International Journal of Multidisciplinary Research and Growth Evaluation
ISSN: 2582-7138
Received: 12-12-2020; Accepted: 17-01-2021
www.allmultidisciplinaryjournal.com
Volume 2; Issue 1; January-February 2021; Page No. 214-218

Network security with internet world wide threat

Muhammad Khuzaifah Nasution[1], Nuzri Rachmat Al Qabri[2], Iskandar Muda[3]
[1-3] Universitas Sumatera Utara, Medan, Indonesia

Corresponding Author: **Muhammad Khuzaifah Nasution**

Abstract
The development of information systems today is followed by an increase in attacks on information systems. This is due to the growing number of information systems that store sensitive data for users such as telephone numbers, population identification numbers, birth dates and even bank account numbers. These data are very prone to be misused by irresponsible parties. So security is one of the factors that must be the main consideration in the development of information systems. This research studies various attack techniques on information systems. To facilitate identification, these attacks are classified based on the components of the information system. The results of this study indicate that there are attacks aimed at each component of the information system. At the end of this study provides suggestions to minimize the impact of attacks and to improve information system security.

Keywords: Network Security, Virus, Treat From World Wide Web

1. Introduction
Today Information Technology has entered human life massively. Various Information Systems were developed to facilitate human life. It is not uncommon for this information system to store user data and even personal data such as telephone numbers, birth dates, population identification numbers, bank account numbers and so on. For reasons of convenience and comfort, users will voluntarily submit their data to be stored in the Information System. Therefore, attacks on Information Systems are increasing with increasingly diverse techniques.
This is due to the growing number of information systems that store sensitive data for users such as telephone numbers, population identification numbers, birth dates and even bank account numbers. These data are very prone to be misused by irresponsible parties. So security is one of the factors that must be the main consideration in the development of information systems.

2. Literature Review
According to a report (SophosLab, 2013) Indonesia is the country with the largest Threat Exposure Rate. Threat Exposure Rate is measured from the percentage of computers affected by malware attacks in a 3 month period. The report shows that Indonesia is the country most targeted by cyber attacks. To address internet security, Indonesia already has a special institution called ID-SIRTII / CC (Security Incident Response Team on Internet Infrastructure / Coordination Center). This institution is the official agency or coordinator for incidents on internet infrastructure in Indonesia. In the 2018 annual report, ID-SIRTII / CC reported that Indonesia received a total of 232,447,974 attacks consisting of 122,435,215 malware activities, 16,939 website incidents, 2,885 incident reports from the public and 1,872 information about security holes (ID-SIRTII, 2018). The report also found the fact that apart from Indonesia being the target of cyber attacks, Indonesia was also the country with the most attacks.
The report above shows that security in cyberspace in Indonesia is quite weak. This can be seen from the large number of attacks aimed at various information systems in Indonesia, both attacks originating from outside Indonesia and attacks originating from within Indonesia itself. Therefore, the security factor in Information Systems today must be a top priority in the development of an information system. So in this study will classify the various attacks received by information systems based on the constituent components of the information system. This needs to be done to facilitate the identification of attack models on each component of the information system so that the most effective preventive measures for each attack model can be identified.

3. Method
This research uses literature study method to find out similar research that has been done. Each study will be discussed briefly to find out the differences between each of the studies that have been carried out.

So that it can be seen clearly the novelty of the proposed method through this study compared to previous research. The flow of this research can be seen in Figure 1 below

