Network Isolation and Security Using Honeypot

By

Foo Ce Sheng

A REPORT

SUBMITTED TO

Universiti Tunku Abdul Rahman

in partial fulfilment of the requirements

for the degree of

BACHELOR OF INFORMATION TECHNOLOGY (HONS)

COMMUNICATIONS AND NETWORKING

Faculty of Information and Communication Technology

(Kampar Campus)

MAY 2019

DECLARATION OF ORIGINALITY

I declare that this report entitled **“Network Isolation and Security Using Honeypot”** is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature : ___________________________

Name : ___________________________

Date : ___________________________

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my supervisor Ts Dr Gan Ming Lee for continuous support and guidance throughout my final year project. Thank you, for his patience, motivation, enthusiasm and immerse knowledge. His guidance helped me in all time of research and system implementation. I could not imagine having a better advisor and supervisor for my university life.

Besides, my sincere thanks also go to my moderator Ts Dr Lau Phooi Yee who provide me support and feedback on the final year project. Thank you for giving me the opportunity to present my project. I appreciate her motivation to provide me a quality final year project. The valuable feedback gives me more insight on how to improve my current system.

I thank my fellow friends: Lim Chia Wei, Eui Ching Sie and Leong Chow Cheng for giving me helps and recommendations in doing my final year project. Last but not least, I would like to thank my family for providing me support financially and emotionally. Thank you very much for the encouragement to pursue my high education in Universiti Tunku Abdul Rahman (UTAR). I would not be able to complete my study and final year project without everyone’s supports.

ABSTRACT

Despite the fact that there are numerous network security tools available to secure the network, but the number of network attacks keep increasing. A way proposed to secure the network is by network isolation and security using honeypot. Honeypot is act as a bait to lure the attacker to attack the system. While the attacker attempts to explore the network of the system, Honeypot will automatically log every action and IP address of the attacker without his knowledge. Then the network administrator gets the log file to analyse the action of the attacker and it is helpful in determine the motive of attacker.

This project implements a virtual honeypot system in a virtual environment which lets the attacker see no difference with the real system. The system is clustering with each other to make it high available. If one of the servers fail, another server still can perform the server function. The system is able to divert the attacker to the honeypot if the user is suspicious. It is integrated with the real network system and able to determine the legitimate or non-legitimate user. The notification will send to network administrator if unauthorized login is detected. For more added value, the Two-Factor Authentication login function is added to make sure the real user is entering the system.

The literature review about types of security systems and types of virtual machines. The development cycle is waterfall approaches. Besides, the uses case diagram, activity diagram and the way to set up the system are plotted. Honeypot is set up to open SSH port for attacker to login to the computers. It can secure the network system by making the attacker frustrated while exploring the network.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IoT	Internet of Things
TCP/IP	Transmission Control Protocol/Internet Protocol
IDS	Intrusion Detection System
DMZ	Demilitarized Zone
LAN	Local Area Network
IPS	Intrusion Prevention System
DoS	Denial of Service
Hyper-V	Microsoft Hypervisor
IP	Internet Protocol
MAC	Media Access Control Address
SSH	Secure Shell
VDI	Native VirtualBox format
VMDK	VMware Virtual Disk Format
VHD	Hyper-V format
HDD	Parallels Desktop Format
OTP	One Time Password

CHAPTER 1: INTRODUCTION

This project involves the research and implementation of network isolation and security using Honeypot. With the increasing number of network attacks, the initiative to secure a network must be expanding continually. Although there are many tools available to secure the network, but it is best to assume vulnerabilities are always existing. Thus, an innovative way proposed to secure the network is to deploy honeypots on top of the standard security mechanisms.

Honeypot is set up in the real network system to work with other security system to enhance the security of the network. It is a system that can be easily discovered and exploit by the attacker. This characteristic enables honeypot to lure and trap the attacker in the system effectively. Every keystroke, IP address, MAC address, date and time of access the system will be recorded once the attacker breaks in the system. The attacker might think that he has gained access to the system successfully, but he is just entered a faked environment.

The network is isolated with the virtual environment using Hyper-V with clustering. Hyper-V enables the system to run several operating system at the same time to provide the virtual environment to the network. User or attacker will see the network system no different with the system implemented with the real hardware machine. The virtualization enables scalability, flexibility and security to the system. It can save the cost to implement compared to using the real hardware machines. Failover clustering is also implemented to enable high availability and better utilizing of hardware resources. If one of the server nodes fails, the other server will carry on the tasks. They can share the resources between the server.

1.1 Problem Statement and Motivation

Computer security is up most important with the emerging of new technologies such as Internet of Things (IoT), Big Data and Cloud Server. We can find out that all the new technologies are conducted on the network and the security of the network is the priority to implement such technologies. Although there are many research and experience in the security, we are still unable fully secure the computer system and prevent the network from attackers.

One way to get alerted of the new vulnerability to the network system is by setting up a computer system on a network that we expect it is easily to broken into. When someone attempt to connect to the system that have no other legitimate function, the activities will be suspected. The system is so called a honeypot. Honeypot have been proposed as another way to complement the defences like firewall and Intrusion Detection system (IDS) for securing the computer networks that are connected to the Internet (Xinwen, F. Wei, Y., n.d.).

The Honeypot has 2 level of interactions such as low-level interaction and high-level interaction. The low interaction honeypot restricts the interaction between an attacker and the honeypot. It limits the scope of attacker’s action and minimize the risk of compromise. Meanwhile, the high interaction honeypot exposes the whole system including the operation system, the files and directories of the system and the network status to the attacker, the attacker can gain full access of the system targeted.

Honeypots can be categorized with respect to their implementations. The implementation are physical honeypot and virtual honeypot (Provos, n.d.). A physical honeypot is a real machine with its own operating system and IP address on the network meanwhile a virtual honeypot is a machine that hosted by another machine and respond to the network traffic directed to the virtual honeypot. Virtual honeypot is proposed to implement in this project because they do not require additional computer systems. It is possible to populate a network with hosts running with many different types of operating systems.

This project come with an idea to provide security and isolate the network using honeypot to improve the security of the existing network systems. On the other hand, to enhance the functionalities of current honeypots as compared to the traditional way of defences. The honeypot implementation is to trap and lure the attacker. Although there are many honeypots, this project makes the different with the functionality to divert the attacker from the real server to the honeypot. Basically, the proposed honeypot can be integrated to the real networking system. It is able to determine the authenticate user and unauthorized user by adding the functionalities such as a login page, OTP authentication and Telegram notification.

1.2 Project Scope

The ultimate deliverable of this project is to research and implementation of network isolation and security using honeypot. To protect the network security by implementing the virtual and isolated of honeypot. As we know that, honeypot is a powerful tool in network security, and it is able to alert the network administrator when there is an unauthorized access. Besides, it can monitor and analyse the information about the attacker and the method they are using to attack the systems. The output of this project is to deliver a honeypot system that can determine authorize and unauthorize user, and then divert the malicious traffic out of the important system.

While diverting the attacker out of the important system, the honeypot also gives early warning to the network administrator before a critical attack hits the system (Anon., 2016). For this statement, the administrator will get notification and can react quickly to the actions of the attack. The attack actually being trapped in an isolated network environment which will not affect to the running operations. While the attacker is exploring the whole system, the information about the attacker and the attack method are captured in the system. This allows the network administrator to analyse and monitor the behaviour of the attacker in the system (Anon., 2016).

For the implementation to the real system, some security countermeasure also implemented to improve the security of the system. The system requires another authentication if there is any new IP address trying to SSH to the system. Meanwhile, Two-Factor Authentication also implemented to make sure the user is being authorized to access the system. For instance, if the network administrator’s username and password have been stolen, the user still unable to access the system. This is because he has to bypass the Two-Factor authentication that makes the system to be more secure.

1.3 Project Objectives

- **To protect the actual network from malicious attack using honeypot virtual/isolated network.**

  The information obtained from IDS (Intrusion Detection System) and Firewall does not show the information of the hacker and the way of their attacks. By implementing honeypot, we can get the information about the intruders as all their activities are recorded in the system log. Besides, honeypot not only records the malicious traffic, they also capture the new methods and techniques used by the attackers (Akkaya, 2010). The Honeypot is deployed in a virtual environment using virtualization technology. Although the Honeypot system is in virtual environment, the attacker is still recognizing the network system same as deploying in a real system. Thus, virtual Honeypot can protect the actual network from malicious attack.

- **To build the honeypot using network virtualization**

  Honeypot is a digital network bait and it is implemented by using network virtualization to attract attackers and distracting them from real production systems (Spitzer, 2003). In order to create deception for the intruders, implementing Kippo Honeypot in the network will aid in network virtualization. The virtualization using Windows Hypervisor, Hyper-V can run some virtual machines in the network. Attacker will see no difference when they perform attack as compared to the real system.

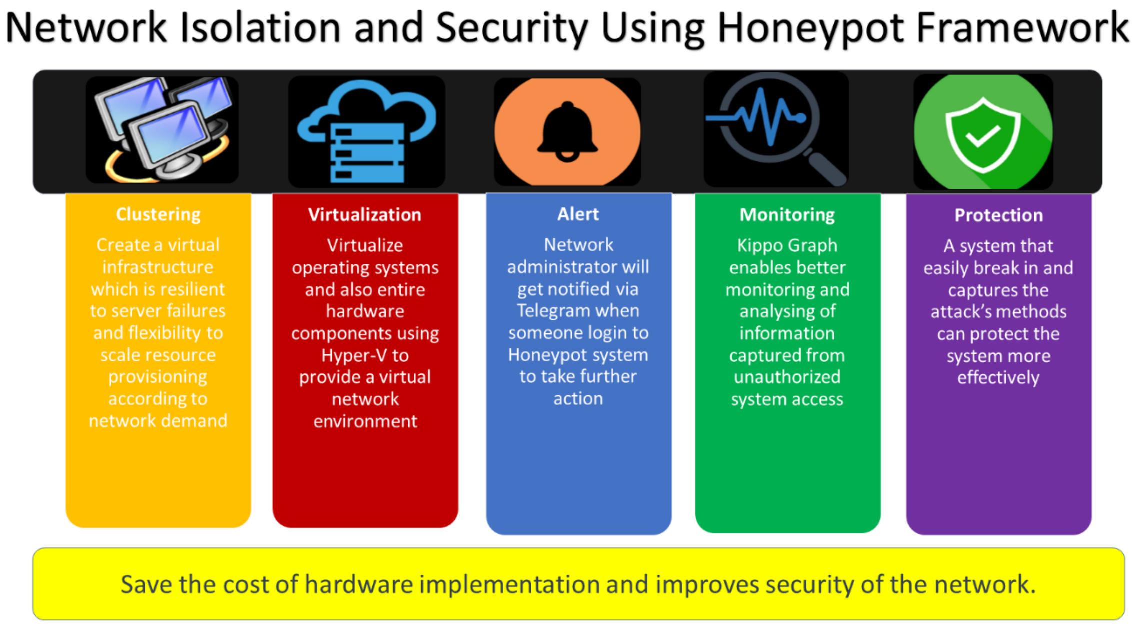
- **To alert the network administrator when is an unauthorized access**

  The deployment of honeypot is to alert the network administrator once captured the unauthorised and malicious activity. It would be easier for the network administrator to analyse and derives the value from data collected (Spitzer, 2003). Intrusion detection and logging applications can be organized within the honeypot. Low-interaction honeypots will create less realistic environment and only deploy a basic event log, yet they capture data and send to network administrator (Rathire & Jain, 2013). The network administrator will get notified once someone get into the Honeypot system by using Telegram mobile application.

- **To monitor and analyse the information about the attackers and the attack methods**

  Whereby Honeypot serve as an essential function by capturing threats, either internal or external (Spitzer, 2003). For instance, Honeypot such as Kippo can open SSH port to attract the intruder to perform attack. Once the intruder interacting with SSH of the Honeypot system, the system will record the keystrokes and capture the attacks (Spitzer, 2003). Thus, honeypot will send a signal to monitor and analyse the information about the attacker and the method they are using in the attack.

1.4 Project Framework



Network Isolation and Security Using Honeypot Framework

Clustering
Create a virtual infrastructure which is resilient to server failures and flexibility to scale resource provisioning according to network demand

Virtualization
Virtualize operating systems and also entire hardware components using Hyper-V to provide a virtual network environment

Alert
Network administrator will get notified via Telegram when someone login to Honeypot system to take further action

Monitoring
Kippo Graph enables better monitoring and analysing of information captured from unauthorized system access

Protection
A system that easily break in and captures the attack's methods can protect the system more effectively

Save the cost of hardware implementation and improves security of the network.

Figure 1.4.1 Project Framework

- **Clustering**

  2 bare metal servers are used to host the virtual machines. The nodes work together to failover the honeypot system with no or little downtime in the virtual environment. Besides, it can maximize the server resources by allocating high load virtual machine to the node with the lower workload.

- **Virtualization**

  Virtualization provides flexibility and scalability for the systems in the network. It can run variety of applications to be handled by multiple users on a single server at the same time. The operating systems will not interfere with other users while they are on the same server. Hyper-V is used to virtualize the system in the network.

- **Alerting**

  Alerting provides a quick notice of any unusual activities to the Honeypot system. The network administrator will get notified once someone logged in to the system. This can provide a fast and efficient response to any possible attacks to the system. The alert system is implemented using Telegram bot and it can notify the network administrator when someone logged in to the system. So that, admin can take further action more effectively.

- **Monitoring**

  Data gathered from SSH Honeypot will be recorded all the time. We can analyse the data for a better interpretation of the attacker motive in the system. Kippo Graph provides a good analysis of data by sorting the data into graph or a table. Network administrator can see the data easily and hence can improve the security of the network system from time to time.

- **Protection**

  A system that is easily break in can provide protection for the network system. It lets the attack feels that he has attacked the system and got the files and information he tends to get. He might be frustrated if he got trapped in the system many times. At the same time, all the actions and behaviours in the system are recorded.

1.5 Impact, Significance and Contribution

Some organization might think that setting Honeypot in a network is wasting of time and money (Dargin, 2017). The most significant value of Honeypot is gathering information that are not available from IDS (Intrusion Detection System). The attacker's behaviour, IP address, keystrokes and MAC address can be logged in the system. When user attempt to get into the system, it can trigger alert to notify the network administrator. The notification will send to the portable device, so that the person in charge will do early prevention if the attack triggered to the system.

Besides, the logged data collected by Honeypot system can use to improve the network security. The data logged and collected is best to analyse the new threads or attack methods in the system, no matter the attack is Denial of Service (DoS) attack, SQL injection, eavesdropping attack and Man-in-the-middle (MitM) attack, just to name a few. This is an effective way to determine the trend to attack the system because the attack method will be always updated and changed from time to time to adapt to the new system.

It is best to work with other network security tools like IDS, firewall and DMZ to reduce the false positive alert. Honeypot is easily to be broken into by using the default username and password of the system. The attack will see no different with the real system because it is installed in the virtual and isolated environment. The attacker will keep exploring the fake system and he can do whatever he wants in the system without the interruption to the real operations. Honeypot can frustrate the attack to stop attacking the network system. This is because Honeypot cause attacker to spend more time to exploit the network.

If the honeypot is implemented in the hardware machine, the cost will be higher to run the machine. Virtualize honeypot can save the cost of implementation by creating the virtual environment in the network. Besides, to provide the high availability and scalability honeypot security system, the system is implemented with Failover Clustering to make the system always available. In the scenario that, one of the systems fail, another system will carry on the job by the previous system. The task in the system can be prioritize if the task is more important.

Moreover, this project is able to determine the legitimate and non-legitimate user who login the system and divert the user to the honeypot. It is implemented in the real network system to trap and lure the attacker.

1.6 Background Information

The motivation behind the name honeypot is inspired from the existing honeypot in the real life. The honey in the honeypot should be resourceful and it can be referring to a child or nest of ants. It is very useful to get the person lured out. The same concept applies when the term honeypot comes to the computer. The honeypot attracts the attackers to exploit the target and perform the attack in between.

Honeypot was started by Lance Spitzner in 1999 in a paper titled “To Build a Honeypot”, he tried to figure out how attacker performed network attack in the mid-1980’s (Christian, S., Ian, W., Peter, K., 2006). In January 1991, while Bill Cheswick was working at AT&T Bell Laboratories, he discovered the log files for attacks. He intended to trace the attacker keystrokes, learn his new techniques and warm the victims by using honeypot. The attacker was recognized by Cheswick after some time. On the other hand, the attacker was kept inside the honeypot until Cheswick shut it down. The first commercial honeypot was released with the name CyberCop Sting in 1998.

The usage of honeypot was spread widely, and it is used to capture the malicious activities, malicious software on the network and raise alert when a new threat occurs. Honeypot became popular in the computer security especially to those who concern about the network security. They implemented honeypot in the network, so that the network is more secure to malicious traffic. Researchers and professionals are always worked to improve the functionalities of honeypot. There are many more features were added to honeypot to achieve a better performance and beneficial to the user of the computer.

In year 2017, Alphabay and Hansa darknet markets were shut down with the help of Honeypot system to lured and trapped the users into the Honeypot trap (Walsh, 2017). Dutch police run the honeypot operation to collect the evidences regarding to the site users. The international police have performed an incredible take down of the darknet drug market. The operation was implemented successfully.

1.7 Review of Honeypots

- **Conpot**

Figure 1.7.1 Conpot Honeypot

Conpot Honeypot is a low interactive honeypot deployed in the control system (Anon., n.d.). It provides variety types of common industrial control protocol to collect the attacking method.

- **Honeyd**

Figure 1.7.2 Honeyd

Honeyd is a little daemon that creates virtual hosts on a network. The hosts can be configured to run subjective administrations and the identity can be adjusted with the goal that they are being running sure working framework. It empowers a solitary host to ensure various locations. Honeyd also improves the network security by providing instruments to risk recognition and appraisal. It stops the enemies by concealing genuine frameworks amidst virtual frameworks (Provos, n.d.).

Honeyd is deploy in the low-level interaction of the system. It is basically capturing the TCP traffic that attacker generated. When the attacker establishes a connection with Honeyd, it will generate a fake message and show to the attacker. It is also able to create fake IP address and interfere the attacker that trying to attack the machine. Honeyd can install several different operating systems at the same time. The advantage of using Honeyd is it can capture the connection on any port. Besides, it is able to change services.

- **Nepenthes**

Nepenthes is a medium level interaction honeypot. It is able to learn new threats and detect the new malware and botnet. The simulation algorithm is based on virtualizing the logical responses for incoming requests. When the request arrives to the Nepenthes, the message is analysing and monitored. Then, the fake responses are created. This level of interaction is not working on network stack and manage it. They just bind to the socket of the operating system itself. Nepenthes is working on five modules such as, vulnerability, fetching, logging, submission and shellcode parsing module.

