive information. Hackers exploit users' confidence by using strategies like masquerading as well as specialized tools like Storm-Breaker from the Social Engineering Tools (SET) framework.

They can use these approaches to collect sensitive information such as phone numbers, operating system specifications, and browser data. This poses a serious risk because users regularly unknowingly provide their data to untrustworthy actors, exposing themselves to potential security breaches and abuse.

1.6 Motivation

The motivation for this study emerges from the growing risks associated with social media platforms and mobile applications. As people become more reliant on these technologies for communication and engagement, the threat landscape develops. Hackers use human psychology to get unauthorized access to personal data by relying on trust and social connections. The study aims to face these vulnerabilities and offer strong solutions to improve users' security and privacy when using mobile applications.

1.7 Propose Solution

The study intends to investigate and implement comprehensive security methods to mitigate the dangers associated with social media and mobile applications. This includes the following:

a. Education and Awareness:

creating and carrying out educational programs intended to improve user awareness of the dangers associated with phishing and social engineering. Training people on how to spot and avoid dubious emails and websites falls under this category.

b. Behavioral Analysis:

carrying out an in-depth review of user behavior patterns on social media sites to uncover potential vulnerabilities and typical hacking tactics.

c. Technological Solutions:

To prevent unauthorized data access and phishing efforts, mobile applications are being equipped with powerful spam filters, URL scanners, and real-time threat detection systems.

d. Collaboration with App Developers:

Collaborating alongside mobile app developers to integrate enhanced security measures into their platforms and advocating for data protection best practices.

e. Continuous Monitoring and Updates:

Setting up a framework for continuous surveillance of security threats and rapidly changing security policies to address growing risks and developing attack techniques.

By implementing these strategies, the study hopes to improve the security of mobile applications, reduce the danger of data breaches caused by social engineering attempts, and empower users to make educated decisions about their online interactions and data sharing habits. The main goal is to create a safer and more secure environment for mobile app users as the cybersecurity landscape expands.

The study involving the analysis, penetration levels and develop attack prevention strategies for android, iOS devices using a storm-breaker as a social engineering tool is a reproducible and advance work whose advancement is still ongoing. Several scientists like (Eric *etal*., 2023) has previously worked on Penetration testing, Hacktivism, and Vulnerability Assessment of individuals using storm-breaker application.

The research will use storm-breaker application to find out the following

- Penetration levels of storm breaker
- Vulnerability Assessment using statistical report
- Strategic methods of preventing social engineering attacks on android devices

(Eric *etal*., 2023) device a reproducible method that shows clearly how storm-breaker application could be used to simulate a social engineering attack, the same method of will be adopted here for my studies but a little bit to cover some of the gaps and introduce other important measures.

The researcher would collect the survey data and report the percentage of the user's awareness of social engineering attack. the data collected would be display in Bar chat, Data of the participants who participated in the survey will also be collect, the average of the number of the participants that did the survey will be recorded and would be used to presenting and discussing result that could be seen in the subsequent chapters.

At the end of the research the data obtain could be used to publish the following information

- The extent to which a storm breaker application can penetrate into Android, iOS devices
- Statistical analysis of social media security awareness
- Strategic plans to combat the effect of the social engineering theft

1.8 Security Measures

In order to provide protection against social engineering toolkits "Storm breaker," organizations must implement a comprehensive security strategy that encompasses both technical and procedural protocols. The following are key safety measures that need to be taken:

a. Awareness and Training for Employees

- Security Awareness Training: Hold frequent training sessions to teach staff members how to spot and identify social engineering techniques.
- Phishing Simulations: Conduct simulated phishing attacks on a regular basis to assess and enhance staff members' comprehension of how to spot and handle phishing attempts.

b. Robust Authentication Mechanisms

- Multi-Factor Authentication (MFA): To add an extra degree of protection, implement multi-factor authentication (MFA) for all crucial systems and accounts.
- Strong Password Policies: Implement restrictive password policies, these should include frequent password changes and the usage of complicated passwords.

c. Email and Communication Security

- Email Filtering: To identify and stop phishing emails and other harmful communications, use sophisticated email filtering technologies.
- Email Authentication: To prevent email spoofing and make sure that emails are sent from reliable sources, use SPF, DKIM, and DMARC.

d. Security Policies and Procedures

- Comprehensive Security Policies: Create thorough security policies that address every aspect of information security, then implement and enforce them.
- Regular Audits and Reviews: Regularly detect and address any vulnerabilities by conducting security audits and reviews.

e. Technology Solutions

- Endpoint Protection: Install endpoint security software to protect against viruses and other harmful programs that could be utilized in social engineering schemes.
- Firewall and Intrusion Detection/Prevention Systems (IDS/IPS): For network traffic monitoring and protection, use firewalls and IDS/IPS.

f. Behavioral Analytics and Anomaly Detection

- User Behavior Analytics (UBA): Use UBA tools such as Splunk to identify unusual activity that can point to an insider threat or compromised account.
- Anomaly Detection: Use anomaly detection tools to spot odd behavior that can be a symptom of a social engineering scam.

2. THEORETICAL CONCEPTS

2.1 Definition of Terms:

The purpose of this chapter is to review a set of related research on the creation of tools for social engineering such as Storm Breaker. It offers a thorough synthesis of previous research on social engineering attacks, with a focus on social network attacks. The investigation explores the extent to which these attacks are able to gain access to Android devices and attempts to develop countermeasures. This chapter attempts to provide insights into the changing field of social engineering tactics by carefully examining the literature, explaining various aspects of attack methodology, and exposing new developments in attack avoidance techniques.

2.2. Vulnerabilities of social media

Social media networks have revolutionized communication, information exchange, and the broadcast of multimedia material throughout time. Nonetheless, a deficiency of knowledge among users has resulted in a surge in online fraudulent activities, aggravating the spread of cyber incidents and threats. Twitter, Facebook, Snapchat, YouTube, and other social media platforms are now widely used, especially by people who utilize mobile devices. Global internet users reached 4.388 billion in 2019, according to statistics, and there were over 5.112 billion mobile phone users worldwide (Mohammed et al., 2020). Through the use of these platforms, cybercriminals carry out nefarious actions that put billions of users at risk and jeopardize the security of their user data. Usually, these attacks use deception techniques, tricking people into giving hackers on social media platforms who pose as reliable sources of information their login credentials and private information. More and more educational programs, like MOODLE (Modular Object-Oriented Dynamic Learning Environment) Learning, are being used to teach internet security concepts not only in academic settings but also in other institutions. The goal of these programs is to equip people with the knowledge and techniques they need to protect themselves from vulnerabilities that hackers can exploit (Eric et al., 2023).

2.3. Ethical Hacking

Personal data and information are only accessible to a small number of authorized organizations. Preventing threat actors from using this data for their own gain requires protecting it from unauthorized access. Through the use of a team or a person, ethical hacking offers organizations a practical means of evaluating the security of their systems by simulating harmful activity and looking for weaknesses (Alana et al., 2019). "The lawful use of technology to probe system weaknesses and gather information" is the definition of ethical hacking given by Ahmad et al. (2020). Ethical hacking encompasses several techniques such as vulnerability assessment, penetration testing, and hacktivism. To guarantee the protection of user data, it is therefore imperative that enterprises adopt ethical hacking techniques and integrate key security measures (Eric et al., 2003).

2.4. Cyber Security

Cyber security is widely defined as the use of techniques, procedures, and technologies to protect computers, networks, electronic devices, systems, and data against cyber-attacks. Individuals and organisations utilise cyber security to reduce the risk of theft, attacks, damage, and unauthorised access to computer systems, networks, and sensitive user data. Cyber security began in the 1970s and has evolved ever since. Currently, it goes beyond computer security to defend persons from hostile intrusions. The major goal of cyber security is to prevent the exposure of sensitive data while also creating cyber resilience, which allows for a more effective reaction and recovery from cyber-attacks with minimal harm (Eric *etal*., 2023)

2.5. Cyber-Attack

This is the process of obtaining data illegally or breaking into computer networks and systems by using one or more intermediate machines. It usually represents the first stage that hackers take to gain access to private or business networks prior to carrying out a data breach. Hackers can use cyberattacks to achieve a variety of goals, such as damaging the targeted computer and making it unusable or breaking into linked networks and systems to steal information. Cyber-attacks range in sophistication, with attackers using techniques such as denial of service, malware, phishing, and ransom ware. One obvious example is the hack on CMA CGM in September 2020, when ransom ware hit the company's systems, resulting in a data breach and the temporary suspension of internet services (Ma *etal*., 2021)

2.6. Cyber-Crime

Cybercrime refers to illicit activities that use computer systems, networks, or digital devices as instruments or targets. It encompasses a variety of unlawful activities such as hacking, identity theft, financial fraud, malware distribution, child pornography distribution, online frauds, and unauthorised data access. Cybercriminals use their technical talents to exploit weaknesses in digital systems, committing criminal acts for profit or other evil goals (Palmieri *etal*., 2021).

