UNIVERSITI PUTRA MALAYSIA

DESIGN OF A LIGHTWEIGHT VIRTUAL HONEYNET BASED ON LINUX CONTAINER VIRTUALIZATION

NOGOL MEMARI

FK 2014 100

DESIGN OF A LIGHTWEIGHT VIRTUAL HONEYNET BASED ON LINUX CONTAINER VIRTUALIZATION

By

NOGOL MEMARI

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

November 2014

DEDICATION

This thesis is dedicated to

ALL I LOVE

Specially

My Beloved Family

And

My Friends

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

DESIGN OF A LIGHTWEIGHT VIRTUAL HONEYNET BASED ON LINUX CONTAINER VIRTUALIZATION

By

NOGOL MEMARI

November 2014

Chairman: **Shaiful Jahari b. Hashim, PhD**
Faculty: **Engineering**

Since the beginning of the Enterprise IT infrastructures, security remained a major concern for both the hardware vendors and software developers. Over a period of time, a number of security solutions are proposed to address the known security issues. There are many commercially available tools for securing information assets like Firewalls, IDS (Intrusion Detection Systems), IPS (Intrusion Prevention Systems), Anti-virus, etc. But they are mostly used to protect computers and networks against known/identified/reported vulnerabilities. In case of zero day attacks, things may go unidentified for quite a long time. Hence there is a need of a tool and/or solution which can be used to spy on the attacker, slowing them down and possibly deceiving them. Honeynets and related technologies exactly promise to do so.

Honeynets generally are decoys created to lure hackers and are closely monitored within a network to have a trail of attacks and to provide necessary alerts. It is intentionally designed insecurely and serves as an electronic bait to study the behavior of adversaries or protect an organization against Internet threats. Due to these characteristics, a honeynet complements traditional, more defense oriented solutions such as firewalls or intrusion detection systems. honeynet is an expandable system hence the cost associated with creating and maintaining it must be minimized. In this thesis single server hardware is being used as platform for inexpensive honeynet emulating as section of campus or corporate network with container based honeynet supporting both low-interaction and high-interaction honeypots .Virtualization is the key to increase the performance of honeynet for emulating large networks, by minimizing the hardware resources required. Virtual honeynet is implemented in this thesis as it provides ease of further deployment and configuration as the whole honeynet is encapsulate in a virtual environment.

In this thesis, some virtualized honeynet platform is created using the different virtualization methods and then compared with each other to determine the minimum hardware requirements and suitability of each of these virtualization methods for use in deploying our honeynet to protect computer infrastructure of any organization including factories, educational and research oriented. Although all the virtualization methods showed promising results, LXC came out as the most viable alternative to other virtualization methods as it proved the most stable, required the least amount of resources and was able to run almost five times the nodes that other virtualization methods were capable of running. The light weight container based virtual honeynet is then implemented and deployed in a real network environment exposed to the internet. It is proven to be capable of detecting and alerting attacks on the network with minimum hardware resources.

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

REKABENTUK HONEYNET MAYA RINGAN BEBANAN BERASASKAN KEMAYAAN KONTENA LINUX

Oleh

NOGOL MEMARI

November 2014

Pengerusi: Shaiful Jahari b. Hashim, PhD
Fakulti: Kejuruteraan

Sejak bermulanya perusahaan infrastruktur IT, keselamatan menjadi perhatian utama bagi kedua-dua penjual perkakasan dan pembangun perisian. Dari semasa ke semasa, beberapa penyelesaian keselamatan telah dicadangkan untuk menangani isu-isu keselamatan tersebut. Terdapat banyak peralatan yang boleh didapati secara komersial untuk melindungi aset-aset maklumat seperti Tembok Api, IDS (Sistem Pengesanan Pencerobohan), IPS (Sistem Pencegahan Pencerobohan), Anti-virus, dan lain-lain. Tetapi kebanyakannya digunakan untuk melindungi komputer-komputer dan rangkaian-rangkaian terhadap ancaman-ancaman yang telah diketahui/dikenalpasti/dilaporkan. Dalam kes serangan hari sifar, ianya boleh berlanjutan tanpa dikenalpasti untuk jangkamasa yang lama. Oleh itu terdapat keperluan akan sebuah alat dan/atau penyelesaian yang boleh digunakan untuk mengintip penyerang, memperlahankan urusan mereka dan mungkin juga memperdayakan mereka. Rangkaian madu dan teknologi berkaitan benar-benar menjanjikan untuk berbuat demikian.