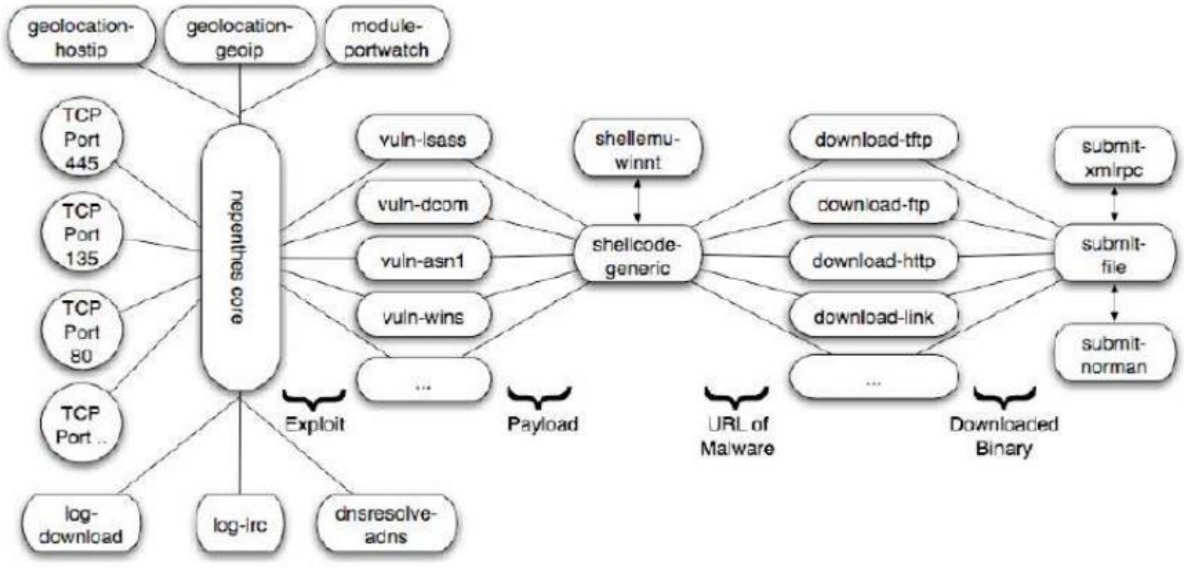


Figure 1.7.3 Nepenthes architecture from Maggi F and Zanero S. (2008)

- **Honeywall**

Honeywall is a high-level interaction honeypot. It is a gateway device in the honeypot. The Honeywall is usually placed in the honeynet network. It is the main point of entry and exit for all network traffic for a honeynet honeypot. This allows for complete control and analysis of all network traffic to and from a honeynet system.

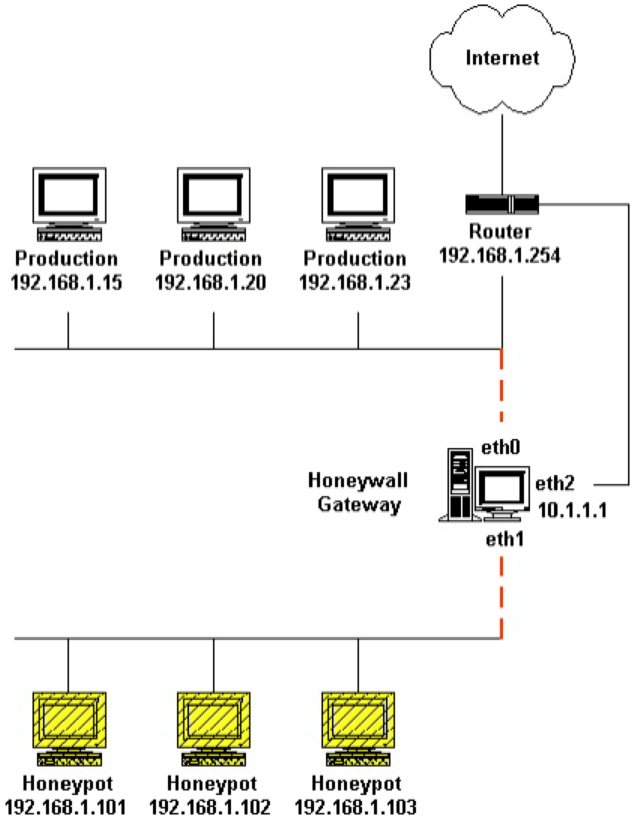


Figure 1.7.4 Example of Genll Honeynet (Brough, 2003)

CHAPTER 2: LITERATURE REVIEW

2.1 Review of the Security Systems

2.1.1 Firewall

Firewall is a security system that screens the incoming and outgoing network traffic. It can opt whether to accept or decline particular traffic based on a set of defined security rules (Anon., n.d.). Firewalls lies in the front line of the defence of network security. It builds up a barrier amongst secured and controlled internal networks. The internal network is more trusted, while outside network is likely untrusted. The advantages of firewall are it can deny the traffic that is non-legitimate, it can filter the protocols and services that can be easily exploited, it helps to protect the network by hiding the names of internal systems from outside hosts and firewalls can concentrate extended logging of network traffic on the system.

The firewall is intended to keep the attackers out of the system meanwhile the honeypots are intended to entice the hackers to attack the network (Tejvir, K., Vimmi, M., Dheerendra, S., n.d.). This is done as such that a security analyst can know how the attacker work and can know which systems and ports the attacker are keenest on. Likewise, firewall also has the log services which can record all incoming and outgoing traffics. Meanwhile, Honeypot log the activities while attacker attempt to attacker the system, this can save a lot of memory. As comparison, the firewall log may contain thousands of entries in the network, while the honeypot contains only a few entries.

The weakness of firewall is that the set of rules has to configured manually, in order to differentiate either it is legitimate traffic or non-legitimate traffic. Besides, the firewall is not effective to react to network attacks and thus it is unable to initiate effective counter-measures. If firewall is not pre-set with defined rules, it does not analyse the contents of the data packets that make up the network traffic. On the other hand, the firewall cannot prevent attack coming from application layer due to the filtering rules (X. Jhang, C. Li, W. Zheng,, 2004).

2.1.2 Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a security tools intended to alarm the administrator automatically when somebody is endeavouring to compromise the information system through malicious activities or violates the security policy (Anon., n.d.). IDS monitor the network system activity by detecting the vulnerabilities in the network traffic, checking the integrity of files and conducting the analysis of patterns based on the knowing attacks. It can screen the network to get the most recent threats which could result in the future attacks.

IDS likewise to suffer from the high false positive rates. Meanwhile, Honeypot is less likely to suffer from it. Screening the data that enters and leaves a honeypot gives us a chance to assemble the information that is not available to IDS. To identify malicious behaviours, IDS require signatures of known attacks and it is frequently failed to recognize the compromises that were unknown at the time it was deployed. Meanwhile, honeypot can detect the vulnerabilities that are not yet comprehended. Subsequently, the forensic analysis data that gathered from honeypot is less likely to be false positives than the data gathered by IDS.

IDS is utilized as an alternate option to protect the network system. The shielding approach is deficient in a few different ways, IDS is unable to prevent attacks from the insiders. Besides, IDS have to rely on signature matching or statistical models to identify new kind of attacks. This implies that the latest and unknown threats may not be detected if the system is not updated frequently. Conversely, honeypots are designed to capture all kind of attacks directed against them. When the network traffic act abnormally, Honeypot will capture the information in the system (Provos, 2004).

2.1.3 Demilitarized Zone (DMZ)

Demilitarized Zone (DMZ) adds an extra layer of security to the network and it provide buffer in the local area network (LAN) and the Internet. A DMZ server is also known as Data Management Zone and it gives secure services to local area network users for ftp, web applications and email that require the access to Internet. DMZ is known as demilitarized zones because it is based on the military concept which use as a barrier against the enemy.

Honeypot is placed in between of two firewalls that implies all of the inbound traffics. It is monitored using security appliances before they enter the server of the organizations which is hosted in the DMZ. It acts as a security system to block the most casual of threats (Margaret, n.d.). If the attacker is able to get through the outer layer firewall, they must gain the unauthorized access to the services before they can do attacks. DMZ allows user to isolate the network that offers public services to Internet users. DMZ comes with limited access to the internal network to reduce the ability of an intruder to attack the internal network.

Meanwhile honeypot works on the idea that all of the traffic coming to the honeypot is suspicious. Honeypot is place in the DMZ. Means that the actual server is hidden and invisible to the attackers. Honeypot gather the save logs and record event of the attacked system in DMZ to improve the overall security of the cooperation. The weakness of DMZ is it falls short in protecting the network is packet sniffing.

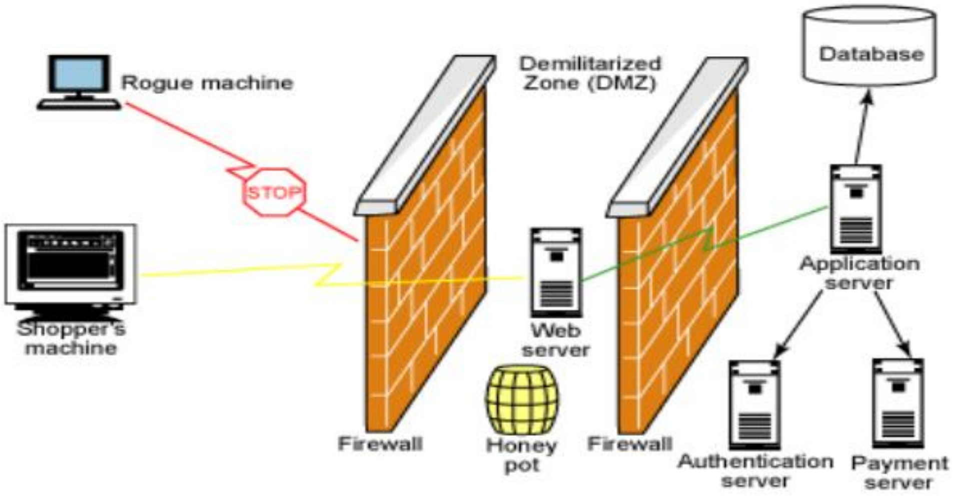


Figure 2.1.3.1: The Honeypot is placed inside the DMZ (Akshay, H., Sanket, T., Ganesh K.,, n.d.)**.**

2.1.4 Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is a network security countermeasure that analyse the flow of traffic and prevent the vulnerability exploits. The malicious input to target application causes the vulnerability exploits and the hacker uses the vulnerability to interrupt and gain control to the system. If the exploit is deployed successfully, the hacker can disable target machine application by denial of service (DOS) attack, and they can grant the permission to compromise the system attacked.

The IPS is placed behind the firewall and give a complementary layer of screening of vulnerabilities in the system (Anon., n.d.). If compared to Intrusion Detection System (IDS), it is a passive system that scans the traffic and log the threats, the IPS is placed in the direct communication path amongst the source and destination, it analyses the automated actions on all of the network traffic that enter the system actively. The main function of IPS includes alarm the administrator about the vulnerabilities, killing the malicious packets, blocking the traffic from source address and resetting the connection.

However, IPS most common problem is the detection of false positives or false negatives (Nick, I., Cesar, U., Richard, B., 2005). This is happened when the system blocks the activity of someone’s system due to some abnormal behaviour and IPS will assume it is a malicious action and this causes the denial of service (DOS) to a valid user. On the other hand, if the detection is false negative, it will allow the attack to bypass the network and the system. Besides, IPS is not effective in detecting the new types of security threats.

2.1.5 Sandbox

A sandbox in computer security refers to a safe isolated environment that replicates the end user operating environment for running applications that could present a security risk. It is a form of software virtualization that lets applications run in its isolated virtual environment. In this statement, the sandbox provides a safe environment that allow user to execute files, control the network traffic and prevent the hidden malware in the sandbox. The user can observe any malicious activities run by the program in the safe environment. As compared to honeypot, the virtualization of honeypot can be deployed to the network meanwhile sandbox deployment is limited to the own computer system.

2.2 Summarize of the security system

Security Systems	**Strengths**	**Limitations**
Firewall	Accept or decline particular traffic based on a defined set of security rules. Filter those protocols and services that can be easily exploited. It helps to protect the network by hiding the names of internal systems from outside hosts. Concentrate extended logging of network traffic on the system.	Most firewalls do not analyse the contents of the data packets that make up the network traffic. Set of rules has to be configure manually to differentiate legitimate traffic from non-legitimate traffic. Cannot react to a network attack.
Intrusion Detection System (IDS)	Detecting the vulnerabilities in the network traffic. Check the integrity of files Conduct an analysis of patterns based on the knowing attacks. Automatically screens the Internet to get the most recent threats which could result in the future attack.	Suffer from the high false positive rates. IDS require signatures of known attacks and it is frequently failed to recognize the compromises that were unknown at the time it was deployed.
Demilitarized Zone (DMZ)	Secure server that include an extra layer of security to the network.	Falls short in protecting the network is packet sniffing.

	Act as a buffer between the local area network. Allows user to isolate the network that offers public services to Internet users.	
Intrusion Prevention System (IPS)	Analyse the flow of traffic and prevent the vulnerability exploits. Alarm the administrator about the vulnerabilities Killing the malicious packets. Blocking the traffic from source address. Resetting the connection.	Detection of false positives or false negatives. Not effective in detecting the new types of security threats.
Sandbox	Safe isolated environment that replicates the end user operating environment.	Sandbox deployment is limited to the own computer system.

Table 2.2.1: Summarize of the security system

2.3 Review of Virtual Machines

2.3.1 Hyper-V

Hyper-V is a computer firmware which can run virtual machines, it is only available in Microsoft Windows machines from Windows 8 onwards. The software allows multiple virtual machines to run on a computer and the computer is known as a host machine. Hypervisor is recognized as type 1 hypervisor (Bose, 2018). Type 1 hypervisor is called a bare metal because it runs on the computer hardware. The hypervisor takes control of the BIOS or UEFI during the computer start up. User will have more preference to set the virtual machine on or off automatically in the setting. Hyper-V can only support VHD and VHDX virtual disk files. Hyper-V can do hardware virtualization. It can create an abstraction layer between software and the real hardware to the emulating virtual machines. However, the setting must be enabled in the BIOS menu of the host machine.

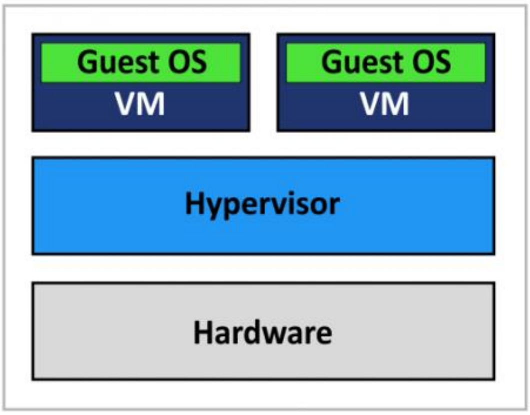


Figure 2.3.1.1 Type 1 Hypervisor Architecture (Bose, 2018)

2.3.2 VirtualBox

VirtualBox is an open source hypervisor developed by Oracle Corporation. VirtualBox can be installed in different types of operating system such as Linux, MacOS, Microsoft Windows and Solaris. For some operating system, user may improve the performance of the virtual machine by using “Guest Additions” package of device drivers. It is recognized as type 2 hypervisor which as known as hosted hypervisor. It is run on the operating system that already installed on a host. VirtualBox support many types of virtual disks like VDI, HDD, VMDK and VHD. VirtualBox can perform hardware and software virtualization.

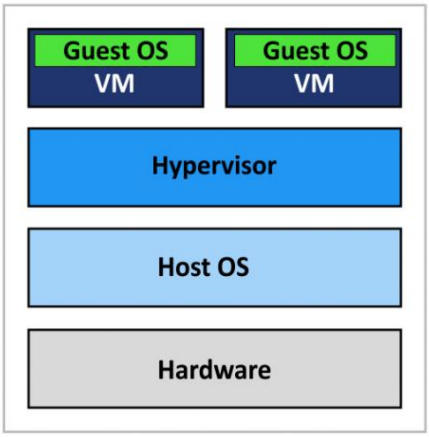


Figure 2.3.2.1 Type 2 Hypervisor Architecture (Bose, 2018)

2.4 Resolution of the Limitations Highlighted in Literature Review

There are limitations of security systems highlighted in the literature review. However, the proposed method to implement Honeypot in the network system is able to resolve the disadvantages of the security systems.

- **Reaction to Network Attacks**

As mentioned in the literature review, Firewall and Intrusion Prevention System (IPS) is not effective in reacting to network attacks. Meanwhile, Honeypot can capture the behaviour of attacker in the network. Network administrators can observe the malicious activities and analyse the way they use to attack the system. The attacker's hacking method will become more familiar because network administrator can learn the way on how attacker perform the attack. They can protect the system by using the knowledge gaining on how attacker perform new attacking method in the system (Hsamanoudy, 2018).

- **False positives or False Negative Alarm Rates**

Traditional network security system such as Firewall and Intrusion Detection System (IDS) will make wrong decision and blocks the legitimate connections (Babak Khosravifar, 2008). Honeypot will give alert to the network administrator when there is an attack or suspicious behaviour in the system. Honeypot is an emulated system which can let the attack to interact with the system, the attacker's action can be easily determined by observing what the attacker do in the system. Hence, it can reduce the false positives or false negative alarm rates effectively.

- **Capturing of the Data Packets**

Honeypot do not capture the whole packet traffic like Firewall does. When capturing all the traffic, the log files will become very bulky to be analyse. Likewise, the keystrokes captured by Honeypot will be analyse in Kippo-Graph and give the network administrator the summary of attack performed by the attacker. This can make the analysing process become easier. Besides, the Honeypot captures the traffic while attacker attempting to break the system. So that, there is no need a high storage to store all of the log files in the system.

- **Scalability**

The Sandbox deployment is limited to the own computer system. However, the Honeypot system proposed is able to scale easily by using virtual environment. In the virtual system, attacker will see the Honeypot same as the real machine in the virtual environment. The deployment is not limited to the real machine itself but can deploy on wherever that can attract the attacker to perform attack to the system.

CHAPTER 3: SYSTEM DESIGN

3.1.1 Methodology

The methodology proposed for development of Honeypot system is waterfall approach. With this approach, the requirements are documented in a clear and fixed direction. The progress will flow downwards steadily. The next phase will be started after the proposed goals are reached. Besides, the phases like requirement analysis, system design, implementation, testing, deployment and maintenance will not overlap.