2.7. Cyber-Criminal

Hackers use technology to carry out destructive operations against digital systems or networks in an attempt to steal confidential company or personal information for financial gain. They can operate alone or as part of larger organizations. In the deep web underground marketplaces, these actors frequently participate in covert operations. There, they trade illegal commodities and services, including hacking tools and stolen data, highlighting particular goods or services that they find appealing (Palmieri et al., 2021).

2.8. Social Engineering

In order to obtain unauthorized access to computer systems, social engineering refers to a variety of tactics used to trick, persuade, or manipulate people into disclosing private information or taking activities that jeopardize financial and personal information. This dishonest method uses psychological manipulation, coercion, and exploitation to trick users into making security blunders or divulging private information. Human connections are exploited in these attacks, which frequently convince victims to circumvent established security procedures. (Fatima et al., 2019) highlights that social engineering is a highly effective approach because it takes advantage of human dispositions to trust others or be enticed by fresh information or offers.

2.9. Social Engineering Attacks

Social engineering attacks refer to the strategic methods utilized by malevolent entities with the intention of manipulating individuals into divulging sensitive information, executing specific acts, or making choices that undermine the integrity of security measures. These assaults leverage aspects of human psychology, trust, and vulnerabilities instead of

capitalizing on technological vulnerabilities. Social engineering attacks have the potential to manifest in both the tangible physical environment and the intangible virtual domain of cyberspace.

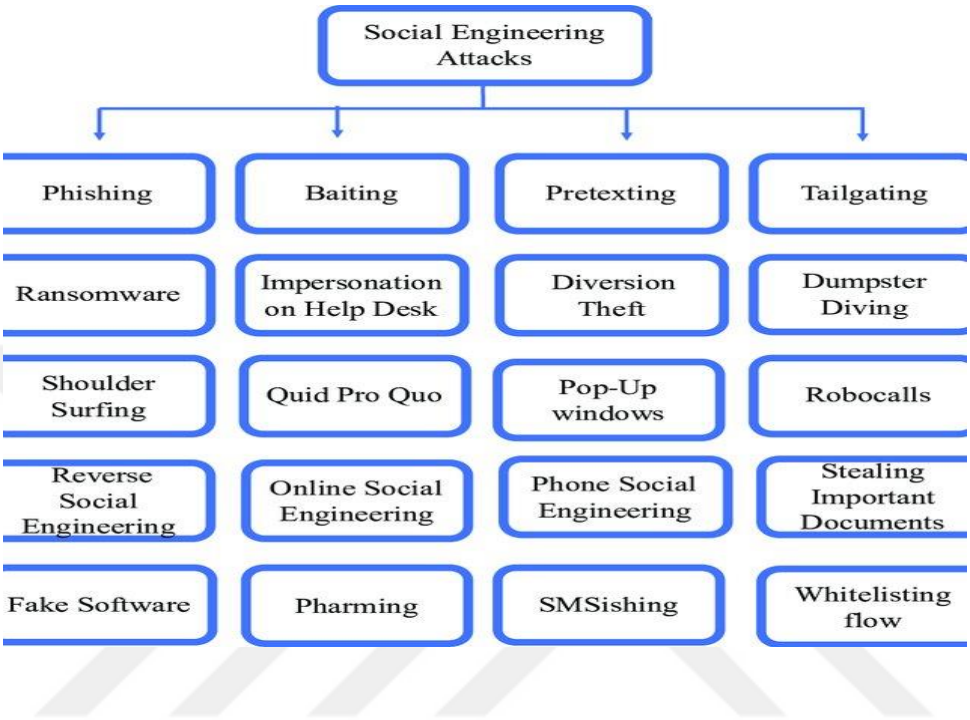

Fig. 1. Different Types of Social Engineering Attacks

2.9.1. Different Types of Social Engineering Attacks

These techniques span a broad spectrum of strategies, which may include:

a. **Phishing:** explains the practice of sending phoney emails that are designed to look authentic, with the intention of tricking recipients into clicking on hazardous links, downloading dangerous software, or divulging personal content.

b. **Pretexting:** using trickery and emulation to gain the trust of another person in order to accomplish a goal. An attacker must gain the target's trust before gaining access to sensitive data or coercing the victim into acting.

c. **Baiting:** encouraging people to download harmful software or expose sensitive information by offering alluring incentives, such as free software or downloads.

d. **Quid Pro Quo:** giving something of value in exchange for access or knowledge. For instance, the offender can pose as IT assistance and offer to fix a false issue in exchange for login information.

e. **Tailgating:** using the tendency of authorized people to hold doors open for others to gain unauthorized access to restricted locations by tailing them.

f. **Impersonation:** Posing as someone else to gain trust and access, whether in person, over the phone, or online.

2.9.2Examples of social engineering attacks in the physical world:

a. **Tailgating:** An attacker dresses as a delivery person and waits near a secure entrance. When an employee enters using their access card, the attacker follows closely, gaining unauthorized entry.

b. **Pretexting:** An attacker calls a company's reception, claiming to be from the IT department. They state they need certain employee credentials to fix a technical issue. The receptionist, unaware of the ruse, provides the information.

c. **Impersonation:** An attacker poses as a fire inspector, using a fake badge and uniform. They gain entry to an office building and claim they need to inspect the fire extinguishers. While inside, they could plant listening devices or steal sensitive information.

2.9.3 Examples of social engineering attacks in cyberspace

a. **Phishing:** The user is presented with an electronic communication that purports to be from a well-established financial institution, wherein they are urged to click on a hyperlink and proceed with the modification of their account particulars. The provided hyperlink directs users to a fraudulent website specifically created with the intention of illicitly acquiring login credentials.

b. **Baiting:** The perpetrator strategically places USB devices with the explicit label "Employee Payroll Information" within the premises of the organization's parking area. Inadvertently, employees with a sense of curiosity retrieve the disks and proceed to place them into their computer systems, so unintentionally facilitating the installation of malicious software.

c. **Quid Pro Quo:** The perpetrator assumes the identity of a representative from a software firm, enticing the user with the prospect of a complimentary software trial, with the ulterior motive of obtaining the victim's login credentials. The user furnishes their personal details, presuming the acquisition of a genuine commodity.

2.10. Social media manipulation and information gathering:

Attackers personalize their attacks by using information provided on social media platforms. They may gather information about a person's interests, career, or connections in order to develop persuasive messages that boost the likelihood of success.

2.10.1. Attack Surface:

a. **Physical World:** In-person attacks target physical access points and human interactions.

b. **Cyberspace:** Attacks are carried out remotely via digital channels, taking advantage of communication and psychological manipulation.

2.10.2. Tactics:

a. **Physical World:** Impersonation, manipulation, and abuse of trust in face-to-face contact.

b. **Cyberspace:** Creating convincing emails, messages, or information in order to trick receivers into taking action.

2.10.3. Physical vs. Digital Interaction:

a. **Physical World:** Manipulating in-person interactions, exploiting body language, tone of voice, and immediate human reactions.

b. **Cyberspace:** Replying on written communication and digital clues, often requiring careful attention to details in content and formatting.

2.10.4. Access and Information Extraction:

a. **Physical World:** Physical access to restricted places, document theft, or hardware device installation.

b. **Cyberspace:** Obtaining login credentials, personal information, or sensitive data through deception and bogus websites.

2.11. Advanced Strategies of Social Engineering:

According to Edger et al. (2015), social engineering has become a prominent challenge and method of information system attack in online communities. Social engineering attacks also target workers in organizations, and BYOD (bring your own device) guidelines, online forums, and teamwork tools exacerbate the problem (Eric et al., 2023). Due to their often geographically distributed workforces, global organizations are more vulnerable to social engineering attacks since they rely more on email, instant messaging, Skype, Dropbox, LinkedIn, and Lync and experience a decrease in face-to-face encounters. According to reports from RSA and The New York Times, spear-phishing is a powerful social engineering tactic that can be especially dangerous when paired with zero-day vulnerabilities to pose a serious threat from advanced persistent threats (APTs). This study highlights advanced social engineering attacks directed towards knowledge workers and offers valuable insights on their classification. An example of how spyware programs can access capabilities including contacts, camera, microphone, location, and SMS was given through a simulated attack in which data from Android smartphones was infiltrated using spyware. The malware was created and then released based on the threat actor's preferences using the open-source program Metasploit from Kali Linux. Pistol et al. (2020) conducted a study wherein malware was purposefully put on the device to emulate an assault.

