International Journal of Synergy in Engineering and Technology
IJSET

Encrypted Honeypot Security System

Muhd Zakaria Sharbudin*, Azham bin Ahmad

Faculty of Computing, UCTATI, Kemaman, Kuala Terengganu
*Corresponding author: mzsharbudin97@gmail.com

KEYWORDS

Honeypot
honeyd
DDOS
Port Scanning
Nmap
TorsHammer

ABSTRACT

A cyber honeypot operates in a similar way in computer security terms, baiting a trap for hackers. It is a sacrificial computer device that, like a decoy, is supposed to attract cyberattacks. It mimics a destination for hackers and uses their attempts at infiltration to collect data about cyber criminals and how they work or to divert them from other targets. The purpose of this project is to create the Encrypted Honeypot System and, by port scanning and DDOS attack, to demonstrate or test the Encrypted Honeypot System. The configuration of the honeypot and tools to be used for the attack that is Port Scanning will also show in this project that Nmap will be used and TorsHammer will be used for the DDOS attack and the result of the honeypot will show the two attacks by the attacker in this project for the last segment.

1.0 INTRODUCTION

In the age of security and technology for communication networks, organizational networks have become a central problem in each of them. To provide a powerful, stable forum for the enterprise, Honeypots is built into a network of firewalls and intrusion detection systems. To better examine any malicious behavior or any policy transgression of access controls, firewall rules, firewalls provide filtering and generate logging. Methods such as firewall and Demilitarized Zone (DMZ) have been used differently, but for today's network protection it is not effective. The limitations of the current network would then be resolved by intrusion detection systems. The intrusion detection system quietly monitors the traffic of the network and provides warnings to say about any form of intruders based on the current intrusion signature database. The Honeypots will be introduced in the network to run the unused IPs of the network and the actions of the attacker on these honeypots will be analyzed.

In order to detect and defend attacks by advanced persistent threat actors, honeypots are most frequently used by large corporations and businesses interested in cybersecurity research. For large organizations to take an active defensive posture against attackers, or for cybersecurity researchers who want to learn more about the methods and tactics that attackers use, honeypots can be an effective tool. The cost of holding a honeypot can be high, partially due to the specialized expertise needed to enforce and manage a device that seems to expose the network resources of the enterprise while also preventing attackers from gaining access to any production systems.

Received April 2021; received in revised form May 2021; accepted June 2021.

The many explanations and specifics about the problem statement, aim, scope, literature review, methodology and also the outcome of the honeypot encrypted system at the end of the chapter will be seen in this project.

2.0 THE DEFICIENCIES OF THE SYSTEM

Two items found on the honeypots environment, firstly, particular servers are not secure or do not use a firewall system to detect intruders from outside. As a result, when the server does not use a firewall device to detect foreign intruders or attackers, the attacker will have the ability to attack the server. Secondly, minimize system administrator positions while monitoring a server or PC system. So, the administrator has to investigate the security framework that can provide the server with great shield or vindication from attackers or intruders.

3.0 PREVIOUS STUDIES REFLECTED TO THE CASE STUDIES

From(Mathur et al., 2019)Honeypot is a specific security capability in an enterprise that is part of the security process. These are the black hat guys' means to communicate with. Honeypot is essentially an IT tool whose importance lies in an IT resource.

Secondly, from (Kambow & Passi, 2014),unauthorized or illegal use of them, means that from the threats using them, the value of honeypots could be derived. If attackers didn't communicate with them, honeypots will have no benefit. Indeed, particular problems are not solved by honeypots. Instead, they are instruments that have security applications.

3.1 DEGREE OF HONEYPOT 'S CONTACT

Firstly, Low-interaction honeypot do not provide the attacker with operating system access based on interaction. It only provides services such as ftp, http, ssh, etc. Such low contact honeypots play the role of passive IDS where there is no shift in network traffic. Honeyd, Specter, BOF are several examples of low interaction honeypots. Honeyd is an open source instrument and the honeyd service emulation facility is unregulated, although spectre is not an open source tool created by Netsec. The well-known instance of low honeypot interaction is Honeyd. Honeyd is a daemon which is used on a single host to simulate large networks (Jain et al., 2016; Kambow & Passi, 2014).