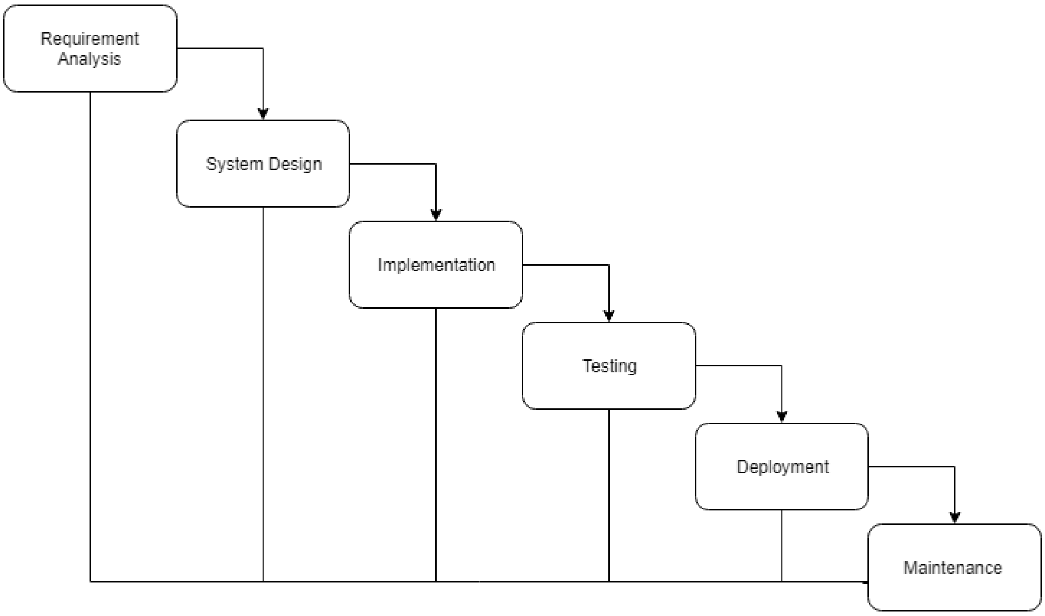


Figure 3.1.1.1 Waterfall Approach

Requirement Gathering and Analysis

In this phase, all of the possible requirements in Honeypot system are determined and recorded for analysis. The requirement such as the functionalities of current security systems, type of operating system to develop and the Honeypot system that are reliable to use is determined.

System Design

After the requirement specifications are studied, the system design is prepared to specify the hardware and system requirements. For example, the system design in implementing virtual machines in a host and how the system will work is designed.

Implementation

From the system design phase, the system is develop using lab computer with the VirtualBox environment for testing. The virtual operating system with Honeypot is set up by setting the SSH port in the system. The functionalities of the Honeypot system are tested.

Integration and Testing

The Honeypot system is integrated in the real server hosted by Windows Server 2016. The virtual machines are enabled by using Hyper-V which can host 4 virtual operating systems at the same time. Honeypot is enabled in the entire system and tested for any failures.

Deployment of system

The system is deployed once the testing of functional and non-functional is done. The users in the network can do port scanning by determining which port to enter the system. Once they are trapped in the Honeypot, the system will record every keystroke, Ip address and analysis of the behaviour of attacker.

Maintenance

When some issue come up, the system is kept maintain to deliver the working environment for the user. The system is always kept updated to get the latest virus signature and protect against attack.

3.1.2 Tools and Technology Involved

Hardware:

- **Server Machine**

  Server machine is used to host the virtual machines. There are 4 operating systems to be installed in the system. The system must be powerful enough to provide service for the virtual environment.

Operating System	Microsoft Windows Server 2016 Standard 1607
Processor	Inter® Xeon® CPU X3430 @2.4 GHz
RAM	4.0 GB
Storage	500 GB
System Type	64-bt operating system, x64-based processor
Network Connectivity	x2 Intel Gigabit 82578DM Network Adapter

Table 3.1.2.1 Specification of server machine

- **Lab Computer**

  The lab computer will be set up as either normal user or attacker to access the service provided by the server.

Operating System	Microsoft Windows 10 Pro
Processor	Intel® Core ™ i5-3340 @ 3.10 GHz
RAM	4.0 GB
Storage	500 GB
System Type	64-bt operating system, x64-based processor
Network Connectivity	Intel Network Adapter

Table 3.1.2.2 Specification of lab computer

- **Cisco Catalyst 2960 Switch**

  Switch is used to scale the network system. It allows connections to multiple devices including managing the ports and VLAN security settings.

Platform:

- **Microsoft Windows Server 2016 Standard**
  Microsoft Windows Server is chosen because it has Windows PowerShell for the script and commands, Hypervisor to host the Honeypot systems, Failover Clustering for future implementation and Windows Defender to protect the system.

- **HoneyDrive 3**
  HoneyDrive is installed as a virtual environment in Hypervisor. It is a premier honeypot Linux distro (Anon., n.d.). The system comes with Xubuntu Desktop 12.04.4 LTS edition installed and contains many Honeypot software packages.

- **Ubuntu Desktop 18.04.2 LTS**
  Ubuntu desktop is a GUI based Linux operating system which is set up as a real user computer in the virtual environment of the system. It will provide the SSH service to the legitimate user when they log in with the correct username and password.

Software:

- **Microsoft Hypervisor (Hyper-V)**
  Hyper-V can host multiple operating system as a virtual machine on the server. It is used to create a virtual and isolated environment of the Honeypot system.

- **Nmap**
  Nmap is used as a port scanner in the network. This is to determine which port is open for any kind of service in the network.

- **Putty**
  Putty is an SSH client which allows the user to SSH inside the virtual environment.

- **Kippo Honeypot**
  Kippo is a medium-interaction SSH honeypot written in Python. It can log the brute force attack and every command typed in the system.

- **Telegram**

  A mobile apps that receive notifications sent from Honeypot to alert the network administrator

- **Xampp**

  Used to host the php web server and the login database in the server

- **Google Chrome**

  Access the Internet or the localhost of the server webpage

- **Google Authenticator**

  Mobile apps to retrieve the one-time password (OTP) for the validation to login to the honeypot SSH

- **Windows Failover Clustering**

  To enable the clustering and assign clustering roles in the server. It can let the network administrator to check the configuration weather correct or not.

3.2 System Design

3.2.1 Design Specifications

The approach of this project is to build a virtual and isolated honeypot which protect the network from malicious attack. This includes alert network administrator and analyse the information of attacker from virtual Honeypot. A virtual Honeypot is set up in a virtual environment by using hypervisor, a bare metal virtual machine host. The honeypot is configured to open SSH port along with the real computer. When the attacker performs port scan, he can see every open port in the network. Honeypot will be one of the ports they discovered and can get into the system easily with the wrong password.

The attacker can successfully enter the Honeypot system using SSH port, he will see no different with any other real computer. He can perform ping, get files, remove entries, explore the system and many more. On the other hand, the attacker does not know currently he is being trapped in a system which record every keystroke, logging every activities and the attacker's computer IP address. Honeypot system will analyse attacker's behaviour by sorting the most attempted password, the most keyed in command and the top IP address by country. The network administrator can replay the behaviour like a video form in the browser.

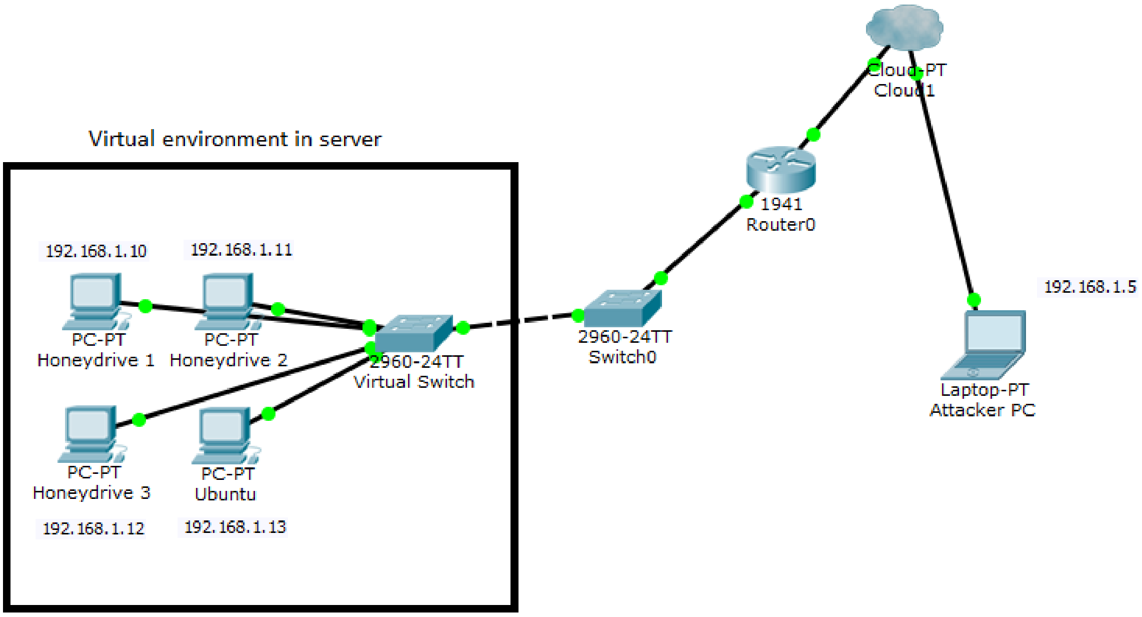


Figure 3.2.1.1 Design Specification

The virtual environment in the server is clustered with 3 servers which consists of 1 iSCSI storage server and 2 server nodes. The benefits of clustering are increase resource availability, effective resource usage, enhance performance, provide scalability and more simplified management. This system enables more resilient to server failures and provides high availability of the processing power. It has the flexibility for scaling the resources provisioning according to network demand.

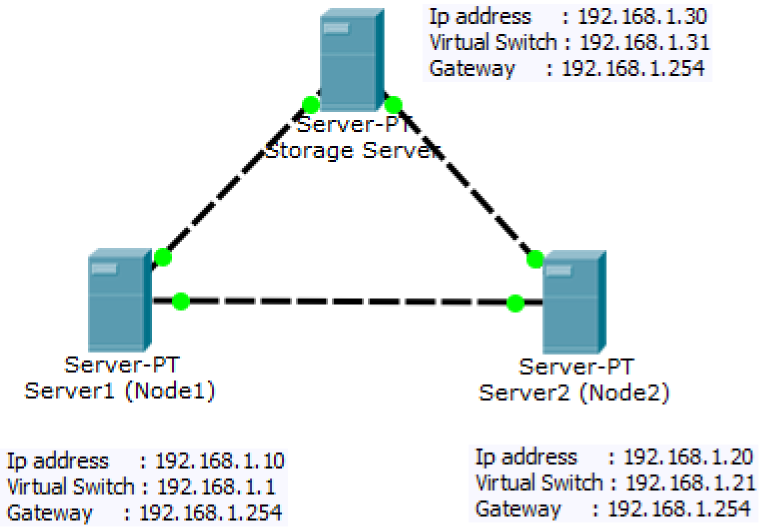

Ip address : 192.168.1.30
Virtual Switch : 192.168.1.31
Gateway : 192.168.1.254
Server-PT
Storage Server
Server-PT
Server1 (Node1)
Server-PT
Server2 (Node2)
Ip address : 192.168.1.10
Virtual Switch : 192.168.1.1
Gateway : 192.168.1.254
Ip address : 192.168.1.20
Virtual Switch : 192.168.1.21
Gateway : 192.168.1.254

Figure 3.2.1.2 Clustering Design for Virtual Environment

3.2.2 Use Case Diagram

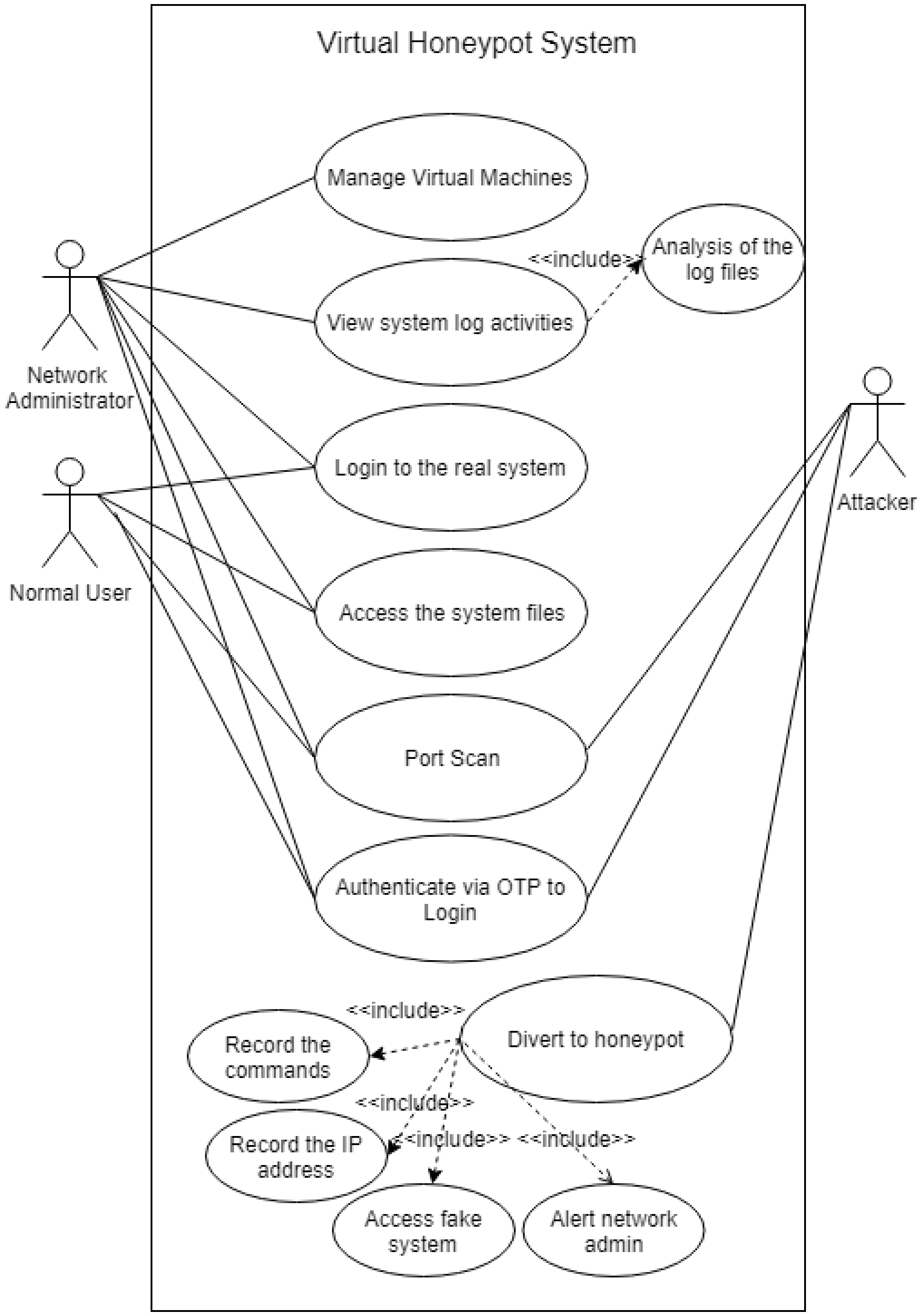


Figure 3.2.2.1 Use case diagram of Virtual Honeypot System

- **Manage Virtual Machines**

  Network administrator can manage the virtual machine in Windows Server 2016. The 3 HoneyDrive and 1 Ubuntu virtual machine is running on a server. He can determine to open which SSH port to lure the attacker. The port number also can be changed to make the fake system looks more real.

- **View System Log Activities**

  Network administrator can view the log files and every keystrokes of the attacker in the browser. The log files will analyse the command, password and keyword that are used by attacker to enter the system. The system will alert network administrator if someone is trapped in Honeypot system.

- **Login to the Real System**

  User are able to login to the real system to get the crucial data or information they are needed. The files may be confidential document that are stored in the real system.

- **Access the System Files**

  User are able to login to the real system files to add, edit or delete the files in the system if they are legitimate user.

- **Port Scan**

  User, Network administrator and attacker basically perform port scan to determine which is the open port in the system. When got the port number, they can easily SSH to the real system or honeypot by using login details.

- **Authenticate via OTP to Login**

  User, Network administrator and attacker who wants to login to the real system must gain the OTP to access the system. It is a way to enhance the security if the attacker has stolen the username and password to login to the system.

- **Divert to Honeypot**

  Attacker who tried to enter the real machine will be diverted to Honeypot. Honeypot password is easily break and he might think that it is a real system. In the Honeypot, the system automatically records the keystroke, command and IP address of the attacker.

3.2.3 Activity Diagrams

i. Access to Login System

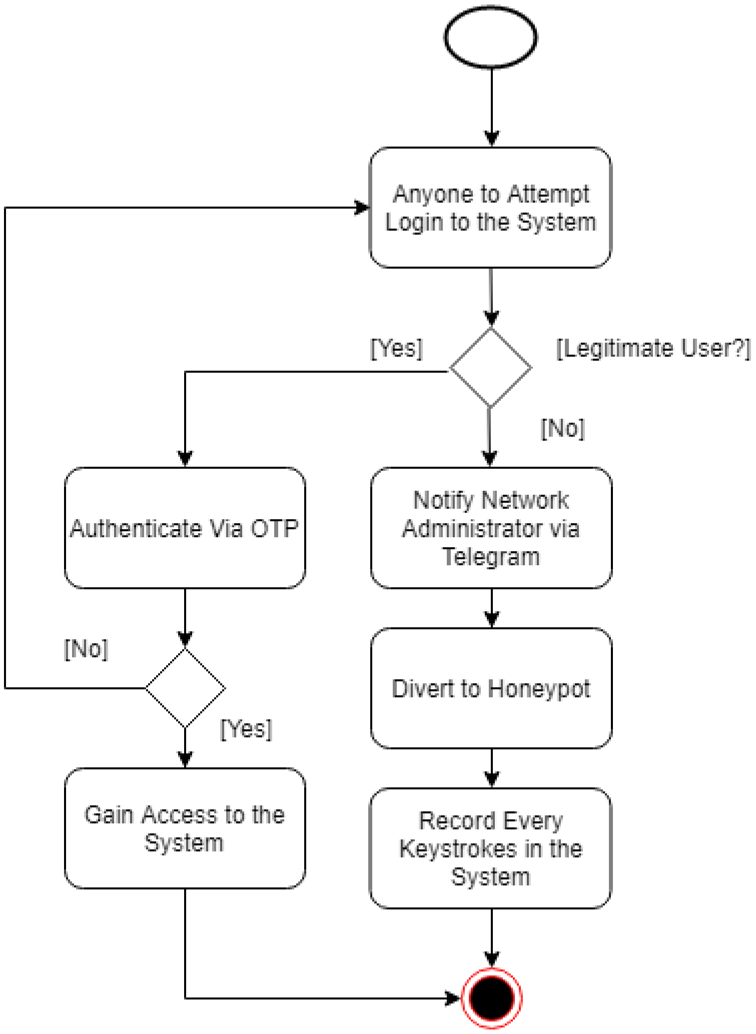

Anyone to Attempt Login to the System
[Yes]
[Legitimate User?]
[No]
Authenticate Via OTP
Notify Network Administrator via Telegram
[No]
Divert to Honeypot
[Yes]
Gain Access to the System
Record Every Keystrokes in the System

Figure 3.2.3.1 Activity Diagram of Login System

From the activity diagram, when the user or attacker attempting to login to the system. The system will determine who is the legitimate user to access the system. If the user has entered the correct username and password, he will enter the two-way authentication, which is OTP authentication. The user must get the OTP from the phone and type in the terminal correctly to gain access to the real system. Otherwise, the attacker who does not know the password and tried to enter the incorrect password will be diverted to the Honeypot system. The network administrator will get notified when someone login to the system. In the Honeypot, the keystrokes and commands will be recorded as a log files until the attacker log out from the system.