2.12. Making Use of Msfvenom to Exploit Android

2.12.1. Adding NGROK to the System

This study used Zip, NGROK, and the MSF Venom tool to simulate attacks on Android and iOS devices. The results of the study show that NGROK was used to connect to the devices

throughout the investigation, and that MSF venom along with Zip's aid in injecting the aforementioned asset acted as the principal instrument for backdooring the victim's device. Kali Linux was used to configure these tools in preparation for deployment. The researchers started the simulation assault by sending the user an email or SMS with the URL to the malicious program that they had uploaded to Google Drive. A session would start when the malicious program was opened, giving threat actors access to sensitive data and the ability to carry out commands.

2.13. Related Works

2.13.1 Introduction

This section will analyze earlier studies, with a focus on (Eric et al., 2023), regarding Storm-breaker's efficacy as a social engineering instrument. Hackers leverage social media posts to obtain personal information due to the quick development of mobile technology and the widespread use of different mobile applications in daily activities. Victims can provide them with information like as phone numbers, browser details, operating system versions, and more. As the number of people using social media platforms like Facebook, Snapchat, Twitter, YouTube, and others rises, hackers can profit from these valuable sources of sensitive data (Arana, 2022). Since new security technologies have significantly expanded over the years, information security techniques have evolved rapidly (Hatice et al., 2021). Instead of using brute force attacks, hackers frequently employ masquerades and phoney identities to interact with victims, win their trust, and deceive them into willingly revealing their data (Mohammed et al., 2020). Spam is the term for unsolicited emails or texts that contain malicious URL links that, if clicked, can damage the recipient's device. Further concerns arise from the proliferation of hazardous URLs on social media. When utilizing social networking tools, people frequently neglect to carefully examine URLs, which might result in phishing and other attacks. Due to the widespread scope of this issue and the scarcity of available internet resources, social engineering tools (SET) are being used more frequently. In order to learn how users can be tricked into providing information that could compromise them, comparable to spam emails and texts, these tools mimic attacks on Android smartphones (Fatima and Naima, 2019).

nevertheless, the following research issue was put out at the 6th International Conference on Information and Computer Technologies (ICICT) in 2023:

In what ways may Storm-Breaker mimic a social engineering attack that focuses on user weaknesses in social networking apps? (Eric et al., 2023) developed a repeatable technique that shows how to launch an attack using the Storm-Breaker program.

2.13.2 Research Design

Using a controlled experimental design, the authors conducted simulated attacks on an Android handset that had been rooted, making sure that the data gathered came solely from the tester's device (Eric et al., 2023). They were cautious to make sure the experiment did not violate any data privacy rules. A lone attacker utilizing a laptop outfitted with the Social Engineering Toolkit (SET) was the research design. To find out more about people's awareness and knowledge of dangerous behaviors that could jeopardize their private information, they also ran an online poll.

The environment in which the study was conducted ensured that the data was unique to the experimental scenario because the attacker and the test subject were not too far apart. In order to simulate internet-based attacks via identity fraud or masquerading, the research environment was created to resemble a home environment. Kali Linux, VMWare, ngrok, Storm-Breaker, and a social messaging app were among the tools and libraries used in this study.

2.13.3 Population of the Study

The population studies conducted by the authors centre on two scenarios: one in which a participant is involved in a social engineering attack, and the other involves simulated attacks in a controlled environment using a rooted device. Facebook Messenger and other social messaging apps were used to carry out this attack. Due of their regular usage of social media apps, participants are vulnerable to interacting with the Storm-Breaker disguised URL used by the researchers. Furthermore, an online survey concerning dangerous URLs that were making the rounds on social media was mandatory for at least twenty participants to finish (Eric et al., 2023).

2.13.4 Result

The case study's simulated attacks using Storm-Breaker are presented in this part along with their results. Additionally, a survey was sent out online to 24 respondents to gauge their

knowledge and comprehension of dangerous links on social media. The outcomes of the simulation attack are interpreted and presented in this part as well.

2.13.5 Survey Interpretation

With 91.7% of respondents 22 people using Google Chrome, it is the most popular browser. With seven responders and a usage rate of 29.2%, Microsoft Edge comes in second. With five responders, Mozilla Firefox is ranked third with 20.8%. Fourth position goes to Brave, with two respondents using it 8.3% of the time. Furthermore, 4.2% of users (one responder) favor different browser programs like Ecosia and Safari.

Faked URL links are known to 95.8% of respondents (23 people), whereas 4.2% of respondents (one person) are unaware of them. One respondent indicated they just ignored the URL links, while 33% (8 respondents) said the communications with odd URLs were irrelevant. Approximately 63% (15 respondents) reported receiving messages with strange URLs that were relevant to them.

Nineteen respondents, or 79.2% of the total, reported that Facebook had the largest percentage of unknown links or URLs. With 8 responders (33.3%) pointing out unknown links or URLs, Instagram comes in second. According to 7 respondents, 29.2% of them are unsure about links or URLs, placing Twitter in third place. At the bottom, with only 4.2% (1 respondent) naming them, are other platforms and programs including Reddit, TikTok, banking apps, Cashbee, phoney websites mimicking well-known ones, Messenger, and Yahoo.

Seventy-five percent (18 respondents) said they have received suspicious messages or emails with questionable attachments from reliable sources; only six respondents did not report receiving such messages. Furthermore, whilst 13.5% (3 respondents) are unaware of URLs that could access their location or other personal data, 87.5% (21 people) are. 25% of respondents (6 respondents) denied having been victims of cyberattacks, while 75% of respondents (18 respondents) acknowledged having been. Finally, while 70.8% (17 respondents) have thought about taking defenses against social engineering assaults, such as employing security software and vetting information sources, 29.2% (7 respondents) have not.

3. MATERIAL AND METHODOLOGY

3.1. Materials

a. Ngrok

The study uses Ngrok tool which is a well-liked development tool that allows local servers to be exposed to the internet without the need for complicated configurations, using Ngrok tool it's makes the remote access to local service flexible and effective by facilitating real time testing bypassing network restriction and providing secure tunnel for easy set ups, It does this by building secure tunnels between public endpoints and local network services. Special subdomains, request inspection, tunnelling, HTTPS support, multi-region support, authentication, and persistent URLs are some of the important features. Web development, API testing, Internet of Things development, remote access, and demonstrations are just a few of its common uses. It is easy to install: just download from the official website, use a command to launch a tunnel, and go to the public URL that is provided. Providing a safe and adaptable solution for different development requirements, Ngrok simplifies the process of making local services accessible from a distance.

b. Python

Python3 library was also use during the study a popular high-level programming language with many applications, Python 3 is also just called Python. It is an advance over Python 2 and is noted for being more readable and flexible. A large standard library, dynamic typing, readability, object-oriented programming support, and being an interpreted language are some of its key features. NumPy, Pandas, Matplotlib, SciPy, Requests, Django, Flask, TensorFlow, scikit-learn, Requests for HTTP requests, NumPy for scientific computing, NumPy for numerical computations, and Beautiful Soup for web scraping are some of the popular Python 3 libraries. Its Liberia's has a great impact running storm breaker tool and also by utilizing the `pip` package manager, libraries may be installed with ease. Web development to scientific computing is just a few of the many applications that Python 3 may be used for because of its large ecosystem and focus on simplicity.

c. Mendeley

Mendeley serves as an efficient reference management system and is an essential tool for academics, researchers, and students. It gives scientific articles and research papers a complete way to be organized, shared, and cited. Mendeley makes managing large bibliographies easier with its collaborative features, which improve communication and knowledge exchange across academic organizations. Mendeley proved beneficial when I was writing my thesis. My ability to effectively classify and arrange a variety of study resources was facilitated by its intuitive interface. Mendeley's actual strength is its citation and reference functionality, which integrates with word processors like Microsoft Word smoothly to make creating bibliographies and inserting citations simple. In addition to saving plenty of time, this made sure that all references complied with the rigorous guidelines for academic citations. Mendeley's adaptability and user-friendliness significantly enhance the caliber and professionalism of academic writing, making it a fantastic resource for managing the challenges of academic labor.