Honeynets secara umumnya adalah umpan-umpan yang dicipta untuk memikat penggodam-penggodam dan dipantau secara rapi dalam sesebuah rangkaian untuk mendapatkan jejak-jejak serangan dan mengeluarkan amaran sekiranya perlu. Ianya sengaja direka dalam keadaan tidak selamat dan berfungsi sebagai umpan elektronik untuk mengkaji tingkah laku penyerang atau melindungi sesebuah organisasi daripada ancaman Internet. Dengan ciri-ciri ini, sesebuah honeynet melengkapi penyelesaian yang lebih berorientasikan bertahan dan tradisional, sepertimana tembok api atau sistem pengesanan pencerobohan. Honeynet adalah sebuah sistem boleh kembang, dengan itu kos yang berkaitan dengan mewujudkan dan mengekalkannya mesti dikurangkan. Dalam tesis ini, perkakasan pelayan tunggal telah digunakan sebagai platform untuk honeynet murah meniru seksyen sesebuah kampus atau rangkaian korporat dengan honeynet berasaskan kontena menyokong kedua-dua honeypots interaksi-rendah dan interaksi-tinggi. Kemayaan adalah kunci untuk meningkatkan prestasi honeynet dalam meniru rangkaian-rangkaian yang besar, dengan meminimumkan sumber-sumber perkakasan yang diperlukan. Honeynet maya telah dilaksanakan di dalam tesis ini kerana ianya menyediakan kemudahan penggunaan dan konfigurasi lanjutan kerana keseluruhan honeynet adalah terkapsul di dalam sebuah persekitaran maya.

Dalam tesis ini, beberapa platform honeynet maya telah diwujudkan dengan menggunakan kaedah kemayaan yang berbeza dan kemudiannya dibandingkan antara satu sama lain dalam menentukan keperluan perkakasan yang minimum dan kesesuaian setiap kaedah kemayaan yang digunakan dalam menggerakkan honeynet kami untuk melindungi infrastruktur komputer bagi mana-mana organisasi termasuk kilang-kilang, berorientasikan pendidikan dan penyelidikan. Walaupun semua kaedah kemayaan menunjukkan hasil yang memberangsangkan, LXC muncul sebagai alternatif yang paling berdaya maju berbanding kaedah kemayaan lain kerana ia terbukti sebagai yang paling stabil, memerlukan jumlah sumber yang paling kecil dan mampu menjalankan hampir lima kali ganda jumlah nod-nod yang kaedah kemayaan lain mampu laksanakan. Honeynet maya berasaskan kontena ringan bebanan tersebut telah dilaksanakan dan digunakan dalam persekitaran rangkaian sebenar yang terdedah kepada internet. Ia terbukti untuk mampu mengesan dan memberi amaran berhubung serangan-serangan ke atas rangkaian dengan sumber-sumber perkakasan yang minimum.

ACKNOWLEDGEMENTS

First of all I would like express my deepest thanks to my supervisor, Shaiful Jahari b. Hashim, for his sincerity, patience and support. I am really grateful for all the things he has done for me. God bless him and his family.

As for my co-supervisor, Khairulmizam b. Samsudin, who helped me a lot in the all aspects of my research including the guidance on the methods and helping in evaluation of my work, Thank you. God bless him and his family.

At the end I thank my family and friends for their continuing support and believe.