ii. In the Honeypot System

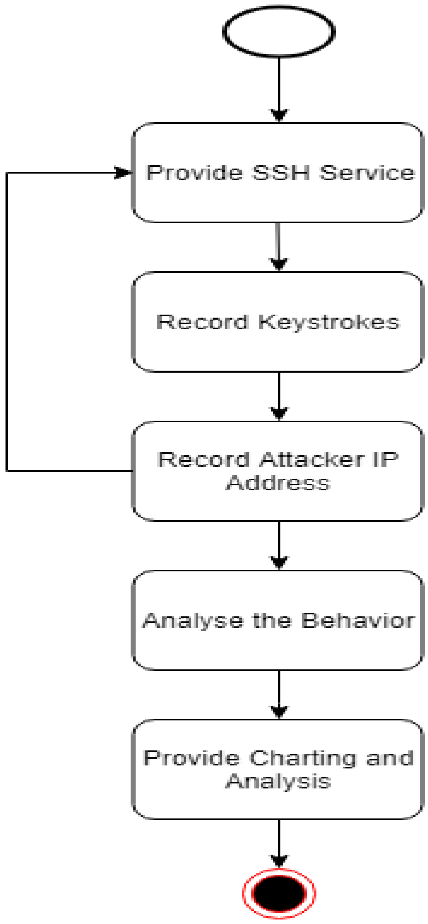


Figure 3.2.3.2 Activity Diagram of Honeypot System

In the Honeypot system, the system provides SSH service like normal computers do. The attacker will not aware of he is being trapping in a system which is record the keystrokes and IP address of the system. The Honeypot will analyse the behaviour and provide charting and analysis by using Kippo Graph.

iii. Network Administrator

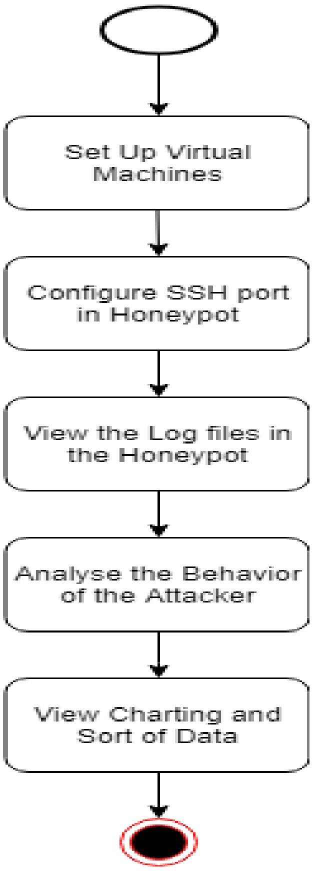

Set Up Virtual Machines
Configure SSH port in Honeypot
View the Log files in the Honeypot
Analyse the Behavior of the Attacker
View Charting and Sort of Data

Figure 3.2.3.3 Activity Diagram of Network Administrator

The network administrator is the person who set up the virtual machines. He can configure the SSH port and the port number in the system. When attacker is trapped in the Honeypot system, he can view the log files, analyse the behaviour and view charting of the data.

3.3 Issues and Challenges

There are some issues and challenges while implement the Honeypot system. The HoneyDrive system downloaded comes with .ova and .vmdk format which is not compatible with Windows Hypervisor Virtual machine. It requires some commands to convert the system files to a more compatible system file. Besides, this project involves the configuration from installing hard disk to the server machine to the setting of codes to the machine.

During the implementation of the system. One of the servers suddenly breaks down, the root cause of the server breaks down problem have to be determined. The checking is carried out to check weather it is battery problem, RAM problem or the hard disk problem. It requires some effort and knowledge to the server's hardware to make use of the repairing process. Later, I find out it is the power supply problem which let the server machine cannot power up. So, I have to configure and replace the server machine with a good condition machine. It is a good experience to expose me to repair the hardware side of the project. I believe it will beneficial to me in the future if the problem arises.

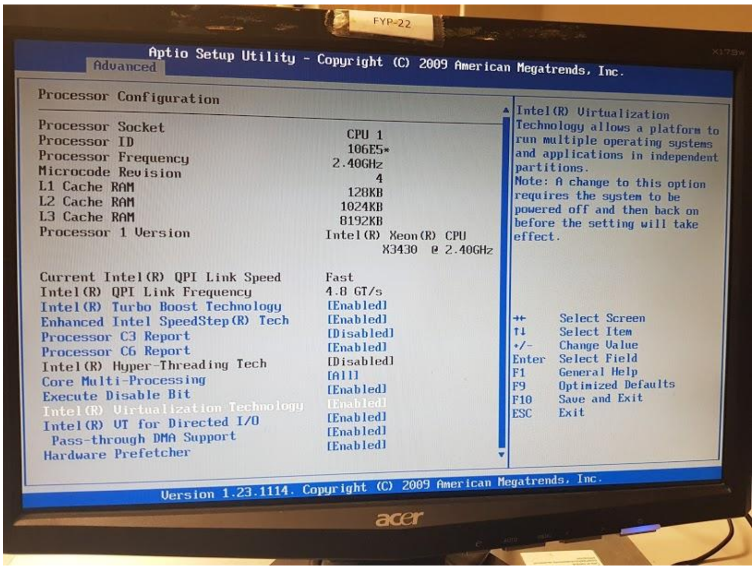
On the other hand, due to this project involves the communication between 3 servers. The connection between the server node is the most important matter. At first, once I connect the 2 server and cluster with each other, the virtual storage has been set up in each of the server. The clustering turns out that it is failed to cluster. Then, I tried to set up the virtual storage on the other server and the clustering also turns out unsuccessfully. By doing checking and solving the problem. I find out the Active Directory Domain (AD) have to implement to the system. Besides, one more server have to be added to be the virtual storage provider to the system.

CHAPTER 4: SYSTEM IMPLEMENTATION

4.1 Server Implementation

- Set Up Hyper-V in the server

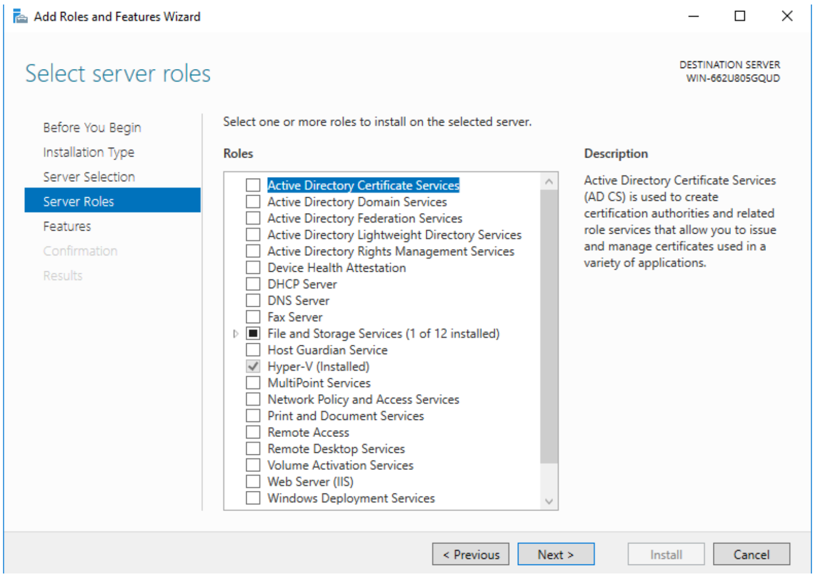
Hyper-V is set up by enabling Intel Virtualization Technology in the BIOS advance menu.



```
Aptio Setup Utility - Copyright (C) 2009 American Megatrends, Inc.
Advanced

Processor Configuration                                   Intel(R) Virtualization
                                                          Technology allows a platform to
Processor Socket                       CPU 1              run multiple operating systems
Processor ID                          106E5*              and applications in independent
Processor Frequency                  2.40GHz              partitions.
Microcode Revision                         4              Note: A change to this option
L1 Cache RAM                           128KB              requires the system to be
L2 Cache RAM                          1024KB              powered off and then back on
L3 Cache RAM                          8192KB              before the setting will take
Processor 1 Version          Intel(R) Xeon(R) CPU         effect.
                                 X3430  @ 2.40GHz

Current Intel(R) QPI Link Speed      Fast
Intel(R) QPI Link Frequency          4.8 GT/s
Intel(R) Turbo Boost Technology      [Enabled]            →←     Select Screen
Enhanced Intel SpeedStep(R) Tech     [Enabled]            ↑↓     Select Item
Processor C3 Report                  [Disabled]           +/-    Change Value
Processor C6 Report                  [Enabled]            Enter  Select Field
Intel(R) Hyper-Threading Tech        [Disabled]           F1     General Help
Core Multi-Processing                [All]                F9     Optimized Defaults
Execute Disable Bit                  [Enabled]            F10    Save and Exit
Intel(R) Virtualization Technology   [Enabled]            ESC    Exit
Intel(R) VT for Directed I/O         [Enabled]
  Pass-through DMA Support           [Enabled]
Hardware Prefetcher                  [Enabled]

Version 1.23.1114. Copyright (C) 2009 American Megatrends, Inc.
```

Figure 4.1.1 BIOS Menu of the Server

The Hyper-V is installed in the system by configuring the setting in server manager > Add Role and Features Wizard.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-662U805GQUD

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☑ Hyper-V (Installed)
- ☐ MultiPoint Services
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services

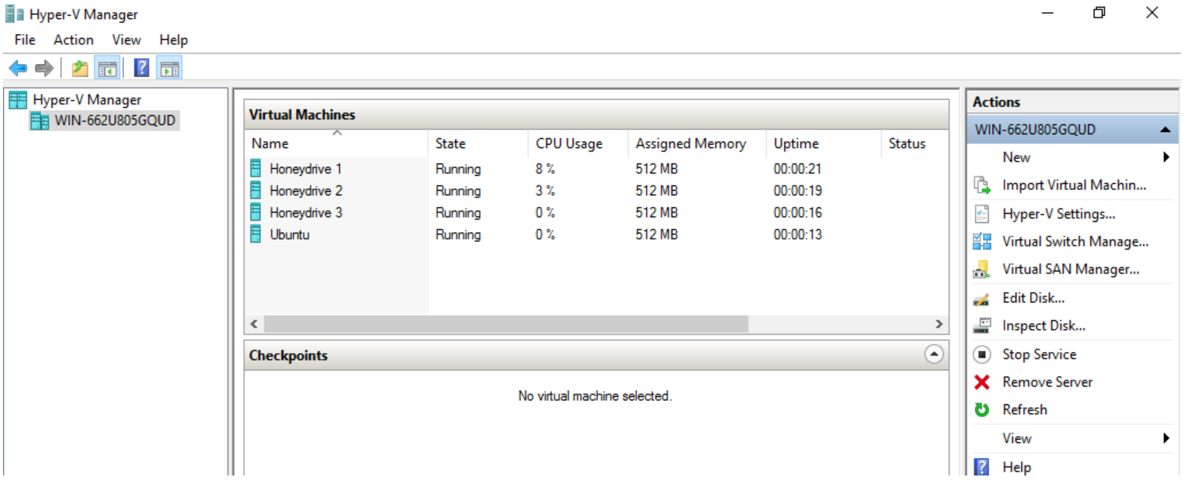
Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Figure 4.1.2 Hyper-V is installed in Server Role Wizard

- Set up Virtual Machines

Three HoneyDrive systems and one Ubuntu system is installed in the Hyper-V manager each system is allocated 512MB of RAM due to the server have only 4GB of total RAM. The system can run simultaneously at the same time to create a virtual environment.



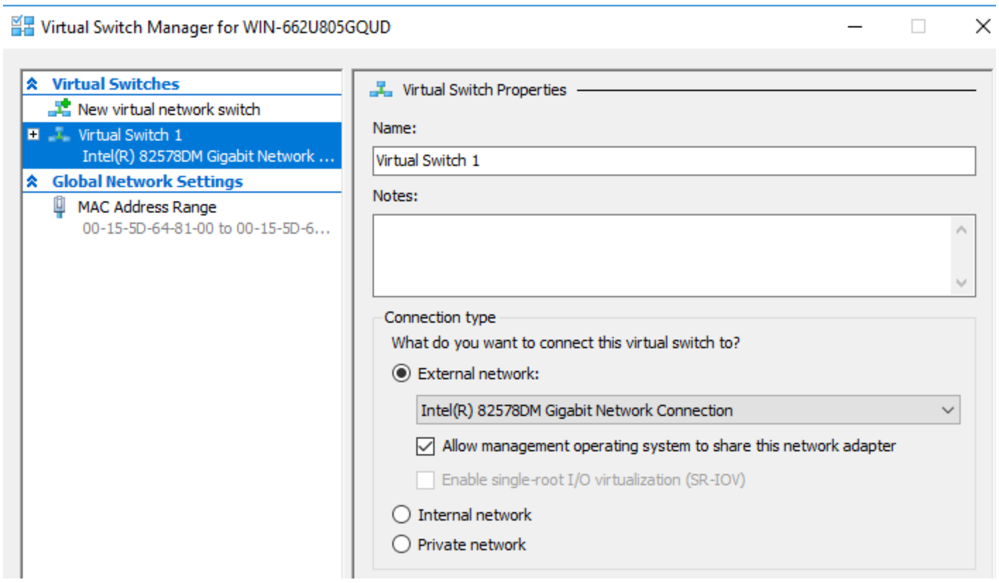
Name	State	CPU Usage	Assigned Memory	Uptime	Status
Honeydrive 1	Running	8 %	512 MB	00:00:21	
Honeydrive 2	Running	3 %	512 MB	00:00:19	
Honeydrive 3	Running	0 %	512 MB	00:00:16	
Ubuntu	Running	0 %	512 MB	00:00:13	

No virtual machine selected.

Figure 4.1.3 Screenshot of Hyper-V Manager

- Set up Virtual Switch

Virtual switch is created to provide connection for all 4 virtual computers in the virtual environment. The switch setting is connected to external network mean that it can connect to the Internet by using Intel 82578DM Gigabit Network Connection.


Virtual Switch Manager for WIN-662U805GQUD
Virtual Switches
New virtual network switch
Virtual Switch 1
Intel(R) 82578DM Gigabit Network ...
Global Network Settings
MAC Address Range
00-15-5D-64-81-00 to 00-15-5D-6...
Virtual Switch Properties

Name: Virtual Switch 1

Notes:

Connection type

What do you want to connect this virtual switch to?

● External network:

Intel(R) 82578DM Gigabit Network Connection

☑ Allow management operating system to share this network adapter

□ Enable single-root I/O virtualization (SR-IOV)

○ Internal network

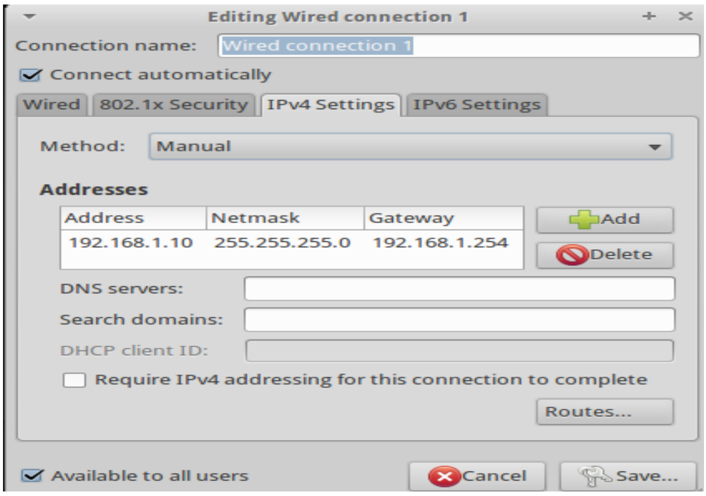
○ Private network

Figure 4.1.4 Virtual Switch Manager

- Configure IP address of the system

  The IP address for each system is configured as follow

HoneyDrive 1	:	192.168.1.10/24
HoneyDrive 2	:	192.168.1.11/24
HoneyDrive 3	:	192.168.1.12/24
Ubuntu	:	192.168.1.13/24
Windows Server	:	192.168.1.2/24



Editing Wired connection 1

Connection name: Wired connection 1

☑ Connect automatically

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.1.10	255.255.255.0	192.168.1.254

DNS servers:

Search domains:

DHCP client ID:

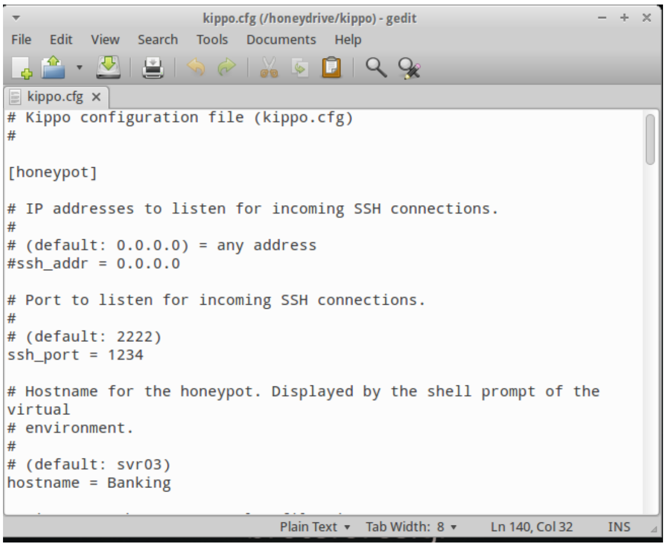
☐ Require IPv4 addressing for this connection to complete

☑ Available to all users

Figure 4.1.5 Set Up IP Address of HoneyDrive 1

- Configure Kippo Honeypot

Kippo Honeypot is configured with Kippo.cfg file in the system. The SSH port and hostname can be configured.



kippo.cfg (/honeydrive/kippo) - gedit

```
# Kippo configuration file (kippo.cfg)
#

[honeypot]

# IP addresses to listen for incoming SSH connections.
#
# (default: 0.0.0.0) = any address
#ssh_addr = 0.0.0.0

# Port to listen for incoming SSH connections.
#
# (default: 2222)
ssh_port = 1234

# Hostname for the honeypot. Displayed by the shell prompt of the
virtual
# environment.
#
# (default: svr03)
hostname = Banking
```

Figure 4.1.6 Configure Kippo Honeypot files

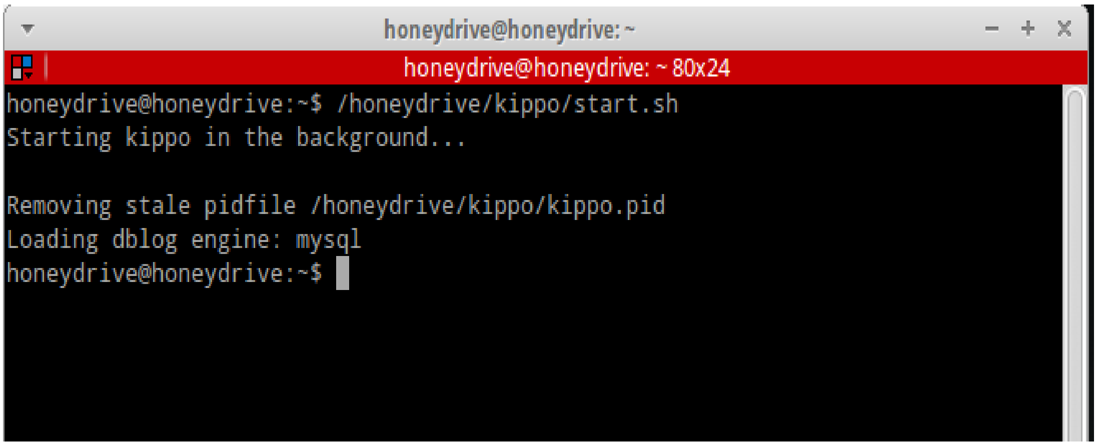
- Run Kippo Honeypot

  Open system terminal

  The Honeypot is started by using command

  /honeydrive/Kippo/start.sh

  The Honeypot will start in the background.