3.2. Methodology

3.2.1. Research Design

The study will make use of a well-regulated experimental configuration that includes simulated attacks on iOS and Android smartphones to ensure that data collection is limited to the tester's device data. Throughout the experiment, this strategy will maintain stringent respect to data privacy standards. The research approach is based on a single attacker using a laptop that has the Social Engineering Toolkit installed (SET). In addition, an online survey will be used to determine how well-informed people are about potential risks to their personal data. In order to make sure that the data gathered accurately represents the settings provided by the research scenario, the study will be carried out in an environment where the attacker and the test subject are in close proximity.

3.2.2. The Population of the Study

Two simulated attack scenarios one involving a participant in a social engineering attack and the other on a device in a controlled environment will be the focus of the researchers' attention. The messaging programs WhatsApp, facebook will be used to carry out the attack. The chosen subject interacts with social media sites on a regular basis, making it possible for the researchers' Storm-Breaker URL to be used with ease. To help with the simulation process, the link will also be emailed to five separate individuals.

3.2.3. Statistical Analysis

The researcher would collect the data and report the percentage of the user awareness of social engineering attack. the Bar chat data would be collected and explained, Data of the participants who participated in the survey will also be collect, the average number of the participants that participated in the survey will be recorded, this will enable a well-defined report of a statistical representation of the participant in the survey and also will provide a good report on the awareness of social engineering attack in the region where the survey will be conducted.

4. RESULT DISCUSSION

The following section explores the results and significance of the Storm Breaker-based simulated attacks that were conducted for the case study. It also concerns the understanding and presentation of simulated attack results. Furthermore fifty-two (52) people were surveyed online to assess their awareness and expertise of social engineering.

a. Simulation Attack

Storm Breaker was run with root privileges to use superuser rights, which explains why the terminal displays root@kali. Storm Breaker provides five options: Access Webcam, Microphone, Retrieve Normal Data, and Obtain Location and Exit the Menu. Selecting the first option gives you access to the webcam of the target device; selecting the second one gives you access to the microphone of the device. The target's device details are retrieved without their consent in the third option, and the position of the smartphone is acquired in the fourth. In addition, choosing the fifth choice will stop the simulation attack. The first option was set up to access the victim's webcam during the initial test. The link that is generated on port 2525 is shown in Figure 3. Use the command 'ngrok http 2525' in a different root terminal to acquire this URL.

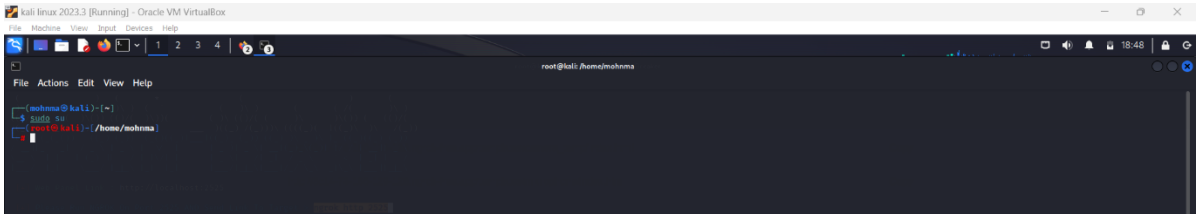

Fig. 2. Changing The Normal User to Root User.

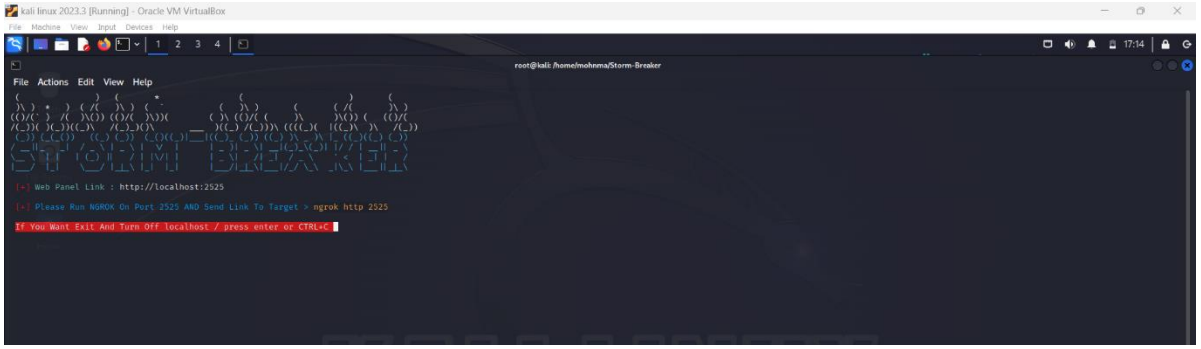

Fig. 3. Starting The Storm Breaker Tool.

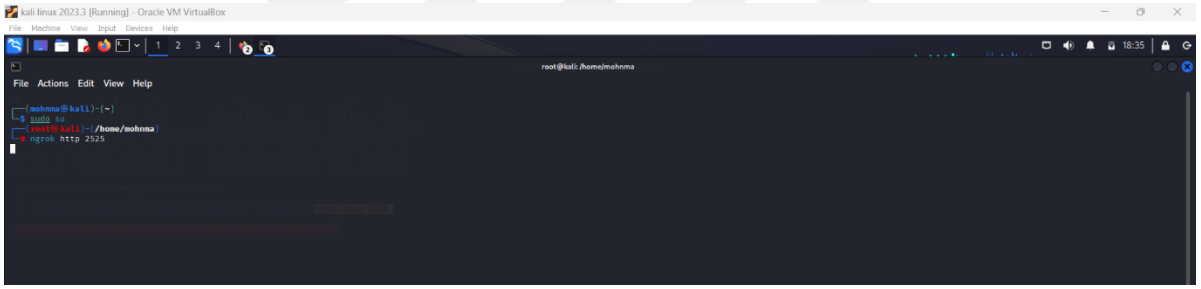

Fig. 4. Establishing a Connection with the Designated ngrok Local Server

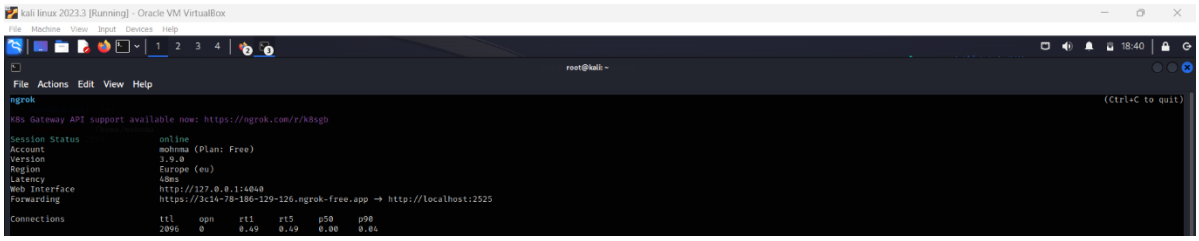

Fig. 5. ngrok information and a created link

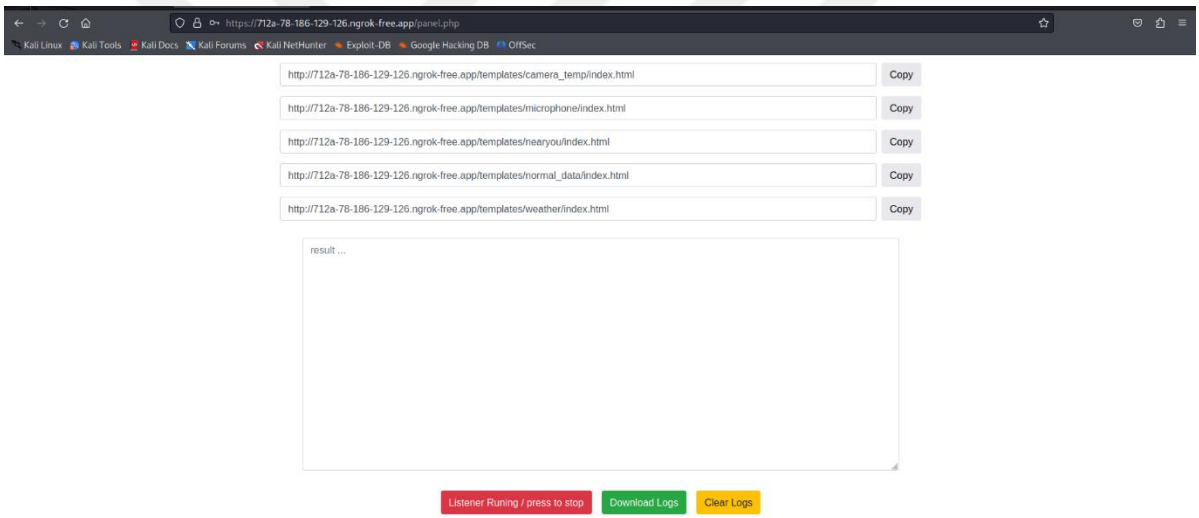

Fig. 6. Results interface

Figure 6 shows the result interface with five generated links for each task, like Access the microphone, web camera, General data, weather, and location of the target device, this links are been re-edited or shorten so that the target victim would not suspect anything about the link send to them.

