UNIVERSITI PUTRA MALAYSIA

HONEYNET AS A SERVICE DEPLOYMENT APPROACH IN ENABLING VIRTUAL CRIME SCENE INVESTIGATION

HAMIDREZA HASHEMINEJAD

FK 2015 29

HONEYNET AS A SERVICE DEPLOYMENT APPROACH IN ENABLING VIRTUAL CRIME SCENE INVESTIGATION

By

HAMIDREZA HASHEMINEJAD

Thesis Submitted to the School Graduate Studies, Universiti Putra Malaysia, in Fulfillment of the Requirements for the Degree of Master of Science

July 2015

COPYRIGHT

DEDICATIONS

In the name of Allah, Most Gracious, Most Merciful

This thesis is dedicated to:

My beloved wife, Fereshteh, for her unconditional help, her loyalty, and all of her supports in a foreign country.

And

My dear parents, for their love and endless support

My friends for their unlimited support, their endless care and encouragement

To all those who stand by me

Thank you

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

HONEYNET AS A SERVICE DEPLOYMENT APPROACH IN ENABLING VIRTUAL CRIME SCENE INVESTIGATION

By

HAMIDREZA HASHEMINEJAD

July 2015

Chairman: Shaiful Jahari Bin Hashim, PhD
Faculty: Engineering

With the exponentially spread of the Internet usage, information technology or cyber security is now an issue for anyone. There is a range of different security threats including hacking, intrusions, computer worms and viruses in the cyberworld. In order to prevent these attacks, technologies such as firewall and intrusion prevention systems depend on known attack signature. However, much less focus has been given to finding new systems' vulnerability that can lead to new attack signature. Honeypot is valuable cyber security tool that can act as baits for intruders. It is an indispensable tool to discover, explore and study new attacks with a low false positive rate. Preparing a honeypot, however, is difficult, time consuming and expensive especially for High Interaction Honeypot (HIH). It is because its deployment processes involves design, installation and maintenance that require expertise and experience due to the high risk nature of the honeypot especially for the HIH. Furthermore, incident data analysis of any honeypot intrusion can be very costly in term of network bandwidth transfer due the huge amount of incident data transfer. From the perspective of incident data analysis and investigation, companies need to hire computer security and forensic analysis personnel who have good knowledge of different aspects of computer security. These experts are most probably located outside the company hence the data transfer for investigation are necessary.

This study proposes and demonstrates a new paradigm of cyber defense in the form of a honeynet architecture based on cloud computing which offers a fully managed Honeynet-as-a-Service (HaaS). This system introduces a new and efficient technique to serve honeynet for other networks without the need of physical installation. In fact by using cloud computing to install different honeypots, it can provide an efficient service for other organizations. The cloud-based honeynet would be connected to any network

by using a tunnel interface as a communication layer. It also introduces a new concept of virtual crime scene (VCS) by enabling "live-recording" and "snapshot" of intrusion events. In "live-recording" almost all attacker activities is captured. Using "snapshot" technique, the concept of forensic science namely Locard's Exchange Principle is applied to the virtual realm. The "snapshot" is a valuable technique for preservation of evidence for the investigation process against any modification (removal or addition).

Based on the cloud nature of the proposed system, minimum intervention for its installation, maintenance and analysis is required by the participated organization since it is fully managed by the operator. For the participated organizations, unused IP addresses are being used as IP addresses for the HaaS honeypots. The connections are re-directed via virtual private network (VPN) to the cloud backend.

Specifically HaaS provided efficient bandwidth usage, cost and time. The cloud reduced the amount of bandwidth transfer significantly especially for "live-recording" and "snapshot" of incident data for further processing and analysis. For a single HaaS honeypot "live-recording", measurement in real experiment has shown that the size of log files in this model is 5.4 times more (i.e. saving) than network traffic which is passed into HaaS. For a single HaaS honeypot "snapshot" the saving is 68 times than the physical honeypot. For multiple HaaS honeypots, these bandwidth saving will be much more significant i.e. few hundred times saving. It is primarily because the recording and logging are performed in the cloud side. Furthermore, a single HaaS honeypot installation can be ready in five minutes which is a very short time compare to a single physical honeypot's installation. As a result of that, a single HaaS honeypot is 95 times faster than physical honeypot installation. In addition, single HaaS honeypot installation can also be roll backed by 4 minutes in comparison to single physical honeypot roll back time which is 28 minutes in average i.e. 7 times faster.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

PENDEKATAN PENEMPATAN JARINGAN KOMPUTER MADU SECARA PERKHIDMATAN DALAM MEMBOLEHKAN PENYIASATAN TEMPAT KEJADIAN JENAYAH MAYA

Oleh

HAMIDREZA HASHEMINEJAD

Julai 2015

Pengerusi: Shaiful Jahari Bin Hashim, PhD
Fakulti: Kejuruteraan

Dengan kepesatan penggunaan Internet yang semakin banyak, keselamatan teknologi maklumat atau siber sekarang telah menjadi suatu isu untuk sesiapa sahaja. Terdapat pelbagai ancaman keselamatan yang berbeza termasuk penggodaman, pencerobohan, cecacing komputer dan virus dalam dunia siber. Untuk mengelakkan serangan ini, teknologi seperti sistem pencegahan tembok api dan sistem pencegahan pencerobohan bergantung kepada tandatangan serangan yang telah diketahui. Walau bagaimanapun, tumpuan yang sangat kurang telah diberikan untuk mencari kelemahan sistem baharu yang boleh menjana kepada serangan tandatangan baharu. Komputer madu adalah perkakasan keselamatan siber yang berharga yang boleh bertindak sebagai umpan untuk penceroboh. Ia adalah yang perkakasan yang amat diperlukan untuk menjumpai, meneroka dan mengkaji serangan baharu dengan kadar positif palsu yang rendah. Menyediakan komputer madu, bagaimanapun, adalah sukar, memakan masa dan mahal terutamanya bagi komputer madu interaksi tinggi (HIH). Ini adalah kerana proses penempatan yang melibatkan reka bentuk, pemasangan dan penyelenggaraan yang memerlukan kepakaran dan pengalaman kerana sifat risiko komputer madu yang tinggi terutamanya bagi HIH. Tambahan pula, analisis data insiden pencerobohan komputer madu boleh menjadi sangat mahal daripada segi pemindahan jalur lebar rangkaian kerana jumlah pemindahan data kejadian yang sangat besar. Daripada perspektif analisis kejadian data dan penyiasatan, syarikat perlu mengupah pakar analisis keselamatan dan forensik komputer yang mempunyai pengetahuan yang baik dalam pelbagai aspek keselamatan komputer. Pakar ini berkemungkinan besar berada di luar syarikat tersebut, justeru itu pemindahan data untuk penyiasatan adalah perlu.

Kajian ini mencadangkan dan menunjukkan paradigma baharu pertahanan siber dalam

bentuk seni bina rangkaian komputer madu yang diuruskan sepenuhnya berasaskan pengkomputeran awan (HaaS). Sistem ini memperkenalkan teknik baharu dan berkesan untuk menawarkan perkhidmatan rangkaian komputer madu untuk rangkaian lain tanpa memerlukan pemasangan fizikal. Malah dengan menggunakan pengkomputeran awan untuk memasang komputer madu berbeza, ia boleh memberi perkhidmatan yang cekap untuk organisasi lain. Rangkaian komputer madu berasaskan awan akan berhubung dengan sebarang rangkaian dengan menggunakan antara muka terowong sebagai lapisan komunikasi. Ia juga memperkenalkan satu konsep baharu iaitu tempat kejadian jenayah maya (VCS) dengan membolehkan "rakaman-langsung" dan "petikan" peristiwa pencerobohan. Dalam "rakaman-langsung" hampir semua aktiviti penyerang dirakam. Prinsip Pertukaran Locard iaitu suatu konsep sains forensik telah diaplikasikan kepada alam maya dengan menggunakan teknik "petikan". “Petikan” adalah merupakan ialah suatu teknik yang berharga untuk pemeliharaan bukti untuk proses penyiasatan terhadap sebarang pengubahsuaian (pembuangan atau penambahan).

Berdasarkan sifat awan sistem yang dicadangkan itu, campur tangan minimum oleh organisasi yang mengambil bahagian untuk pemasangan, penyelenggaraan dan analisis kerana ia diuruskan sepenuhnya oleh pihak pengendali. Untuk organisasi yang telah mengambil bahagian, alamat IP yang tidak digunakan akan digunakan sebagai alamat IP bagi komputer madu HaaS. Sambungan diarahkan semula menerusi rangkaian persendirian maya (VPN) untuk pelayan di awan.

Secara khusus, HaaS menyediakan pengunaan lebar jalur yang cekap, kos dan masa. Awan mengurangkan jumlah pemindahan lebar jalur secara ketara terutamanya untuk "rakaman-langsung" dan "petikan" data kejadian untuk pemprosesan dan analisis lanjut. Untuk satu komputer madu "rakaman-langsung" HaaS, pengukuran dalam eksperimen sebenar telah menunjukkan bahawa saiz fail log dalam model ini adalah sebanyak 5.4 kali lebih (iaitu penjimatan) berbanding trafik rangkaian yangmelalui HaaS. Untuk petikan satu komputer madu HaaS, penjimatan adalah sebanyak 68 kali lebih berbanding satu komputer madu fizikal. Untuk berbilang komputer madu HaaS, penjimatan lebar jalur akan menjadi lebih ketara iaitu beberapa ratus kali penjimatan. Ia adalah terutamanya kerana rakaman dan penyimpanan dijalankan di bahagian awan. Tambahan pula, pemasangan satu komputer madu Haas boleh disiapkan dalam masa lima minit yang merupakan masa yang singkat berbanding dengan pemasangan satu komputer madu fizikal. Hasil daripada itu, satu komputer madu HaaS adalah 95 kali lebih cepat daripada pemasangan komputer madu fizikal. Selain itu, pemasangan satu komputer madu HaaS juga boleh dikembalikan kepada asal dalam masa 4 minit berbanding dengan satu komputer madu fizikal yang mengambil masa purata 28 minit iaitu 7 kali lebih cepat.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank Almighty Allah (S.W.T) for giving me the strength, patience, courage, and determination to complete this work. All grace and thanks belongs to Almighty Allah (S.W.T)

Many special thanks go to my supervisor Dr. Shaiful Jahari bin Hashim, for his incredible guidance, continuous support, and encouragement. He always has time for me and readily providing his technical expertise throughout the period of my study. I owe more than I can ever repay. The completion of this work becomes possible due to his supervision. His high stance of diplomatic power and professionalism set a great model for me to follow.

I would also like to thank Dr. Syed Abdul Rahman Syed Mohamed AlHaddad and Dr. Fazirulhisyam Hashim for serving on my thesis committee. Their helpful suggestions and advices on various aspects of my research work have certainly been very constructive. Without their kind cooperation and support, my graduate study would not have been accomplished.

I would also like to include acknowledgment to my colleague, Rahman Mousavian. He provided me a valuable advices and positive critics during my candidature. He guided me during the implementation of my work. Also special Thanks to all kindness network support engineer at UPM IDEC to help us to evaluate this model as a first client.

I certify that a Thesis Examination Committee has met on 13 July 2015 to conduct the final examination of Hamidreza Hasheminejad on his Master of Science thesis entitled "Honeynet as a Service Deployment Approach in Enabling Virtual Crime Scene Investigation" in accordance with the Universities and University Colleges Act 1971 and the Constitution of the University Putra Malaysia [P. U. (A) 106] 15 March 1998. The Committee recommends that the student be awarded the degree of Master of Science.

Members of the Thesis Examination Committee were as follows:

M. Iqbal bin Saripan, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Abd. Rahman bin Ramli, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Mahamod Ismail, PhD
Professor
University Kebangsaan Malaysia
Malaysia
(External Examiner)

ZULKARNAIN ZAINAL, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Data: 12 August 2015

This thesis was submitted to the Senate of University Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of **Master of Science**.

The members of the Supervisory Committee were as follows:

Shaiful Jahari bin Hashim, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairperson)

Syed Abdul Rahman Al-Haddad b. Syed Mohamed, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Fazirulhisyam bin Hashim, PhD
Senior Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

_____

BUJANG KIM HUAT, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Data:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: _____

Name and Matric No.: Hamidreza Hasheminejad, GS37208

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of the thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to,

Signature: _____

Name of Chairman of Supervisory Committee: Shaiful Jahari bin Hashim, PhD

Signature: _____

Name of Chairman of Supervisory Committee: Syed Abdul Rahman Al-Haddad, PhD

Signature: _____

Name of Chairman of Supervisory Committee: Fazirulhisyam bin Hashim, PhD

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVATIONS

API	Application Programming Interface
AS	Autonomous System
BGP	Border Gateway Protocol
BSD	Berkeley Software Distribution
CCTV	Closed Circuit Television
CDROM	Compact Disk - Read Only Memory
CPP	C ++
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DOS	Denial of Service
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HaaS	Honeynet as a Service
HIH	High Interaction Honeypot
LIH	Low Interaction Honeypot
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IAAS	Infrastructure as a Service
ID	Identification
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IT	Information Technology
KVM	Kernel Virtual Machine
L2TP	Layer2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LKM	Linux Kernel Module
LVM	Logical Volume Manager
LXC	Linux Containers
NASA	National Aeronautics and Space Administration
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
OS	Operating System
P2P	Point to Point
PAAS	Platform as a Service
QEMU	Quick Emulator
SAAS	Software as a Service
SCSI	Small Computer System Interface
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer

TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VPS	Virtual Private Server

CHAPTER 1

INTRODUCTION

1.1 Background

The need of data security in the field of information technology (IT) assets at consumer and business level was drawn into public when the Internet has been introduced in the late 1980s. Innella [1] associate it with emergence of the first malware (Marris worm) in 1988, and explain: “In the autumn 1988, the first evidence of a threat in network security had been seen. In that time, the first internet virus had infected all 60,000 computers that were connected to the network and those were unable to work for at least two days.”

Previously, there were no actual threat, as the early Internet network was only shared between some military organization and few universities for research collaboration [1]. It should not be looked at the security as an out-of-the-box solution. “It needs accurate analysis of the environment before proposing a solution for prevention. It is a procedure that needs a depth understanding of the system functionality and its limitation. No system is 100% protected, the system security is as powerful as its weakest point” [2].

The security of the services accessible over these networks specially which connected to the Internet directly show a huge threat to the IT companies. Every day, all kind of known and unknown malwares (zero day malwares) are extremely threaten the IT industries and business related to that with mission critical systems.

Different type of IT infrastructures are threaten every day with various techniques ranges from intrusion to the systems, attack to computers, denial of service (DOS), viruses, worms and more. Intruders take advantage of the Internet and other features to use them as a transport system to spread their malware around the world and exploit other remote services. Many different mechanisms and devices in computer security are invited to provide various layers of security defense. It is because that if an intruder bypasses one layer, other security layers protect the network and stay in front of that.

As Figure 1.1 shows, the two main categories of security tools are detection and prevention tools. Intrusion detection in computer systems is the art of detecting the malicious activities [3]. In cyber security the detection term means monitoring the network for suspicious patterns that may threats our network. Then sending intrusion data to security team for analysis. These kind of tools will not prevent attackers from their illegitimated activities because they are considered to be passive-monitoring tools. They monitor traffic behind the firewall or packets cross inside DMZ and based on their signature or pre-defined configuration, they apply own rules. When malicious activity has been detected, the detection systems send alarm to system administrator and record that event. For example, antiviruses are based on some signature and patterns that can inform client to put certain action on different situations. The development of intrusion detection system has become an important tool for the security teams who are

responsible for patch the vulnerable system and protect production networks. These techniques have ability to detect malicious traffic through public and private networks. Furthermore, the advantage of detection system is that it does not interfere with normal operation.

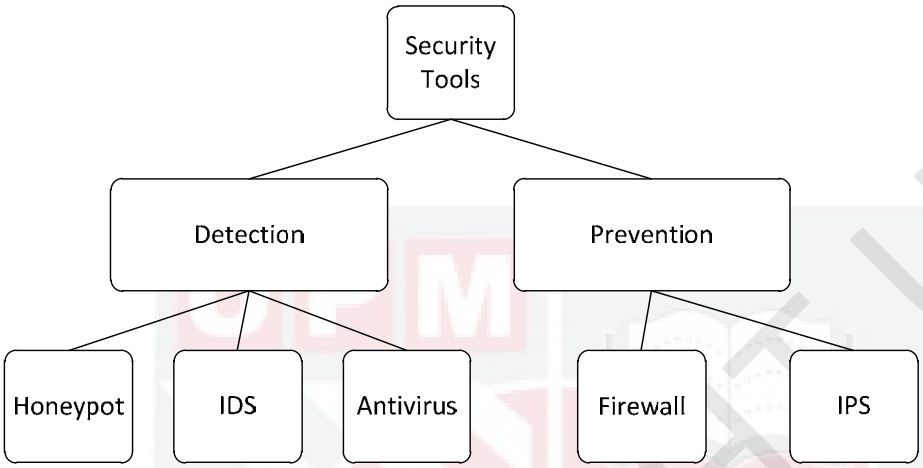

Figure 1.1: Security Tools Taxonomy

On the other hand, prevention systems are naturally active and with this ability they can detect and stop suspect traffic from transmission. Prevention systems are commonly based on some rules and pattern to block or allow types of traffic to flow. For example, firewalls only pass specified traffics which are not restricted by plenty of pre-configuration settings. Also, the disadvantage of prevention system is that it can interfere with normal operation and impeding or reducing the system's performance.

Detecting as many as possible attacks and having a few false positive alarm are some of the performance criteria for a security tools. Today, unfortunately there is no one comprehensive method to protect a whole system against every type of attacks based on the network [4]. The 2013 Computer Security Institute/FBI Computer Crime and Security Survey [5] reports 94% of respondents are using firewalls in their network. However, still it is obvious that our network are not completely protected. Most of the time, attackers use unblocked ports to attack. HTTP/HTTPS or SSH traffics are examples of these type of allowed packets by firewalls especially to the company's DMZ. Web server traffic cannot be blocked by firewall to prevent attacks. However, it is obvious that security holes like Shellshock (CVE-2014-6271) [6], Heart bleed [7] or Poodle [8] which have been detected recently are using same allowed protocol rules in firewalls. Actually those attackers have used allowed firewall's ports. Because their techniques was completely new, nothing could not detect that.

As a result, only a system that combines a variety of technologies to detect different types of attacks can get provide comprehensive protection. To sum up, there is no any ready to use or static solution to protect our assets.

As explained, there is a need for techniques to capture and study new attacks in order to find malicious patterns for detection and prevention systems. By learning the tactics and techniques used by malicious attackers, it can help to secure our IT assets and infrastructure.

Honeypots are tools to investigate attacker's tactics. It is greatly useful to know about which intruders are able to gain from network resources along with different approaches. Honeypot provides methods for gathering information for further analysis. A vulnerable environment that seems to have useful resources is a key tool to get information about attackers. Honeypot has no production value and they are always massively logged. Compare to normal firewalls, honeypots have low false positive rate. As a matter of fact, any connection to honeypot is suspicious and is a malicious interaction.

Honeypots singly and directly cannot tackle security problems like intrusion detection or firewall systems, however they gather information about vulnerability holes in the systems and helps system administrators to improve overall network security. The honeypot's output data can be entered to other systems to trigger prevention systems for immediate action. One of the honeypots advantages in contrast with other intrusion detection systems is that they produce low false-positive alerts. Detecting a legitimate connection as a security breaches or an attack mistakenly called false positive. However because of honeypot's nature, all the traffic to honeypots are suspicious and need to be analyzed carefully.

To improve the chance of capturing more data and distracting attacker from the main servers, using of honeynets are more useful. Honeynets are two or more honeypots on a network with the same goal as mentioned before. In the whole, a honeynet is used for monitoring a large network with variety of honeypots sensors and provide more comprehensive and realistic system trap. As they are consisted from a group of honeypots, using them needs more consideration. Honeynets produce huge log files in size. These information should be analyzed to extract useful data in order to know the attackers' behavior. Each honeypot needs to be cleaned after each attack. Hence almost all the honeynet systems use a watcher mechanism to see when the attacking process start and when it finishes, it is necessary to make the honeypot as clean as before attack. All of these maintenance procedure plus deployment and analysis the log files are costly. Here the mentioned cost associate with hardware cost, maintenance cost, human resource for log analysis and time for both installing and cleaning the honeypot environment.

On the other hand, cloud computing provides huge pool of computing resources as well as large amount of data which are accessible from anywhere. By using cloud computing technology, access to a variety of resources accessible anywhere with a low cost and on a 'pay-per-use' principal is already prepared. Hence companies are not required to spend so much money for installing and maintaining honeynet while cloud computing can

reduce the costs. The aim of this research study is to present a method to utilize cloud computing to improving the honeynet deployment, maintenance and distribution of log files.

In this research, as Figure 1.2 shows, a honeynet system based on cloud computing is proposed to build and provide robust virtual trap in order to improve the methodology to learn, expose and discover APT tool and techniques. Our proposed solution is called HaaS, combining honeypot/honeynet technology with cloud computing to overcome the difficulties of honeynet installation and maintenance. At the same time, this solution can comprehensively capture attacker's activities ("live recording") and freezing the crime scene in order to keep our incident environment intact for further investigation ("snapshot"). In addition, due to the nature of the cloud system being used, the amount of bandwidth consumption for transferring "live recording" and "snapshot" data for forensic and incident response can be significantly reduced.

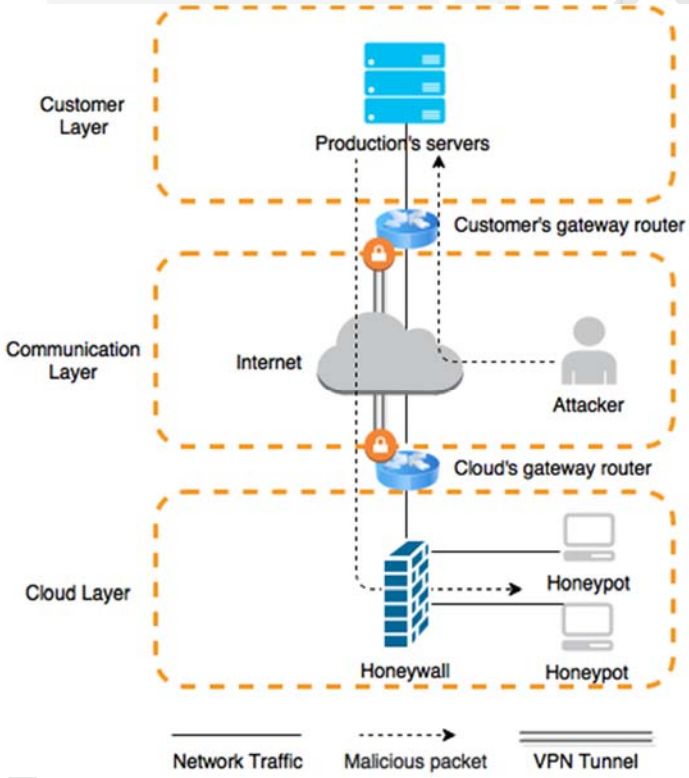

Figure 1.2: HaaS concept

1.2 Motivation and Problem Statement

There is a common problem with knowledge based tools such as firewalls and intrusion prevention systems that they produce false alarm. False-positive is a widespread issue

that cause IPS/IDS to produce an alarm when no attack has been taken place. However, in honeynet, because of its nature, most of network packets accessing honeypots are suspicious to be illegitimated. For this reason, the rate of honeynet's false-positive is very low [9].

Next problem is related to Advanced Persistent Threat (APT) [10]. They are some kind of network attacks which an unauthorized person gains access to a network and stay there undetected for a long period of time. In some cases, a super malwares is supported by an organization or a big company and they are very sophisticated for some specific purposes. The two sophisticated malwares like Stuxnet [11] and recently discovered Regin (Nov 2014) [12] are obvious examples of this kind of aggressive computer worms. Some experts assume huge money also has been paid to antivirus companies to ignore detecting them. It is a low probability that a malware can exist for a long period as 6 years without disclosure. Or maybe by finding a new unknown malware sooner in few days instead of few months, can decrease their damage or even prevent their information theft. So if an organization wants to inspect all of its subsection, they should buy hardware and install honeypot in different locations. It is because that their branches are located in different geographic locations and in order to know their enemies, it is necessary to have some sensors in each location. In this case the whole system is depending on the availability of hardware, bandwidth and maintenance experts.

The installation of honeynet needs not only good knowledge about Linux and Windows operating system but also proper hardware should be devoted to them. This is one of issues with honeynets that the installation of them is expensive. Moreover, honeypots need to be maintained periodically. It means after each attack the whole system should be clean and become ready for lure other attacker. It is obvious that this procedure is also costly, too. Another problem with honeynet is that they have no immediate action for to network security improvement, and companies assume they are not so much worth efficient to invest. These are plenty of reasons why motivation for utilizing them is low. Hence, Honeynet as a Service with all of cloud profit can make honeynets more expendable.

Next problem is that honeypots always produce huge log files because they generate detailed information about attack time and all happened stuffs in the systems. Honeynet do not perform any direct action for network security. Companies which use honeynet should send these log files to other third party company for analysis. The size of the log files are depend on attack complexity and they are almost huge. Sending these type of log files for investigation is not only a time consuming task but also need huge network bandwidth for transferring. In this proposed model, all data included log files will be stored on cloud computers and because of cloud's features there is no need to send them to other location for investigation. As nowadays the cost of bandwidth traffic in cloud servers is much more expensive than storage, the HaaS can come with more efficiency in order to final log file investigation.

These problems lead to have an expensive system. Their analysis and maintaining parts need professional security team to analysis in order to propose security personal for vulnerable parts. Also maintaining this system log files is essential.

To put it in a nutshell, since the installation, deployment and analysis of the log files of the honeynet takes much time and need to devote hardware and bandwidth, the whole procedure increase the costing. Therefore, the solution presented in this research should speed up the whole procedure from installation to data analysis process, and save cost by reducing the incident data transfer considerably.

1.3 Research Aim and Objectives

The main aim of this research is to design and implement a system to provide honeynet service based on cloud computing technology. The focus, in this study, will be on a system that customers just plug it into any desirable network and this proposed model can provide a honeynet system for them to producing information about their intruders. Moreover, saving total cost in different view during deployment and analysis of the log files is another goal of this research.

Furthermore, another goal of this research is to reduce the probability of attack against production servers and also increase time for penetrator to reach the main servers. This can be similar to landmines analogy to bore enemy to progress. As Figure 1.3 is shown, with some fake servers (honeypots) which are spread among the real production server, the statistical probability of attack will be reduced by 50%. It means an intruder needs to spend two times more time to find real production servers in a network's system, or maybe some sophisticated worms get trapped by this mines.

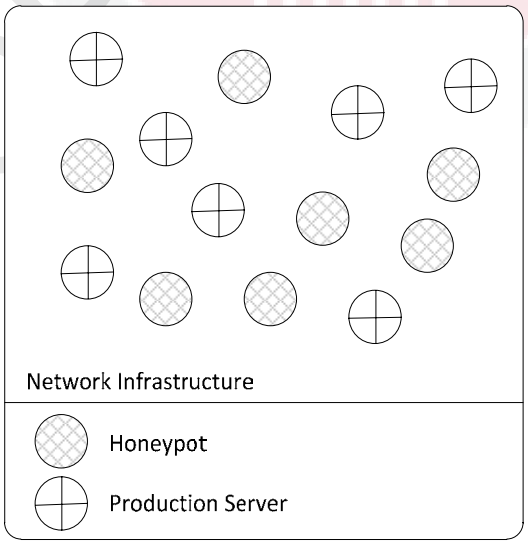

Figure 1.3: Honeynet and land mines analogy

From the mentioned problems, main objectives are specified and listed as the following:

- Design and implement a system to provide honeynet service based on cloud computing technology that is easy to deploy and has easy maintenance
- Enable virtual crime scene investigation for discovering APT attacks
- Reduce the amount of bandwidth transfer for incident data (log files)

In this research, we proposed a new virtual crime scene (VCS) concept to keep all the necessary evidence into specific files. It means that almost all of the attacker's activities during the intrusion inside the honeypots are stored in the files which can be either analyzed or archived for more in depth investigation purposes if the need arises.

1.4 Study Scope

In this part, the scope of this research is clarified by explaining the type/number of honeypots and test bed limitation. The total number of three honeypots are used to implement a honeynet inside a cloud computing area. They consist of two HIH and one LIH that are connected to a honeywall. All of these software are installed on two servers as cloud compute hypervisors. Moreover, for testing purpose, one organization is chosen to prove functionality of this system. The cloud computing environment is also isolated from other part of network for privacy and security purposes. In addition, aim of this research is not neither design a new honeypot sensor nor new tunneling technology for connecting two networks. While there is some security devices for studying stream attacks like DDOS, this research is mostly for investigating intruders' behavior.

1.5 Thesis Organization

This research report is arranged in five chapters, including this first chapter which was for introduction. The explanation of various kind of honeypots, different models of honeynet implementation and analysis approaches will be explored and highlighted in Chapter 2. Additionally, explanation of cloud computing, its components and related previous works will be discussed in this chapter. Chapter 3 will define and explain used methodology to assert the achievements of this research objectives with elaborate used settings. At the end, an explanation of other two honeynet models for proving the feasibility of proposed model is presented. After that, obtained results from those experiments will be represented in Chapter 4. Finally, conclusion and future work of this research will be defined in Chapter 5.

BIBLIOGRAPHY

[1] P. Innella, "A brief history of network security and the need for adherence to the software process model," 2000.

[2] S. Marcinkowski, "Extranets: The Weakest Link and Security," 2001. [Online]. Available: http://www.sans.org/reading_room/whitepapers/basics/extranets-weakest-link-security_432.

[3] Phoha, Vir V, Internet security dictionary, Springer Science & Business Media, 2007.

[4] S. Sorensen, "Intrusion Detection and Prevention ,Protecting Your Network From Attacks," *Juniper Network*, 2006.

[5] "The Current State of Computer Network Security," 2013. [Online]. Available: http://www.fbi.gov/. [Accessed 2014].

[6] L. Garber, "Hackers Exploit Critical Shellshock Vulnerability.," pp. 14-14.

[7] Durumeric, Zakir and et al, "The matter of Heartbleed.," in *Proceedings of the 2014 Conference on Internet Measurement Conference, ACM*, 2014.

[8] Levillain, Olivier, Baptiste Gourdin and Hervé Debar, "TLS Record Protocol: Security Analysis and Defense-in-depth Countermeasures for HTTPS.," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. ACM*, 2015.

[9] Dagon, David, "Honeystat: Local worm detection using honeypots, Recent Advances in Intrusion Detection," *Springer Berlin Heidelberg*, 2004.

[10] Virvilis, Nikos and Dimitris Gritzalis, "The big four-what we did wrong in advanced persistent threat detection?," in *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on, IEEE*, 2013.

[11] Karnouskos, Stamatis, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society. IEEE*, 2011.

[12] Askin, Osman, Riza Irmak and Mustafa Avsever, "Cyber warfare and electronic warfare integration in the operational environment of the future: Cyber Electronic Warfare.," *SPIE Defense+ Security. International Society for Optics and Photonics*, 2015.

[13] Tankard, Colin, "Advanced Persistent threats and how to monitor and deter them," *Network security*, pp. 16-19, 2011.

[14] Cheng-Yuan Ho ,Yuan-Cheng Lai ; I-Wei Chen ; Fu-Yu Wang ; Wei-Hsuan Tai, "Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems," *Communications Magazine, IEEE*, pp. 146 - 154, 2012.

[15] Spitzner, Lance, "The honeynet project: Trapping the hackers," *IEEE Security & Privacy*, pp. 15-23, 2003.

[16] Project, honeynet , "Know Your Enemy," 2006. [Online]. Available: http://old.honeynet.org/papers/honeynet/. [Accessed 2015].

[17] "Know Your Enemy: GenII Honeynets Easier to deploy, harder to detect, safer to maintain.," Honeynet Project, 12 May 2005. [Online]. Available: http://old.honeynet.org/papers/gen2/. [Accessed 2014].

[18] Kulkarni, Santosh, "Honeydoop-a system for on-demand virtual high interaction honeypots," in *Internet Technology And Secured Transactions, 2012 International Conference for. IEEE,*, 2012.

[19] da Costa, "Improved blind automatic malicious activity detection in honeypot data," in *The International Conference on Forensic Computer Science (ICoFCS)*, 2012.

[20] Abbasi, Fahim UH, "Detection and classification of malicious network streams in honeynets: a thesis presented in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Computer Science at Massey University, Palmerston North, New Zealand.," 2013.

[21] "Honeywall," [Online]. Available: https://projects.honeynet.org/honeywall/. [Accessed 2015].

[22] Abbasi, Fahim H., and R. J. Harris, "Experiences with a Generation III Virtual Honeynet," in *Telecommunication Networks and Applications Conference (ATNAC), 2009 Australasian. IEEE*, 2009.

[23] R. M. Magalhaes, "Understanding Virtual Honeynets," 6 March 2003. [Online]. Available: http://www.windowsecurity.com/articles-tutorials/intrusion_detection/Understanding_Virtual_Honeynets.html.

[24] Kellep Charles , "An Overview of HoneyPots," Blacks in technology, [Online]. Available: https://www.bitdigest.net/an-overview-of-honeypots/. [Accessed 26 aug 2014].

[25] Muhammad Fahd, Kaleem Ullah Saleh, "A Force Multiplier in Educational Domain," Luleå University of Technology, jun 2012.

[26] Y. Bouzida, F. Cuppens, N. Cuppens-Boulahia, and S. Gombault, "Efficient intrusion detection using principal component analysis," in *Conférence sur la Sécurité et Architectures Réseaux (SAR)*, France, Jun. 2004.

[27] Dacier, F. Pouget and M., "Honeypot-based forensics," in *in AusCERT Asia Pacific Information technology Security Conference*, 2004.

[28] J. Zimmermann, A. Clark, G. Mohay, F. Pouget, and M. Dacier, "The use of packet inter-arrival times for investigating unsolicited internet traffic," in *Systematic Approaches to Digital Forensic Engineering*, 2005.

[29] N. Provos, "A virtual honeypot framework," in *13th USENIX Security Symosium*, Aug 2014.

[30] Zero Day Initiative, "Adobe Flash Player JPEG Parsing Heap Overflow Vulnerability," 9 December 2009.

[31] Watson, David, and Jamie Riden, *The honeynet project: Data collection tools, infrastructure, archives and analysis,* WOMBAT Workshop on Information Security Threats Data Collection and Sharing. IEEE, 2008.

[32] Project, HoneySpider Network, "The Honeyspider Network – Fighting Client-Side Threats," 2009.

[33] BBC, "Google Searches Web's Dark Side," 11 May 2007.

[34] G. Raul Siles, "Sebek 3: tracking the attackers, part one," [Online]. Available: http://www.symantec.com/connect/articles/sebek-3-tracking-attackers-part-one. [Accessed Dec 2014].

[35] Edward Balas, Gregory Travis and Camilo Viecco, "A dynamic filtering technique for Sebek system monitoring," in *Workshop on Information Assurance United States Military Academy, IEEE,* NY, 2006.

[36] Balas, Edward, and Camilo Viecco, "Towards a third generation data capture architecture for honeynets," in *6th Information Assurance Workshop, IEEE,* Jun 2005.

[37] T. Honeynet, "A Brief Introduction to Qebek," Honeynet, [Online]. Available: https://projects.honeynet.org/sebek/wiki/Qebek.

[38] Sochor, Tomas, and Matej Zuzcak, "Study of internet threats and attack methods using honeypots and honeynets," *Computer Networks. Springer International Publishing,* pp. 118-127, 2014.

[39] Sysdig, "A New System Troubleshooting Tool Built for the Way You Work," [Online]. Available: http://www.sysdig.org/. [Accessed Dec 2014].

[40] Ntop, "High-speed packet capture, filtering and analysis," [Online]. Available: http://www.ntop.org/products/pf_ring/. [Accessed Nov 2014].

[41] Parkhill, Douglas F. , *The challenge of the computer utility.,* AddisonWesley, p. 206, 1966.

[42] Amazon, "Amazon Cloud EC2," [Online]. Available: http://aws.amazon.com/ec2/. [Accessed 08 Jul 2014].

[43] P. M. a. T. Grance, "The NIST Definition of Cloud Computing," *NIST Special Publication,* p. 7, 2011.

[44] Neidecker-Lutz, K. Jeffery and B., "The Future Of Cloud Computing Oppprtunities For European Cloud Computing Beyond 2010," 2010.

[45] "RackSpace," [Online]. Available: http://www.rackspace.com. [Accessed 24 March 2014].

[46] "Microsoft Windows Azure," [Online]. Available: www.microsoft.com/azure. [Accessed 4 aug 2014].

[47] "Google App Engine," Google, [Online]. Available: http://code.google.com/appengine. [Accessed 08 feb 2014].

[48] "SalesForce.com," [Online]. Available: www.salesforce.com. [Accessed 5 aug 2014].

[49] I. Foster, "What is The Grid? A Three Point Checklist," 2002. [Online]. Available: http://dlib.cs.odu.edu/WhatIsTheGrid.pdf. [Accessed 15 aug 2014].

[50] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindne, "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Computer Communication Review," vol. 39, pp. 50-55, 2009.

[51] R. Goldberg, "Survey of Virtual Machine Research," *IEEE Computer,* vol. 7, no. 6, p. 34–45, 1974.

[52] Wes Felter, Alexandre Ferreira, Ram Rajamony, Juan Rubio, "An Updated Performance Comparison of Virtual Machines and Linux Containers," *IBM*, 2014.

[53] S. Soltesz, H. P¨otzl, M. E. Fiuczynski, A. Bavier, and L. Peter son, "Container-based operating system virtualization A scalable, high-performance alternative to hypervisors," *In Proceedings of the 2nd ACM SIGOPS/EuroSys European Conference on Computer Systems*, p. 275–287, 2007.

[54] R. Pike, D. Presotto, K. Thompson, H. Trickey, and P.Winterbottom, "The Use of Name Spaces," *In Proceedings of the 5th Workshop on ACM SIGOPS European Workshop*, p. 1–5, 1992.

[55] Kivity, Avi, Yaniv Kamay, Dor Laor, Uri Lublin, "kvm: the Linux virtual machine monitor," in *Proceedings of the Linux Symposium*, 2007.

[56] Formal, G. J. Popek and R. P. Goldberg., "Formal requirements for virtualizable third generation architectures," *Commun. ACM*, p. 412–421, July 1974.

[57] Bellard, Fabrice, "QEMU, a Fast and Portable Dynamic Translator.," in *USENIX Annual Technical Conference, FREENIX Track*, 2005.

[58] R. R. Virtio, "Towards a de-facto standard for virtual I/O devices," *SIGOPS Oper. Syst*, p. 95–103, July 2008.

[59] Anderson, R. McDougall, "Virtualization performance: Perspectives and challenges ahea," *SIGOPS Oper. Syst*, p. 40–56, Dec. 2010.

[60] A. Balogh, "Google Compute Engine is now generally available with expanded OS support, transparent maintenance, and lower prices.," Google, [Online]. Available: http://googledevelopers.blogspot.com/2013/12/google-compute-engine-is-now-generally.html. [Accessed 23 aug 2014].

[61] M. Bolte, M. Sievers, G. Birkenheuer, O. Nieh¨orster, and A. Brinkmann, "Non-intrusive virtualization management using libvirt," in *European Design and Automation Association*, 2010.

[62] KVM, "Kernel Based Virtual Machine," [Online]. Available: www.linux-kvm.org. [Accessed Dec 2014].

[63] Sutton, James, David Grawrock, Richard Uhlig, "System and method for protection against untrusted system management code by redirecting a system management interrupt and creating a virtual machine container". 7 June 2002.

[64] Eucalyptus, [Online]. Available: http://www.eucalyptus.com. [Accessed 12 aug 2014].

[65] Steinmetz, Dylan, et al., "Cloud computing performance benchmarking and virtual machine launch time.," in *Proceedings of the 13th annual conference on Information technology education. ACM*,, 2012.

[66] Von Laszewski, G., Diaz, J., Wang, F., & Fox, "Comparison of Multiple Cloud Frameworks," in *IEEE Fifth International Conference on Cloud Computing*, 2012.

[67] Junjie Peng, Xuejun Zhang, Zhou Lei, Bofeng Zhang, Wu Zhang, Qing Li, "Comparison of Several Cloud Computing Platforms," *IEEE International Symposium on Information Science and Engineering*, 2009.