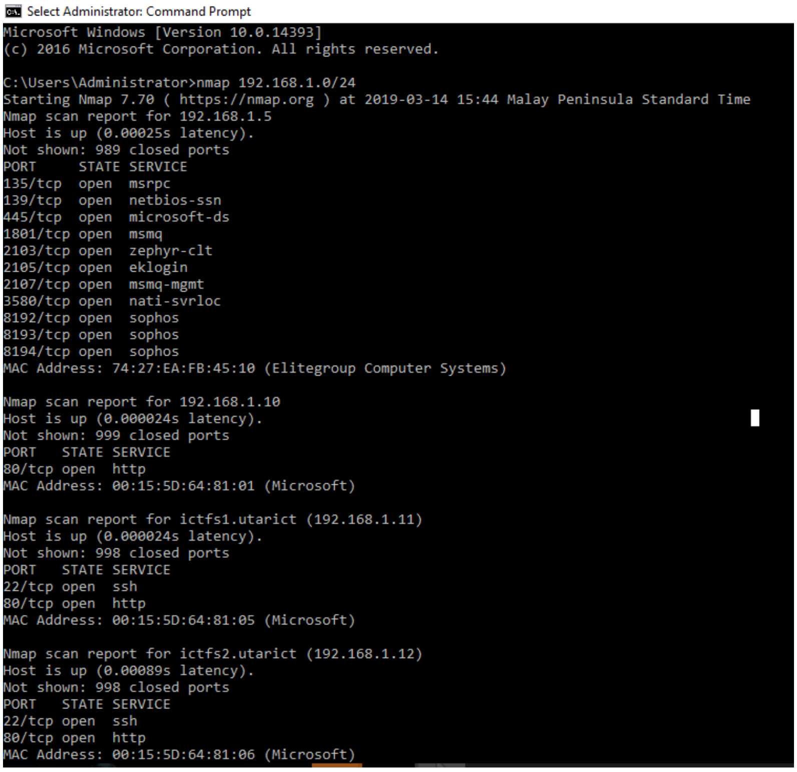
```
honeydrive@honeydrive:~$ /honeydrive/kippo/start.sh
Starting kippo in the background...

Removing stale pidfile /honeydrive/kippo/kippo.pid
Loading dblog engine: mysql
honeydrive@honeydrive:~$
```

Figure 4.1.7 The Command Input in Terminal

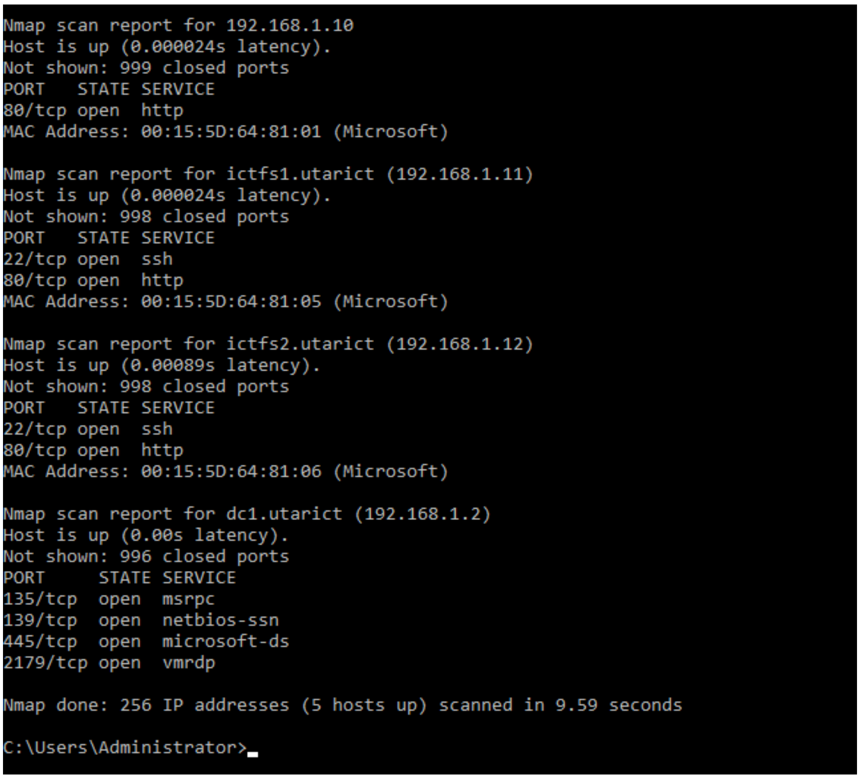
4.2 Kippo Implementation

- Perform post scan using Nmap

  The results show that port 22 is opened for 192.168.1.11 and 192.168.1.12



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nmap 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-14 15:44 Malay Peninsula Standard Time
Nmap scan report for 192.168.1.5
Host is up (0.00025s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
3580/tcp open  nati-svrloc
8192/tcp open  sophos
8193/tcp open  sophos
8194/tcp open  sophos
MAC Address: 74:27:EA:FB:45:10 (Elitegroup Computer Systems)

Nmap scan report for 192.168.1.10
Host is up (0.000024s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
80/tcp open  http
MAC Address: 00:15:5D:64:81:01 (Microsoft)

Nmap scan report for ictfs1.utarict (192.168.1.11)
Host is up (0.000024s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:64:81:05 (Microsoft)

Nmap scan report for ictfs2.utarict (192.168.1.12)
Host is up (0.00089s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:64:81:06 (Microsoft)
```

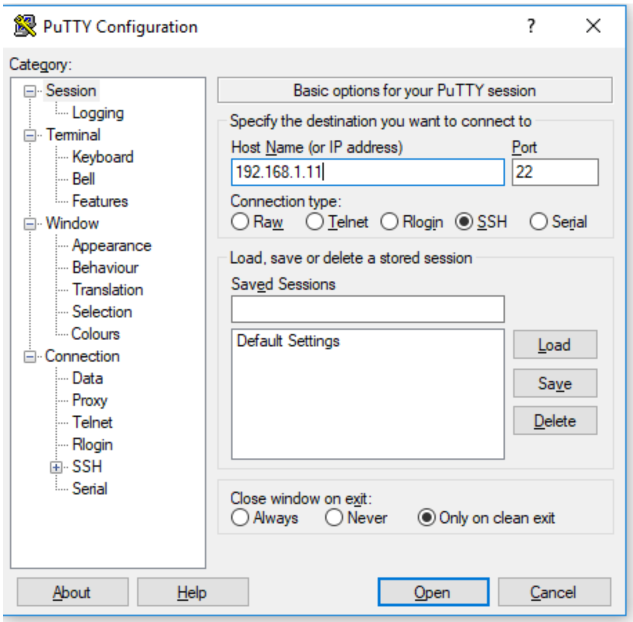


```
Nmap scan report for 192.168.1.10
Host is up (0.000024s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:15:5D:64:81:01 (Microsoft)

Nmap scan report for ictfs1.utarict (192.168.1.11)
Host is up (0.000024s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:64:81:05 (Microsoft)

Nmap scan report for ictfs2.utarict (192.168.1.12)
Host is up (0.00089s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:64:81:06 (Microsoft)

Nmap scan report for dc1.utarict (192.168.1.2)
Host is up (0.00s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp

Nmap done: 256 IP addresses (5 hosts up) scanned in 9.59 seconds

C:\Users\Administrator>_
```

Figure 4.2.1 Port Scan Result

- SSH into Honeypot by using Putty

  The IP address of 192.168.1.11 with port number 22 is keyed in Putty to SSH into the system.



Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.11

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions:

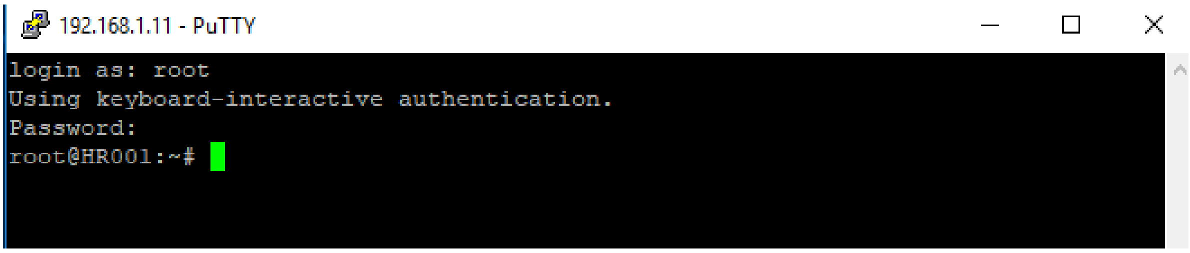
Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 4.2.2 Putty Configuration

- Log in Honeypot System with Simple Password

Honeypot can be login in with simple and default password like username as root and password as 123456.

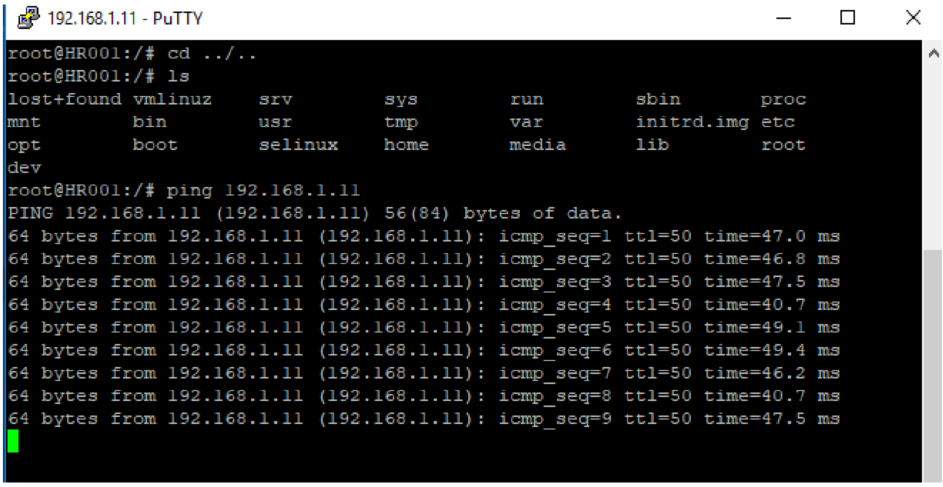


```
login as: root
Using keyboard-interactive authentication.
Password:
root@HR001:~# 
```

Figure 4.2.3 Login Interface in the System

- Get into the Honeypot and try to Ping another Computer

The attacker can access the files system like normal computer and perform ping to another computer in the network.

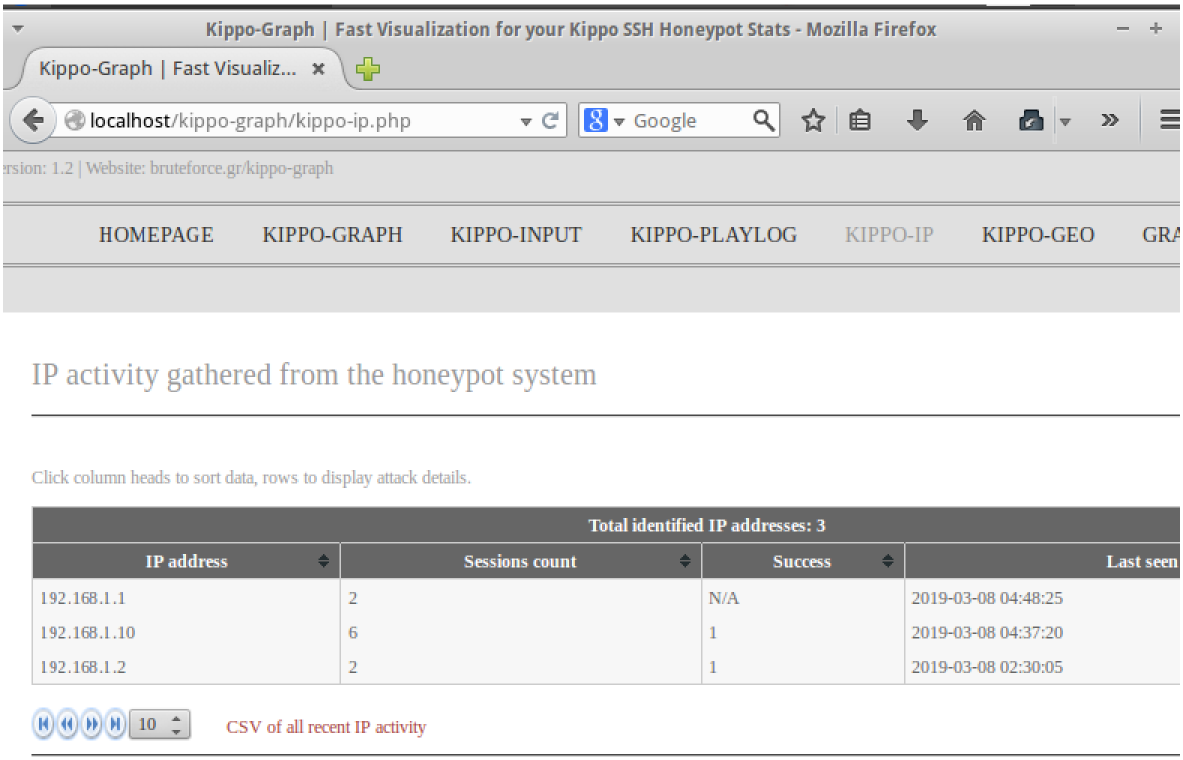