The superuser terminal where the command 'ngrok http 2525' was run is depicted in Figure 5, “ngrok information and a created link” The online status of the ngrok session is shown by the

software version 3.9.0. The link offered by the web interface lets the attacker keep an eye on specific incoming HTTP requests on port 4040. This interface provides information on the victim's endpoint interface, including time, length, payloads, requests, and HTML code. Nevertheless, neither TCP nor TLS are supported by the inspection web interface. Moreover, the forwarding section displays two URLs that are produced using port 2525 and support HTTP and HTTPS. It is noteworthy that the experiment was carried out on the researchers' devices with their express authorization, guaranteeing compliance with security regulations.

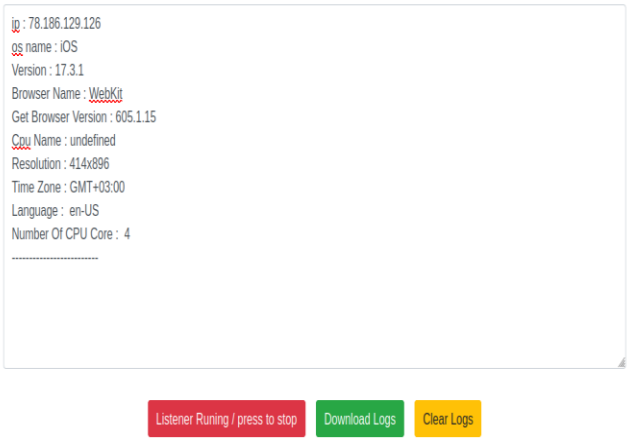

Fig. 7. Acquired Device General Information.

The complete data retrieved from the targeted device is shown in Figure 7. It discloses that the smartphone has a quad-core CPU, runs iOS 17.3.1, and has 78.186.129.126 as its public IP address. It additionally shows that Web Kit version 605.1.15 was used by the victim to visit the URL.

As may be seen in Figure 5, Storm Breaker is regularly used from the superuser terminal (root@kali). During the second simulation assault attempt, the decision was made to gain access to the target's front camera. Storm Breaker then opened a connection using port 2525 after making this choice, as seen in Figure 5. The displayed localhost link and this match. Run 'ngrok http 2525' in a different root terminal to acquire the victim's link.

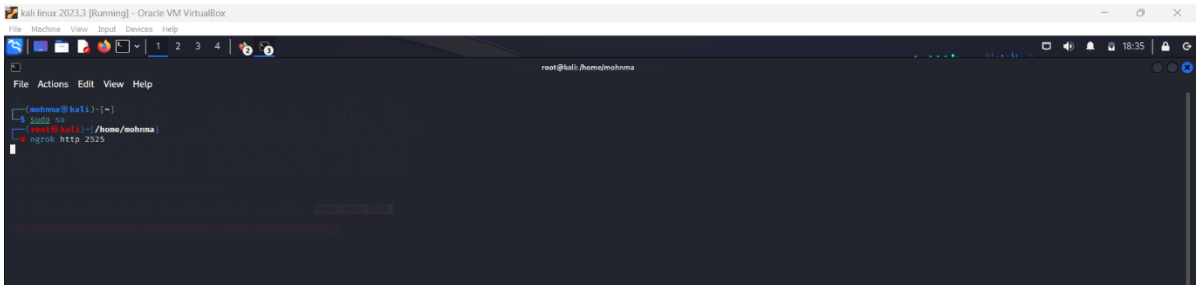

Fig. 8. Setting Up a Connection to the Designated ngrok Local Server

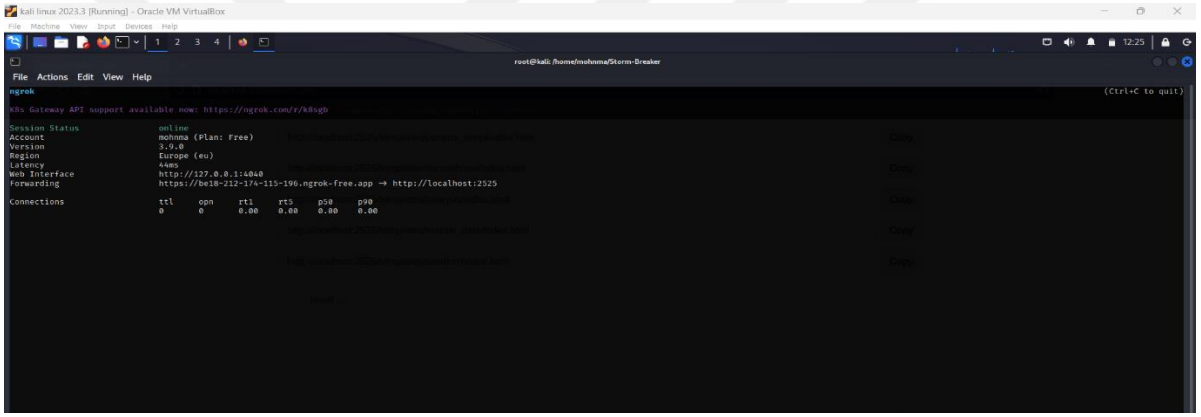

Fig. 9. ngrok information and a created URL

Figure 9 shows the command 'ngrok http 2525' being executed on another root terminal. With the help of this command, ngrok starts a local server and creates an online session. The last two lines display two created links that work with HTTP and HTTPS protocols. Additionally, the web interface allows the attacker to monitor incoming HTTP requests.

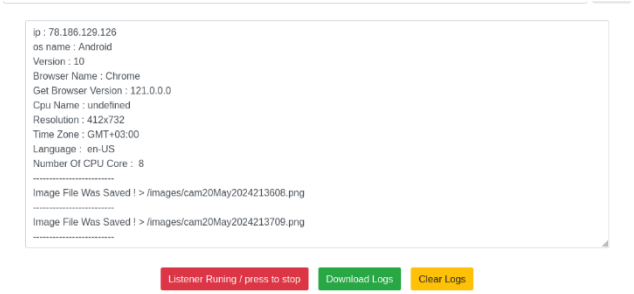

Fig. 10. Device Information and Image Obtained

Figure 10 shows the data that was taken from the victim's Android device, which ran Chrome version 120.0.0.0 and was running Android version 10. The gadget had an eight-core CPU and 78.186.129.126 was its public IP address. The researchers timed how quickly and how long it took to get an image from the victim's device during the process. In less than a minute, Storm Breaker completed this mission. Surprisingly, the image would remain viewable on the attacker's terminal even if the victim closed the link before Storm Breaker could show and save it. The /image directory contains all of the taken photographs.