[68] opennebula.org, "Architectural Overview , Planning the Installation," opennebula, [Online]. Available: http://archives.opennebula.org/documentation:rel4.4:plan.

[Accessed Dec 2014].

[69] Xiaolong Wen, Genqiang Gu, Qingchun Li, Yun Gao, Xuejie Zhang, "Comparison of Open-Source Cloud Management Platforms: OpenStack and OpenNebula," in *IEEE, International Conference on Fuzzy Systems and Knowledge Discovery*, 2012.

[70] "CloudStack," [Online]. Available: http://incubator.apache.org/cloudstack. [Accessed 13 aug 2014].

[71] "Openstack Conceptual architecture," Openstack, [Online]. Available: http://docs.openstack.org/admin-guide-cloud/content/conceptual-architecture.html. [Accessed Oct 2014].

[72] Xiaolong Wen1, Genqiang Gu1, Qingchun Li1, Yun Gao1,2, Xuejie Zhang1,2,*, "Comparison of Open-Source Cloud Management Platforms: OpenStack and opennebula," in *International Conference on Fuzzy Systems and Knowledge Discovery, IEEE*, 2012.

[73] "Openstack components," [Online]. Available: http://docs.openstack.org/training-guides/content/operator-getting-started.html. [Accessed Dec 2014].

[74] Numbus. [Online]. Available: http://www.nimbusproject.org.

[75] N. Compute. [Online]. Available: http://nova.OpenStack.org/runnova/index.html.

[76] "Open Cloud Computing Interface," [Online]. Available: http://occi-wg.org.

[77] "Open Grid Forum," [Online]. Available: http://www.ogf.org/.

[78] "Quantum NEC OpenFlow Plugin," [Online]. Available: http://wiki.openstack.org.

[79] "Open vSwitch," [Online]. Available: http://openvswitch.org/.

[80] M. Sqalli, R. AlShaikh and E. Ahmed, "Towards Simulating a Virtual Distributed Honeynet at KFUPM: A Case Study," in *UKSim 4th European Modelling Symposium on Computer Modelling and Simulation*, 2010.

[81] R. McGrew, "Experiences with Honeypot Systems: Development, Deployment, and Analysis," in *Proceedings of the 39th Annual Hawaii International Conference*, 2006.

[82] S. Brown, R. Lam, S. Prasad, S. Ramasubramanian, a, "Honeypots in the Cloud," in *University of Wisconsin - Madison Student Project*, 2012.

[83] Sebastian Biedermann ,Martin Mink ,Stefan Katzenbeisser, "Fast Dynamic Extracted Honeypots in Cloud Computing," in *CCSW'12*, Raleigh, North Carolina, USA., October 19.

[84] B. Borisaniya, A. Patel, D. R. Patel and H. Patel, "Incorporating Honeypot for Intrusion Detection in Cloud Infrastructure," *International Journal of Information Security*, 2012.

[85] M Balamurugan, B Sri Chitra Poornima, "Honeypot as a Service in Cloud," in *International Conference on Web Services Computing (ICWSC)*, 2011.

[86] Nithin Chandra S.R, Madhuri T.M, "Cloud Security using Honeypot Systems," *International Journal of Scientific & Engineering Research*, vol. 3, no. 3, 2012.

[87] "Definition of Crime scene investigation," [Online]. Available: http://www.medicinenet.com/script/main/art.asp?articlekey=23306. [Accessed

Dec 2014].

[88] "What Is a Crime Scene?," [Online]. Available: http://www.wisegeek.com/what-is-a-crime-scene.htm. [Accessed Nov 2014].

[89] "Law enforcement and prosecution," Toolkit to Combat Trafficking in Persons.

[90] Wen, X., Gu, G., Li, Q., Gao, Y., & Zhang, X., "Comparison of open-source cloud management platforms: OpenStack and OpenNebula," in *Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on. IEEE*, 2012.

[91] Landmann, R., Cantrell, D., De Goede, "Red Hat Enterprise Linux 6 Installation Guide," 2010.

[92] D. Ocean, "Digital Ocean," VPS, [Online]. Available: http://digitalocean.com.

[93] Sysdig, "Sysdig," Draios Inc, [Online]. Available: http://www.sysdig.org/. [Accessed 2015].

[94] Sebek, "Honeynet Project," [Online]. Available: https://projects.honeynet.org/sebek.

[95] qemu, Openstack, "HypervisorSupportMatrix," openstack, [Online]. Available: https://wiki.openstack.org/wiki/HypervisorSupportMatrix. [Accessed 2014].

[96] Virtio, "Virtio," Libvirt, [Online]. Available: http://wiki.libvirt.org/page/Virtio.

[97] Virtio-win, "FedoraProject," Fedora, [Online]. Available: http://alt.fedoraproject.org/pub/alt/virtio-win/latest/images/bin/.

[98] S. documentation, "Honeynet," [Online]. Available: http://old.honeynet.org/papers/sebek.pdf. [Accessed 24 aug 2014].

[99] Birkin, Luke, "Intrusion Detection Using Honeynets," Engineering Project Submitted as Part Requirement for B. Eng (Hons). Diss. Massey University, Palmerston North, 2010.

[100] Xavier, Miguel G, "Performance evaluation of container-based virtualization for high performance computing environments.," in *Parallel, Distributed and Network-Based Processing (PDP), 2013 21st Euromicro International Conference on. IEEE,*, 2013.

[101] Wade, Susan Marie, "SCADA Honeynets: The attractiveness of honeypots as critical infrastructure security tools for the detection and analysis of advanced threats," Digital Repository @ Iowa State University, 2011.

[102] "Neutron," Openstack, [Online]. Available: https://wiki.openstack.org/wiki/Neutron.

[103] DigitalOcean, "DigitalOcean Service price," [Online]. Available: https://www.digitalocean.com/pricing/. [Accessed Dec 2014].