Secondly, Medium-interaction honeypots. These also may not provide OS access to attackers like low interaction honeypots, but there are more than low interaction honeypots that are likely to be checked. Some examples are Napenthes, Dionaea, honeytrap, Mwcollect, for medium contact honeypots. These honeypots also provide attackers with face-to-face services and may use Mwcollect and Napenthes to collect the malware that spreads (Jain et al., 2016; Kambow & Passi, 2014).

Lastly, High-interaction honeypots, it is the most advanced honeypots are these. They are difficult to plan and execute. As they include real OS with them, these honeypots are very time consuming to build and have the highest risks associated with this. Nothing is simulated or constrained in high-interaction honeypots. Sebek, Argos, is example of high interaction honeypots. Since these honeypots require a real operating system, the risk level is increased by several levels, but it is a kind of trade off to collect vast quantities of information by allowing an intruder to communicate with the real operating system. This helps to capture and document the actions of the attacker, which can be studied later on (Jain et al., 2016; Kambow & Passi, 2014).

Table 1: Types of Honeypots. Adopted from (Kambow & Passi, 2014)

No	**Honeypots**	**Types of Honeypots**	**Examples**
1	Basic Interaction	Low interaction honeypots. Medium interaction honeypots. High interaction honeypots.	Honeyd, Kippo. Dionaea, Napenthes. Specter

From the Table 1 above, illustrate the types of honeypots from the basic of interaction. There a type of Honeypots based on the level starting from low, medium and high interaction that comes with samples honeypots systems.

3.2 HONEYD

Honeyd described as a "tiny daemon on a network that creates virtual hosts." It is software that is open source and is published under the GNU General Public License. The Honeyd framework is very versatile since it provides users with the ability to configure various arbitrary services that tend to run on different operating systems. It also offers logging features that can be used to boost the services-emulating scripts. On a modified Linux machine consumed mainly for penetration testing, called Backtrack, they installed Honeyd (Musca et al., 2013).

3.3 FIREWALL

In the early 1990s, firewalls were invented. They provide a fireproof buffer between parts of the buildings, making it more difficult for a fire to spread to other parts of one section of the building. Likewise, to protect it from the outside, a network firewall is installed around a network or subnetwork. In order to achieve the following objectives, Steven and William describe the firewall as a set of components installed between an internal network and an external network; all traffic must pass through the firewall, only traffic permitted by the security policy of the internal network is allowed to pass, the firewall that cannot be breached (Amalina et al., 2013).

In addition, firewalls work in two ways, either by refusing or accepting all messages based on a list of appropriate or unacceptable sources designated, or by approving or denying all messages based on a list of acceptable or unacceptable target ports designated. Firewalls are relatively easy to install, configure and run, even though they sound complex. A brief introduction to firewalls will be given in this post. It is not act as an analysis of particular items for the firewall. It will instead serve as a summary of what firewalls are, how they function, the various forms of firewall technology and their suitability for users of small offices or home offices and personal computers (Hazari, 2011).

3.4 INTRUDERS

Intruders have various motivations and objectives. Financial gain, manipulating public sentiment, and espionage, among many others, from lone attackers to advanced organized-crime groups, the motivations and objectives of intruders differ. Intruders also have various levels of resources, knowledge, access and risk tolerance that contribute to the level of portability of an attack that occurs (Varga et al., 2017).

From (Abomhara & Køien, 2015), state that, an insider seems to have more access than outsiders to a system. Many intruders are well-funded and others run on a minimal to no budget. Every attacker chooses an economical attack, an attack based on budget, capital and experience, with a strong return on investment. Intruders are classified in this section according to attributes, motives and aims, skills and resources.

3.5 DEMILITARIZE ZONE (DMZ)

DMZ splinted into two independent sub-networks, the boundary network and the cluster network, to prevent external intruders from accessing the cluster hardware by leveraging vulnerabilities in the Grid middleware, the Grid or cluster subnet. The DMZ protects all networks with a firewall designed to meet the unique requirements of the network in question. The boundary firewall philters Internet connexons and denies unauthorized connexons inside the DMZ to all computers (Schmidt et al., 2007).

The border firewall is relatively open, however, because Grid middleware's need a large number of open ports to execute correctly and efficiently, and a large number of fluctuating users need to access the Grid. In the DMZ, the Grid head node is located. The cluster network is secured by an internal firewall and direct connexons to the cluster subnet are prevented. The internal firewall is very strict to secure the cluster network and only allows a single specially built cluster connector to pass through and does not allow any interactive sessions to pass into the network of the cluster. The cluster consists of a cluster head node and a series of virtual worker nodes and resides in the cluster network (Anugrah & Rahmanto, 2018).