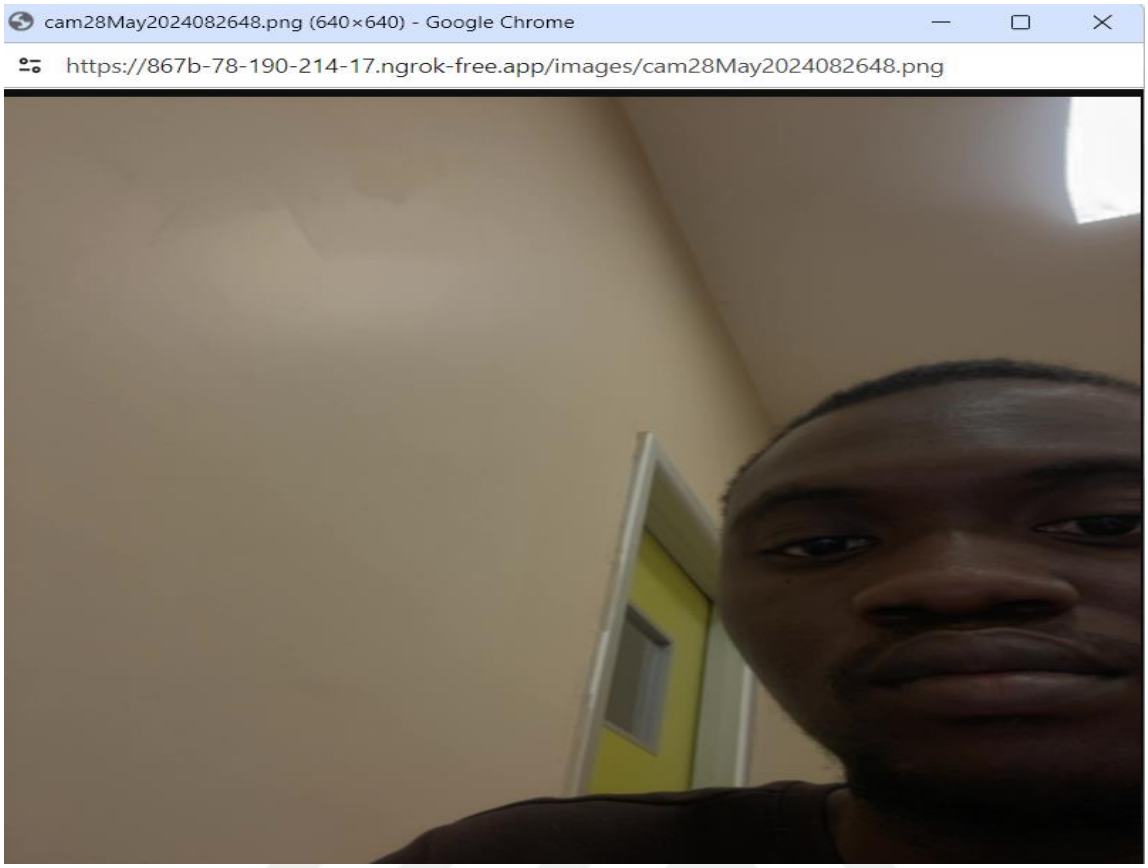

Fig. 11. Front-facing camera image

The /image folder accessed through the attacker's file manager is shown in Figure 11. There are two stored photos in this directory. This proves that Storm Breaker was able to successfully apprehend them.

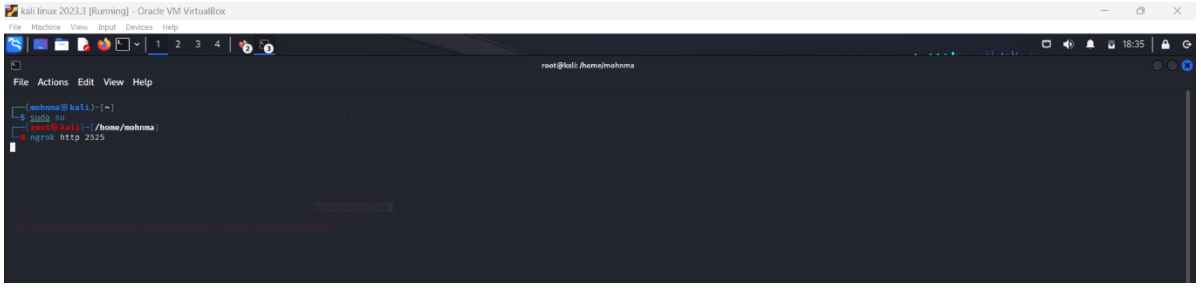

Fig. 12. Setting Up a Connection to the Designated ngrok Local Server

Storm Breaker is frequently used from the superuser terminal, root@kali, as shown in Figure 12. The victim's front camera was accessed in the ensuing simulation assault attempt.

Storm Breaker connected to port 2525 after selecting this option, as seen in Figure 5. The localhost URL was displayed as a result of this. In a different root terminal, enter 'ngrok http 2525' to acquire the victim's link.

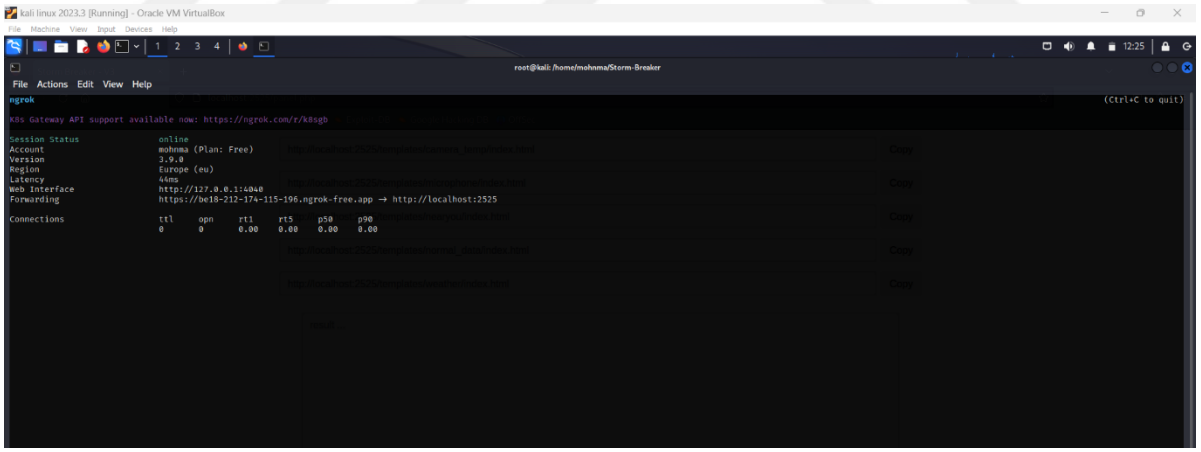

Fig. 13. Established Connection with ngrok Data

A local server is started and an internet session is established by running 'ngrok http 2525' on the root terminal, as shown in Figure 13. Both HTTP and HTTPS connections are shown in the final two lines. The web interface also allows the attacker to keep an eye on incoming HTTP requests

Fig. 14. Gaining Access to Microphone and Device Details

With iOS version 17.4.1 and a public IP address of 151.135.40.157, the target device's data is displayed in Figure 14. It was Facebook version 458.0.0.34.108 that allowed access to the link. A processor with four cores was installed in the gadget. Every voice memo that is recorded gets stored in the /audio folder. It was found that Safari has a strong security mechanism that prevents these kinds of assaults after simulating attacks on iOS and Android devices with different browsers. All other browsers had effective simulations that captured and projected comprehensive data, including a picture of the target user. Safari, on the other hand, constantly rejected the attacks by showing a picture of the attacker. Throughout several tries, this behavior was consistently seen. The security architecture of the browser directly affects how effective these assaults are; the more vulnerable the browser's security programming, the faster the attack can be carried out, while the stronger the security programming makes the attack much more difficult.

b. Survey Interpretation

Regarding the 52 participants, 88.5% were men and 13.5% were women. The age distribution was 71.2% from 18 to 24, 28.8% from 25 to 34, and 1.9% from 35 to 44. Educational qualifications varied: 0% had no schooling, 9.6% had a high school/professional/vocational education, 28.8% had undergraduate degrees, and 63.5% had graduate degrees. Regarding social media usage, 5.8% spent less than an hour per day, 53.8% spent a few hours (3-7 hours), 30.8% spent more than 10 hours, and 11.5% were

always connected. 88.5% of online activities involved social media platforms, 7.7% did not, and 5.8% were unclear. The favored platforms were Instagram (7.7%), Facebook (17.3%), Twitter (23.1%), and WhatsApp (53.8%).

To avoid phishing attacks, 76.9% used strong, unique passwords, 11.5% ignored software updates, 5.8% freely supplied personal information, and 7.7% turned off firewalls. In terms of social engineering assaults, 34.6% reported firewall breaches, 15.4% pharming, 17.3% encryption problems, and 34.6% network intrusions. To avoid social media theft, 11.5% accepted friend requests from strangers, 5.8% utilized public Wi-Fi for important transactions, 82.7% used robust privacy settings, and 0% exchanged passwords with friends or family.

13.5% checked their privacy settings every day, 26.9% checked weekly, 19.2% checked monthly, 38.5% checked infrequently, and 3.8% checked never. To prevent pretexting, 19.2% did not recommend sharing sensitive information without verification, 34.6% did not recommend being wary of unsolicited requests, 40.4% did not recommend sharing sensitive information without verification, and 5.8% did not recommend reporting suspicious activity.

Concerning the effectiveness of education in social engineering, 26.9% highly agreed, 36.5% agreed, 15.4% disagreed, 11.5% were neutral, and 9.6% severely disagreed. 19.2% obtained social engineering awareness training in the workplace, 19.2% from educational institutions, 13.5% via online courses, and 46.2% received no training at all.

