INTERNATIONAL JOURNAL of DYNAMICS in ENGINEERING and SCIENCES (IJDES)
LLDIKTI WILAYAH X
Vol. 7, No. 2, Nov 2022
e-ISSN: 2502-0692

ANALYSIS OF PREVENTION OF ILLEGAL ACTIVITIES ON THE NETWORK

Romi Wijaya*[1)], Rahmad Hidayat[2)]
[1,2] Universitas Putra Indonesia "YPTK" Padang, Indonesia
doi. 10.22216/jod.v7i2.1090
*Correspondence should be addressed to romiwijaya@upiyptk.ac.id

Submitted : 15 May 2022
Accepted : 20 Sept 2022
Published : 1 Nov 2022

Abstract

Computer network security factor is an absolute thing in building a network. On basically the security system owned by the operating system is not enough to secure the network computer. Therefore, to get a computer network security, tools are needed which can detect the existence of an attack mechanism from the network. The type of attack that occurs can be flooding or syn flood. Where the purpose of this attack is to make the computer unable to access it running normally so that this wireshark can help to detect attacks that will occur so that internet network users are not worried about these attacks.

Keywords: Network Security, Networking, Illegal Activity

INTRODUCTION

Computer network security is a very important priority in its existence. In this case, computer network security is divided into 2 parts, namely physical security (hardware) and non-physical security (software). These disturbances can be in the form of disturbances from within (internal) or interference from outside (external). Internal disturbances are disturbances originating from the scope of the infrastructure network. In this case, it is interference from parties who already know the security conditions and weaknesses of the network. External interference is interference that really comes from outsiders who want to try or deliberately want to penetrate existing security [1]. External disturbances are usually more common on external networks, such as web servers, telnet, FTP, SSH servers. Basically, network security is divided into two types, namely rule-based and adaptive systems. A rule-based system detects an attack based on rules that have been defined in a data set of rules, while an adaptive-system can identify a new type of attack by comparing the current conditions with the normal conditions of a system. Wireshark is software for analyzing computer network activity that has functions that are useful for network professionals, administrators, researchers, to network software developers[2]. Network security in general is that computers connected to a network have greater security threats than stand-alone computers. With careful control, these risks can be reduced. However, network security is usually the opposite of network access, which is easier, so network security is more vulnerable and if network security is getting better, network access is getting uncomfortable. A network is designed as a data communication highway with the aim of increasing access to computer systems, while security is designed to control access. The provision of network security is a balancing act between open access and security[3].

According to Garfinkel, an expert in computer security or computer security, it includes four aspects, namely the first is privacy, where this aspect relates to the confidentiality of information. The main point of the privacy aspect is how to protect this information from unauthorized access. For example, a user's e-mail may not be read by other people, even by an administrator to

protect this privacy aspect requires security using encryption.

Figure 1. Security Method (Cisco, 2020)

One of the efforts to fulfill the first problem, proving the authenticity of documents, can be done with watermarking and digital signature technology[4]. Watermarking can be used to protect intellectual property, by marking documents or works with the creator's signature. The second problem, namely access control, relates to limiting access rights to people who can access information. The standard method used for access control is by logging in and password[5].

Connection oriented means that two TCP user applications must establish a relationship in the form of exchange of control information (handshaking), before data transmission occurs. Reliable is the process of detecting TCP packet errors and retransmitting them. Bytestream service is packets that are sent and arrive at their destination sequentially. Basically this type of TCP protocol is hard to abuse. Unless the intruder controls a router between two systems, the intruder can always be tracked and used, such as using a syn attack[6].

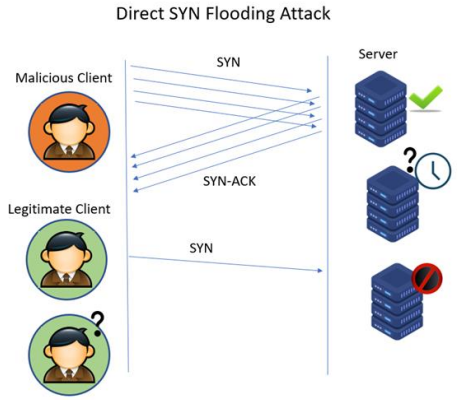

Figure 2. SYN Flooding Attack

The picture above explains that a SYN packet with a sender address that has been disguised, when the SYN packet arrives at the server, the server will then allocate the necessary memory buffers. Then if the memory allocation has been given to the attacker's host, the attacker's host will continue to send SYN packets that have been manipulated by the attacker and the IP address that has been disguised. The attacker host will force the server to accumulate half-open connections so that at its peak the server is unable to accumulate half open connections so that the resources owned by the server are totally paralyzed[7]. Data traffic that is in a network will fluctuate during its use. During busy hours the data traffic will be very dense so that the data traffic will be disrupted. Both data sent or data that will come will experience data queues which result[8]. protocol and many are also used to sniffer or sniff out private data on the network. Wireshark is now likened to a media or tool that can be used by users for their use, whether for good or evil. This is because wireshark can be used to search for sensitive information roaming the network, for example passwords, cookies and so on[9]. If the computer is connected to a high-speed network and the computer is being used by a network-based application, the wireshark application will display lots of data packets and cause confusion because so many network data packets appear. Wireshark applications can filter certain types of protocols that you want to display [10].

RESEARCH METHODS

The analysis used is system development analysis. Research with a development approach, is a research that seeks to find the effect of certain variables on other variables under controlled conditions. The research method is carried out using direct experiments, below is a flowchart for the process of illegal activity in the network.

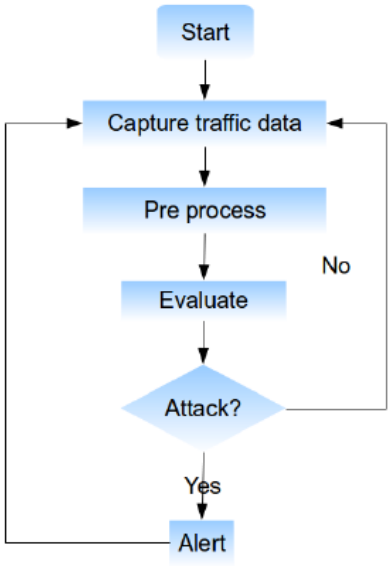

Figure 2. Illegal Activity Detection Flowchart In Networking.

The picture above explains that the user is given access rights in the form of an upload process, so the system to be built uses a hard disk limiter using disk quotas, so users cannot upload randomly because they have been limited by quotas to carry out the upload process. The process that is carried out is monitored by the wireshark so that users can safely upload data without the need to worry about someone infiltrating it when uploading the data. To capture packets according to the wishes of the user where after selecting one of the interfaces to be monitored network activity online it will appear as shown below.

RESULTS AND DISCUSSION

The test results below are testing activities that were successfully captured by Wireshark on the source information, the protocol destination and the capture time. Strategy in making promotional videos can be summarized in the production stage which includes pre-production activities, namely determining the concept and theme as well as the selection model as an addition to the appeal in video, where is the next stage of production video shooting was carried out in the field and the last is activity post-production namely selection, image editing and packaging video content by displaying featured tours in Pandai Sikek, with attention to the main aspects showing the beauty that exists at every tourist destination to attract viewer interest.

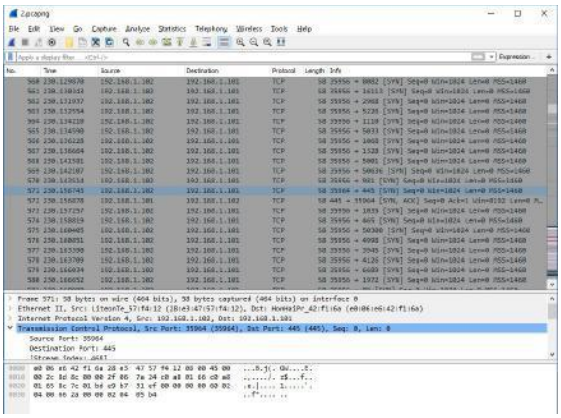

Figure 3. Wireshark Detection SYN Attack

Figure above explains how wireshark can capture illegal activity on the network after selecting the interface to be captured for analysis, if the process is complete then click the start button to start the packet capture process then the wireshark application will perform filtering and the results will be displayed on the wireshark screen for testing, the author filters and analyzing HTTP tcp port 80 packets, the results of capturing the packet are as shown below :

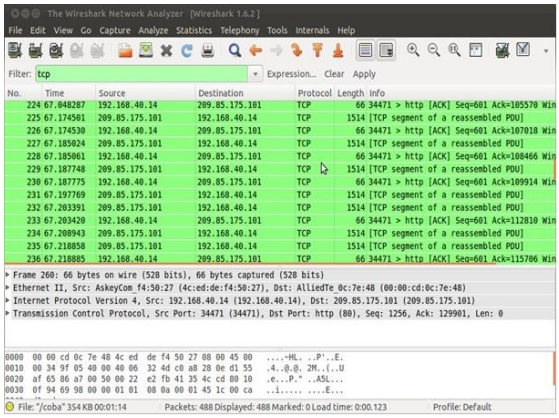

Figure 4. Results Of Capturing The Packet

CONCLUSION

From the data obtained regarding the network protocol, the result of filtering data packets using wireshark is that in wireshark, filtering packets is quite easy compared to applications such as forensic tools, snort, because it requires settings in snort.conf, while in wireshark, it is enough to just select the packet filter in the filter column. So that the network administrator can analyze the ongoing network packets.

BIBLIOGRAPHY

[1] Colladon, A. F., & Remondi, E. (2017). Using social network analysis to prevent money laundering. Expert Systems with Applications, 67, 49-58.

[2] McAndrew, D. (2021). The structural analysis of criminal networks. In The social psychology of crime (pp. 51-94). Routledge.

[3] Svenson, P., Svensson, P., & Tullberg, H. (2006, July). Social network analysis and information fusion for anti-terrorism. In Proceedings of the conference on civil and military readiness (Vol. 2006).

[4] Van der Hulst, R. C. (2009). Introduction to Social Network Analysis (SNA) as an investigative tool. Trends in Organized Crime, 12(2), 101-121.

[5] Carrington, P. J. (2011). Crime and social network analysis. The SAGE handbook of social network analysis, 236-255.

[6] Berlusconi, G., Calderoni, F., Parolini, N., Verani, M., & Piccardi, C. (2016). Link prediction in criminal networks: A tool for criminal intelligence analysis. PloS one, 11(4), e0154244.

[7] Krebs, V. E. (2002). Mapping networks of terrorist cells. Connections, 24(3), 43-52.

[8] Mastrobuoni, G., & Patacchini, E. (2012). Organized crime networks: An application of network analysis techniques to the American mafia. Review of Network Economics, 11(3).

[9] Lavorgna, A. (2014). Wildlife trafficking in the Internet age. Crime Science, 3(1), 1-12.

[10] Calderoni, F., Brunetto, D., & Piccardi, C. (2017). Communities in criminal networks: A case study. Social Networks, 48, 116-125.