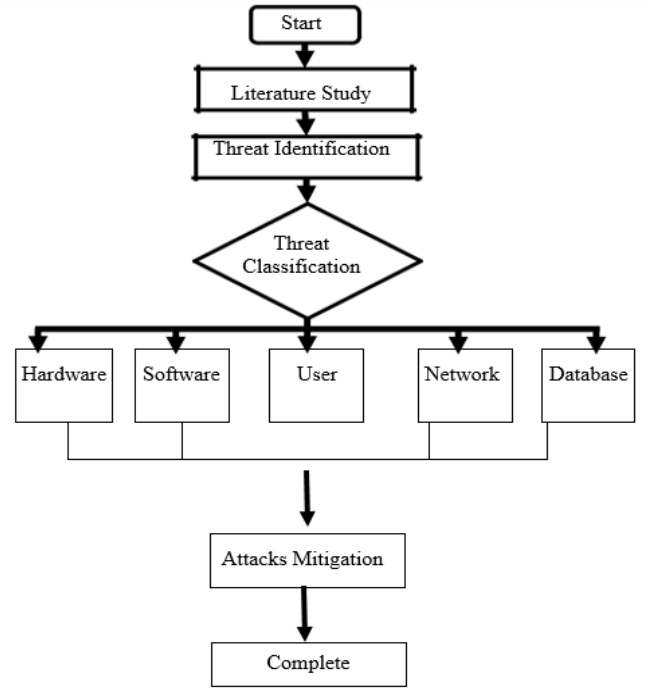

Fig 1: Ericka, J., & Prakasa, W,. (2020). Increasing Information System Through Classification of Attacks Againts Information Systems. Asian Scientific Journal of Asian Information

Previous studies have mostly focused on certain parts of information systems (databases, communication networks and so on). One of the approaches used is to use a framework. Research that has been conducted (Mohammed & Mohammed, 2017) reveals that efforts to form a Security Risk Management framework have been carried out in forming a National Infrastructure Protection Plan. This framework is built based on a system risk assessment process, implementation of the security framework, activity monitoring and review. To get the most optimal results an integrated approach is needed starting from the use of assessment tools, identification of internal and external threats and the formation of a flexible framework so that it can be used in various kinds of information systems. In other studies (Ali, Husain, & Sharma, 2017) have also discussed attacks on the latest technology such as cloud computing, internet of things, drones and big data. From this research, it is known that the latest technological developments are also followed by the development of attack techniques. Attacks on relatively new technologies such as attacks on cloud computing, botnets that turn IoT devices into zombies (Mirai botnet), are increasingly massive ransomware attacks, attacks on drones (drone-jacking) as well as attacks on big data. Research on user / human factors on data security has also been carried out (Safianu, Twum, & Hayfron-Acquah, 2016). The results of this study indicate that technology alone is not sufficient to prevent data leakage. The human factor is the weakest point of the information system. More and more attack models are aimed at users of information systems, because it is easier and has a higher success rate than attacking the information system itself. So training on data security for information system users is needed to minimize the possibility of data leakage. Research on cyber attacks against government agencies has also been carried out (Babate, Musa, Kida, & Saidu, 2015). This research mentions several attack techniques used by cyber criminals, including phishing and email spamming, botnets, malware and spyware, key loggers, social engineering, distributed denial of services, viruses and worms.

This research is about how to strengthen firewall performance so that security systems and computer data in information systems are better. Apart from that, this research is also about how to overcome security holes that allow malware and attacks from outside. The result of this research is a computer network design that is suitable to be implemented in a gateway system as well as a firewall that applies packet filtering where the package filtering method will regulate all packets either heading, passing or going to the packet. The packet will be regulated whether to accept, forward or reject.

This research focuses on network design, IP configuration, topology and implementation. As well as optimizing the existing bandwidth and firewall. The result of this research is the design of a network system that is aimed at dividing the bandwidth of the internet network so that each user can get bandwidth fairly according to the number of active users. Apart from that all interfaces can be monitored properly on the proxy, especially the interface that goes to the internet. Implementation of Network Security with the Firewall Filtering Method Using Mikrotik by (Astari, 2018). This research is about how to design and build network security in school areas using Mikrotik to prevent the negative impact of the internet in the form of adult sites and social media in order to create conducive teaching and learning. The result of this research is configuration of network security system using Mikrotik with Firewall Filtering method. This system performs filtering using layer 7 protocols to block sites with adult content and social media that are indicated to contain pornographic content based on keywords.