Nogol Memari

I certify that a Thesis Examination Committee has met on 11November 2014 to conduct the final examination of Nogol Memari on her thesis entitled “Design of a Lightweight Virtual Honeynet Based on Linux Container Virtualization” in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Siti Barirah Binti Ahmad Anas, PhD
Senior lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Fazirulhisyam Hashim, PhD
Senior lecturer
Faculty of EngineeringUniversiti Putra Malaysia
(Internal Examiner)

Wan Azizun Binti Wan Adnan, PhD
Senior lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Suhaidi Hassan, PhD
Professor
Faculty of computing
Universiti Utara Malaysia
(External Examiner)

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

Date: 23 January 2015

This thesis submitted to the Senate of Universiti 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 b. Hashim, PhD
Senior lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Khairulmizam b. Samsudin, PhD
Senior lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

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

Date:

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.: Nogol Memari (GS30954)

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this 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 b. Hashim, PhD**

Signature:
Name of
Member of
Supervisory
Committee: **Khairulmizam b. Samsudin, PhD**

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DDoS	Distributed Denial of Service
DNS	Domain Name Server
FTP	File Transfer Protocol
HD	Hard Disk
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IIS	Internet Information Services
IP	Internet Protocol
IPS	Intrusion Prevention System
IRC	Internet Relay Chat
ISP	Internet Service Provider
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
LCD	Liquid Crystal Display
LXC	Linux Containers
MAC	Media Access Control
NIC	Network Interface Card
OpenVZ	Open Virtualization
OS	Operating System
PC	Personal Computer
PCAP	Packet Capture
SQL	Structured Query language
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
SYSLOG	System Logging
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VM	Virtual Machine

CHAPTER 1

INTRODUCTION

Traditionally, the protection of information security has been primarily based on defensive approaches such as Intrusion Detection Systems (IDS), Data Encryption and Firewall. This strategy is based on the notion of defending the network and computer systems by detecting any failures in the defense and then reacting to those failures by reinforcing the compromised firewall and IDS systems. These systems cannot protect the network effectively as the enemy has the initiative as this approach is based purely on defensive strategies. In order to overcome this limitation, researchers turned to a new method called honeynet. Honeynet take the fight to the intruders by interacting with them by emulating real systems while gathering information about their tactics, tools and attack pattern. The gathered intelligence data and information is then used by the security personnel to harden the system against future attacks.

Since honeynet does not add to the productivity of the information system, it is better to minimize the expense on creating and maintaining it. In order to reduce the resource dependency, honeynet usually leverage on the enhancements offered by virtualization technologies. A honeynet based on virtual machines can offer great value in terms of hardware utilization and ease of deployment. As opposed to standalone honeypot, honeynet can emulate an entire network of computer systems inside a campus or a company network. Honeynet is designed for the purpose of being attacked hence it is expendable from the company perspective. The goal is to create an emulation system with a highly controlled network of computers and nodes, where all activities are controlled, monitored and captured.

Concept of virtualization and virtual machines was developed by IBM to provide resource sharing between users as acquisition and maintaining multiple powerful mainframe computers was not an option for many organizations. Virtualization enabled running of multiple different operating systems and the use of multiple users within a single computer. For the purpose of implementing a honeynet consisting of large numbers of simulated services and virtual machines, and to control the system automatically and effectively, a reliable visualization technique is required. The fact that the virtual honeynet is contained within a single virtual machine makes deployment and maintenance of honeynet much easier as without virtualization many parameters of honeynet must be manually adjusted many times during deployment.

1.1. Problem Statement

As network security is a prominent concern the current situation of security demands more active measures in order to successfully fight computer crime. For this reason, one needs to study and analyze the tools, utilized to compromise vulnerable systems on the Internet by today‘s cyber criminals. The operation of electronic decoys, so called honeynets, greatly supports this process. Equipped with special logging facilities, honeypots pretend to be a vulnerable target, thus luring an attacker into the trap, the collected information can be used to further strengthen defensive measures.

