International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 35-46 www.ijaem.net ISSN: 2395-5252

A Review on Adapting Social Engineering Attack as One of the Penetration Testing Techniques

Nor Naematul Saadah Ismail[1], Fatin Izzati Fammy Rikzan[2], Suren Krishnan[3], Nur A'fyfah Zaimy[4], Mohamad Fadli Zolkipli[5]

[1,2,3,4] *Awang Had Salleh Graduate School, School of Computing, Universiti Utara Malaysia, Kedah, Malaysia*
[5]*School of Computing,Universiti Utara Malaysia,Kedah, Malaysia.*

Date of Submission: 25-02-2023 Date of Acceptance: 05-03-2023

ABSTRACT: In cyber security, there are plenty of threats and attacks used by the hackers to exploit vulnerabilities in any organization's system or network. Social engineering attack is one of the threats that is accomplished through human interactions instead of using software or system breach. Social engineering, which is known to use psychological manipulation, usually tricks humans to get sensitive information by luring them into making security mistakes. This attack can make the companies face financial loss and lack of trust from the clients due to the crucial information data leakage to the attacker. Ignorance and lack of awareness about this social engineering is one of the reasons this attack occurs. Penetration testing has been studied to be the efficient defense towards this attack. In this paper, there are several techniques of penetration testing to be discussed towards social engineering. This discussion came up with solutions and ideas which can reduce the social engineering attacks.

KEYWORDS: Penetration testing, social engineering, pen-test techniques.

I. INTRODUCTION

[1]described social engineering is as long as human existed and has been accomplished in a variety of ways, including written, nonverbal, and verbal forms. In contrast, social engineering is defined in the context of information security as the emotional and psychological exploitation of humans to convince them to disclose sensitive information or perform unwanted actions.It is a type of chaos that is used to gain access to a secure system, gather information, or commit fraud. It is a complex psychological manipulation process that differs from the typical deceptive job, which is one of many steps in a complex fraud scheme. The psychological manipulation of any individual of accessing secured data immediately focuses on information security, a crucial aspect of data protection and privacy in many different scenarios.The majority of organisational cultures place this at the core of personnel management[2].

Even though it is considered as old as human history, social engineering is still possible to occur and still maintains its powerful method. A social engineer can perform a reconnaissance attack to collect information regarding the targeted organization and their employees so that human vulnerabilities can be exploited[1]. To prevent social engineering attack from happen, typically to protect at end user side is more crucial than the technical one. This is because, human is easily deceptive. Preventing such attacks is a varied activity that includes, but is not limited to, the confidential information that has been disclosed to the third parties. The review process before obtaining confidential information, the configuration of the information security infrastructure, and the most important action which is individual training [2].

While penetration testing can be said as an authorized access to perform security testing to the organization. Purpose of penetration testing is to test the system or network vulnerabilities. After the weaknesses have been found, the IT security

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 35-46 www.ijaem.net ISSN: 2395-5252

personnel can suggest to the organization to improve the security system of the network.

The aim of this study is to review the penetration testing that can be performed to evaluate social engineering awareness level.

The rest of this paper will be organized based on this arrangement. Brief introduction about types of penetration testing and social engineering threat. After that, factors influencing user awareness of social engineering threats and its countermeasure. Lastly, we will discuss the implementation of penetration testing for social engineering attacks.

II. PENETRATION TESTING

A. Type of Penetration Testing

According to Bacudio et al. [3], there are three different kinds of penetration testing (pen-test): network pen-test, application pen-test, and social engineering pen-test. However, in 2017, Baloch classified the various types of pen-tests: physical pen-test, social engineering pen-test, network pen-test, web application pen-test and mobile application pen-test.

i. Network Penetration Testing

Network pen-test is an effort to assess the security of a network or infrastructure by securely trying to exploit vulnerabilities[3]. It aids in the discovery of network loopholes. The gaps in the network infrastructure may enable an attacker to infiltrate and exploit the vulnerabilities. The entire network is examined during a pen-test, with special attention paid to some vital parts of network[4], including firewalls, the servers of databases, server for website, and employees' workstations. Port scanning, IP spoofing, session hijacking, denial-of-service (DoS) attacks, and buffer overflow are just a few techniques employed in this test type comparable to those used in actual network-based attacks[5].