```
root@HR001:/# cd ../..
root@HR001:/# ls
lost+found vmlinuz    srv        sys        run        sbin       proc
mnt        bin        usr        tmp        var        initrd.img etc
opt        boot       selinux    home       media      lib        root
dev
root@HR001:/# ping 192.168.1.11
PING 192.168.1.11 (192.168.1.11) 56(84) bytes of data.
64 bytes from 192.168.1.11 (192.168.1.11): icmp_seq=1 ttl=50 time=47.0 ms
64 bytes from 192.168.1.11 (192.168.1.11): icmp_seq=2 ttl=50 time=46.8 ms
64 bytes from 192.168.1.11 (192.168.1.11): icmp_seq=3 ttl=50 time=47.5 ms
64 bytes from 192.168.1.11 (192.168.1.11): icmp_seq=4 ttl=50 time=40.7 ms
64 bytes from 192.168.1.11 (192.168.1.11): icmp_seq=5 ttl=50 time=49.1 ms
64 bytes from 192.168.1.11 (192.168.1.11): icmp_seq=6 ttl=50 time=49.4 ms
64 bytes from 192.168.1.11 (192.168.1.11): icmp_seq=7 ttl=50 time=46.2 ms
64 bytes from 192.168.1.11 (192.168.1.11): icmp_seq=8 ttl=50 time=40.7 ms
64 bytes from 192.168.1.11 (192.168.1.11): icmp_seq=9 ttl=50 time=47.5 ms
```

Figure 4.2.4 Get into the Root Files and Perform Ping

- View from Network Administrator

Network administrator can view the actions of the attacker in localhost by accessing the localhost/Kippo-graph website. Kippo-IP will show the IP addresses, session count, success rate and the time attacker enter the system.


Kippo-Graph | Fast Visualization for your Kippo SSH Honeypot Stats - Mozilla Firefox
Kippo-Graph | Fast Visualiz...
localhost/kippo-graph/kippo-ip.php
Google
ersion: 1.2 | Website: bruteforce.gr/kippo-graph
HOMEPAGE
KIPPO-GRAPH
KIPPO-INPUT
KIPPO-PLAYLOG
KIPPO-IP
KIPPO-GEO
GRA
10
CSV of all recent IP activity

IP activity gathered from the honeypot system

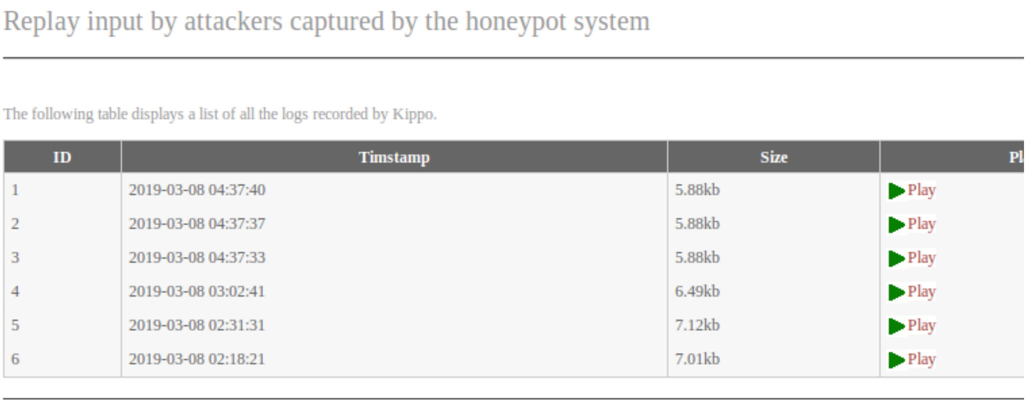
Click column heads to sort data, rows to display attack details.

Total identified IP addresses: 3			
IP address	Sessions count	Success	Last seen
192.168.1.1	2	N/A	2019-03-08 04:48:25
192.168.1.10	6	1	2019-03-08 04:37:20
192.168.1.2	2	1	2019-03-08 02:30:05

Figure 4.2.5 Kippo IP shows the Ip address of the Attackers

- Kippo Play Log Files

Every session of attacker enters the system is captured in a log file, the user is able to replay all the actions attacker performed in the system.



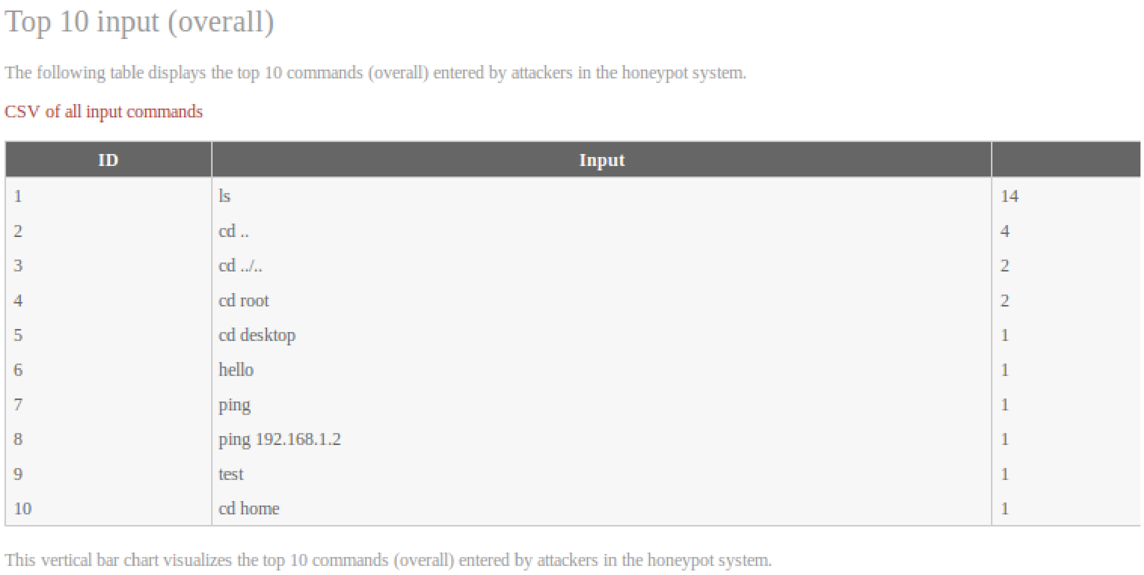
Replay input by attackers captured by the honeypot system

The following table displays a list of all the logs recorded by Kippo.

ID	Timstamp	Size	Pl
1	2019-03-08 04:37:40	5.88kb	▶Play
2	2019-03-08 04:37:37	5.88kb	▶Play
3	2019-03-08 04:37:33	5.88kb	▶Play
4	2019-03-08 03:02:41	6.49kb	▶Play
5	2019-03-08 02:31:31	7.12kb	▶Play
6	2019-03-08 02:18:21	7.01kb	▶Play

Figure 4.2.6 Kippo Play Log Files with Timestamps

- Top 10 Inputs



Top 10 input (overall)

The following table displays the top 10 commands (overall) entered by attackers in the honeypot system.

CSV of all input commands

ID	Input	
1	ls	14
2	cd ..	4
3	cd ../..	2
4	cd root	2
5	cd desktop	1
6	hello	1
7	ping	1
8	ping 192.168.1.2	1
9	test	1
10	cd home	1

This vertical bar chart visualizes the top 10 commands (overall) entered by attackers in the honeypot system.

Figure 4.2.6 Summary of Top 10 input in the Honeypot System

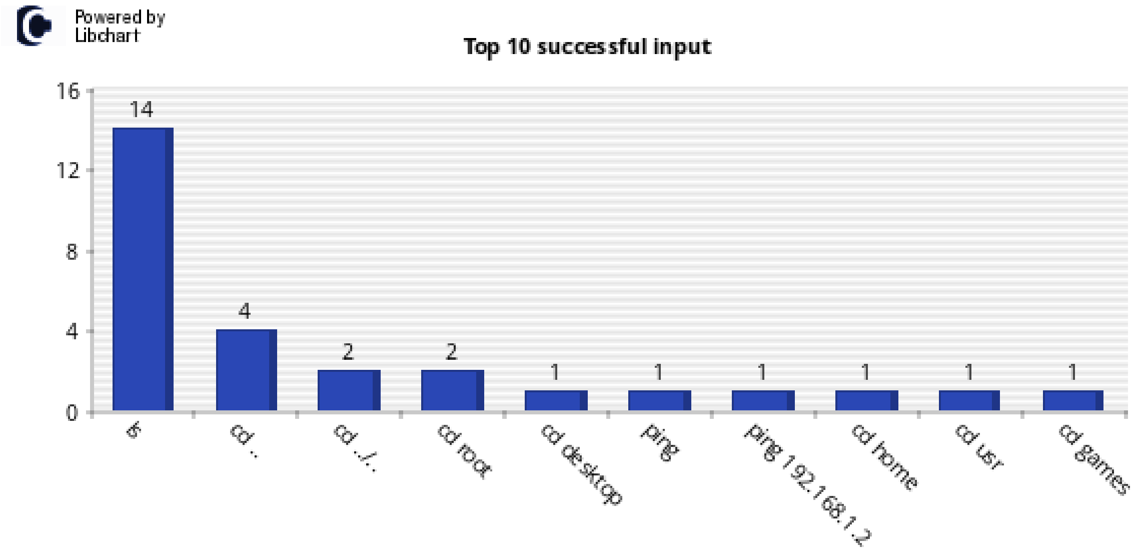
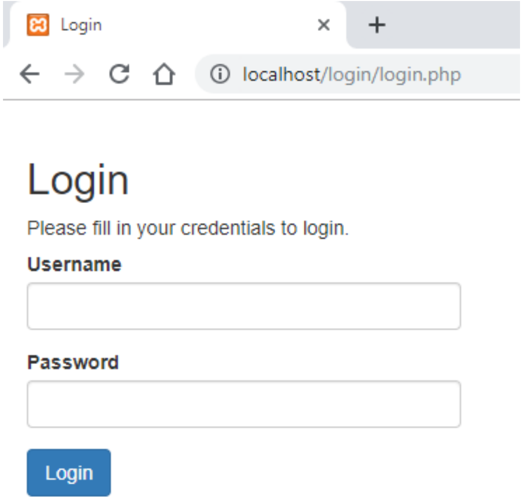


Figure 4.2.6 Summary of Top 10 input in Graph

4.3 Website

A login page is created to enable the user to login to the system more easily.



Login

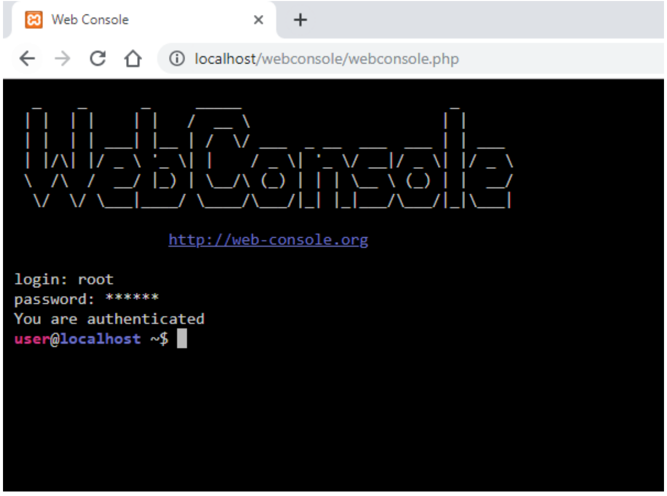
Please fill in your credentials to login.

Username

Password

Figure 4.3.1 Login Page

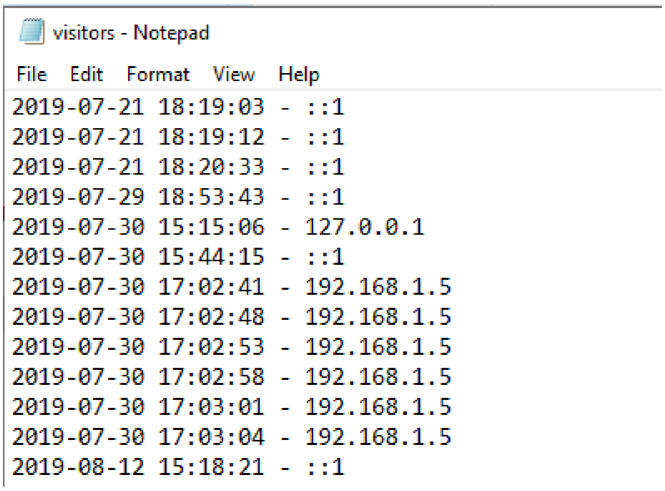
If the user login successfully into the login page, it will be directed to the real system SSH terminal by Web Console. If the user logged in with the correct user name but wrong password. It will be directed to the Honeypot web console.



```
http://web-console.org

login: root
password: ******
You are authenticated
user@localhost ~$
```

Figure 4.3.2 SSH terminal on the Web Browser

While the user login to the system via website, the system will log the date, time and ip address of the user who login to the system. If the system failure in the Kippo Honeypot, we can trace back the data in the visitor.txt file of the login page.

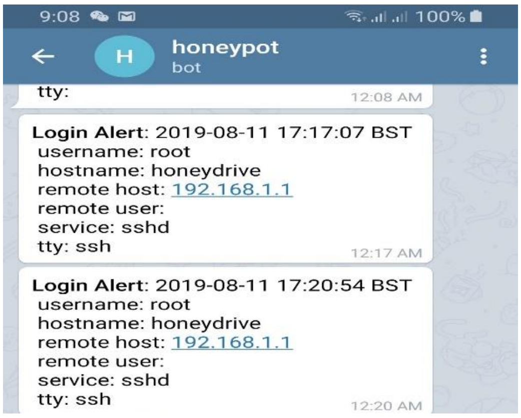


```
2019-07-21 18:19:03 - ::1
2019-07-21 18:19:12 - ::1
2019-07-21 18:20:33 - ::1
2019-07-29 18:53:43 - ::1
2019-07-30 15:15:06 - 127.0.0.1
2019-07-30 15:44:15 - ::1
2019-07-30 17:02:41 - 192.168.1.5
2019-07-30 17:02:48 - 192.168.1.5
2019-07-30 17:02:53 - 192.168.1.5
2019-07-30 17:02:58 - 192.168.1.5
2019-07-30 17:03:01 - 192.168.1.5
2019-07-30 17:03:04 - 192.168.1.5
2019-08-12 15:18:21 - ::1
```

Figure 4.3.3 The Date, Time and Ip Address Logged in the Login Page

4.4 Notification Via Telegram

If someone logged in to the Honeypot system, the network administrator will get notified in Telegram apps. The login alert consists of time, date, username, hostname, remote host address, remote user and the service attempt use.



tty: 12:08 AM

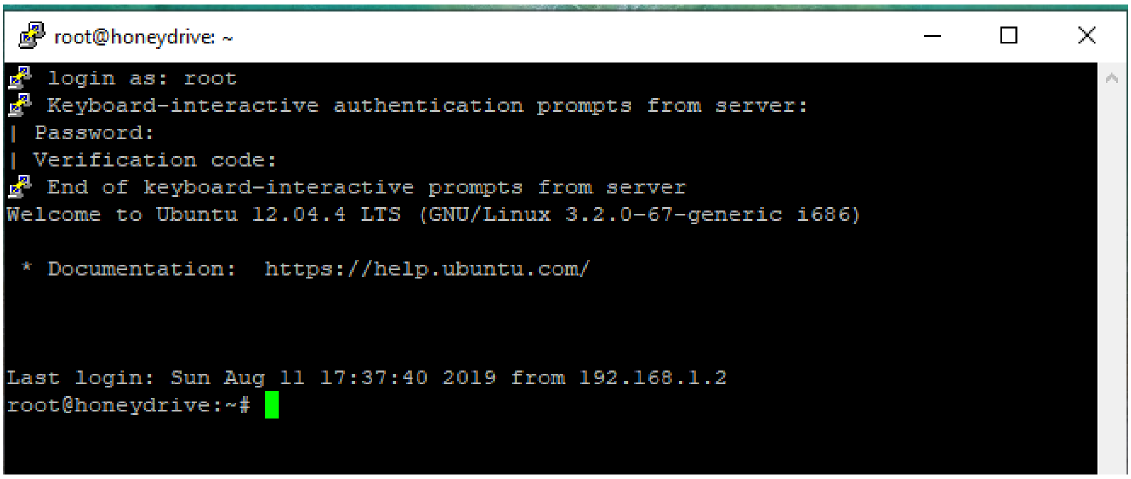
Login Alert: 2019-08-11 17:17:07 BST
username: root
hostname: honeydrive
remote host: 192.168.1.1
remote user:
service: sshd
tty: ssh 12:17 AM

Login Alert: 2019-08-11 17:20:54 BST
username: root
hostname: honeydrive
remote host: 192.168.1.1
remote user:
service: sshd
tty: ssh 12:20 AM

Figure 4.4.1 Telegram Notification from Telegram

4.5 OTP Authentication on SSH

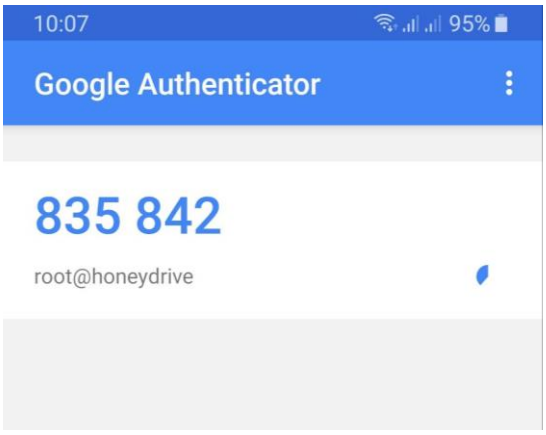
If the user wants to login to the real system, he must enter the correct username and password. For a better security, the system will prompt the user to get OTP from Google Authenticator. If the verification code is correct in the system. The user will gain access to the system successfully.



```
login as: root
Keyboard-interactive authentication prompts from server:
| Password:
| Verification code:
End of keyboard-interactive prompts from server
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.2.0-67-generic i686)

 * Documentation:  https://help.ubuntu.com/


Last login: Sun Aug 11 17:37:40 2019 from 192.168.1.2
root@honeydrive:~#
```

Figure 4.5.1 Added Verification Code to Login

Only the authorized user who get the permission to access the server will get the OTP verification code via Google Authenticator. The OTP will update every 30 seconds to ensure more secure system implemented.

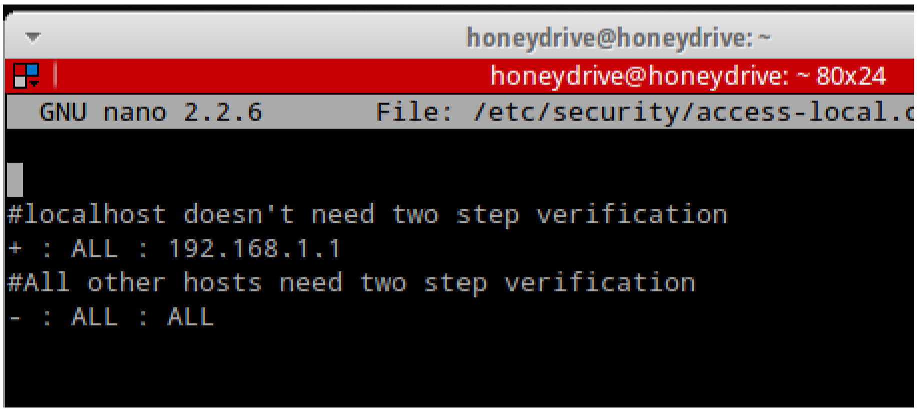


835 842

root@honeydrive

Figure 4.5.2 Google Authenticator

The login process might be troublesome if the authenticated user must key in the correct username, password and verification code many times to log in the system. The whitelist function is added for the convenience of the user. The function can whitelist the authorized user or network administrator to skip the two-step verification every time they try to log in to the system. So that they can have a faster log in process.