In terms of duty for defending individuals from social engineering assaults, 30.8% said individuals should bear it, 28.8% thought social media platforms should, 25% thought cybersecurity corporations should, and 13.5% thought government officials should. To discourage social media theft, 28.8% stated that adopting two-factor authentication (2FA) was the most beneficial, 7.7% believed in raising public awareness, 9.6% supported stronger cybercrime punishments, and 53.8% supported all of these measures.

The survey finds that the majority of respondents are young and educated men who use social media extensively, particularly on WhatsApp. Respondents prefer strong passwords to avoid phishing and identify firewall breaches and network intrusions as prevalent social engineering assaults. They majority feel that strong privacy settings are necessary to prevent social media theft, and that both individuals and social media networks bear responsibility for protection. Comprehensive procedures, such as two-factor authentication and awareness campaigns, are viewed as necessary for deterring social media theft.

5. CONCLUDION AND RECOMMENDATION

This study emphasizes the serious threat of social engineering assaults on Android devices, particularly using tools like Storm Breaker from the Social Engineering Toolkit. It identifies significant vulnerabilities in Android systems that attackers might exploit to access and harvest sensitive data. The findings highlight the importance of better security measures and user awareness. Key initiatives include user education, behavioral analysis, technology solutions, and collaboration with app developers. Educational initiatives should promote knowledge of social engineering and phishing attacks, teaching users how to identify and avoid suspicious activity. Social media user behavior analysis can help discover vulnerabilities, and mobile apps should feature effective spam filters, URL scanners, and real-time threat detection systems.

It was found that Safari has a strong security mechanism that prevents these kinds of assaults after simulating attacks on iOS and Android devices with different browsers. All other browsers had effective simulations that captured and projected comprehensive data, including a picture of the target user. Safari, on the other hand, constantly rejected the attacks by showing a picture of the attacker. Throughout several tries, this behavior was consistently seen. The security architecture of the browser directly affects how effective these assaults are; the more vulnerable the browser's security programming, the faster the attack can be carried out, while stronger security programming makes the attack much more difficult. Based on these findings, it is recommended that users and organizations prioritize using browsers with strong security mechanisms, such as Safari, to enhance protection against social engineering attacks. Additionally, developers should focus on strengthening the security architecture of their browsers to mitigate such threats effectively.

It is critical to collaborate with app developers on implementing these security features, as well as advocating for strong privacy settings, two-factor authentication, and regular security upgrades. Prioritizing user safety in guidelines and supporting ongoing awareness activities will strengthen defenses against social engineering threats. Following these suggestions will improve mobile application security, lower the risk of data breaches, and enable users to make more informed decisions, protecting against new cyber threats.

REFERENCE

RafsanjanyKushol, Imamul Ahsan, and Md. nishatraihan, "An androidbased Useful text extraction framework using image and natural language Processing," *International Journal of Computer Theory and Engineering* vol. 10, no. 3, pp. 77-83, 2018

Frizell, S. 2018. How kenya's new data privacy bill could hurt its economy, Accessed November 8, 2018. https://www.cfr.org/blog/how-kenyas-new-data-privacy-bill-could-hurt-its-economy.

HaticeIşıkOzata, Onder Demir, and BuketDoğan, "Analysis of Patentsin Cyber security with text mining," *International journal of computer theory and engineering* vol. 13, no. 1, pp. 24-28, 2021.

Abdulateef. M. Yaser Al-Bustani, "RBYG Behavior Patterns Theory= @psy_bustani,"2020.[Online].Available:https://www.instagram.com/stories/highlights/17893960822538579/.[Accessed: 09-Feb-2023].

Mohammed A. M., Siddeeq Yousif Ameen and Subhi RR. M. Zeebaree.2020. Social Media Networks Security Threats, Risks andRecommendation: A Case Study in the Kurdistan Region. *International Journal of Innovation, Creativity and Change*, Vol. 13, Issue 7.

Alana Maurushat. 2019. *Ethical Hacking*. University of Ottawa Press,Canada.

[6] Fatima Salahdine and Naima Kaabouch. 2019. *Social EngineeringAttacks: A Survey*. Future Internet 11, No. 4:89. DOI: 10.3390/fi11040089[7] Ahmad MtairAlhawamleh. AlorfiAlmuhannad Sulaiman M, Ghada Al-Rawashdel and Jassim Al-Gasawneh. 2020. Cyber Security and Ethical Hacking: The Importance of Protecting User Data. Solid State Technology, Vol. 63, Issue 5.

Edgar Weippl, HeidelindeHobel, Katharina Krombolz and MarkusHuber. 2015. *Advanced Social Engineering Attacks*. Journal ofInformation Security and Applications. Journal of Information Securityand Applications, Vol. 22, 113-122. DOI:10.1016/j.jisa.2014.09.005

Pistol, M. S., Popescu, F., Paun, M. A., &Paun, V. P.Simulation Of New MethodsUsing Applications Which Exflitrate Data From Android Phones.11] Siby, A., & GS, M. A. 2020. Android Hacking Using Msfvenom:Integrating NGROK.

Palmieri, M., Shortland, N., McGarry, P., 2021. Personality and online deviance:The role of reinforcement sensitivity theory in cybercrime. Comput. Hum.Behav. 120, 106745

a, L., et al., 2021. Security control for two-time-scale cyber physical systemsWith multiple transmission channels under DoS attacks: The input-to-stateStability. J. Franklin Inst. B

www.ijcrt.org © 2023 IJCRT | Volume 11, Issue 9 September 2023 | ISSN: 2320-2882IJCRT2309500 *International Journal of Creative Research Thoughts* (IJCRT) www.ijcrt.org e169

RafsanjanyKushol, Imamul Ahsan, and Md. nishatraihan, "An androidbaseduseful text extraction framework using image and natural language processing," *International Journal of Computer Theory and Engineering* vol. 10, no. 3, pp. 77-83, 2018.

AranaM. 2017. How much does a cyberattack cost companies? Retrieved October 2022 from https://opendatasecurity.co.uk/how-much-does-acyberattack-cost-companies/

HaticeIşıkOzata, Onder Demir, and BuketDoğan, "Analysis of Patents in Cyber security with text mining," *international journal of computer theory and engineering* vol. 13, no. 1, pp. 24-28, 2021.

Mohammed A. M., Siddeeq Yousif Ameen and Subhi RR. M. Zeebaree. 2020. Social Media Networks Security Threats, Risks and Recommendation: A Case Study in the Kurdistan Region. *International Journal of Innovation*, Creativity and Change, Vol. 13, Issue 7.

Alana Maurushat. 2019. *Ethical Hacking*. University of Ottawa Press,Canada.

Fatima Salahdine and Naima Kaabouch. 2019. *Social Engineering Attacks: A Survey*. Future Internet 11, No. 4:89. DOI:10.3390/fi11040089

Ahmad MtairAlhawamleh. AlorfiAlmuhannadSulaiman M, Ghada Al-Rawashdel and Jassim Al-Gasawneh. 2020. Cyber Security and Ethical

Hacking: The Importance of Protecting User Data. Solid State Technology, Vol. 63, Issue 5.

APPENDIX 1

INSTALLATION OF KALI APPLICATION

A Linux distribution built on the Debian platform, Kali Linux was created especially for enhanced security testing and auditing. It provides a full package of tools for network analysis, vulnerability assessment, and digital forensics, tailored exclusively to security professionals. This operating system is strong and well-suited for evaluating the security of computer systems, networks, and software applications.

Setting up Kali Linux is straightforward and can be done on a variety of hardware configurations, including desktops, laptops, and virtual machines. Regardless of your platform, installing Kali Linux gives you simple access to its powerful security features.

Before choosing and configuring a new virtual machine to run Kali Linux, the 64-bit ISO image has to be downloaded. Here, the name of the virtual machine, the ISO image location, and the RAM and CPU count were set. Based on the system specs, 2GB of RAM and 1 CPU were selected. A virtual hard disc was generated with the choice to add a new virtual hard disc file or use an existing one after the VM hardware was configured. Preinstallation tweaks included changing the Attached to field in the network section to Bridge Adapter and setting Shared Clipboard and Drag'n'Drop to Bidirectional. And then Kali started to be installed.

The Kali Linux installer menu showed up when the new virtual machine (VM) powered on, and users could choose between Graphical install, default language, country, and keyboard mapping. After setting up the hostname, domain, and system setup, the virtual hard disk's bootable partition was created. Furthermore, the operating system underwent customization. The virtual machine was restarted when the installation was finished, and a login screen showed up. The screen would show the Kali Linux desktop after inputting login credentials.

APPENDIX 2

STOMBREAKER INSTALLATION

The URL for storm-breaker repository on git-hub where secured, which would be subsequently use to download the Storm-Breaker file. After securing the link, the running of storm-breaker file from a local machine called Kali where employed. The kali machine terminal from legal root user were employed to be the next step, so as to enable me conduct whatever task I want to conduct. The CD /OPT (CD: change directory & OPT: optional) to be on the OPT directory where used, follow by using the command git clone https://github.com/ultrasecurity/Storm-Breaker.git to clone the program to the local machine. After the file would have been successfully downloaded, the command "LS" to see the files where performed, some couple of file and directories where then used. In it, it would be expected to have a file called Storm-Breaker, the "CD Storm-Breaker" command were used to change directory to that of storm-breaker, the "LS" command would be also use to open the storm-Breaker file, it would be expected that we would have a file inside, called "install.sh" script. However, before the install script program will be perform, the command "apt update" would be perform to update the all the files, the operation will now be ready to command "apt install" so as to install the required packages which are python3-request, python3-colorama, and python3-PSutil and after all the packages are installed and then clear the screen, follow by performing "LS" on the "OPT/Storm-Breaker" directory so as to locate where the install.sh script is found, the script using the command "bash install.sh" will be perform, in order to further the complete installation and configuration, the program would be further perform by using python3 st.py. Two links are expected to be obtained after the running of the program, which the first one is the link to the admin panel that would only work on a particular machine and the second one is the NGROK programme which would allow people to have access to the link from different places and different devices.

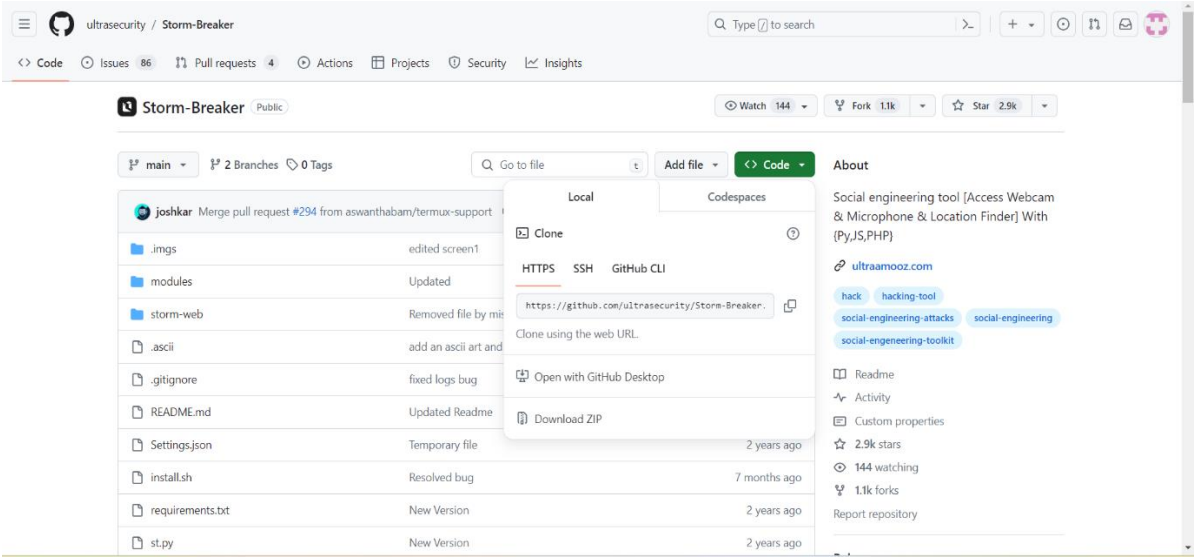

Fig. 15. GitHub cloning link

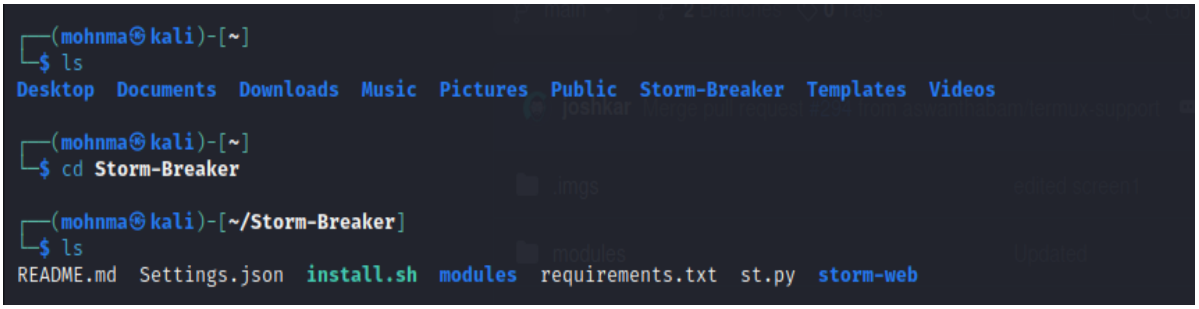

Fig. 16. Listing the files on the machine

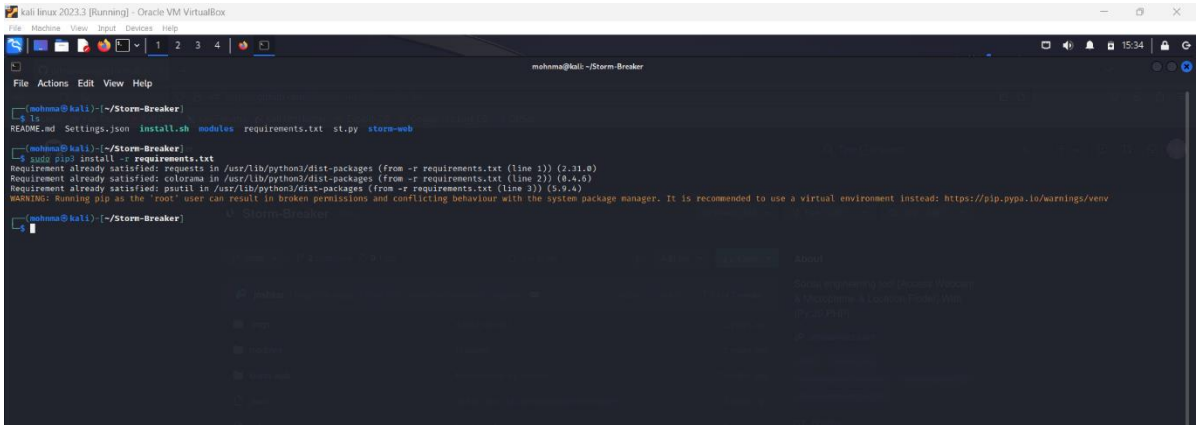

Fig. 17. Downloading the requirement.txt file

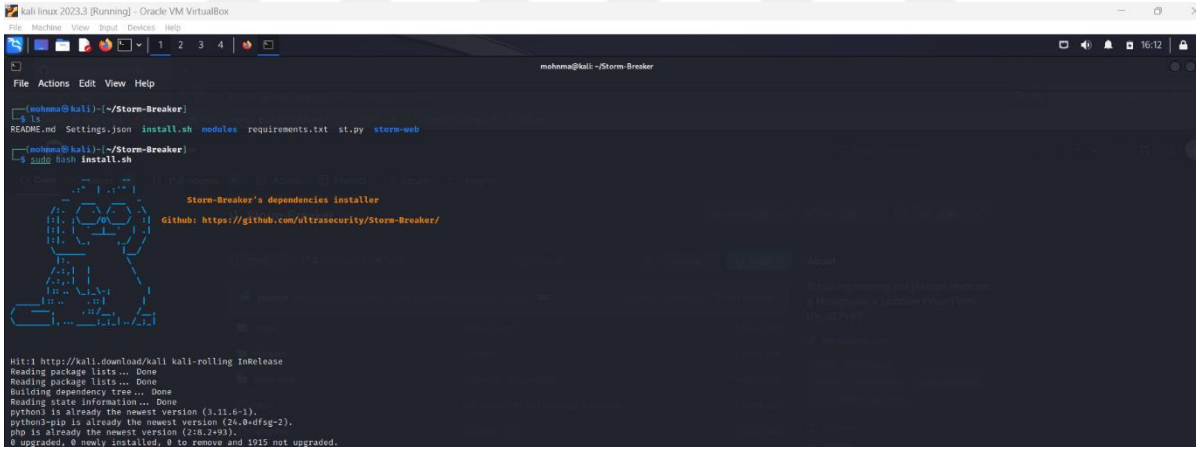

Fig. 18. Installation complete