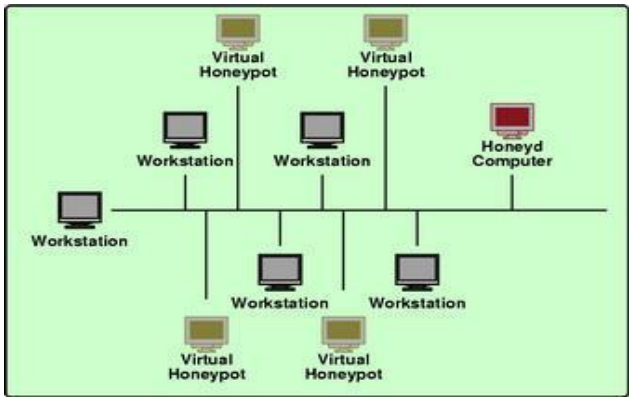

Diagram 1: An integrated honeypot configuration. Sources from: (Provos, 2010)

From the Diagram 1 above, the honeypot is primarily an instrument for collecting and learning knowledge. Its main goal is not to ambush the black hat group in order to capture them in action and bring charges against them. The emphasis lies on a quiet compilation of as much data as possible about their patterns of attack, programmed used, attack intent, and the black hat group itself. All this data is used to learn more about the techniques and explanations for the black hat, as well as their professional expertise and skills. This is just the main goal of a honeypot. For a honeypot, there are a number of other possibilities-diverting hackers from efficient

networks or capturing a hacker while carrying out an attack are only two potential examples. They are not the ideal solution to solving computer crimes or stopping them.

4.0 METHODS

In order to create Encrypted Honeypot Framework, it is important since, several surveys have been done for server problems, such as collecting information on server security vulnerability and how the server can be targeted by intruders or attackers with the use of many types of attacks, refer to the other article. After that, the Cisco PPDIOO is the right model in this project because it is the best model in the network context. In this process, the approximate time required to complete the production of this project must also be planned. Otherwise, for this project, you need to know how the honeypot implementation uses the Honeyd in the server and the server demonstration attack, such as styles of attack.

Table 2: Activity preparation and output (Sources: Develop for this project)

Activity	Output
Survey (self-monitoring) the weakness of the server in network and how to protect the server from the intruders by refer to the journal.	Implement the honeypot can protect the server from the intruders. Not only protect but, it can trace the intruders.

Table 3: Activity planning and output (Source: Develop for this project)

Activity	Output
To identify how the honeypot system, prevent the attack that use in the practical demonstration to the honeypot system in the server.	For creating the honeypot, Honeyd will be used. And, the demonstration of attack use is DDOS attack and Port Scanning to attack the server. Use the open source for the software.

From the table 2 and 3 above, the tables are continue starting from the preparation activity and planning. The survey must be performing to investigate the difficulties in server's security system and identified how honeypot system helps secure the servers system from the intruders.

5.0 IMPLEMENTATION

Any such approach demonstrates step by step how to configure Kali Linux and honeypot using PentBox in Raspberry pi 3 (model B), how to configure Kali Linux dual boot with Window 10, how to instal Nmap and TorsHammer, and how to build Port Scanning attacks using Nmap and DDOS using TorsHammer software. In addition, Raspberry Pi is a small device that means credit card-sized computers that do not need a lot of power to use and will get a super-portable network testing system that can take you anywhere when paired with Kali Linux. And, the testing will be on the same network for the results.

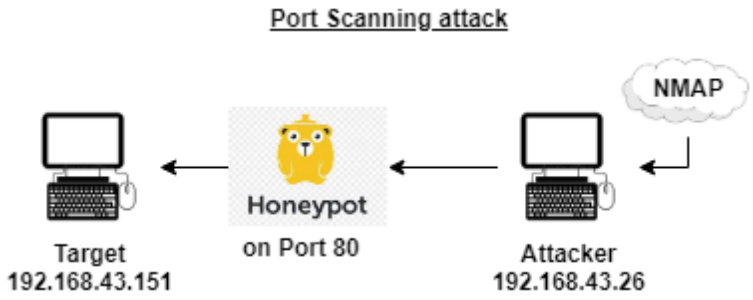

Diagram 2: Diagram of Port Scanning attack for this project. (Develop for this project)