```
  GNU nano 2.2.6        File: /etc/security/access-local.c

#localhost doesn't need two step verification
+ : ALL : 192.168.1.1
#All other hosts need two step verification
- : ALL : ALL
```

Figure 4.5.3 Whitelist IP Address

4.6 Failover Clustering

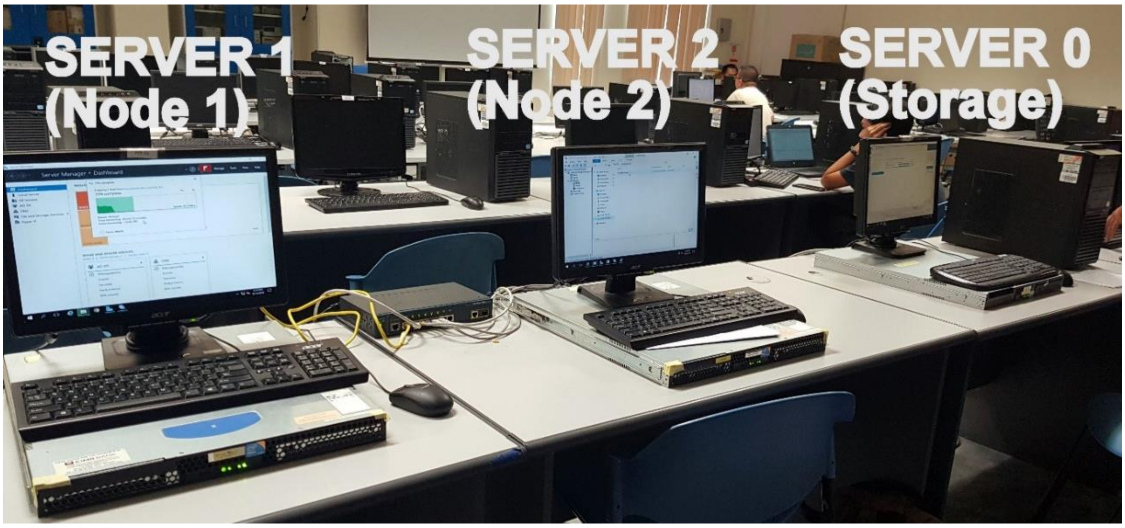
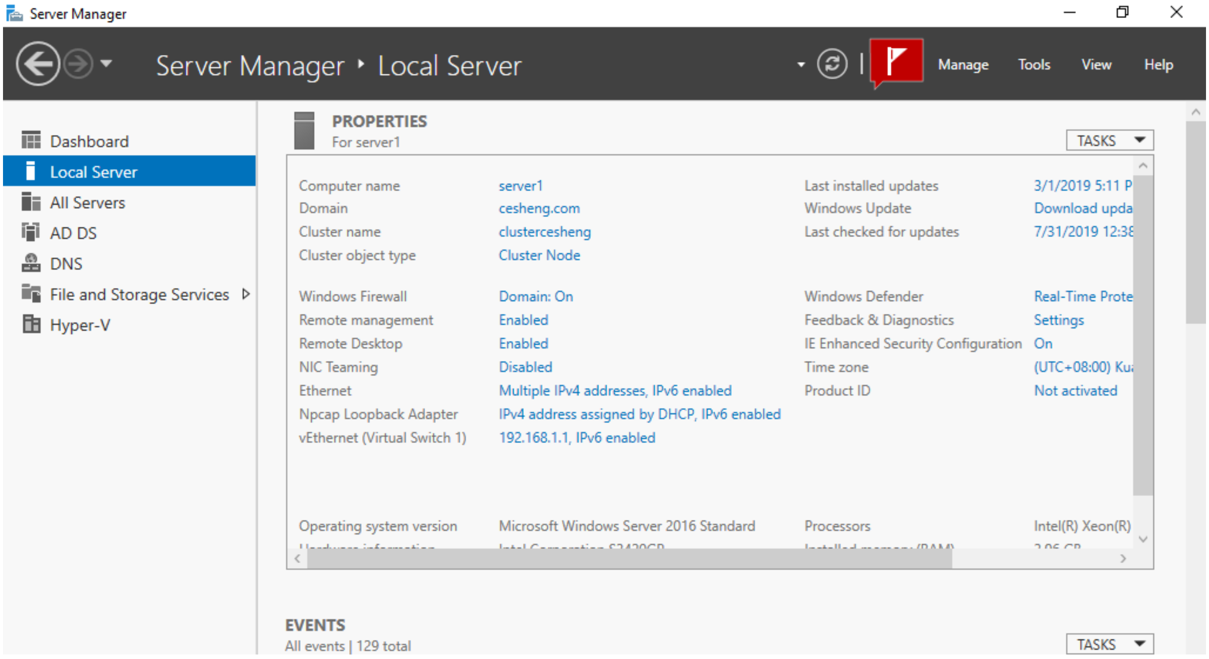


Figure 4.6.1 Failover Clustering System Design

3 Servers are used to set up the failover clustering of Hyper-V. Server 1 and Server 2 act as Node 1 and Node 2 in the system. Sever 0 acts as the storage server which let both node 1 and node 2 share the virtual storage in the network. 3 servers are connected to a Cisco Catalyst 2960 Switch to connect with each other.



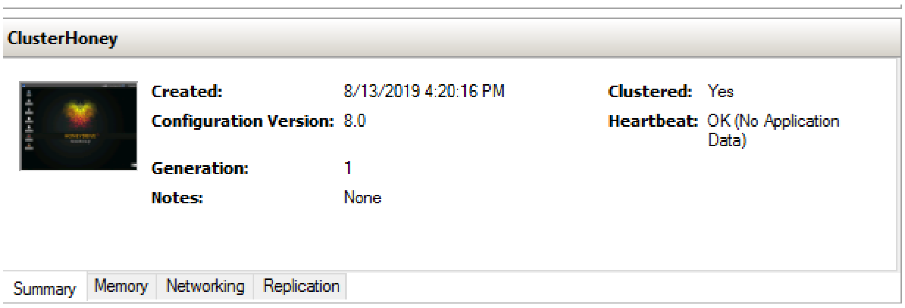
PROPERTIES
For server1

Computer name	server1	Last installed updates	3/1/2019 5:11 P
Domain	cesheng.com	Windows Update	Download upda
Cluster name	clustercesheng	Last checked for updates	7/31/2019 12:38
Cluster object type	Cluster Node		
Windows Firewall	Domain: On	Windows Defender	Real-Time Prote
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC+08:00) Kua
Ethernet	Multiple IPv4 addresses, IPv6 enabled	Product ID	Not activated
Npcap Loopback Adapter	IPv4 address assigned by DHCP, IPv6 enabled		
vEthernet (Virtual Switch 1)	192.168.1.1, IPv6 enabled		
Operating system version	Microsoft Windows Server 2016 Standard	Processors	Intel(R) Xeon(R)
Hardware information	Intel Corporation S2420GP	Installed memory (RAM)	2.06 GB

EVENTS
All events | 129 total

Figure 4.6.2 Server 1 Configuration

To set up the failover clustering, the Active Directory (AD) have to implemented to the system, so the network administartor can manage the permission to provide the access to the network resources. The Active Domain of cesheng.com is set up. All three servers are connected to the same active domain. The cluster with the name clustercesheng is connected with node 1 and node 2. Before the cluster is created, the cluster have to be validated with both of the node to ensure the disks, network and shared storage pool are running without issue.



ClusterHoney

Created:	8/13/2019 4:20:16 PM	Clustered:	Yes
Configuration Version:	8.0	Heartbeat:	OK (No Application Data)
Generation:	1		
Notes:	None		

Figure 4.6.3 Hyper-V Configuration

Hyper-V is configured to support the Hyper-V failover clustering. The disk image of Honey drive is moved to the iSCSI virtual storage, so that the server pool can share the resources between each other. If one of the systems fails, the other server can bring the server online with the failover clustering. It can set the priority of which server job is more important to utilize the hardware resources of the server.

CHAPTER 5: SYSTEM TESTING

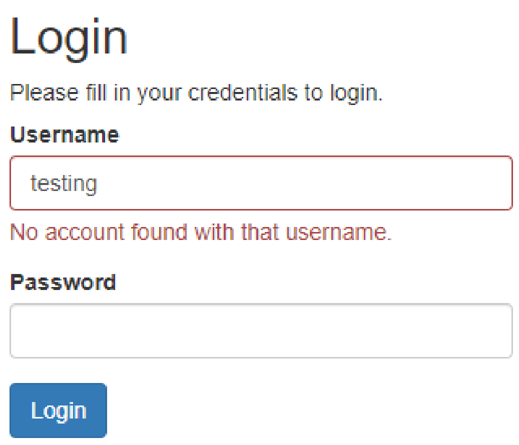
System testing is a process to evaluate the system tested for its compliance to functional and non-functional requirements. The expected functionalities of the system will be documented, and the performance of the system will be evaluated using appropriate standard.

5.1 Website Testing

The main function of website is to allow the user and network administrator can easily login to the real or honeypot system. If the user is authenticated, he will enter the real SSH system. Meanwhile, if the user is not authenticated, the user will be diverted to honeypot system. The testing comes with some different scenario.

No	Scenario	Result Shown	Expectation
1	Real user login to the system with correct user name and password	Real user can access the real SSH server	Matched
2	User login to the system with the wrong user name and password	Cannot access the real or honeypot server	Matched
3	User login to the system with correct user name and incorrect password	User is diverted to honeypot	Matched
4	Network administrator login to the system	He can view Kippo graph and the recorded data from the unknown users	Matched

Table 5.1.1 Website Testing



Login

Please fill in your credentials to login.

Username

testing

No account found with that username.

Password

Figure 5.1.1 Scenario 2, User Unable to Login with Wrong Username and Password

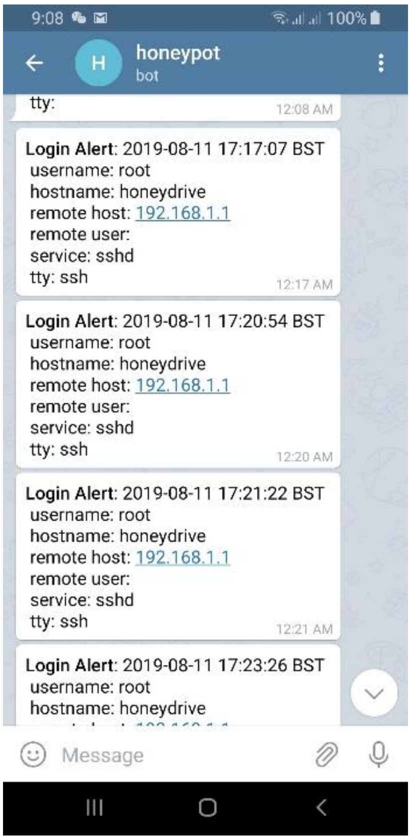
5.2 Notification Testing

Honeypot system will alert the network administrator if there is unauthorized access to the server. The notification will send to the network administrator in real time by using Telegram mobile application. This testing will determine the reliability of notification to the network administrator. The testing will perform repeatedly to test whether the system will miss any notification to the network administrator.

No	Scenario	Notifications		Expectation
		Sent from Honey drive	Receive from Telegram	
1	User Logged in to Honey Drive	Yes	Yes	Matched
2		Yes	Yes	Matched
3		Yes	Yes	Matched
4		Yes	Yes	Matched
5		Yes	Yes	Matched

Table 5.2.1 Notification Testing

The test shows that the network administrator would not miss any notification provided the network connection is stable and the configuration setting is correct all the time.



```
tty:                                  12:08 AM

Login Alert: 2019-08-11 17:17:07 BST
 username: root
 hostname: honeydrive
 remote host: 192.168.1.1
 remote user:
 service: sshd
 tty: ssh                             12:17 AM

Login Alert: 2019-08-11 17:20:54 BST
 username: root
 hostname: honeydrive
 remote host: 192.168.1.1
 remote user:
 service: sshd
 tty: ssh                             12:20 AM

Login Alert: 2019-08-11 17:21:22 BST
 username: root
 hostname: honeydrive
 remote host: 192.168.1.1
 remote user:
 service: sshd
 tty: ssh                             12:21 AM

Login Alert: 2019-08-11 17:23:26 BST
 username: root
 hostname: honeydrive
```

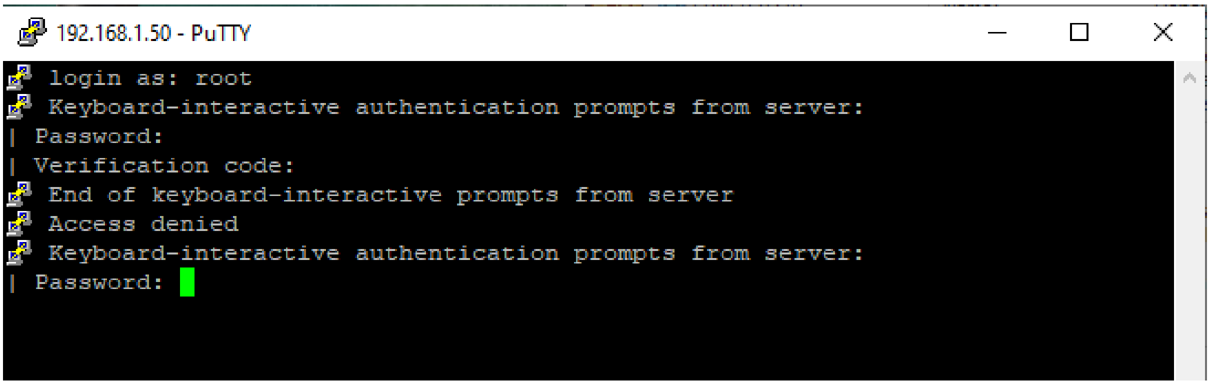
Figure 5.2.1 Notification Received in Telegram Application

5.3 SSH Authentication Testing

When the user wants to log in to the SSH server. He will need to perform SSH Authentication using Google Authentication before he is able to log in to the system.

No	Scenario	OTP Code	Able to Log In?	Expectation
1	Authenticate user logs in to the system	330 760	Yes	Matched
2	Non-Authenticated user who knows username and password	N/A	No	Matched
3	Non-Authenticated user who get Google Authentication access but no username and password	977 492	No	Matched

Table 5.3.1 SSH Authentication Testing



```
login as: root
Keyboard-interactive authentication prompts from server:
| Password:
| Verification code:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
| Password:
```

Figure 5.3.1 Scenario 2 Access denied with Wrong Verification Code

5.4 Clustering Testing

Clustering enables the high availability of the servers and scalable of the network. If either one of the servers fails, another server will carry on the job of the previous server.

No	Scenario	Results	Expectation
1	Server 1 shuts down	Server 2 carry on the operating system on Server 1	Matched
2	Server 2 shuts down	Server 1 carry on the operating system on server 2	Matched

Table 5.4.1 Clustering Testing

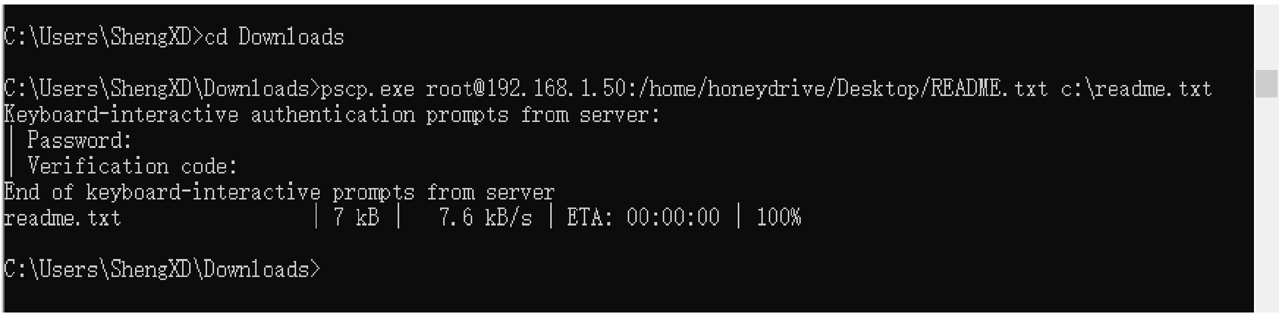
5.5 Honeypot Testing

The main function of Honeypot is to record every keystroke inputted by the user in the system.

No	Scenario	Results	Expectation
1	The user tried to key in a different password on the log in page	The password is recorded in the Kippo Graph	Matched
2	The user enters the default username and password to log in to the system	The user logged in to the honeypot, the password entered was recorded and the keystrokes was recorded	Matched
3	The user perform ping to another PC in the network	Honeypot recorded the actions and the action would not affect another PC	Matched
4	The user runs command to change the setting of the network	The settings changed only applicable on Honeypot only. It will not affect the real running machines	Matched

5	The user retrieves files in the Honeypot	The files stored in Honeypot is the unrelated fake files and the user can download to his PC	Matched

Table 5.5.1 Honeypot Testing



```
C:\Users\ShengXD>cd Downloads

C:\Users\ShengXD\Downloads>pscp.exe root@192.168.1.50:/home/honeydrive/Desktop/README.txt c:\readme.txt
Keyboard-interactive authentication prompts from server:
| Password:
| Verification code:
End of keyboard-interactive prompts from server
readme.txt                | 7 kB |   7.6 kB/s | ETA: 00:00:00 | 100%