For the purpose of implementing a large scale honeynet consisting of large numbers of simulated services and virtual machines, and to control the system effectively, a reliable visualization technique is required. Although many virtualization methods exist, their ability and suitability in deploying a large scale honeynet effectively and more importantly reliably must be put to the test. A reliable virtualization approach can decrease the time and efforts required to setup and maintain a honeynet dramatically while enabling the organization deploying the honeynet to increase the number of required nodes and change the configuration of the honeynet within the least required time frame. Furthermore, the honeynet platform is expandable hence minimum hardware resources and setup is desirable. Two types of virtualization methods namely full system virtualization and container based virtualization were examined. VMware, Virtual Box and KVM from full system virtualization and LXC From container based virtualization were compared to achieve the most reliable virtualization approach among the other solutions.

1.1.Research Aim and Objectives

This thesis intends to develop an improved light weight virtual honeynet for increasing the security of the network while deployed with LXC based virtualization platform for decreased hardware requirements and increased reliability. The objectives of the thesis are as follows:

i) To evaluate performance of different virtualization methods to determine the suitable and light weight virtualization solution for deploying virtual honeynet.
ii) To design and implement virtual honeynet.
iii) To monitor and analyze attacks on honeynet while connected to public internet.

1.2.Scope of the study

For this study HP ProLiant DL160 server running Ubuntu 12.04.2 LTS with 4GB of memory and an Intel Xeon L5630 @ 2.13 GHz CPU connected to the internal network of the university was used.

The designed honeynet is based on typical layout of a lab inside UPM; the same honeynet is deployed on the most popular virtualization methods to evaluate the performance. Evaluation of the performance of each virtual machine is done by industry accepted Geekbench and Unixbench solutions, each of these solutions is run eight times and the results are combined to provide the final performance figure.

From the evaluation results it was clear that container based virtualization provided the best blend of reliability, hardware requirements and speed. The designed honeynet was then connected to internet for evaluation.

A public IP address provided by the university was used to evaluate the performance of the honeynet. Honeynet was placed before the firewalls of the University for Undisrupted Access from outside, and was online for a period of slightly more than two weeks (15 days). During this time more than a million probes scanned our honeynet while more than 32,000 attacks were carried out against the deployed honeynet.

To deploy the mentioned honeynet, devices and services that used in experiment are listed in below:

Host machine:
- HP ProLiant DL160 server
- Processors: 8-cores Intel Xeon L5630 @ 2.13 GHz
- RAM: 4GB
- Hard disk: 300GB
- 2 network interface card
- Running Ubuntu 12.04 LTS

Virtualization solution used in this study is summarized as:
- LXC (Linux container)
- Each LXC runs Ubuntu 12.04 LTS

Low-interaction honeypots:
- Benefits from Honeyd 1.5c emulator
- Honeyd is running on separate LXC virtualization solution

Operating systems emulated are as:
Microsoft Windows 7, Microsoft Windows XP sp3

High-Interaction honeypots:
Benefits from LXC virtualization solution Software and Demons were used in High-interactions are:
- MySQL
- PHP
- Apache2
- phpMyAdmin
- Nmap

1.3.Contribution of Thesis

In this thesis a light weight virtual honeynet is introduced. The framework proposed can handle large amounts of honeypots for deployment inside the honeynet. The best virtualization method is determined by comparing latest virtualization methods while running the same honeynet with the same configuration. These virtualization methods are then tested to their limits and then pitted against each other. Evaluation of the performance of each virtual machine is done by industry accepted Geekbench and Unixbench solutions, each of these solutions is run multiple times and the results are combined to provide the final performance figure. From the results container based virtualization was chosen for the deployment of light weight virtual honeynet. As the deployed honeynet is contained within single server hardware in addition to Honeywall gateway, it makes it easy to deploy and configure honeypots while reducing the time required to setup the network as additional nodes can be added much more quickly.

1.4.Outline of Thesis

The organization of the remaining chapter of thesis is as follows:

Chapter 2 acquaintances the reader with different concepts in internet/network security while introducing different approaches in building a honeynet. On the second part of the chapter different virtualization methods are introduced and discussed.

Chapter 3 deals with the methodology behind the developed framework and discusses the main ideas and theories relevant to implementation of the different approaches to the virtual honeynet. Steps involved with implementing virtual honeyet are discussed and the reader is introduced to the methods utilized to monitor the data gathered from the honeynet.

Chapter 4 deals with evaluation of the obtained data and highlights the performance figure of different virtualization methods. On the second part of these chapter different attacks gathered by the deployed honeynet is discussed.

Chapter 5 summarizes the implementation and discusses the obtained performance figures and attack patterns while discussing possible future enhancements and usability in the field of internet/network security.

REFERENCES

Abbasi, F. H., & Harris, R. J. (2009, November). Experiences with a Generation III virtual honeynet. In Telecommunication Networks and Applications Conference (ATNAC), 2009 Australasian (pp. 1-6). IEEE.

Albin, E. (2011). A comparative analysis of the snort and suricata intrusion-detection systems (Doctoral dissertation, Monterey, California. Naval Postgraduate School).

Awad, J., & Derdmezis, A. Implementation of a high interaction honeynet testbed for educational and research purposes. 2005. URL: http://www. aitdspace. gr/xmlui/handle/123456789/245 (4th March, 2012).

Bao, J., Ji, C. P., & Gao, M. (2010, October). Research on network security of defense based on honeypot. In Computer Application and System Modeling (ICCASM), 2010 International Conference on (Vol. 10, pp. V10-299). IEEE.

Benzel, T., Braden, B., Faber, T., Mirkovic, J., Schwab, S., Sollins, K., & Wroclawski, J. (2009, March). Current developments in DETER cybersecurity testbed technology. In Conference For Homeland Security, 2009. CATCH. Cybersecurity Applications & Technology IEEE (pp 57-70).

Binu, A., & Kumar, G. S. (2011). Virtualization techniques: a methodical review of XEN and KVM. In Advances in Computing and Communications (pp. 399-410). Springer Berlin Heidelberg.

Bugnion, E., Devine, S., Rosenblum, M., Sugerman, J., & Wang, E. Y. (2012). Bringing virtualization to the x86 architecture with the original vmware workstation. ACM Transactions on Computer Systems (TOCS), 30(4), 12.

Cavalca, D., & Goldoni, E. (2010). An open architecture for distributed malware collection and analysis. In Open Source Software for Digital Forensics (pp. 101-116). Springer US.

Caswell, B., & Beale, J. (2004). Snort 2.1 intrusion detection. Syngress.

Chamotra, S., Sehgal, R. K., Kamal, R., & Bhatia, J. S. (2011, April). Data diversity of a distributed honey net based malware collection system. In Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on (pp. 125-129). IEEE.

Chang, J. C., & Tsai, Y. L. (2010, October). Design of virtual honeynet collaboration system in existing security research networks. In Communications and Information Technologies (ISCIT), 2010 International Symposium on (pp. 798-803). IEEE.

Chierici, A., & Veraldi, R. (2010, April). A quantitative comparison between xen and kvm. In Journal of Physics: Conference Series (Vol. 219, No. 4, p. 042005). IOP Publishing.

Gani, A. (2012). Improving exposure of intrusion deception system through implementation of hybrid honeypot. The International Arab Journal of Information Technology, 9(5), 436-444.

Geekbench availablefrom:http://www.primatelabs.com/geekbench , Last access date: 6/6/2014.

Graziano, M., Leita, C., & Balzarotti, D. (2012, December). Towards network containment in malware analysis systems. In Proceedings of the 28th Annual Computer Security Applications Conference (pp. 339-348). ACM.

Gurav, U., & Shaikh, R. (2010, February). Virtualization: a key feature of cloud computing. In Proceedings of the International Conference and Workshop on Emerging Trends in Technology (pp. 227-229). ACM.

Hatt, N., Sivitz, A., & Kuperman, B. A. (2007, November). Benchmarking Operating Systems. Conference for Undergraduate Research in Computer Science and Mathematics.

Honeyd Website availablefrom: http://www. honeyd. Org,Last access date: 6/6/2014.

honeynet available from: www.honeynet.org ,Last access date: 6/6/2014.

Hunter, S. O. (2010). Virtual honeypots: Management, attack analysis and democracy.

IP location availablefrom: http://www.ipligence.com/iplocation ,Last access date: 6/6/2014.

Joshi, R. C., & Sardana, A. (2011). honeypots: A New Paradigm to Information Security. Science Publishers.

Kaur, J., Singh, G., & Singh, M. (2012). Design & Implementation of Linux based Network Forensic System using honeynet. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1(4), pp-504.

Konovalov, A. M., Kotenko, I. V., & Shorov, A. V. (2013). Simulation-based study of botnets and defense mechanisms against them. Journal of Computer and Systems Sciences International, 52(1), 43-65.

KVM availablefrom: http://www.linux-kvm.org/page/Main_Page, Last access date: 6/6/2014.

Li, P. (2010). Selecting and using virtualization solutions: our experiences with VMware and VirtualBox. Journal of Computing Sciences in Colleges, 25(3), 11-17.

Li, Z., Goyal, A., & Chen, Y. (2008). honeynet-based botnet scan traffic analysis. In Botnet Detection (pp. 25-44). Springer US.

Liao, Y. (2011). EXAMINING EFFECTS OF VIRTUAL MACHINE SETTINGS ON VOICE OVER INTERNET PROTOCOL IN A PRIVATE CLOUD ENVIRONMENT _ A dissertation Presented to (Doctoral dissertation, Indiana State University).

Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2010). Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Wiley Publishing.

Linux Container availablefrom:https: http://linuxcontainers.org, Last access date: 6/6/2014.

Liu, X., Peng, L., & Li, C. (2011). The dynamic honeypot design and implementation based on Honeyd. In Advances in Computer Science, Environment, Ecoinformatics, and Education (pp. 93-98). Springer Berlin Heidelberg.

Loglady availablefrom:http://www.kaska.demon.co.uk/loglady.htm,Last access date: 6/6/2014.

LXC availablefrom:http://lxc.sourceforge.net,Last access date: 6/6/2014.

Marchese, M., Surlinelli, R., & Zappatore, S. (2011). Monitoring unauthorized internet accesses through a ‘honeypot’system. International Journal of Communication Systems, 24(1), 75-93.

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53.

Mokube, I., & Adams, M. (2007, March). honeypots: concepts, approaches, and challenges. In Proceedings of the 45th annual southeast regional conference (pp. 321-326). ACM.

Most vulnerable systems availablefrom:http://www.zdnet.com/2013-most-vulnerable-systems-and-software-its-not-just-internet-explorer-7000025924/ Last access date: 6/6/2014.

Musca, C., Mirica, E., & Deaconescu, R. (2013, May). Detecting and Analyzing Zero-Day Attacks Using honeypots. In Control Systems and Computer Science (CSCS), 2013 19th International Conference on (pp. 543-548). IEEE.

Nikkhahan, B., Aghdam, A. J., & Sohrabi, S. (2009). E-government security: A honeynet approach. E-government, 5.

Open SSH availablefrom:http://www.openssh.com/,Last access date: 6/6/2014.

Pelletingeas, C. (2010). Performance evaluation of virtualization with cloud computing (Doctoral dissertation, Edinburgh Napier University).

Philippine honeynet Project. Available from: http://www.philippinehoneynet.org/ , Last access date: 6/6/2014.

Provos, N., & Holz, T. (2007). Virtual honeypots: from botnet tracking to intrusion detection. Pearson Education.

Provos, N. (2003, February). Honeyd-a virtual honeypot daemon. In 10th DFN-CERT Workshop, Hamburg, Germany (Vol. 2).

Qassrawi, M. T., & Hongli, Z. (2010, April). Deception methodology in virtual honeypots. In Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on (Vol. 2, pp. 462-467). IEEE.

Rate of cyber-attacks available from: http://media.kaspersky.com/pdf/KSB_2013_EN.pdf , Last access date: 6/6/2014.

Rose, R. (2004). Survey of system virtualization techniques.

Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., & Sommerlad, P. (2013). Security Patterns: Integrating security and systems engineering. John Wiley & Sons.

Singh, A. N., & Joshi, R. X. (2011, July). A honeypot system for efficient capture and analysis of network attack traffic. In Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on (pp. 514-519). IEEE.

Snort availablefrom: http://www.snort.org/,Last access date: 6/6/2014.

Tang, Y., & Li, J. P. (2010, December). VON/KVM: A high performance virtual overlay network integrated with KVM. In Apperceiving Computing and Intelligence Analysis (ICACIA), 2010 International Conference on (pp. 129-132). IEEE.

Terzo, O., & Vipiana, F. (2012). Grid Infrastructure for Domain Decomposition Methods in Computational ElectroMagnetics.

Unixbench availablefrom:http://code.google.com/p/byte-unixbench , Last access date: 6/6/2014.

Vacca, J. R. (2012). Computer and information security handbook. Newnes.

Virtualbox availablefrom:https://www.virtualbox.org , Last access date: 6/6/2014.

Vmware availablefrom:ttp://www.vmware.com/company/news/release/vmw-workstation,Last access date: 6/6/2014.

Vrable, M., Ma, J., Chen, J., Moore, D., Vandekieft, E., Snoeren, A. C., ... & Savage, S. (2005). Scalability, fidelity, and containment in the potemkin virtual honeyfarm. ACM SIGOPS Operating Systems Review, 39(5), 148-162.

Wang, J., & Zeng, J. (2011). Construction of large-scale honeynet Based on Honeyd. Procedia Engineering, 15, 3260-3264.

Watson, D., & Riden, J. (2008, April). The honeynet project: Data collection tools, infrastructure, archives and analysis. In WOMBAT Workshop on Information Security Threats Data Collection and Sharing (pp. 24-30).

Whitman, M., & Mattord, H. (2011). Principles of information security. Cengage Learning.

Wireshark availablefrom:http://www.wireshark.org/,Last access date: 6/6/2014.

Xavier, M. G., Neves, M. V., Rossi, F. D., Ferreto, T. C., Lange, T., & De Rose, C. A. (2013, February). 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 (pp. 233-240). IEEE.

Xu, J., Zhang, J., Gadipalli, T., Yaun, X., & Yu, H. (2011). Learning Snort rules by capturing intrusions in live network traffic replay. Proc. 15th Colloquim for Information Systems Security Education, 145-150.

Yegneswaran, V., Barford, P., & Paxson, V. (2005). Using honeynets for internet situational awareness. In Proc. of ACM Hotnets IV.

Yeh, C. H., & Yang, C. H. (2008, June). Design and implementation of honeypot systems based on open-source software. In Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on (pp. 265-266). IEEE.

Zakaria, W. Z. A., Ahmad, S. R., & Aziz, N. A. (2008, August). Deploying virtual honeypots on virtual machine monitor. In Information Technology, 2008. ITSim 2008. International Symposium on (Vol. 4, pp. 1-5). IEEE.

Zhuge, J., Holz, T., Han, X., Song, C., & Zou, W. (2007). Collecting autonomous spreading malware using high-interaction honeypots. In Information and Communications Security (pp. 438-451). Springer Berlin Heidelberg.