4. Result and discussion

From the results of literature studies, found several types of attacks on information systems. The attacks are then classified based on the components of the information system as follows:

4.1 Attacks against hardware

The attack on the hardware component of the information system (server / workstation) is still one of the attacks with fatal consequences. In the research that has been done (Alves & Morris, 2018) there are several malware that attacks hardware, including chipset level backdoor, stealth hard-drive backdoor, Intel Processor's SMM exploit, I / O MMU vulnerability, L3 cache side channel attack and malicious USB Device . Although practically this attack is more difficult to carry out because it requires direct access to the hardware, if it occurs it will be very fatal. Other research in this area has been conducted with a major focus on the trojan circuit (Bloom, Leontie, Narahari, & Simha, 2012). This study discusses that it is possible to enter a trojan (malicious code) into the IC used by the computer. If this happens, computer component manufacturers will experience distrust which can result in huge losses. Because so far there is no control at the IC manufacturer so that trojan injection into the IC by interested parties is very possible.

4.2 Attacks against Software

4.2.1 Attack on the operating system

Attacks on the operating system mostly target memory or what is known as a memory-corruption vulnerability. In research conducted in his dissertation (Gens, 2018) states that attacks such as Rowhammer attack DRAM so that it can cause operating system instability (crash) or can even result in privileges escalation. This study proves that access to forbidden memory addresses can result in ordinary users being able to run applications equivalent to an administrator (root). Another attack on the operating system called CLKscrew (Tang, Sethumadhavan, & Stolfo, 2017) can be carried out through software and can mess with the computer's electrical system (power). This research proves that the malicious code can lead to instability of the electric current supply to the computer system. Another attack that is quite well known because it affects the Intel x86 processor system and ARM-based microprocessors that are currently widely used in the market (Kee, *et a*l., 2018). This attack has several variants, namely Bounds Check Bypass, Branch Target Injection, Rogue Data Cache Load, Rogue System Register Cache, Speculative Store Bypass. This attack allows for reading data directly through memory (Kocher, 2019) [5]. By exploiting security flaws in Intel x86 and ARM processors, attackers can access restricted memory addresses, allowing direct data leaks from RAM. If these data are chained (reading of the memory address is carried out according to the data placement pattern), information will be obtained which should only be accessible by the operating system.

4.2.2 Attacks on operating system services (services)

The operating system has a service that functions to perform the processes it needs. One of the most well-known attacks aimed at services is Distributed Denial of Service (Jaafar, Abdullah, & Ismail, 2019) [4]. This research describes several DDoS techniques, including Session Flooding Attack, Request Flooding Attack, Asymmetric Attack, Slow Request / Response Attack. The purpose of this attack is to keep the service (eg HTTP) busy so that it cannot serve requests from other users and the website cannot be accessed. Another attack that is mostly done on operating system services is an attack on the secure shell (ssh). Secure shell is a service for remote server management. The only technique that can be used to attack the Secure Shell is a brute-force attack. Even though this technique has been used for a long time and is considered less effective, with the botnet, this technique has become much more effective than before (Salamatian, Huleihel, Beirami, Cohen, & Medard, 2019). A botnet is a device connected to the internet that can be used to carry out attacks (one of which is Denial of Services) in a distributed manner.

4.2.3 Attacks on applications

Applications are the main targets of attack. Because it is the application that stores user information / data. The most common attack against applications is Cross Site Scripting (XSS). Based on a report from Akamai in 2018, XSS is one of the 3 most frequent attacks on websites (Akamai, 2018). This technique is also called the client-side code injection attack because the client will enter the program code that will be executed (accidentally) by the information system. For example, entering the program code in email input so that when the information system is asked to display the email the program code will automatically run. Furthermore, XSS can be used as an opening for other attacks such as CSRF (Cross Site Request Forgery) (Niakanlahiji & Jafarian, 2019) [9]. CSRF is an attack technique that forces authenticated information system users to carry out unwanted actions such as changing data (password / email) (Moustafa & Lalia, 2019) [8]. What is dangerous is that the action is carried out by an authenticated user so that the system does not detect any illegal action.

4.3 Attacks against communication networks

The data communication network is one of the points that gets a lot of attacks. Attacks on computer networks are more towards data interception. Although since the emergence of network switch devices it is no longer possible to intercept data on computer networks, the increasingly massive use of wireless networks makes data tapping techniques even easier. Research that has been conducted (Zou, Zhu, Wang, & Hanzo, 2016) shows that there are basically 2 attack models on computer networks. The first model is an active attack using a signal jammer which aims to disrupt data transmission. Meanwhile, the second model is the passive model, which is more about tapping data. This research describes various possible attack techniques at the physical layer (signal jamming), the data-link layer (ARP spoofing), the network layer (Smurf attack) to the application layer (SMTP attack, cross site scripting).

4.4 Attacks against database

The database is the place where all data is located. Information systems will depend heavily on databases. Therefore, attacks on databases were still the most attacks carried out until 2018 (Akamai, 2018). The most famous attack on databases is SQL Injection. However, attacks on the database can also be caused by misconfiguration of the database system, for example, the absence of restrictions on the host user which can result in the user being able to access the database from anywhere, using the default port and using the common username & password (Sharma, 2016.

4.5 Attacks against users / humans

Social engineering is the most widely used attack to obtain confidential information known to users regarding the information system they access (for example: user username & password to enter the information system). The technique that is widely used is Evil Twin. Evil Twin will deflect the target's internet connection by pretending to be an Access Point that the target has known before. Because the data packet is sent via the Evil Twin device, data tapping can be done (Agarwal, Biswas, & Nandi, 2018). Another attack on computer users that has had a fairly high success rate is phishing. Phishing is an attempt to obtain confidential computer user information (username / password / pin / bank account no. Etc.) by tricking the user into entering this information on a website that has been made to resemble the original website. Even in its latest report, the Anti-Phishing Working Group stated that in the fourth quarter of 2019 there were 162,155 phishing websites detected (Group, 2020) although this number decreased from the previous quarter.

Table 1: Ericka, J., & Prakasa, W,. (2020). Increasing Information System Through Classification of Attacks Againts Information Systems. Asian Scientific Journal of Asian Information

Information System Components	Type of Attack
Hardware	▪ chipset level backdoor ▪ stealth hard-drive backdoor ▪ Intel processor's SMM exploit ▪ I/O MMU vulnerability ▪ L3 cache side channel attack ▪ Trojan circuit
Software Operating system	▪ Row Hammer ▪ CLKscrew ▪ Bounds Check Bypass ▪ Branch Target Injection ▪ Rogue Data Cache Load ▪ Rogue System Register Cache ▪ Speculative Store Bypass
Operating System Services	▪ Session Flooding Attack ▪ Request Flooding Attack ▪ Asymmetric Attack ▪ Slow Request/Response Attack ▪ SSH Bruteforce Attack
Application	▪ Cross Site Scripting (XSS) ▪ Cross Site Request Forgery
Network	▪ Signal Jammer ▪ ARP Spoofing ▪ Smurf Attack ▪ SMTP Attack
Database	▪ SQL Injection ▪ Buffer overflow ▪ Weak form of encryption
User	▪ Social Engineering ▪ Evil Twin Attack ▪ Phising attack

4.6 Hardware Attack Prevention

From the research that has been done, attacks on hardware devices are quite difficult to carry out because the attacker must have physical access to the computer to be attacked. So the steps that can be taken to mitigate this attack are to provide physical security in the server / data center room (AL-FEDAGHI & Alsumait, 2019) [1]. Physical security ranging from access control to the data center room, access control to the server rack and access control to the physical server. By implementing controls on users who access the server room, this attack will be minimized.

4.7 Software Attack Prevention

4.7.1 Prevention of attacks on the operating system

Mitigation of attacks on the operating system can be done by updating the information system used. Updates will provide improvements to the operating system especially in terms of security (in addition to improving other aspects such as appearance, adding features). By always following the updates provided by the operating system manufacturer, any security holes can be closed. In addition, the use of pirated software can harm the operating system. Most crack applications to hijack software will open a backdoor that allows malware to enter the system.

4.7.2 Prevention of attacks on operating system services

Attacks on operating system services can be caused by vulnerabilities in these services or from attacks (deliberately). The purpose of attacks on operating system services is to gain access to these services (on SSH, FTP services) or so that these services cannot be accessed (DDoS). Mitigation that can be done is to install and configure a firewall on the server to reduce these attacks.

4.7.3 Application attack prevention

Attacks on applications are often carried out by exploiting security holes that are accidentally exposed by the application maker. This is often caused by programming logic errors. To mitigate attacks on applications is to implement secure coding techniques. Secude coding is a programming technique that considers the security side of the program code used.

4.8 Prevention of attacks on computer networks

Prevention of attacks on computer networks can be done starting from the correct computer network design and installation of a network monitoring application that features an Intrusion Detection System / Intrusion Prevention System. The recommended network design is a computer network design that can develop following the development of the organization, and in the process of developing it will have a minimal impact on the existing network. Especially on wireless computer networks, you must pay attention to the security factor of its access. Computer network user authentication also needs to be done to identify each computer network user, for example using 802.1x (Kovačić, Đulić, & Šehidić, 2017) or using a captive portal system.

4.9 Database attack prevention

SQL Injection with its various variants is the main attack on databases. The cause of this attack is not a Data Base Management System error but rather a programming logic error. So the use of SQL code as input to the information system must be limited. This limitation technique has been

carried out in previous studies (O.P, O.S, & L.M., 2016). In this study, the researchers converted the special characters into HTML format and then checked them using regular expressions and exceptions.

4.10 Prevention of attacks on users of information systems
Education is the most effective way to mitigate attacks on users of information systems. With education, users will be able to know things that can be done as well as things that are potentially dangerous. To strengthen education, certain organizations such as companies can apply policies / rules in the use of information systems. Supported by a standard Standard Operational Procedure, it will be very effective in mitigating attacks on information system users because everything must be done in accordance with the procedure.

5. Conclusion
From the research that has been done, it is known that there is an attack model on each component of the information system. By doing the classification of attacks, it will be easier to identify any attacks that may be aimed at information systems. The results of this study indicate that there is an attack model on each component of the information system that can harm the information system. Mitigation is an action taken to minimize the impact caused by each attack. Mitigation of attacks on each component has also been presented in this study. By knowing the various attacks on information systems and their mitigation, it will be possible to develop a more secure information system in all aspects.

6. References
1. AL-FEDAGHI S, Alsumait O. Towards a conceptual foundation forphysical security: Case study of an it department. International Journal of Safety and Security Engineering, 2019.
2. Ericka J, Prakasa W. Increasing Information System Through Classification of Attacks Againts Information Systems. Asian Scientific Journal of Asian Information, 2020.
3. Group AP. Phishing Activity Trends Report, 4th Quarter. APWG, 2019-2020.
4. Jaafar GA., Abdullah SM, Ismail S. Review of recent detection methods for HTTP DDoS attack. Journal of Computer Networks and Communications, 2019.
5. Kocher PH. Spectre attacks: Exploiting speculative execution. IEEE Symposium on Security and Privacy (SP), 2019.
6. Kothari H, Suwalka AK, Kumar D. Various Database Attacks, Approaches and Countermeasures To Database Security. International Journal of Advance Research in Computer Science and Management, 2019.
7. Langobelen ESOB, Rachmawati RY, Iswahyudi C. Analysis and Optimization of Network Security Using Firewall Mikrotik Study Case at Smart Garden Yogyakarta. Jurnal Jarkom, 2019.
8. Moustafa K, Lalia S. Implementation of Web Browser Extension for Mitigating CSRF Attack. WorldCIST'19. Advances in Intelligent Systems and Computing Springer, 2019.
9. Niakanlahiji A, Jafarian JH. WebMTD: Defeating Cross-Site Scripting Attacks Using Moving Target Defense. Security and Communication Networks, 2019.