C:\Users\ShengXD\Downloads>
```

Figure 5.5.1 README.txt is Able to Retrieve from SSH

CHAPTER 6: CONCLUSION

In the nutshell, the virtual Honeypot system is set up in the server machine. 3 Honeypot and 1 Ubuntu virtual machines are installed in the Hyper-V hypervisor, they can run at the same time to realise the virtual and isolated environment to mitigate the attacker in the Honeypot. The Honeypot software, Kippo provide SSH service to the virtual machine without the realise of attacker they are actually in a fake system. Every keystroke, IP address and commands are recorded in a play log file in the honeypot. In the Kippo Graph, network administrator can use the log files to analyse the behaviour of the attacker. The Honeypot also provide charting and sorting service which can sort out the highest number of passwords attempted to enter the system.

This project involved setting up 3 server machines in the hardware site. One server is the iSCSI virtual storage server meanwhile the rest are the clustering server. From implementing the hardware site, I learn on how to open a server to perform installation and checking for the server hardware. While I am implementing the honeypot in the servers, one of the servers suddenly break down. I have to do checking by my own and determine what is the problem inside the machine. Then I have to repair and replace the server with a new working condition one. In the implementation of Failover Clustering, it is important to fulfil the prerequisite condition such us connect the servers to the same Active Directory, Active Domain and the Clustering server. I learnt the iSCSI storage will not works if the it is implemented in either one of the clustering servers.

The virtual honeypot system is implemented in virtual environment which lets the attacker see no difference with the real system. The system is clustered with each other to make it high available. If one of the servers fail, another server still can perform the server function. The hardware resources can be shared with each other, to maximize the system performance. The things that makes this project is the system is able to divert the attacker to the honeypot if the user is suspicious. It is integrated with the real network system and able to determine the legitimate or non-legitimate user. The condition like if the user input the correct username but wrong password, the system will automatically divert the user to the honeypot. If the user has the correct username and password, he can access the real server.

The notification will send to network administrator if unauthorized login is detected. The mobile application to receive the notification is using Telegram. This is because mobile devices are portable, the user can get alerted wherever he is. So that the effective countermeasures and actions will be carried out to prevent the system from attacks. For more added value, the Two-Factor Authentication login function is added to make sure the real user is entering the system. The system will prompt the unauthorized user to enter the correct username, password and verification code to enter the real system. If the user fails to do so, he will no able to login to the system.

Honeypot system can make the attacker more frustrated to attack the organization. This is because, the Honeypot system mask the real system. Once they are implementing in a virtual environment, the organization can save a lot of cost to install each Honeypot system in every hardware machine. User can also perform port scan and every system is shown like the real-world system. The attacker may find out there are too many machines to explore and some of it there are easily exploit is Honeypot. All in all, it is beneficial to deploy Honeypot in organization network with the other network security tools to make the system more secure.

BIBLIOGRAPHY

Akshay, H., Sanket, T., Ganesh K.,, n.d. Detection and Analysis of Network & Application Layer Attacks.

Anon., 2016. *Introduction to Honeypots.* [Online]
Available at: https://blog.rapid7.com/2016/12/06/introduction-to-honeypots/

Anon., n.d. [Online]
Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

Anon., n.d. *CONPOT ICS/SCADA Honeypot.* [Online]
Available at: http://conpot.org/

Anon., n.d. *HoneyDrive.* [Online]
Available at: https://bruteforcelab.com/honeydrive

Anon., n.d. *Intrusion Detection System (IDS).* [Online]
Available at: https://www.techopedia.com/definition/3988/intrusion-detection-system-ids

Anon., n.d. *What Is a Firewall?.* [Online]
Available at: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Babak Khosravifar, J. B., 2008. An Experience Improving Intrusion Detection Systems False Alarm Ratio by Using Honeypot.

Bose, M., 2018. *Hyper-V or VirtualBox – Which One to Choose for Your Infrastructure?.* [Online]
Available at: https://www.nakivo.com/blog/hyper-v-virtualbox-one-choose-infrastructure/

Brough, D., 2003. Second Generation Honeynet Honeywall.

Christian, S., Ian, W., Peter, K., 2006. *Taxonomy of honeypots.* s.l.:s.n.

Dargin, M., 2017. *Increase your network security: Deploy a honeypot.* [Online]
Available at: https://www.networkworld.com/article/3234692/increase-your-network-security-deploy-a-honeypot.html

Hsamanoudy, 2018. *Advantages vs Disadvantages of Honeypots.* [Online]
Available at: https://es.infosecaddicts.com/advantages-vs-disadvantages-of-honeypots/

Margaret, R., n.d. [Online]
Available at: https://searchsecurity.techtarget.com/definition/DMZ

Nick, I., Cesar, U., Richard, B., 2005. Intrusion prevention systems.

provos, N., Holz, T., 2007. Virtual Honeypots: From Botnet Tracking to Intrusion.

Provos, N., 2004. *A Virtual Honeypot Framework.* s.l.:s.n.

Provos, N., n.d. Honeyd: A Virtual Honeypot Daemon.

Tejvir, K., Vimmi, M., Dheerendra, S., n.d. Comparison of network security tools- Firewall, Intrusion Detection System and Honeypot.

Walsh, A., 2017. *Alphabay and Hansa darknet markets shut down after international police operation.* [Online]
Available at: https://www.dw.com/en/alphabay-and-hansa-darknet-markets-shut-down-after-international-police-operation/a-39776885

X. Jhang, C. Li, W. Zheng,, 2004. *Intrusion Prevention System Design.* s.l.:s.n.

Xinwen, F. Wei, Y., n.d. On Recognizing Virtual Honeypots and Countermeasures.

APPENDICES A: WEEKLY REPORT

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.: 2**
Student Name & ID: Foo Ce Sheng 15ACB05137	
Supervisor: Ts Dr Gan Ming Lee	
Project Title: Network Isolation and Security Using Honeypot	

1. WORK DONE FYP 1 documentation and presentation
2. WORK TO BE DONE Implement Clustering Implement website
3. PROBLEMS ENCOUNTERED **-**
4. SELF EVALUATION OF THE PROGRESS To discuss about the things to do in FYP 2

_________________________ _________________________

Supervisor’s signature Student’s signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.: 5**
Student Name & ID: Foo Ce Sheng 15ACB05137	
Supervisor: Ts Dr Gan Ming Lee	
Project Title: Network Isolation and Security Using Honeypot	

1. WORK DONE

The requirements are determined

The clustering implementation started

2. WORK TO BE DONE

Implement the website with notification function in SSH

3. PROBLEMS ENCOUNTERED

Connect error and got stuck in the Failover Clustering functions

4. SELF EVALUATION OF THE PROGRESS

The clustering problem must be determined as soon as possible

The problem arises due to the virtual storage must not set up in either one of the clustering nodes, it will cause the clustering to fail

Supervisor’s signature

Student’s signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.: 7**
Student Name & ID: Foo Ce Sheng 15ACB05137	
Supervisor: Ts Dr Gan Ming Lee	
Project Title: Network Isolation and Security Using Honeypot	

1. WORK DONE

The problem of clustering is determined

One more server is added to the network, so now have a total of 3 servers

2. WORK TO BE DONE

The notification of SSH function is still in progress

The website also in developing

3. PROBLEMS ENCOUNTERED

-

4. SELF EVALUATION OF THE PROGRESS

I have the better understanding of how clustering works

I learnt how to implement a cluster network using Active Directory (AD)

__________________________ __________________________

Supervisor’s signature Student’s signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Year 3 Trimester 3	**Study week no.: 10**
Student Name & ID: Foo Ce Sheng 15ACB05137	
Supervisor: Ts Dr Gan Ming Lee	
Project Title: Network Isolation and Security Using Honeypot	

1. WORK DONE A login page is created Tracking Ip address, time and date are implemented
2. WORK TO BE DONE Implement the SSH Authentication using Google Authenticator
3. PROBLEMS ENCOUNTERED A configured server suddenly shut down unexpectedly
4. SELF EVALUATION OF THE PROGRESS I have to try to figure out the problem of the server shut down

_________________________ _________________________

Supervisor’s signature Student’s signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

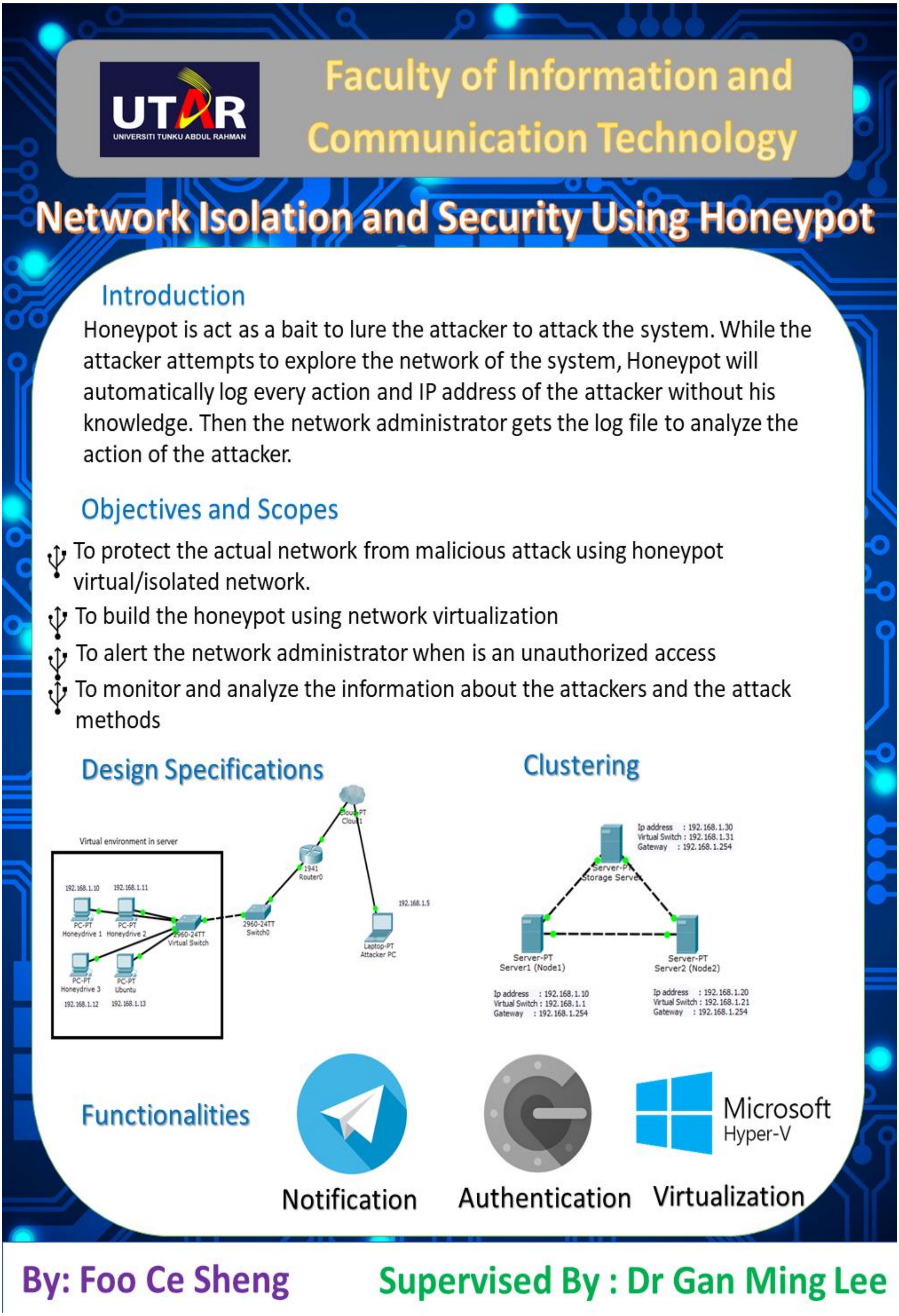
Trimester, Year: Year 3 Trimester 3	**Study week no.: 12**
Student Name & ID: Foo Ce Sheng 15ACB05137	
Supervisor: Ts Dr Gan Ming Lee	
Project Title: Network Isolation and Security Using Honeypot	

1. WORK DONE Done set up the website and notification function Documentation
2. WORK TO BE DONE Presentation and demonstration
3. PROBLEMS ENCOUNTERED **-**
4. SELF EVALUATION OF THE PROGRESS It lets me learn to do the implementation from the hardware to software site

_______________________ _______________________

Supervisor's signature Student's signature

APPENDICES B: POSTER



UTAR UNIVERSITI TUNKU ABDUL RAHMAN

Faculty of Information and Communication Technology

Network Isolation and Security Using Honeypot

Introduction

Honeypot is act as a bait to lure the attacker to attack the system. While the attacker attempts to explore the network of the system, Honeypot will automatically log every action and IP address of the attacker without his knowledge. Then the network administrator gets the log file to analyze the action of the attacker.

Objectives and Scopes

- To protect the actual network from malicious attack using honeypot virtual/isolated network.
- To build the honeypot using network virtualization
- To alert the network administrator when is an unauthorized access
- To monitor and analyze the information about the attackers and the attack methods

Design Specifications

Clustering

Ip address : 192.168.1.30
Virtual Switch : 192.168.1.31
Gateway : 192.168.1.254
Server-PT
Storage Server
Server-PT
Server1 (Node1)
Server-PT
Server2 (Node2)
Ip address : 192.168.1.10
Virtual Switch : 192.168.1.1
Gateway : 192.168.1.254
Ip address : 192.168.1.20
Virtual Switch : 192.168.1.21
Gateway : 192.168.1.254

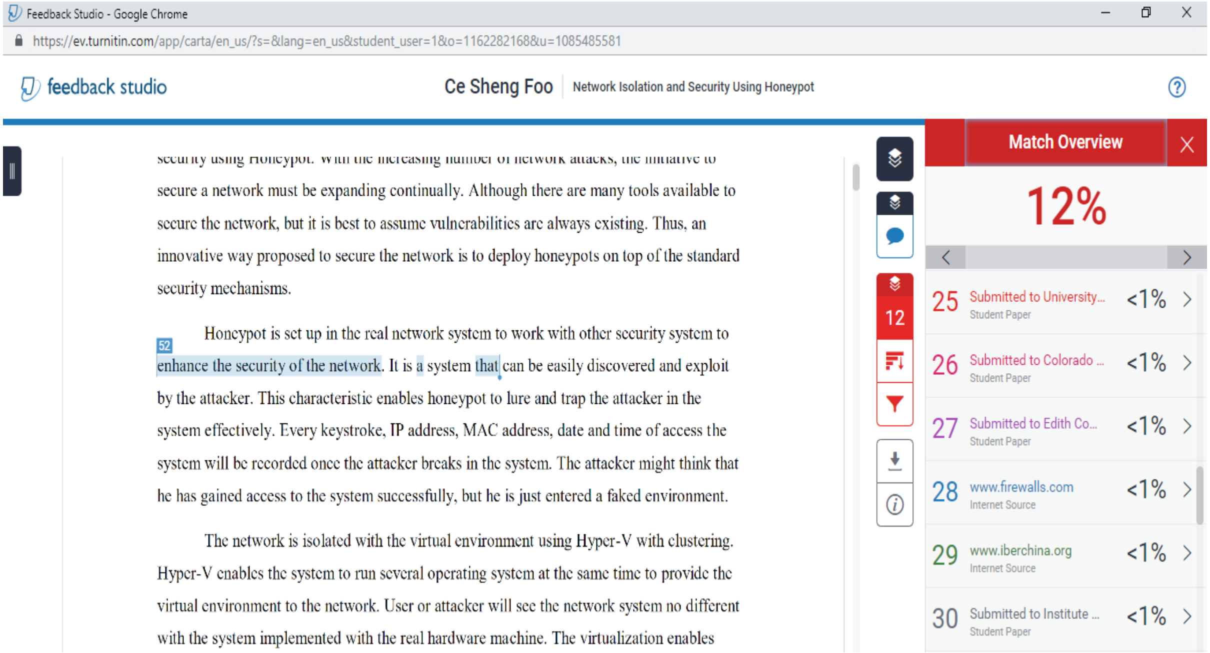
Functionalities

Notification Authentication Virtualization

By: Foo Ce Sheng

Supervised By : Dr Gan Ming Lee

APPENDICES C: TURNITIN REPORT



Feedback Studio - Google Chrome

https://ev.turnitin.com/app/carta/en_us/?s=&lang=en_us&student_user=1&o=1162282168&u=1085485581

feedback studio — Ce Sheng Foo — Network Isolation and Security Using Honeypot

security using Honeypot. With the increasing number of network attacks, the initiative to secure a network must be expanding continually. Although there are many tools available to secure the network, but it is best to assume vulnerabilities are always existing. Thus, an innovative way proposed to secure the network is to deploy honeypots on top of the standard security mechanisms.

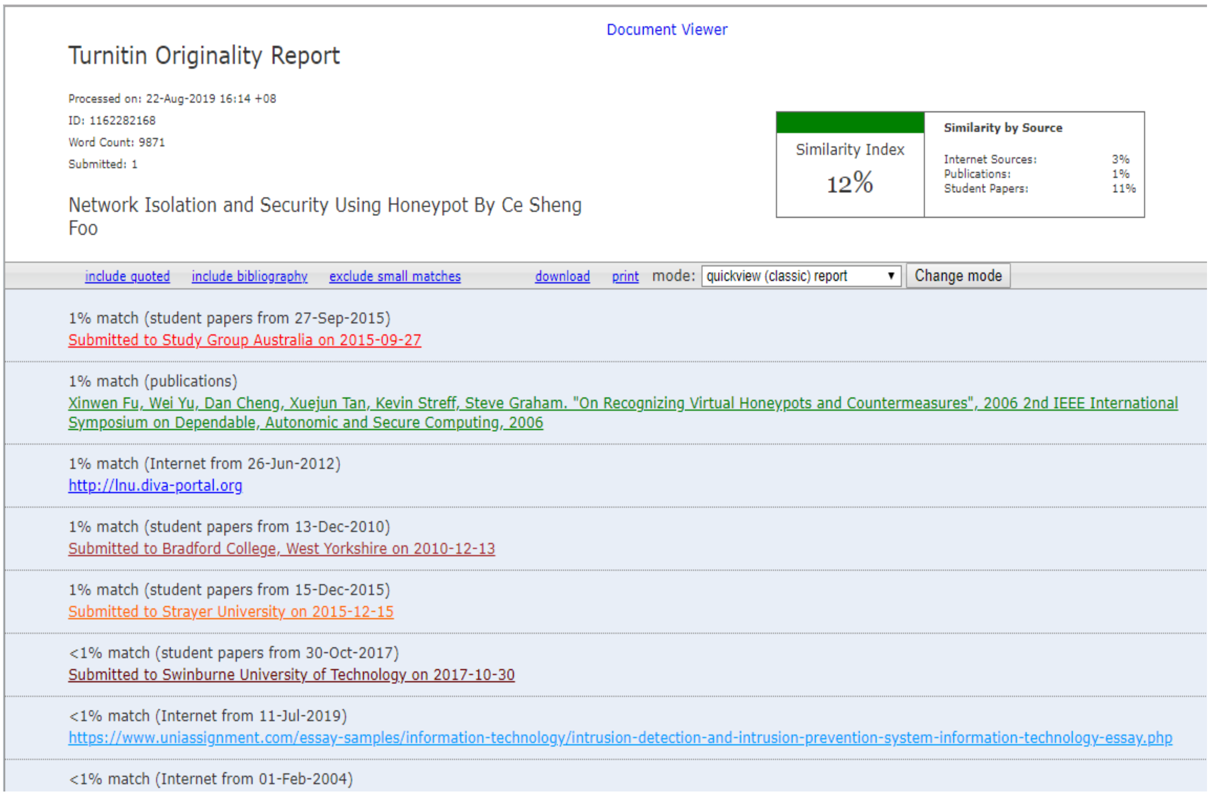
Honeypot is set up in the real network system to work with other security system to 52 enhance the security of the network. It is a system that can be easily discovered and exploit by the attacker. This characteristic enables honeypot to lure and trap the attacker in the system effectively. Every keystroke, IP address, MAC address, date and time of access the system will be recorded once the attacker breaks in the system. The attacker might think that he has gained access to the system successfully, but he is just entered a faked environment.

The network is isolated with the virtual environment using Hyper-V with clustering. Hyper-V enables the system to run several operating system at the same time to provide the virtual environment to the network. User or attacker will see the network system no different with the system implemented with the real hardware machine. The virtualization enables

Match Overview

12%

25	Submitted to University... Student Paper	<1%	>
26	Submitted to Colorado ... Student Paper	<1%	>
27	Submitted to Edith Co... Student Paper	<1%	>
28	www.firewalls.com Internet Source	<1%	>
29	www.iberchina.org Internet Source	<1%	>
30	Submitted to Institute ... Student Paper	<1%	>



Document Viewer

Turnitin Originality Report

Processed on: 22-Aug-2019 16:14 +08
ID: 1162282168
Word Count: 9871
Submitted: 1

Network Isolation and Security Using Honeypot By Ce Sheng Foo

Similarity Index

12%

Similarity by Source

Internet Sources:	3%
Publications:	1%
Student Papers:	11%

1% match (student papers from 27-Sep-2015)
Submitted to Study Group Australia on 2015-09-27

1% match (publications)
Xinwen Fu, Wei Yu, Dan Cheng, Xuejun Tan, Kevin Streff, Steve Graham. "On Recognizing Virtual Honeypots and Countermeasures", 2006 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, 2006

1% match (Internet from 26-Jun-2012)
http://lnu.diva-portal.org

1% match (student papers from 13-Dec-2010)
Submitted to Bradford College, West Yorkshire on 2010-12-13

1% match (student papers from 15-Dec-2015)
Submitted to Strayer University on 2015-12-15

<1% match (student papers from 30-Oct-2017)
Submitted to Swinburne University of Technology on 2017-10-30

<1% match (Internet from 11-Jul-2019)
https://www.uniassignment.com/essay-samples/information-technology/intrusion-detection-and-intrusion-prevention-system-information-technology-essay.php

<1% match (Internet from 01-Feb-2004)

Universiti Tunku Abdul Rahman			
Form Title: Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1of 1

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name of Candidate	Foo Ce Sheng
ID Number	15ACB05137
Programme / Course	Bachelor Information Technology (Hons) Communication and Networking
Title of Final Year Project	Network Isolation and Security Using Honeypot

Similarity	**Supervisor's Comments (Compulsory if parameters of originality exceed the limits approved by UTAR)**
Overall similarity index: 12 % **Similarity by source** Internet Sources: 3 % Publications: 1 % Student Papers: 11 %	
Number of individual sources listed of more than 3% similarity: 0	
Parameters of originality required and limits approved by UTAR are as Follows: **(i) Overall similarity index is 20% and below, and** **(ii) Matching of individual sources listed must be less than 3% each, and** **(iii) Matching texts in continuous block must not exceed 8 words** ***Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.***	

Note: Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

______________________________ ______________________________

Signature of Supervisor

Name: Ts Dr Gan Ming Lee

Date: ____________________________

Signature of Co-Supervisor

Name: Ts Dr Lau Phooi Yee

Date: ____________________________

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF INFORMATION & COMMUNICATION TECHNOLOGY (KAMPAR CAMPUS)

CHECKLIST FOR FYP2 THESIS SUBMISSION

Student Id	15ACB05137
Student Name	Foo Ce Sheng
Supervisor Name	Ts Dr Gan Ming Lee

TICK (√)	**DOCUMENT ITEMS** Your report must include all the items below. Put a tick on the left column after you have checked your report with respect to the corresponding item.
	Front Cover
	Signed Report Status Declaration Form
	Title Page
	Signed form of the Declaration of Originality
	Acknowledgement
	Abstract
	Table of Contents
	List of Figures (if applicable)
	List of Tables (if applicable)
	List of Symbols (if applicable)
	List of Abbreviations (if applicable)
	Chapters / Content
	Bibliography (or References)
	All references in bibliography are cited in the thesis, especially in the chapter of literature review
	Appendices (if applicable)
	Poster
	Signed Turnitin Report (Plagiarism Check Result - Form Number: FM-IAD-005)

*Include this form (checklist) in the thesis (Bind together as the last page)

I, the author, have checked and confirmed all the items listed in the table are included in my report. ________________________ (Signature of Student) Date:	Supervisor verification. Report with incorrect format can get 5 mark (1 grade) reduction. ________________________ (Signature of Supervisor) Date: