IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205344 |

Social Engineering and Cyber Security

Aditi Tanaji Shinde, Mrunali Mangesh Pawar, Prof. Waman Parulekar

P.G. Student, Department of MCA, Finolex Academy of Management and Technology, Ratnagiri, Maharashtra, India

P.G. Student, Department of MCA, Finolex Academy of Management and Technology, Ratnagiri, Maharashtra, India

Associate Professor, Department of MCA, Finolex Academy of Management and Technology, Ratnagiri, Maharashtra, India

ABSTRACT: Social engineering attacks have posed a serious security threat to cyberspace. However, there is much we have yet to know regarding what and how lead to the success of social engineering attacks. This paper proposes a conceptual model which provides an integrative and structural perspective to describe how social engineering attacks work. Three core entities (effect mechanism, human vulnerability and attack method) are identified to help the understanding of how social engineering attacks take effect. Then, beyond the familiar scope, we analysed and discuss the effect mechanisms involving 6 aspects (persuasion, social influence, cognition & attitude & behaviour, trust and deception, language & thought & decision, emotion and decision-making) and the human vulnerabilities involving 6 aspects (cognition and knowledge, behaviour and habit, emotions and feelings, human nature, personality traits, individual characters) , respectively.

KEYWORDS: CyberSecurity, Social Engineering, Security, Phishing**,** Watering Hole, Spyware.

I. INTRODUCTION

In the context of computer and cyber security, social engineering describes a type of attack in which the attacker exploit human vulnerabilities by means such as influence, persuasion, deception, manipulation and inducing, so as to get classified information, hack computer system and network, obtain unauthorized access to restricted areas, or breach the security goals (such as confidentiality, integrity, availability, controllability and auditability) of cyberspace elements (such as infrastructure, data, resource, user and operation). Succinctly, social engineering is a type of attack wherein the attacker exploit human vulnerability through social interaction to breach cyberspace security.

In hacker community, social engineering is a quite popular attack since 1970s. Compared to classical computer attacks such as password cracking by brute-force and software vulnerabilities exploit, social engineering attacks focus the exploitation of human vulnerabilities, to bypass or break through security barriers, without having to combat with firewall or antivirus software by deep coding. In addition, there is not a computer system doesn't rely on humans or involves human factors on earth, and these human factors are obviously vulnerable or can be largely turned into security vulnerabilities by skilled attackers. These inevitable and vulnerable human factors makes social engineering to be a universal cybersecurity threat. For some situations, social engineering attacks may be as simple as making a phone call and impersonating an insider to elicit the classified information. Moreover, with the development of new technology and the formation of new cyber-environment, social engineering threat is increasingly serious. Social Network Sites (SNSs), mobile communication, Industrial Internet and Internet of Things (IOT) generate not only large amounts of sensitive information about people and devices but also more attack channels and a bigger attack surface. Unrestricted office environment (bring your own device, remote office, etc.) leads to the weakening of area-isolation of different security levels and creates more attack opportunities.

II. RELATED WORK

Three core entities (effect mechanism, human vulnerability and attack method) are identified to help the understanding of how social engineering attacks take effect. Then, beyond the familiar scope, we analysed and discuss the effect mechanisms involving 6 aspects (persuasion, social influence, cognition & attitude & behaviour, trust and deception, language & thought & decision, emotion and decision-making) and the human vulnerabilities involving 6 aspects (cognition and knowledge, behaviour and habit, emotions and feelings, human nature, personality traits, individual characters) , respectively. Finally, 16 social engineering attack scenarios (including 13 attack methods) are presented to illustrate how these mechanisms, vulnerabilities and attack methods are used to explain the success of social

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205344 |

engineering attacks. Besides, this paper offers lots of materials for security awareness training and future empirical research, and the model is also helpful to develop a domain ontology of social engineering in cybersecurity.

III. METHODOLOGY

SECTION I

The easy availability of open source intelligence simplifies the information gathering. Specific targets can be carefully selected to craft more creditable and targeted social engineering attacks. A large group of victims can be reached at the same time and some open source tools can be used to launch semi-automated attacks. Technologies such as machine learning and artificial intelligence is likely to make social engineering attacks more efficient and aggressive. Targeted, large-scale, robotic, automated and advanced social engineering attack is becoming possible. Social engineering is evolving to be a serious, universal and persistent security threat. To protect against social engineering attack, an important work is to understand how it works and takes effect. This paper makes the following contributions. An integrative and structural model to describe how social engineering attacks work and take effect.

Three core entities to get an insight into social engineering attacks.
• 30+ effect mechanisms involving 6 aspects.
• 40+ human vulnerabilities involving 6 aspects.

SECTION II

A Conceptual Model of How Social Engineering Attacks Work and Take Effect

In a cyber-attack, attacker and victim (target) are entities at the two ends. For social engineering, the attacker (a.k.a. social engineer) is the party conducting a social engineering attack; the victim is the party suffering a social engineering attack and bring about an attack consequence. In general, the social engineering attack process can be described as follows: We will analyse and discuss the effect mechanisms and human vulnerabilities in the Section III and Section IV respectively. Section V will study a set of social engineering attack scenarios where many attack methods are included, to illustrate how these mechanisms, vulnerabilities and attack methods explain the success of social engineering attacks. Section VI shows the discussion. Section VII concludes the paper.

SECTION III

Effect Mechanisms in Social Engineering

This section analyses and discusses social engineering effect mechanisms in 6 aspects: 1) persuasion, 2) social influence, 3) cognition, attitude and behaviour, 4) trust and deception, 5) language, thought and decision, 6) emotion and decision-making.

A. Effect Mechanisms in Aspect of Persuasion

1) Similarity, Liking and Helping in Persuasion

Similarity invites liking, dissimilarity leads to dislike. The more someone's attitudes are similar to our own, the more we will like the person. On the contrary, we tend to decrease liking when getting to know someone and discovering the person is actually dissimilar.

2) Distraction in Persuasion and Manipulation

People typically have a limited range of attention in sight, hearing and thought. Distraction facilitates persuasion mainly by disrupting the counter-argue process and increasing the effort to communication. It is effective both online and on the scene.

3) Source Credibility and Obey to Authority in Persuasion

People have a tendency to comply with authoritative figures automatically. In most cultures, especially the collectivist culture, people are told that to believe who are authoritative, expert and familiar, since these characteristics signify the credibility, trustworthiness and low-risk.

4) Cognitive Response Model, Two Routes to Persuasion and Elaboration Likelihood Model

Petty conducted a cognitive response analysis of the persistence of attitude changes induced by persuasive communications, in which a cognitive response model was proposed to show that enduring attitudes changes are the result of cognitively responding to the message content, while temporary attitudes shifts are the result of persuasion cues.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205344 |

B. Effect Mechanisms in Aspect of Social Influence

1) Group Influence and Conformity

People live in and influenced by groups almost all the time. Conformity is a change in behaviour or belief to accord with others as the result of real or imagined group influence. There are many factors affect the conformity, such as group size, group unanimity, group cohesion and individual's public response

2) Normative and Informational Influence

Usually, an individual may bend to the group in order to be accepted or to obtain important information. The former is called normative influence and the latter is called informational influence. Conformity caused by normative influence is motivated by the desire to be accepted or liked, or to avoid group pressure. When deviating from social group norms, people often bear social pressure and pay an emotional price.

3) Social Exchange Theory and Reciprocity Norm

Social exchange theory shows that people exchange not only material goods and money but also social goods such as love, services, information and status. The consideration or subtle calculation about cost and reward predict people's decision and behaviour. Reciprocity norm refers that we should return help but harm to those who help us. We shall try to repay similar with what another person has provided us. If others do us a favour, we shall do them a favour in return.

4) Social Responsibility Norm and Moral Duty

Different from the reciprocity norm where the balance of giving and receiving are considered, social responsibility norm advocates that people should help those who need help, without concerning the future reciprocate and exchanges . It is a kind of expectation towards moral duty for helping. In collectivist culture countries, people support the social responsibility norm more strongly than individualist culture countries. They advocate an obligation to help others even they are not facing a life-threatening trouble.

5) Self-Disclosure and Rapport Relation Building

Derange and Berg researched on the self-disclosure and described the disclosure reciprocity effect. It shows that during the building of social relation, self-disclosure begets self-disclosure, and we have a willing to reveal more to those who open their hearts to us. It is gratifying to be selected as the person for another's self-disclosure

C. Effect Mechanisms in Aspects of Cognition, Attitude and Behaviour

1) Impression Management, Cognitive Dissonance and Commitment and Consistency

It is a human nature to care about what others think of us. Self-presentation theory shows that we want to present a favourable impression both internal to ourselves and external to other people, so that to feel better about ourselves, to gain social and material rewards, and even to become more secure in our social identities.

2) Foot-in-the-Door: Behaviour Affects Attitude

If you want people to do you a big favour, an effective strategy is to get them to do a small favour first. In an experiment, experimenters who claim they are from the Community Committee for Traffic Safety asked some Californians (control group) to install a very large sign that said "Drive Carefully" in their front lawn; only 17% people consented.

3) Bystander Effect, Diffusion of Responsibility and Deindividuation

Bystander effect describes the phenomenon that a person is less likely to provide help when there are bystanders' presence. In other words, the person who needs help is actually less likely to get help when many people are around. The person in need is more likely to get help when bystanders present alone, and the more bystanders to an emergency, the less likely or the more slowly a bystander will intervene to provide aid In large cities, the increasing numbers of bystanders who are strangers often depress helping.

4) Scarcity: Perceived Value and Emotion-Arousing

Scarcity manipulates people mainly by affecting value cognition, arousing emotion and enhancing motivation. "Opportunities seem more valuable to us when they are less available". Economics and social experience told people that the scarce resource implies less accessible, more competing risk and less freedom. Hence, people assign more value to the scarce things, although usually this subjective value are overestimated.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205344 |

5) Time Pressure and Thought Overloading

Time pressure affects people's logical thinking. When people have to deal with a large amount of information in a limited time, request messages that shall be examined are often responded rashly and superficially. Besides, time pressure might lead to emotion-arousing, such as anger, tension and anxiety, which inhibits cognition by making thinking difficult.

D. Effect Mechanisms in Aspects of Trust and Deception

1) Relation Between Trust and Social Engineering

Trust is an important variable that predicts the user's susceptibility to social engineering attacks. Chitrey et al. conducted a survey showing that "90% of the participants think that people in India generally have a higher level of social trust, which implies that they are more vulnerable to social-engineering based attacks". In many social engineering attack scenarios, it requires to convince the targets that the attacker is a trustworthy person.

2) Factors Affecting Trust

There are three basic objects involved in analysing factors affecting trust building: the trustee (attacker), the trustor (target, victim) and situation. Mayer presented an integrative model of organizational trust, in which trust propensity, perceived trustworthiness of trustee and perceived risk are considered as factors affecting the trust behaviour (a risk taking) of a trustor.

3) Factors Affecting Deception

Usually, deception is intentional, strategic interaction behaviour's launched by the deceiver. Although most people are confident that they can detect social deception, interpersonal deception theory (IDT) suggests that they cannot. IDT attempts to explain the process and outcomes of deception in interpersonal conversations based on the deception analysis, propositions and evaluation. to receivers' truth biases, context interactivity, senders' encoding skills, informational and behavioural familiarity, receivers' decoding skills, and senders' deviation from expected patterns .

E. Effect Mechanisms in Aspects of Language, Thought and Decision

1) Relation Between Language and Thinking

Language is the most common tool for social interaction meanwhile it is closely related to the processing, generating and expressing of thought. Language can be compared to the computer program used for communication. The words we hear are the inputs and the streams of thought are outputs, vice versa.

2) Framing Effect and Cognitive Bias

Framing effect is an interesting phenomenon reflecting cognitive bias, in which people make decisions and express opinions influenced by the way a question or an issue is described. In other words, for the same problem with different expression, different choices are made. For instance, beef labelled as "25% fat" versus beef labelled as "75% lean", the latter is preferred usually.

3) Indirectness of Thinking and Negative Expression in Language

The dependence of thinking on language (Section III-E1) leads to the indirectness of semantics transmitting, which creates opportunities for language hinting and inducing. Furthermore, the cognitive indirectness for negative language expressions can also result in influence and manipulation.

4) Language Evokes Thinking Confusion

Language can be used to evoke a thinking confusion state, in which behaviours are suggested and commands are embedded; this provides the attacker an opportunity to induce and manipulate the targets to take actions that may breach security policy.

F. Effect Mechanisms in Aspects of Emotion and Decision-Making

1) Emotion and Feeling Affect Decision-Making

A familiar view regarding human decision-making is that people make decisions through the dual systems of emotion and reason: one is generally emotional, fast, automatic, and the other is cognitive, slow, and deliberative. In fact, the mechanisms of emotion and decision is very complex.

2) Emotion, Facial Expression, Deception and Deception Detection

For social engineering attacks where deception is used, the attacker as the deceiver will pay greater cognitive exertion to exhibit strategic information, behaviour and image management meanwhile strive to avoid nonstrategic deception

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205344 |

leakage. However, with the increasing of receivers' familiarity towards information, behaviour and relation, the attacker not only experience more detection apprehension but also exhibit more nonstrategic leakage behaviour . The leakage of deception is usually reflected on non-verbal signals, especially facial expressions. Non-verbal signals permeate in the vast majority of social interactions and people perceive and comprehend them consciously or unconsciously.

Micro Expression Training Tool (METT) and Subtle Expression Training Tool (SETT) have been also developed for facial expression recognition analysis and training. These tools related facial expressions and micro-expression are helpful in social engineering defence.

SECTION IV

Social engineering attacks exploit a wide range of human vulnerabilities. This section discusses these vulnerabilities in the following aspects: 1) cognition and knowledge, 2) behaviour and habit, 3) emotion and feeling and 4) psychological factor. And the psychological vulnerabilities are further divided into three levels, i.e. 1) human nature, 2) personality traits and 3) individual characteristics, from the evolution perspective of human wholeness to individuation.

A. Human Vulnerabilities in Cognition and Knowledge

Thinking set (inertial thinking) is a relatively rigid way, process or mode to think about something. It can be also described as a relatively stable behavioural tendency or psychological readiness state that derived from / built on the previous experience and cognition. Thinking set helps people quickly address problems in the familiar environments, yet it will hamper the right treatment to new matters when situation changed. Stereotype and prejudice are similar vulnerabilities.

B. Human Vulnerabilities in BEHAVIOR and Habit

When a person does not pay enough attention to the security context , does not think about the potential security risk or is unwilling to make necessary work or effort to prevent a security threat , the person will be a target through whom a social engineering attack occurs easily.Fixed action pattern exists in behaviour's of both animals and humans, which consists of a series of relatively invariant instinctive behaviour's triggered by a key stimulus.

C. Human Vulnerabilities in Emotion and Feeling

Emotions and feelings influence cognition, attitude and decision-making (Section III-F1, III-C). Emotions (fear, tension, curiosity, excitement, surprise, anger, impulsion, etc.) and feelings (happiness, sadness, disgust, guilt, etc.) are all human factors can be exploited as security vulnerabilities in social engineering attacks. Fear of getting into trouble with the superiors is often used in name-dropping approach to elicit sensitive information, and fear-arousing presented in Section III-C4 is also a case in point.

D. Human Vulnerabilities in Human Nature

Human nature is a collection of psychological characteristics at the macro level, which describes the fundamental psychological characteristics shared naturally by the whole human being. Some human natures are security vulnerabilities exploitable in social engineering attacks. People who pay close attention to themselves and their desires will magnify the ambient influence and increase the susceptibility to induce, persuade and manipulate in social engineering

E. Human Vulnerabilities in Personality Trait

Individuals' personality traits significantly contribute to their susceptibility to social engineering exploits such as influence, manipulation and deception. Social engineers treat human personality traits as vulnerabilities and use the language as their weapon to deceive, persuade and finally manipulate the victims. Personality traits are the psychological structure or characteristic set of habitual patterns of behaviour, thought, and emotion, which evolve from the biological inheritance predominantly with the influence of environmental factors.

F. Human Vulnerabilities in Individual Character

Individual characters are psychological characteristics that acquired with the influence of external environment and developed based on human nature and personality traits. In the context of cybersecurity, when some positive individual characteristics are immoderate or in an inappropriate situation, negative results can be generated. If trust is substituted by credulity, deception occurs easily.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205344 |

SECTION V

Case Study: Social Engineering Attack Scenarios Analysis

This section presents 16 social engineering attack scenarios (Table 1) to illustrate how to use the three core entities (i.e. effect mechanisms, human vulnerabilities and attack methods) of the conceptual model to get an insight into social engineering attacks. Some of these attack scenarios are based on cases in work, and 13 types of social engineering attack methods are included in these 16 scenarios.

In Table 1, the first column describes the attack method and scenario, and the 2nd and 3rd column respectively show the corresponding effect mechanisms and human vulnerabilities. These items in the latter two columns cover almost all the effect mechanisms discussed in Section III and the human vulnerabilities discussed in Section IV.

We intended to detail every attack scenario in Table 1, yet in order to avoid generating a set of dangerous attack guide or script, as well as to avoid the verbose caused by the same description or the well-known explanation, a trade-off was made: we select the most complex attack scenario as an example and discuss it in great detail .As a case in point, the reverse social engineering attack scenario (No. 16) is expounded as follows.

The attacker firstly sends an email using faked address (technical support department) to a new employee informing he

/ she that “a network test will be conduct recently, and if there is a network failure, please contact xxx xxxx (the attacker’s phone number).”

Then, the attacker makes a network fault and waits for the new employee’s request.

Usually, new employees don’t know many colleagues yet, and they don’t know the procedures or the dos and don’ts of the organization (inexperience). When a network failure occurred, they call to the technical support using the number informed before.

After helping to resolve the problem, the attacker says sincerely “Would you like to do us a favour, just one minute, that completing a survey used for developing a security awareness and training program for new employees; nearly 80% of the employees have already done this.”

In order to make a good first impression, new employees are eager to show how cooperative and quick to respond they can be (agreeableness, the desire to be helpful, conformity). This involves the impression management theory. With the influence of reciprocity norm, the attacker’s help to resolve the problem portends the new employee’s favour and commitment. The benevolence of “security awareness and training program for new employees” and the sincere voice enhance the trust (intuitive judgement).Low time cost (“just one minute”) enhances the desire to be helpful. The group influence and cognitive bias of framing effect (“80% of the employees have already done this”) lead to a conformity. Thus, a commitment is obtained (“Ok, my pleasure”).

The regular conversation that “Are you aware of our email policies?…It can be dangerous to open unsolicited attachment…“ reflects the integrity and benevolence further. A high level of trust is likely obtained.

In this situation, “We need to know your password to evaluate the security awareness of new employees” maybe cause the new employee a slight worry, but “80% of the employees have already done this” lead to the diffusion of responsibility. Furthermore, the commitment and consistency compelling he / she continue the disclosure.

In addition, the expression that “It is a secure matter” not only means “know your password” is a matter about security (a routine that “to evaluate the security awareness of new employees”), but also implies that “know your password” is a secure matter without danger (which relieves the worry).

This language expression evokes the thinking confusion state, in which the new employee’s behaviour and decision are induced and manipulated.

The attacker designs a great deal of strategic activities (interpersonal deception theory, IDT) and uses many factors affect trust and deception.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205344 |

Ultimately, the new employee's password is compromised ("Okay, the password is…").

SECTION VI

Discussion

A. Related Work

Social engineering is an interdisciplinary field which involves computer science, cybersecurity, psychology, social psychology, cognitive science, psycholinguistics, neuroscience, brain science, etc. In work, human vulnerabilities such as credulity, greed, ignorance, curiosity, carelessness, helpfulness have been mentioned. Yet only the human vulnerabilities are not sufficient to describe how social engineering attacks take effect. For effect mechanism, some works discussed or involved it in different context. Many scholars, e.g, employ Coalmine's six principles of influence and persuasion (reciprocation, commitment and consistency, social proof, liking, authority, scarcity) to explain the success of social engineering attacks. Literature also discussed some psychological principles that exhibit some kind of power to influence or persuade people and take effect during a social engineering attack (strong affect, overloading, reciprocation, deceptive relationships, diffusion of responsibility and moral duty, authority, integrity and consistency). Mitnick and Simon describes social engineering based on various kinds of deception. Stajano and Wilson discussed seven principles of scam for system security (distraction, social compliance, herd, dishonesty, kindness, need and greed, time). Ferreira et al. analysed the relation (equal, include, overlap) among the above principles and presented a merged list of social engineering persuasion principles, i) authority, ii) social proof, iii) liking, similarity & deception, iv) commitment, reciprocation & consistency, v) distraction. However, the human vulnerabilities were not carefully concerned in these works, and other aspects of effect mechanisms are not involved.

B. About the Conceptual Model

The conceptual model presented in Section II provides an integrative and structural perspective to understand how social engineering attacks work, rather than a single perspective. The model might be simple, yet it is also easy to understand. Although the model is not sufficient to constitute a domain ontology for social engineering, it identified three significant entities to get an insight into how social engineering attacks take effect. It conveys a concise idea that the attacker formulates certain attack scenarios to drive an organic combination of attack methods, effect mechanisms and human vulnerabilities, through which the attack process take effect to achieve the attack goal.

In addition, this model clarifies and avoids some mix-up among different entity types. For instance, impersonation, decoying, human vulnerabilities (friendliness, sympathy, ignorance) and six influence principles are treated as close-access techniques to exploit someone's trust in.

C. About the Level of Effect Mechanisms

Although some synthesized principles of persuasion were presented in [89], the underlying mechanisms were neglected. For instance, the second merged principle social proof (sp) consisted of three principles: i) diffusion of responsibility and moral duty, ii) social proof and iii) herd, and their logical relation was described as i) $\subset$ iii) $\subset$ ii). However, 1) the underlying mechanism of diffusion of responsibility is that the group situation reduces the individual's evaluation apprehension, which offers the victims an excuse to avoid responsibility for their behaviours; 2) the underlying mechanism of principle social proof and herd is informational influence, in which the victims attempt to avoid unknown risks or seek the correct direction / behaviour with the assumption that the actions (information) of group are correct; 3) moral duty is a kind of social norm in many cultures taking effect by normative influence: people are influenced to do something the norm requires due to the desire to be accepted or liked, regardless of their behaviour is correct or not. Thus, a merged principle to "constitute a basis for principles of social engineering" in fact is based on three different underlying mechanisms.

We conducted an analysis of the effect mechanisms toward the fundamental level as much as possible, rather than a simply and upwards grouping. Hence, this paper offers a more clear explanation why the victims are exploited and why social engineering attacks become effective.

D. About the Coverage and Completeness

Besides the items mentioned in Section VI-A, this paper analysed and discussed a wider range of effect mechanisms and human vulnerabilities. Overall, 30+ effect mechanisms in 6 aspects (persuasion, social influence, cognition, attitude and behaviour, trust and deception, language & thought and decision, emotion and decision) and 40+ human vulnerabilities in 6 aspects (cognition and knowledge, behaviour and habit, emotion and feeling, human nature,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205344 |

personality traits, individual characteristics) were summarized in Figure 2 (Appendix VII). Moreover, 16 attack scenarios together with these mechanisms and vulnerabilities are presented.

Nevertheless, did this paper provides a complete and exhaustive discussion of effect mechanisms, human vulnerabilities and attack methods for social engineering? The answer is 'No'. This is probably an unsolvable problem. Social engineering attacks not only exploit the obvious human vulnerabilities, but also the inconspicuous human factors. It seems every human factor involved provides the attacker a chance to turn it into a vulnerability. With the technology development and cyber-environment change, the attacker will create more attack scenarios, in which new attack methods are crafted, new effect mechanisms are found and more human vulnerabilities are exploited.

Even so, the presented mechanisms, vulnerabilities, scenarios and methods constitute plenty of materials for education, security awareness and training programs. Administrators, staffs, users and the public can use the proposed model as a knowledge schema of these materials. Both the material and model are helpful to increase the ability to understand and tackle with social engineering threat. And more attack scenarios can be generated based on the model and presented items. The education programs can be conducted by reminder, brochures, screensavers, courses, discussion, serious games, role-playing activities, penetration test, etc.

E. Limitation and Implication

This paper analysed and discussed many effect mechanisms and human vulnerabilities, 16 attack scenarios were also presented to illustrate their application. Although many of them are obvious effective or have been validated, there also some items are just theoretical feasible in the social engineering field (based on theoretical analysis and case study), i.e. they have not been empirical investigated. This is a limitation of this paper. Besides, the effectiveness of mechanisms and exploitability of human vulnerabilities may be affected by different environments, such as culture (individualism, collectivism), scenario (reality, cyberspace), medium (email, websites) and industry (IT or non-IT). And, empirical studies focusing on social engineering attacks is still relatively few. Thus, more empirical research is needed in the future. On the other hand, one of the merits of theoretical research might be it explorers a wider range and provides an integrative perspective. This paper offers lots of factors that can be further examined for future empirical research.

The conceptual model consists of 7 entities, but there are also some important entities have not been included, e.g. attack medium, and some relations among these entities have not been carefully defined. Besides, the relations among effect mechanisms, human vulnerabilities and attack methods are many-to-many, which might be clear displayed in the knowledge graph. Thus, in future work we will study the domain ontology of social engineering and its knowledge graph application.

SECTION VII

Conclusion

This paper proposes a conceptual model which provides an integrative and structural perspective to help the understanding of how social engineering attacks work. Three core entities (effect mechanisms, human vulnerabilities and attack methods) to get an insight into how social engineering attacks take effect are analysed and discussed. A total of 30+ effect mechanisms and 40+ human vulnerabilities are summarized. Finally, 16 social engineering attack scenarios (which contains 13 attack methods) are presented to illustrate the application of these mechanisms, vulnerabilities and attack methods to understand how social engineering attacks work and take effect.

IV. EXPERIMENTAL RESULTS

A Socio-Technical Attack Example This section will reveal the detailed methodology of a technical attack by describing the execution of a simple example. For this, it will be used the Social Engineer Toolkit that comes pre-installed in Kali Linux (Fig. 1)

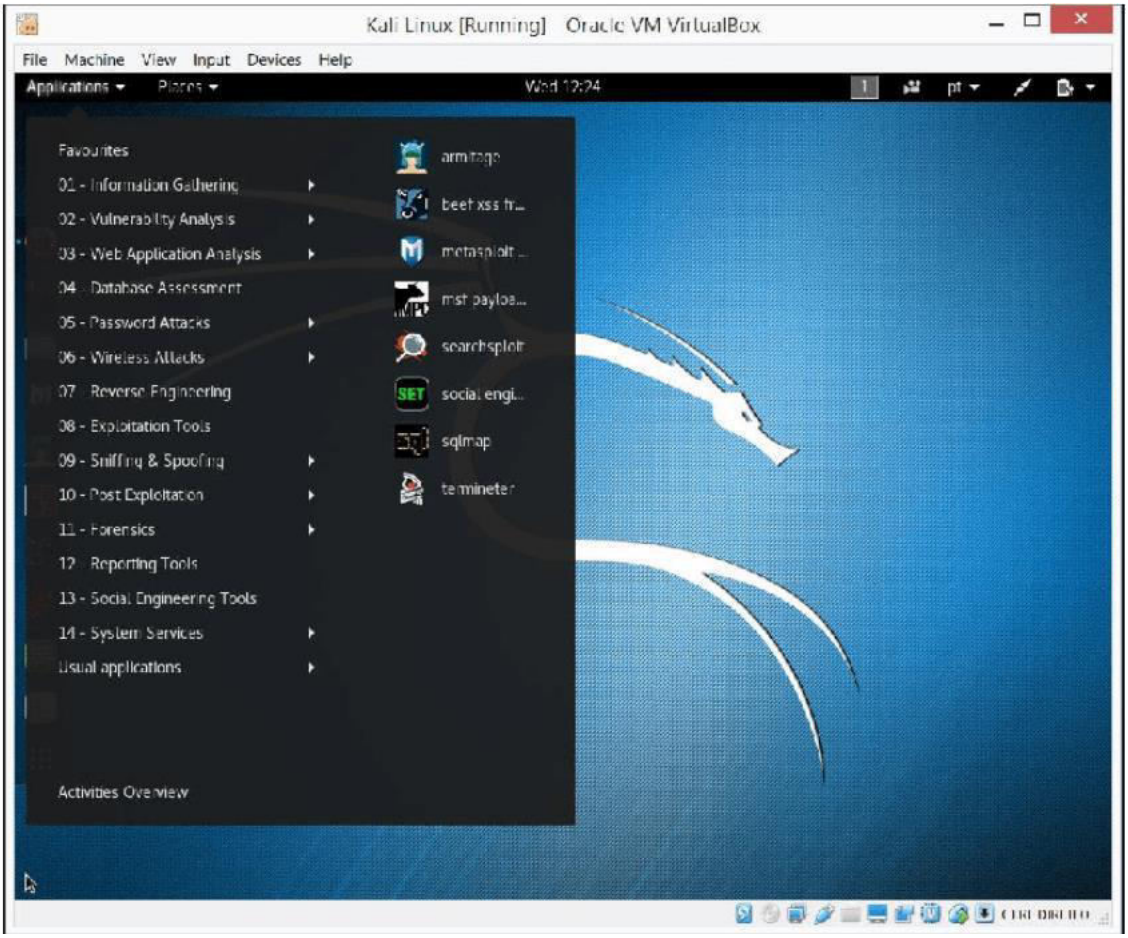
Baiting The attacker can use this physical attack vector by infecting a storage medium with malware, leaving it to be found by the targeted victim, who may naively plug it into the system. Watering hole This is one of the most advanced social engineering attack vectors, as it requires substantial technical knowledge. After researching, the attacker identifies one or more legitimate websites regularly visited by the target. Searches for vulnerabilities, infects the most propitious website for the attack and lies in wait. A Socio-Technical Attack Example This section will reveal the detailed methodology of a technical attack by describing the execution of a simple example. For this, it will be used the Social Engineer Toolkit that comes pre-installed in Kali Linux (Fig. 1). Figure 1 - A few exploitation tools including the Social-Engineer Toolkit Kali is a Debian Linux based operating system for penetration testing purposes, providing

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205344 |

an arsenal of tools designed for analysing and exploiting system vulnerabilities. Funded and maintained by Offensive Security, Kali Linux is a renowned open source project used by cyber security professionals and enthusiasts. The Social-Engineer Toolkit (SET), with over two million downloads is heavily supported within the cyber security community. Created by the founder of TrustedSec as an open source, menu driven, penetration testing tool, SET is now the standard framework for assisting advanced technological attacks in social engineering environments. To initiate the execution in Kali Linux all that is necessary, is to simply type "setoolkit" on the terminal, also accessible through the applications menu. Once the software executes, users are presented with a simple main menu that provides six options, and another one to exit the program (Fig.2). Given the subject of this paper, this attack demonstration is naturally focused on the first option, social engineering attacks. This attack example is a rudimentary phishing attempt of the website vector nature, and thus, in the social engineering attacks menu that follows, “Website Attack Vectors” is selected (Fig. 3).

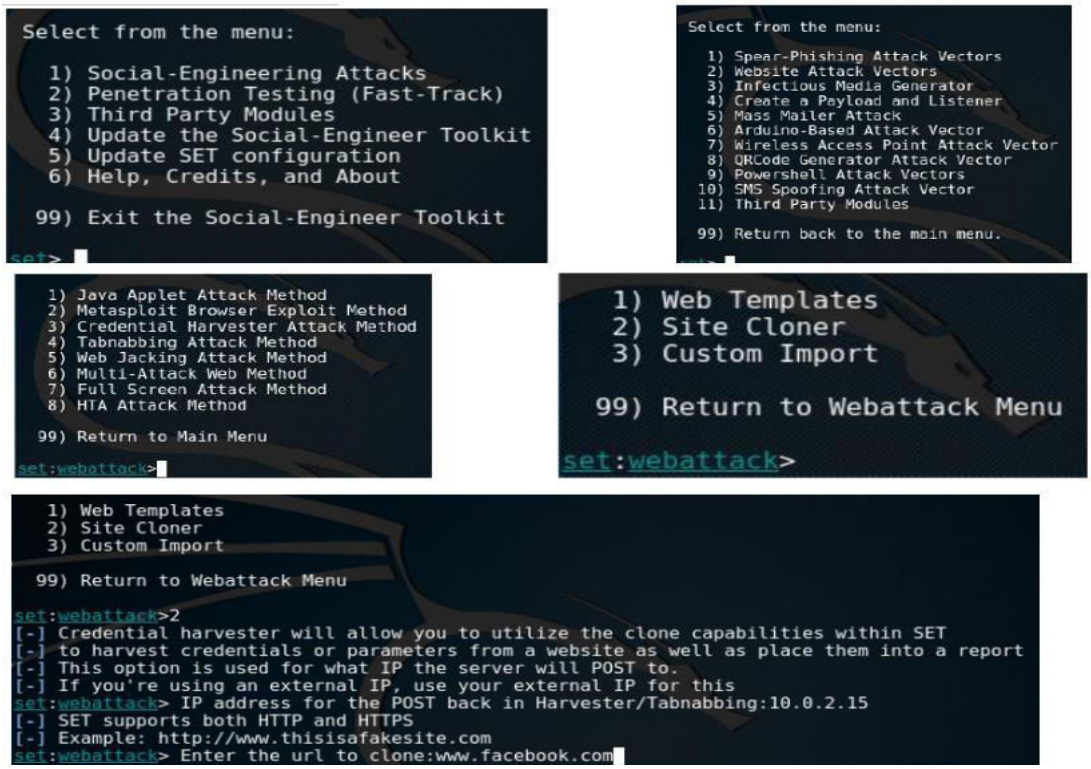


Kali rolling Linux Application tools Menu

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205344 |



V. CONCLUSION

The Information Age is maturing, complemented by an extremely increased usage of the Internet; humanity evolves rapidly as the growth of public accessible knowledge has been greatly nurtured and facilitated. Consequently, an unmistakable dependence on the World Wide Web has been established in civilization. The digital realm, as a propitious infrastructure for a grand variety of criminal offenses, has grown with the society needs to become an increasingly protected environment. Cyber security develops to grow in sophistication but individuals however, are currently more exposed than ever before. At present, cybercrime is practiced by threat actors that

do not necessarily possess a very substantial technical knowledge on information systems, they exploit the human vulnerabilities. Recent studies have shown that people are at the core of the infection chain in the greatest majority of cyber attacks. Social engineering is increasing both in sophistication and ruthless efficiency, because people, make the best exploits. As such, facts point to the conclusion that in the foreseeable future, social engineering will be the most predominant attack vector within cyber security, and thus deserve to be studied further as it evolves in order to advise good practices and measures for individuals and organizations.

REFERENCES

1. Wenke Lee, Bo Rotoloni, “Emerging cyber threats, trends and technologies”, Technical report, Institute for Information Security and Privacy, 2016. “Internet organized crime threat assessment”, Technical report, Europol, 2016.
2. James Comey, “Worldwide threats to the homeland: ISIS and the new wave of terror, statement before the house committee on homeland security”, FBI, July 2016. “Internet security threat report”, Technical report, vol. 21, Symantec, April 2016.
3. Nahal Sarbjit, Ma Beijia, Tran Felix, “Global cybersecurity primer”, Technical report, Bank of America Merrill Lynch, 2015.
4. Nabie Y Conteh, Paul J Schmick, “Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks”, International Journal of Advanced Computer Research, Vol.6 pp.23-31, 2016. [7]Nyirak,A.(2017) The Social Engineering Framework.https://www.social-engineer.org/framework /attack-vectors/attack-cycle/

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details