But then, penetration tests can have severe repercussions for the network on which they are conducted. It can lead to congestion and system failures when it is poorly conducted. In the most extreme case, it can lead to exactly what it is meant to prevent. Hence, it is crucial to get company management permission before running a penetration test on a company's systems or network[3].

ii. Web Application Penetration Testing

Web application pen-test is a type of ethical hacking specifically developed to evaluate a web application's design, setup, and architecture[6]. The goal of testing is to identify vulnerabilities that could allow for unauthorised access or result in a breach of sensitive information[7], which may be brought on by unsafe development procedures in the design, coding, and server configuration of software or websites. Web application penetration testing typically involves testing the web application for vulnerabilities and flaws, including cross-site scripting (XSS), assuring the safety of web servers and databases and checking the browsers' security settings[8].These tests can be regarded as complicated tests. There may be a significant time investment required for planning, carrying out the tests, and compiling the reports. Also, due to the daily rise in threats from web applications, web application penetration testing approaches are constantly evolving. Therefore, each web-based application's endpoints that routinely communicate with the user must be located to conduct a successful test.

iii. Mobile Application Penetration Testing

The most recent kind of penetration test, known as a mobile application penetration test[9], has gained popularity due to businesses' widespread use of mobile applications with an Android or iOS operating system. Since these mobile applications handle sensitive personal data, security is a problem that needs to be addressed to prevent hackers or other bad actors from abusing or exploiting it. These days, it seems to be common for organizations to have "Bring Your Own Device" (BYOD) policies that sanction the use of personal mobile devices on company networks. As a result, perpetrators will be able to breach the network, and a recent survey found that mobile malware attacks are increasing exponentially[10]. Therefore, the responsible penetration test team must ensure that mobile applications are sufficiently secure for users to enter their personal information. The most prevalent ten risks identified by the Open Web Application Security Project (OWASP) Mobile 2016[11] can be utilized to conduct comprehensive security pen-test on Android and iOS applications, as shown in Figure 1.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 35-46 www.ijaem.net ISSN: 2395-5252

No	Risks
M1	Improper platform usage
M2	Insecure data storage
M3	Insecure communication
M4	Insecure authentication
M5	Insufficient cryptography
M6	Insecure authorization
M7	Client code quality
M8	Code tampering
M9	Reverse engineering
M10	Extraneous functionality

Figure 1 Top 10 Vulnerabilities by OWASP
Source: Adapted from [11]

iv. Social Engineering Penetration Testing

Social engineering pen-test can be carried out both physically and digitally. Social engineering pen-test is a method used by ethical hackers to test social engineering techniques on the employees of a company to comprehend the security posture, where the weaknesses are, and how to study those from a cyber intruder perspective[12]. A skilled individual will assume the role of an attacker to examine the barrier of security and asses the user awareness of unsolicited content of emails and links. The technique was developed with the organization's knowledge[13]. For example, in social engineering digital penetration tests, an employee's resilience is usually measured by phone calls or phishing emails that entice the employee to reveal sensitive information. Even then, those penetration tests must always be designed and conducted legally and ethically[14]. The following conditions must be fulfilled for a social engineering penetration test to be beneficial to the organization: the penetration test must be realistic because it mimics an attack carried out by a real adversary; all test participants must be treated with respect; and the pen-test must be regular, trustworthy, and documented[12].

If conducting a penetration test, a penetration tester with knowledge of the organization may employ social engineering attack techniques such as phishing, spear phishing, vishing, smishing, eavesdropping, tailgating, browser exploits, and many others to deceive a user into taking actions they did not intend to take and gauge their level of awareness of cyberattacks.

v. Physical Penetration Testing

Physical penetration testing is crucial for ensuring that an organization's security policies are correctly implemented and that its personnel is at the appropriate degree of security awareness[15]. Because the testers would undoubtedly have to contact the personnel and use deception to reach their target when accessing a site, physical penetration testing is rarely conducted without social engineering. For example, in physical penetration tests, the tester accesses restricted areas to examine physical security measures such as locks and RFID mechanisms[9] while directly interacting with the personnel to persuade them to violate company policy or provide credentials. The tests' execution is complicated and has problems with safety, legality, and ethics because of physical access and contact with the personnel. The aim of a physical pen-test is to either mimic the threat actor stealing assets from a restricted area or to leave things (that should stand in for bombs or recording devices) there.

B.Approaches to Penetration Testing and Its Pros and Cons

Different penetration tests take different approaches and focus on various vulnerabilities. The approaches and the project's scope will be based on the level of information given to the penetration tester. The following are the approaches to pen-test:

i. White Box Testing

White box testing involves examining a software system's internal structure, design, and code[16]. It is also referred to as structural testing, transparent box testing, open box testing, and glass box testing. White box testing is a technique used in penetration testing to find and take advantage of flaws in a software application's source code.

In white box testing, the tester is familiar with the software's internal architecture and design, including the source code, algorithms, data structures, and other internal parts[17]. This information is used to create and carry out tests that target the application's vulnerabilities precisely. White box testing aims to find security problems, including buffer overflows, poor error handling, and logical security flaws that are difficult to spot from the application's interface. SQL injection is a type of white box testing that penetration testers frequently carry out. To test whether the function appropriately handles such information and to see whether any errors could result in a SQL injection vulnerability, the tester would attempt to send input that incorporates SQL injection attacks.

The following Table 1 shows the lists of some white box testing approach benefits and drawbacks [16]:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 35-46 www.ijaem.net ISSN: 2395-5252

Table 1 White Box Test Pros and Cons

Advantage	Disadvantage
By omitting unused code lines, it reveals previously	Due to the need for a qualified tester, it is
Side effects are advantageous.	Since searching into every crevice to uncover llenging, many paths will go unexplored.
In the process of writing test scenarios, the maximum	Some of the missing codes in the code might

ii. Black Box Testing

In software testing, "black box" refers to the practise of evaluating an application's outward appearance rather than its inner workings[16]. Black box testing is a pen-test approach used to find flaws in a software application's external interface without any knowledge of the underlying architecture or code.

The tester in a black box test only has access to the application's inputs and outputs; they are entirely unaware of how it operates internally. The tester interacts with the application via its user interface, APIs, or network protocols and attempts to spot security problems by watching how the application behaves [17]. Cross-site scripting (XSS), cross-site request forgery (CSRF), and unsafe direct object references are examples of security flaws detected from the application's interface and are the focus of black box testing. As discussed before, an example of black box testing is cross-site scripting (XSS). The application would be tested to check if it correctly filters out harmful input and guards against XSS vulnerabilities by having the tester attempt to submit input that includes XSS attacks.

Black box testing helps identify security flaws that can be quickly identified from the interface but not providing as much information about the internal operations of the application as white box testing. It may also be carried out by non-technical testers, making it a helpful method for businesses that wish to evaluate the security of their apps without requiring a high level of technical knowledge.

The following Table 2 shows the lists of some black box testing approach benefits and drawbacks [17]:

Table 2 Black Box Test Pros and Cons

Advantage	Disadvantage
Adequate for long code segments.	The actual execution of only a few test cases is done. There is, therefore, only a small amount of coverage.
Tester perception is straightforward.	It is challenging to construct test cases without precise specifications.
Since programmers and testers are independent of one another, the perspectives of users and developers are divided.	Inadequate testing
Faster development of test cases.	

iii. Gray Box Testing

Gray box testing is a hybrid approach to software testing that draws from both black box and white box approaches. Gray box testing is a penetration testing technique that combines examining an application's external behaviour with knowledge of the code's internal structure and design to find software vulnerabilities [16].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 35-46 www.ijaem.net ISSN: 2395-5252

In gray box testing, the tester has some understanding of the application's underlying architecture and design but does not have full access to the source code [17]. Documentation, network diagrams, or other sources are typically used to gather this data. Through the collected information, the tester creates tests that specifically target known code vulnerabilities while examining how the software behaves outside to find security problems visible from the interface. Organizations who wish to conduct a thorough security analysis of the applications but lack access to the source code can benefit from gray box testing.

The following Table 3 shows the lists of some gray box testing approach benefits and drawbacks [16]:

Table 3 Gray Box Test Pros and Cons

Advantage	Disadvantage
When compared to white and black box testing, gray box testing has benefits from both.	Having no access to the source code results in poor test coverage.
Instead of using source code, the tester in gray box testing depends on interface definition and functional specification.	Identifying defects in distributed applications are challenging.
The tester can create good test scenarios for gray box testing.	Numerous software paths are still untested.
Instead of the designer's perspective, the test is conducted from the user's perspective.	The tests may be unnecessary if the software creator has previously conducted a test case.

C. Phases of Penetration Testing

Penetration testing procedures come in a variety of forms. A particular procedure is selected based on the requirements of the entity that needs the penetration test. Pre-attack, attack and post-attack are the three different phases of the pen-test process. According to the hacking process, the three stages are made up of five phases: reconnaissance (pre-attack), scanning (pre-attack), gaining access (attack), maintaining access (attack), and covering tracks (post-attack) [18]. However, Hua, Ismail, Abas [19], and Mamilla [20] argue that planning, analysis, and reporting phases are also included in the stages of the penetration testing process.

Phase 1: Planning

The goal must be specified and made clear before the penetration tests can begin [21]. Determine the scope and scale of the testing based on elements including current security policies, culture, laws and regulations, best practices, and industry standards [20]. It is a crucial phase since it establishes the parameters for the entire test and directs its output. Additionally, the tester must guarantee that the test processes will not violate any laws or contractual agreements. Conducting a penetration test without fully accounting for pertinent legal aspects may result in criminal or civil law penalties. The breakdown of a production network system could also result in recourse claims due to penetration techniques that were not authorized or dangers related to those techniques that were not disclosed. Therefore, it is necessary to describe and record the operation and its hazards.

Phase 2: Reconnaissance

The tester can gather data on the target once the objectives, scope, processes, and emergency measures have been established while considering the organizational, legal, and other factors. The passive penetration phase is reconnaissance [21]. In the reconnaissance phase of a pen-test, the tester learns as much as possible about the target organization or system so that they can properly protect against any potential attacks[19]. This phase aims to obtain a complete and detailed overview of the installed systems, including areas vulnerable to attack or known security flaws. The test steps may take a long time, depending on the number of computers or the size of the network to be examined.

Phase 3: Scanning

In this phase, hosts that can be accessed remotely are mapped. Another name for the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 35-46 www.ijaem.net ISSN: 2395-5252

scanning phase is vulnerability scanning [20]. This phase involves searching for vulnerabilities in a target system using scanning tools. For example, network scanning can occasionally expose the system vendor brands and operating system versions being used [18]. Network scanning enables finding the position of the firewall, the active routers, and the general layout of the network.

Phase 4: Gaining Access

This stage involves using a variety of approach attacks to identify weak points in the target system, which could be a server, firewall, or application [19]. The penetration tester will enter the target system using the vulnerabilities they discovered during the reconnaissance phase, access the target system's data, and disrupt system traffic [18]. It is possible to conclude that a penetration tester's main objective during any evaluation is to gain access.

Phase 5: Maintaining Access

Even if the system has been reset or altered, the penetration tester must ensure access is still available after gaining access [19]. Once access to a target system is achieved, [18] contend that it is essential to maintain the access for potential future exploitation and attack. It is because actual perpetrators who attack the system will remain logged in for extended periods to steal data from the system they are attacking. Those who wish to remain undetected must take additional precautions to ensure their presence. There are several ways this can occur, but the most common is the installation of hidden infrastructure based on backdoors, Trojan horses, rootkits, and covert channels to allow for repeated and unrestricted access.

Phase 6: Covering Tracks

Covering tracks is the next step in penetration testing after completing the attack and successfully maintaining access. When a pen-test is complete, the tester will conceal their tracks and then go back to each compromised system to remove any traces of their intrusion[18]. The importance of track covering cannot be underestimated, since it gives forensics analysts or intrusion detection systems (IDS) a valuable clue, according to Narwal and Gupta [22]. In the actual world, it can be challenging to cover all tracks completely. An attacker can alter the system to confound the security team and make it nearly impossible to pinpoint the attacker's full scope.

Phase 7: Analysis

At this point, penetration testers will examine all the data they gathered while doing the test and the vulnerabilities they found. They will also recommend remedial actions to address their discovered vulnerabilities [20].

Phase 8: Reporting

The exploited vulnerability evidence will be compiled and presented for the organization's evaluation and remediation plan once all processes have been completed [19]. The final report must ensure that the testing was transparent and that the vulnerabilities they revealed were reported [21]. The management and security team will make decisions regarding how to manage and access hazards to lessen the risk that may affect the organization's assets based on the reporting and results of the test methods [19].

D. Benefits of Penetration Testing

Penetration testing is used to classify the risks such an attacker might pose if they gain access to an organization's computer systems and networks. Running penetration test can help you evaluate mitigation plans to close security gaps afore an actual attack occurs. By conducting penetration testing, organizations can reduce the financial and informational losses that lead to loss of customer confidence due to security breaches. To achieve compliance with industry authorities, clients, and shareholders while avoiding financial loss so that organization can be protected from failure. We help you build trust, improve your corporate image, and streamline your IT security investments. Because penetration testing is a proactive process, it provides impenetrable information that helps organizations meet audit or compliance aspects of regulations. One of the main benefits of penetration testing is that it establishes IT security and its importance at all levels of the organization. Avoid security incidents that can damage confidentiality, integrity, relationships, and customer trust through structured training and awareness programs. penetration testing helps organizations assess employee security awareness, effectiveness of existing security policies and processes, and product efficiency. It helps you make decisions, assess your organization's security, and plan your security investments and IT strategy. Penetration testing also helps form an important aspect of your information security strategy by quickly and accurately identifying vulnerabilities. It also helps improve test configurations to

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 35-46 www.ijaem.net ISSN: 2395-5252

proactively eliminate identified risks. Helps organizations assess the impact and likelihood of vulnerabilities. Organizations can therefore prioritize and implement mitigation action plans for identified vulnerabilities. Penetration testing requires a lot of time, effort and knowledge depending on the complexity of your business. Penetration testing therefore supports the expansion of the knowledge and competence of those involved in the process. Considered a quality assurance tool that benefits both business and operations [23].

III. SOCIAL ENGINEERING ATTACK

A. Type of Social Engineering Attack

Based on [24]study, before 2006 the social engineering attack is based on psychological skills only that manipulate the target via building trust between them. But, after that year, the social engineering attack was also considered related to the technology-based involvement through several research and studies. In this paper, the type of social engineering attack will focus on four types of attacks which are social, physical, technical and socio-technical.

i. Social

Manipulation and persuasion skills are the main factors in social approach in social engineering based on [24]review. The targets or victims will be manipulated by the attacker until they are unaware that the important and confidential security information have been exploited. This type of social engineering basically depends on how the attacker builds relationships and trustworthiness between the target. The skill of communication is also important to apply this attack.

ii. Physical

According to [24] in a physical social engineering attack, the attackers will launch physical actions to gain the sensitive data from the specific target victims. The most known example in physical action attack is dumpster diving other than extortion. [25]reviewed that dumpster diving attack collects the data by the low-tech method towards the target. The process of dumpster diving is looking for torn or unwanted documents that are thrown by the targets into the trash to find any important information contained on it. Figure 2 shows how attackers gain information through the trash.

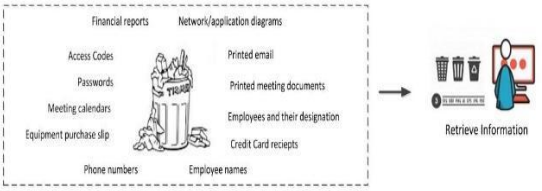

Figure 2 Dumpster Diving
Source: Adapted from [25]

iii. Technical

In technical terms of social engineering attack, it relies on using sophisticated technical tools to gain the crucial information from the targets. Based on [24], Less secure social networking sites are being targeted by the attackers to obtain access to sensitive data of the targets such as passwords by using different technical tools. The attack is easier to conduct since there are many users who use the same password for multiple websites or personal accounts. Some of the attack approaches in this technical social engineering are by email attachments and popup windows.

iv. Socio-Technical

In socio-technical approach there are a variety of types of attacks that can be launched such as vishing, baiting, pretexting, fraudulent websites and phishing [26].

Vishing: Vishing attack uses a phone call to manipulate the targets by creating fraud identity and misleading information to gain the sensitive information from them. For example, the credit card numbers, passwords, banking online security code or home address. The voice over IP (VoIP) is exploited as it is affordable and can make the call from anywhere by the attackers with identity not revealed[26].

Baiting: In baiting attacks, external devices such as USB drives and RAM are used to launch the trick. These devices can attract the target curiosity to use and try the devices. Usually, the USB drives will be left unintendedly somewhere around the target area to make sure they connected the devices to the computer or any devices that contain sensitive data. The external devices are already injected with the malware and it will spread into the target system in order to control their network system once they connect them to the computer.

Pretexting: According to [26], pretexting uses scripted scenarios in exploiting the attack on the targets to make them open up their sensitive information or get into malicious activities without their concern. The fraud scenarios are usually fake

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 35-46 www.ijaem.net ISSN: 2395-5252

topics that deliver to the target on a need and convince them to contact another social engineer that designed the attack for the next step in exploiting the data [24]. Example of the pretexting is reverse social engineering.

Fraudulent Websites: Fraudulent websites attack technique is the hacker will gain the target's trust and lead them to the fraud websites. If the target accesses the fraud website, automatically the malicious files will be downloaded to their device. In this step, the hacker already gets illegal access to sensitive data on the target's local browser.

Phishing: Email is a common medium used by the hacker to do phishing attacks towards the target victims.The method involved in phishing attacks is by sending any message that looks like it comes from a legitimate source[24]. For example, the phishing email that is sent to the targets usually contains fraud information created by the attacker and malicious links or files. When the targets click on the link or files attached, the targets will be brought to the fraud page and be asked to fill up any important details. Once they fill up the details, the attacker will directly receive their confidential information.

B. Factors Influencing of User Awareness Social Engineering Threats

The lack of user awareness still remained as the main cause of the social engineering successful attack. Thus, the awareness of end-users can become the most effective method to protect the organization even though it may seem the simplest way to be implemented [27]. In her research, the author performed two experiments in accessing the end user awareness. The first experiment was a spear-phishing attack. In this experiment, the employees were sent with an email pretending that the sender was the Chief Operating Officer (COO) with a survey link. While the second experiment was memory stick usage. The memory sticks were left at the entrance and exit of the office. The objective was to test the vulnerability of the end-user in recognizing any unknown device that left elsewhere could be used as intrusion to compromise the information system. From the research, it can be concluded that there are several factors that influenced end-users about the social engineering threats such as end-users did not pay attention to the email sent by the pretended COO as the experiment was conducted at the end of working hours, the employees were rushing back to home and just click the link inside the email. According to [28], there are six factors that involved in influencing end-users social engineering threat awareness which are : -

- ✔ Business environmental
- ✔ Social
- ✔ Constitutional
- ✔ Organizational
- ✔ Economical
- ✔ Personal

C. Social Engineering Threats' Countermeasure

According to the research [24], social engineering countermeasures can be classified into human and technology based. Human based factors often became the successor for social engineers. There is proven research that employees or end-users are usually unaware of the techniques used by social engineers. Table 4 below shows Human-based countermeasures that were suggested by the researchers.

Table 4 Human-Based Countermeasures

Countermeasures	Purpose
User Awareness Programs	Users become more aware of the taxonomy of social engineering attacks and manipulation techniques.
Auditing and Monitoring	Periodic checks help organizations create a safe culture.
Identity Management & Access Control	Identifying users' specific job roles and responsibilities mitigates the risk of the insider threat.
Training	Users become more conscious of how to respond to a threat.

Source: Adapted from [24]

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 3 March 2023, pp: 35-46 www.ijaem.net ISSN: 2395-5252

To avoid social engineering threat, organizations should apply necessary effective secure technologies so that the attack can be detected and prevented before it enters the system. Table 5 below shows common technology-based countermeasures that organizations can considered to deploy.

Table 5 Technology-Based Countermeasures

Countermeasures	Purpose
Sender policy framework	To validate sending an email to help prevent spoofing of messages
Implementation of scanning software	To prevent the execution of viruses,spams, and scams
Adopting content-based filtering tools	To filter relevant information to theworkplace and block all phishingemails and websites
Biometric system implementation	To protect physical security in anorganization from unauthorizedaccess to restricted data.
Implementing intrusion detection systems	To identify suspected activities

Source: Adapted from [24]

IV. IMPLEMENTATION OF SOCIAL ENGINEERING ATTACK AS PENETRATION TESTING TECHNIQUE

Any organization's data privacy and confidentiality must be outlined and determined, and they must not violate their rules and regulations before penetration test [29]. Penetration testing for social attacks is a type of security testing that is designed to evaluate an organization's ability to detect, prevent, and respond to attacks that exploit human weaknesses. This type of testing can help organizations identify and mitigate vulnerabilities in their social engineering defences, such as phishing attacks, pretexting, baiting, and other forms of social engineering. Here are the general steps to implement penetration testing for social attacks. Determine which parts of the organization will be tested, what types of social engineering techniques will be used, and what data will be collected. The team should consist of skilled professionals who have experience in social engineering techniques and can conduct the tests without causing any damage or disruption to the organization. The test plan should detail the methods and techniques that will be used to simulate real-world attacks. It should also include the objectives of the test, the tools and technologies that will be used, and the expected outcomes. The test team should simulate real-world social engineering attacks, such as phishing emails, pretexting phone calls, and baiting attacks. The goal is to see how employees react and whether they fall for the simulated attacks. After the test is completed, the team should analyze the results to identify vulnerabilities and weaknesses in the organization's social engineering defences. This analysis should include an evaluation of how well employees responded to the simulated attacks, as well as any technical vulnerabilities that were exploited. The findings should be presented to the organization's management team, along with recommendations for improving the organization's social engineering defences. The organization should implement the recommendations provided by the test team to improve its social engineering defences. This may include training employees on how to recognize and respond to social engineering attacks, implementing new security technologies, and updating policies and procedures. Penetration testing for social attacks should be conducted regularly to ensure that the organization's social engineering defences are effective and up to date. In summary, the implementation of penetration testing for social attacks requires careful planning, a skilled test team, and a thorough analysis of the results. The process should be repeated regularly to

ensure that the organization's social engineering defences are effective and up to date.

V. CONCLUSION

Attacks by social engineers are getting more and more sophisticated, and they can be difficult to spot and avoid. In order to find potential weaknesses and opportunities for improvement, it is crucial to evaluate the efficiency of the methodologies utilized in penetration testing. Penetrating tests can be performed on network, web application, mobile, social engineering and physical. There are three approaches that can be used for penetration testing deployment which are white box, black box and grey box. Meanwhile, social engineering threats still can be said as famous threats that involve planning, reconnaissance, scanning, gaining access, maintaining the access, covering tracks, analysis, and reporting. One of the benefits of doing penetration testing in an organization is that a mitigation plan can be evaluated so that it can close the security gap. Otherwise, social engineering attacks such as social, physical, technical, socio-technical, vishing, baiting, pretexting and fraudulent can possibly occur to the organization or end-user itself. On the other hand, one of the factors that social engineering threats are still on the top of famous threats is that the employee or end-users are quite unaware regarding the social issue. For example, when reading the email containing some links inside, the end-user didn't read the email thoroughly. From this study, authors found that there are several countermeasures that can be taken accordingly to protect the organization's assets.

VI. ACKNOWLEDGEMENT

The authors would like to thank all School of Computing members who were involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by Universiti Utara Malaysia.

REFERENCES

[1] M. Sillanpää and J. Hautamäki, "Social Engineering Intrusion: A Case Study," ACM Int. Conf. Proceeding Ser., 2020.

[2] B. Wilson, "Introducing cyber security by designing mock social engineering attacks," J. Comput. Sci. Coll., vol. 34, no. 1, pp. 235–241, 2018.

[3] C. Shivayogimath, N, "An Overview of Network Penetration Testing," Int. J. Res. Eng. Technol., vol. 03, no. 07, pp. 408–413, 2014.

[4] M. C. Ghanem and T. M. Chen, "Reinforcement learning for efficient network penetration testing," MDPI Inf., vol. 11, no. 6, pp. 1–23, 2019.

[5] N. Y. Hamisi, N. H. Mvungi, D. A. Mfinanga, and B. M. M. Mwinyiwiwa, "Intrusion Detection ByPpenetration Test In An Organization Network," in 2009 2nd International Conference on Adaptive Science & Technology (ICAST), 2009, pp. 226–231.

[6] M. Albahar, D. Alansari, and A. Jurcut, "An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities," MDPI Electron., vol. 11, no. 19, pp. 1–25, 2022.

[7] Y. Pan, "Interactive Application Security Testing," in Proceedings - 2019 International Conference on Smart Grid and Electrical Automation, ICSGEA 2019, 2019, vol. 1, pp. 558–561.

[8] J. Im, J. Yoon, and M. Jin, "Interaction platform for improving detection capability of dynamic application security testing," ICETE 2017 - Proc. 14th Int. Jt. Conf. E-bus. Telecommun., vol. 4, no. Icete, pp. 474–479, 2017.

[9] R. Baloch, Ethical Hacking and Penetration Testing Guide. CRC Press Taylor & Francis Group, 2017.

[10] S. Jadhav, T. Oh, Y. H. Kim, and J. N. Kim, "Mobile Device Penetration Testing Framework and Platform for The Mobile Device Security Course," Int. Conf. Adv. Commun. Technol. ICACT, vol. 2015–Augus, pp. 675–680, 2015.

[11] T. Borja, M. E. Benalcázar, Á. L. V. Caraguay, and L. I. B. López, "Risk Analysis and Android Application Penetration Testing Based on OWASP 2016," in International Conference on Information Technology & Systems, 2021, pp. 461–478.

[12] T. Dimkov, W. Pieters, and P. Hartel, "Two methodologies for physical penetration testing using social engineering," Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC, pp. 399–408, 2010.

[13] A. Bacudio, G, X. Yuan, B. Chu, Tseng, Bill, and M. Jones, "An Overview of Penetration Testing," Int. J. Netw. Secur. Its Appl., vol. 3, no. 6, pp. 19–38, 2011.

[14] J. M. Hatfield, "Virtuous human hacking: The ethics of social engineering in penetration-testing," Comput. Secur., vol. 83, pp. 354–366, Jun. 2019.
[15] T. Dimkov and W. Pieters, "Physical Penetration Testing: A Whole New Story in Penetration Testing," PenTest Magazine, pp. 1–4, 2011.
[16] M. Ehmer and F. Khan, "A Comparative Study of White Box, Black Box and Grey Box Testing Techniques," Int. J. Adv. Comput. Sci. Appl., vol. 3, no. 6, pp. 12–15, 2012.
[17] J. N. Goel and M. Mehtre, B, "Vulnerability Assessment and Penetration Testing as a Cyber Defence Technology," in 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015), 2015, pp. 710–715.
[18] D. Bertoglio, Dalalana and A. Zorzo, Francisco, "Overview and Open Issues on Penetration Test," J. Brazilian Comput. Soc., vol. 23, no. 1, pp. 1–16, 2017.
[19] T. W. Hua, S. A. Ismail, and H. Abas, "Penetration Testing Process: A Preliminary Study," Open Int. J. Informatics, vol. 10, no. 1, pp. 37–46, 2022.
[20] S. R. Mamilla, "A Study of Penetration Testing Processes and Tools," 2021.
[21] Federal Office for Information Security (BSI), "Study: A Penetration Testing Model Security," 2010.
[22] R. Narwal and G. Gupta, "Tracks Covering in Penetration Testing and Cyber Attack," Int. J. Appl. Stud. Prod. Manag., vol. 1, no. 3, pp. 89–99, 2015.
[23] H. M. Z. Al Shebli and B. D. Beheshti, "A study on penetration testing process and tools," 2018 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2018, pp. 1–7, 2018.
[24] H. Aldawood and G. Skinner, "An Advanced Taxonomy for Social Engineering Attacks," Int. J. Comput. Appl., vol. 177, no. 30, pp. 1–11, 2020.
[25] M. A. Siddiqi, W. Pak, and M. A. Siddiqi, "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures," Appl. Sci., vol. 12, no. 12, 2022.
[26] C. L. Okafor, O. Okonkwo, and U. P. Onwuka, "International Digital Organization for Scientific Research Social Engineering Attack , Its Effects and Countermeasures in Nigeria Banking System," vol. 7, no. 1, pp. 25–32, 2022.
[27] T. Bakhshi, "Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors," Proc. - 2017 13th Int. Conf. Emerg. Technol. ICET2017, vol. 2018–Janua, pp. 1–6, 2018.
[28] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues," Futur. Internet, vol. 11, no. 3, 2019.
[29] A. Aibekova and V. Selvarajah, "Offensive Security: Study on Penetration Testing Attacks, Methods, and their Types," IEEE Int. Conf. Distrib. Comput. Electr. Circuits Electron. ICDCECE 2022, 2022.