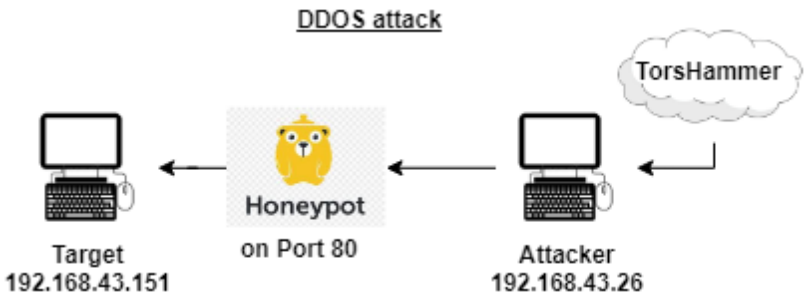

Diagram 3: DDOS attack for this project. (Develop for this project)

From the diagram 2 and 3 above, a port scan is an attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service. Scanning, as a method for discovering exploitable communication channels. While DDOS attack, using the TorsHammer, used as a tool as a slow-rate DDoS attack that is efficient and very disruptive on most servers.

5.1 PROJECT EXECUTION

Firstly, the hardware use in this setup is Raspberry pi 3 (model B), SD Card at least 8GB, HDMI cable, Monitor, Keyboard, Mouse, and USB cable to on the raspberry pi. After that, the software that had use in this setup is Kali Linux and Etcher. Etcher is for flash OS images into SD Card and USB Drive, safely and easily.

Secondly, need to download the Kali Linux image from the Offensive Security official download page. On the download page locate the “Raspberry Pi Foundation” drop-down box then downloads the version of Kali Linux for the Raspberry Pi. Next step, downloaded the “Kali Linux Raspberry Pi 2, 3 and 4 32bit” image from their website. If using a Raspberry Pi 2 or the Raspberry Pi 3, Kali does offer a 64bit version of their modified operating system.

Thirdly, to write the Kali Linux image to an SD Card, will be making use of a piece of software called Etcher. It can obtain Etcher by going to their official website and downloading the software. Once have installed the Etcher software to the device and can proceed with this guide.

6.0 RESULTS AND DISCUSSION

Test results that have been successfully completed and honeypot performance get all the attacker 's data from the testing with two port scanning and DDOS counterattacking attacks. The honeypot was successfully detected by the attacker Port Scanning using the Nmap for the port scanning attack, as shown in the diagram below (Diagram 4,5 and 6).

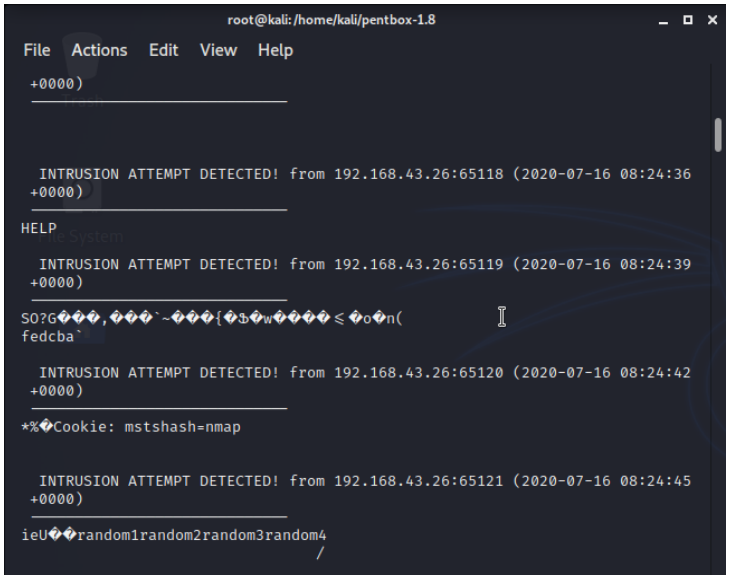

Diagram 4: Result of Port Scanning attack to the honeypot 1.

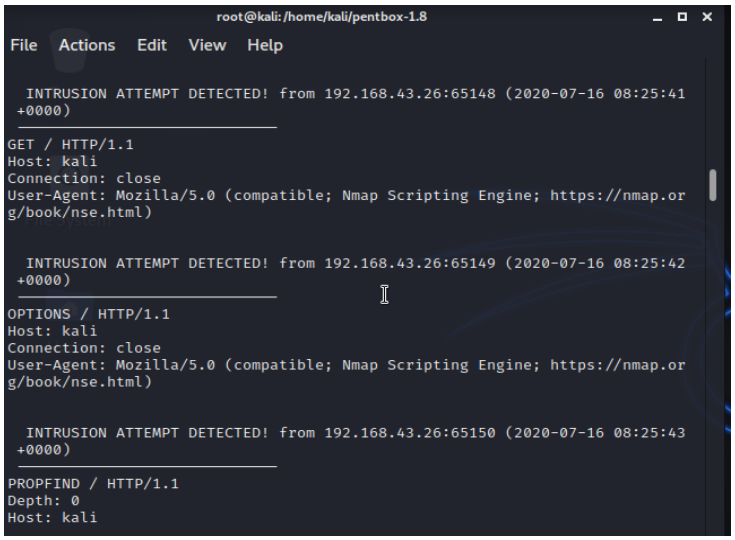

Diagram 5: Result of Port Scanning attack to the honeypot 2.

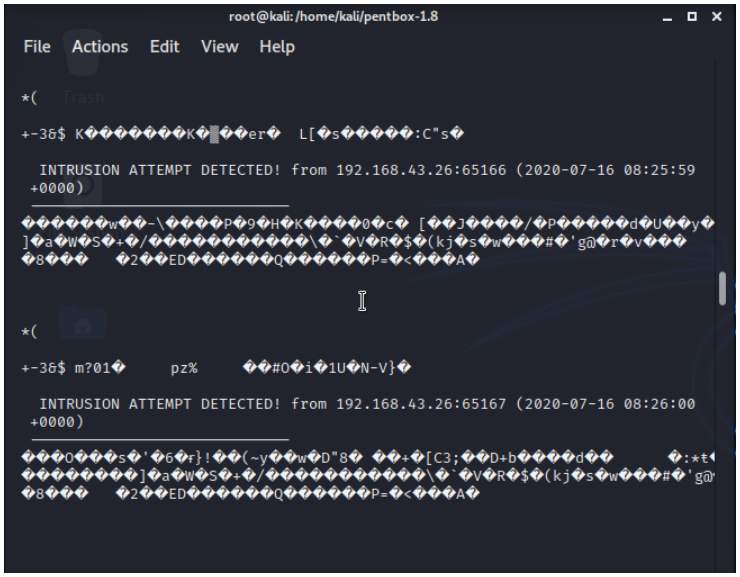

Diagram 6: Result of Port Scanning attack to the honeypot 3.

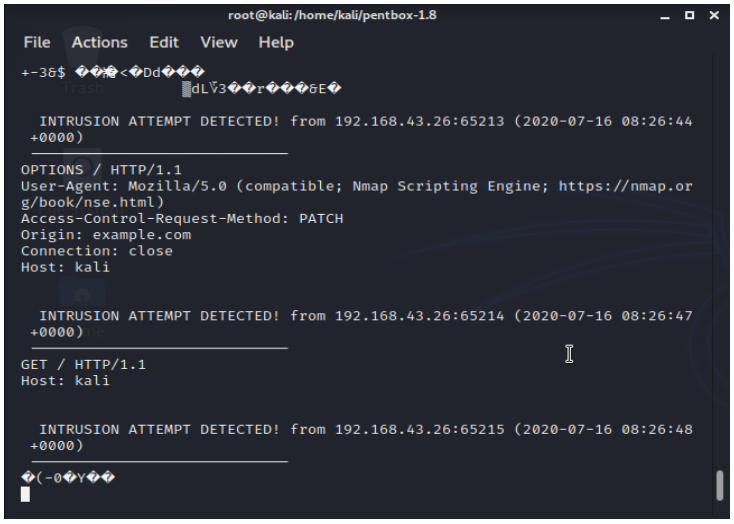

Diagram 7: Result of Port Scanning attack to the honeypot 4.

As seen in the diagram above (Diagram 7), the honeypot detected the attacker information such as IP address 192.168.43.26, as well as other data such as user agent, name host, and many more that have been traced as a server by the honeypot. Based on diagrams 4 till diagram 7, the honeypot was shown to be able to detect or track the intruder while checking the honeypot by Nmap of the Port Scanning attack. Several details that have been discovered about the intruder from the honeypot such as the IP address, User Agent, Host, etc. The result of checking the honeypot with the Port Scanning attack was therefore successfully detected by the honeypot.

As for diagram 8 below, it shows the outcome of the Honeypot Encrypted Device DDOS attack. Show the honeypot to effectively detect the attack by the attacker using the TorsHammer using the DDOS attack.

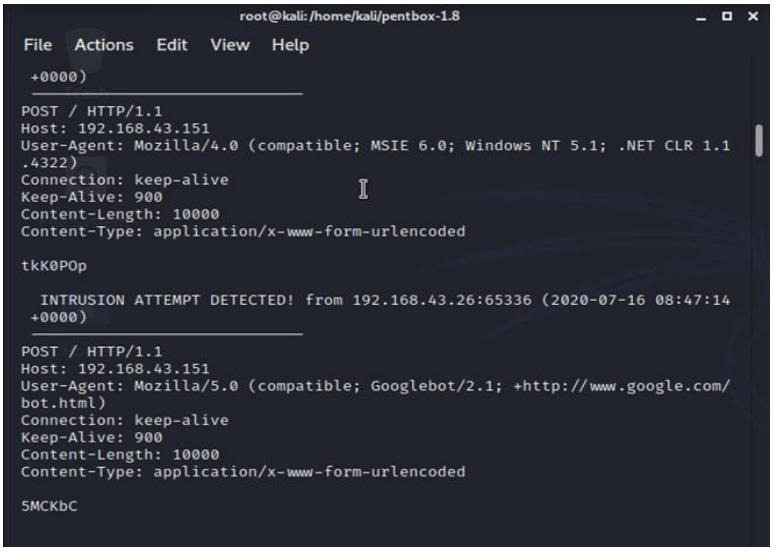

Diagram 8: Result of DDOS attack to the honeypot 1.

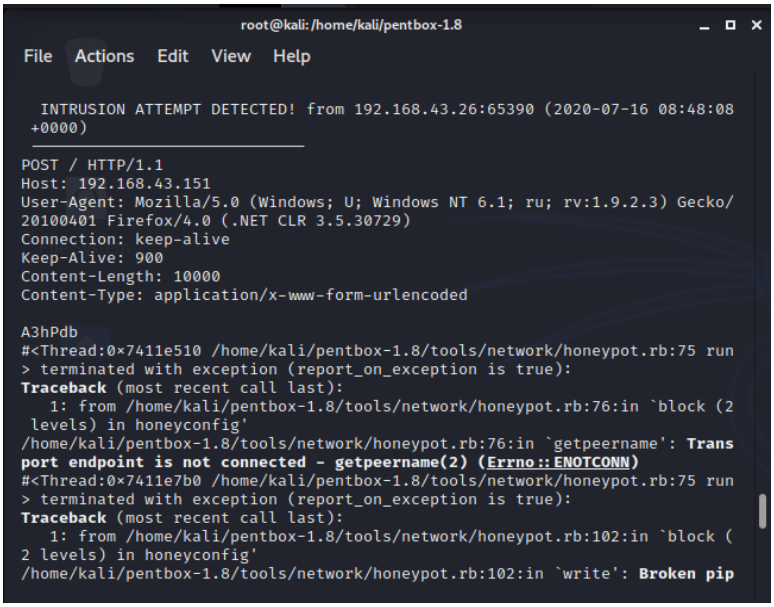

Diagram 9: Result of DDOS attack to the honeypot 2.

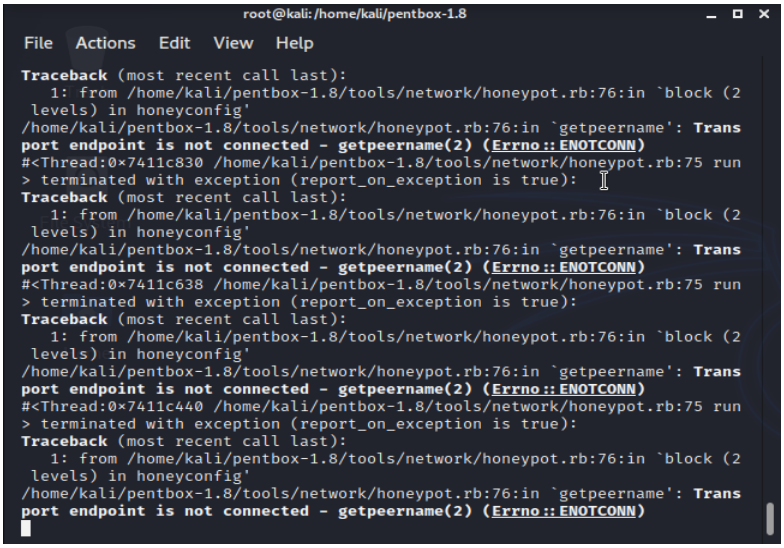

Diagram 10: Result of DDOS attack to the honeypot 3.

The honeypot can also detect the attacker's DDOS attack, as the diagram above indicates. Besides, honeypot can also see some of the attacker's details, which is the attacker's IP address, user agent, link, and much more. Next, in diagram 7, the honeypot tries to trace and is not related to the transport endpoint. Last but not least, for this research, honeypot was able to effectively detect all the attacks from the tests that were conducted.

The honeypot has also been shown to be able to detect or track the intruder while checking the honeypot by TorsHammer of the DDOS attack, based on diagrams 8,9 and 10. As a result, honeypot detected a lot of information about the intruder, such as IP address, link, host, user agent and so on. Therefore, the honeypot has also successfully established the outcome for testing the honeypot using DDOS attack. As the table below shows the outcome.

Table 4: Result of the Honeypot.

	Port Scanning	**DDOS**
Honeypot was detected	Yes	Yes
Information about the attacker	Yes	Yes

7.0 CONCLUSION

The project was successful because it had accomplished its goals of designing the Encrypted Honeypot Protection Framework and demonstrating through the Honeypot attack such as Port Scanning and DDOS attack. The attack used has been shown to be detected by this Encrypted Honeypot Protection Framework. Furthermore, this honeypot using honeyd that was low level of interaction can also detect and display attacker information. Even, using an open source for the honeypot, it also shows good and easy to use results. This PentBox can be used by businesses who save budgets and want to use the best security solution to provide a strong security system based on this project for the network industry.

REFERENCES

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*. https://doi.org/10.13052/jcsm2245-1439.414

Amalina, N., Alsaqour, R., Uddin, M., Alsaqour, O., & Al-Hubaishi, M. (2013). Enhanced network security system using firewalls. *ARPN Journal of Engineering and Applied Sciences*.

Anugrah, I., & Rahmanto, R. H. (2018). Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone. *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*. https://doi.org/10.33558/piksel.v5i2.271

Hazari, S. (2011). Perceptions of End Users on the Requirements in Personal Firewall Software. In *Contemporary Issues in End User Computing*. https://doi.org/10.4018/9781591409267.ch008

Jain, A., Sharma, B., & Gupta, P. (2016). Honeypot: an External Layer of Security Against Advance Attacks on Network. *Verdant College of Engineering And Technology*.

Kambow, N., & Passi, L. K. (2014). Honeypots : The Need of Network Security. *International Journal of Computer Science and Information Technologies*.

Mathur, R., Pathak, V., & Bandil, D. (2019). Emerging Trends in Expert Applications and Security. In *Emerging Trends in Expert Applications and Security*. https://doi.org/10.1007/978-981-13-2285-3

Musca, C., Mirica, E., & Deaconescu, R. (2013). Detecting and analyzing zero-day attacks using honeypots. *Proceedings - 19th International Conference on Control Systems and Computer Science, CSCS 2013*. https://doi.org/10.1109/CSCS.2013.94

Provos, N. (2010). A Virutal Honeypot Framework. *IEEE Security & Privacy Magazine*.

Schmidt, M., Smith, M., Fallenbeck, N., Picht, H., & Freisleben, B. (2007). Building a demilitarized zone with data encryption for grid environments. *GridNets 2007 - Proceedings of the 1st International Conference on Networks for Grid Applications*. https://doi.org/10.4108/gridnets.2007.2160

Varga, P., Plosz, S., Soos, G., & Hegedus, C. (2017). Security threats and issues in automation IoT. *IEEE International Workshop on Factory Communication Systems - Proceedings, WFCS*. https://doi.org/10.1109/WFCS.2017.7991968