Honours Project (MHG405293)

Final Report

Student DD

Matriculation No: S091xxxx

BSc (Hons) Computer Networking and Systems Support

Supervisor: Professor Huaglory Tianfield

Second Marker: Dr Richard Foley

"Creating a Eucalyptus Cloud Computing Environment and Evaluating the Ability of the Snort Intrusion Detection System to Detect Denial of Service Attacks Within It"

Except where explicitly stated, all work is my own

Signed:

Date:

ABSTRACT

Cloud computing is a relatively new concept in the field of Information Technology. A widely used term to describe it is 'Utility Computing.' Cloud computing involves the provision of computing services to users in an 'elastic' manner – by as little or as much as is required with the user paying only for what has been used. This model removes the overheads that businesses have previously been burdened with when responsible for their own computing infrastructure. What may at first seem the perfect answer to a difficult problem has however shown that it has weaknesses of its own. Globally publicised incidents regarding security breaches within cloud environments have occurred in the last few years which have seriously affected consumer confidence in what the cloud has to offer. Users considering the uptake of these services need to know that their data is secure within the cloud.

This project investigated and evaluated open source technologies developed for creating cloud computing platforms. It looked at Intrusion Detection System (IDS) which are part of the solution to securing these platforms. The role of the Intrusion Detection System is to perform data packet inspection on the cloud network and produce alerts when it detects attacks. After evaluating several IDS, one was selected to be tested upon the cloud framework, this IDS was Snort.

An experiment was developed to assess the detection capability of Snort within a Ubuntu Enterprise Cloud framework. Snort was placed within the framework and analysed traffic. A series of malicious attacks were launched towards the cloud framework and the results analysed for detection capabilities. The results of the experiment produced very accurate detection rates by Snort and proved that it can be reliable in the task of making a cloud secure.

ACKNOWLEDGEMENTS

I would like to thank Professor Tianfield for the help and guidance that he has given to me

I would like to thank Dr Foley for his clear guidance throughout the duration of this module

Thank you to my daughter, husband and friends whose support and patience I appreciate.

Contents

1.0 INTRODUCTION

1.1 BACKGROUND

1.1.1 The Emergence of Cloud Computing

Until recently, businesses used a standard approach when implementing new IT infrastructure. It consisted of investing in the necessary hardware and software required, hiring the appropriate staff needed, constructing their own private network and maintaining it themselves. There are however drawbacks to this implementation method. These can range from high costs for equipment and staff - to under-utilisation of the equipment purchased. In certain scenarios, equipment which may be needed to provide adequate processing power may be used only ten percent of the time. {{56 Krutz, L. R. 2010}}{{56 Krutz, L. R. 2010}}

This was a problem faced by Amazon approximately 10 years ago. They needed to have a level of computational resources that would be able to cope with their busiest business period prior to Christmas. However, this meant that the system was over provisioned and partly idle for the rest of the year. In an effort to transfer costs associated with this plan, Amazon rented their system resources out to other enterprises that required extra computing facilities during the time that Amazon did not i.e. January to November. The companies who took advantage of this service gained access to a reliable, secure system and did not suffer the disadvantage of having to commit financially or strategically towards it, {{90 Rhoton,John. 2011}}This example is widely seen as one of the first developments of cloud computing.

Nowadays, many providers such as Google (Google App Engine) and Microsoft (Microsoft Windows Azure) offer cloud services in a variety of forms such as provisioning infrastructure, software and development platforms. Multiple organizations exist as 'tenants' on the cloud provider's infrastructure paying only for services they use within the cloud. Access to the network is rented by customers and charging is based on amount of resources consumed. Provision of resources is highly flexible – consumers can have as much or as little processing, memory or storage as is required {{88 Mell, P. 2010}} Likening it to the consumption of power, water and other utilities the term 'Utility Computing' has been coined to describe it.{{80 Anonymous}}

1.1.2 The Benefits Provided by Cloud Computing

Cloud computing practises present an attractive proposition for many businesses. Users receive a service which provides as much or as little resources as are required at any one time, {{70 Buyya,R. 2008}} This service can adapt to the consumer's needs without need to contact the provider to arrange greater or lesser resources {{2 Mell,P. 2010}} - meaning that an organisation which may require additional computational power on occasions no longer has to invest in an IT infrastructure which remains underutilised for most of the time. There is no requirement to invest in expensive equipment or the facilities to accommodate it. Commercially developed loud companies also provide year round 24hr help to support their clients. {{81 Amazon}}

1.1.3 What a Cloud Is

The part of the cloud which the majority of users would be familiar with is the launching and use of 'instances.' Instances are virtual computers that are created from image templates which are already stored upon the cloud network. A network administrator would typically customise image templates with the processing capabilities, operating system and applications required for specific users within the business – for example, an image specifically tailored with accounting software and appropriate processing power for use by Finance Department staff. Staff then access these instances via a web interface and once launched the instance appears and acts no different from that of a typical business local area network PC. However, any data saved or stored upon the instance will be placed upon the cloud storage and not on the PC itself – just like the operating system and the applications already are. This adds a high degree of flexibility for users meaning that they can change their geographical position but still access their own personalised machine.

The technical process for sourcing such an instance is as follows:

1) Request for a virtual machine instance is sent by user using web interface
2) Virtual machine template disk is pushed to a compute node
3) The disk image is padded and packaged to the correct size needed by the Hypervisor on the compute node
4) Compute node sets up networking to provide a network addresses such as IP and MAC
5) DHCP gets set on the head node with the MAC/IP addresses
6) Instance is spawned onto the virtual machine manager

7) User can now access the virtual machine instance using a secure shell connection {{92 Sempolinski, Peter. 2010}}

1.1.4 The Structure of the Cloud

Before creating a cloud network, the hardware intended to run the system has to be assessed for suitability, likewise the operating system that is intended to run on the components. A particular need of open source cloud platforms is that they need to be flexible enough to work with a wide variety of components and applications. Commercial platforms are only required to work with the hardware that they have, {{92 Sempolinski, Peter. 2010}}

There are a number of different elements within a typical cloud environment. A hierarchical structure exists with various levels of management of other components. As an example, the cloud platform Eucalyptus has been used to illustrate the general physical structure of such an environment, however each individual open source platform has its own features which will be particular to it only.

The cloud environment consists of 5 main physical elements:

- Node Controller - the node controller runs a Hypervisor. The hypervisor manages the actual running of the virtual machines from the nodes which store the virtual machines. Liaises with the cluster controller regarding the operational state of nodes
- Cluster Controller - the cluster controller manages the Node Controllers. Liaises between the Cloud Controller and the Node Controllers – it receives requests from the cloud controller for instances and relays these to the node controller. Also providing networking services for the virtual instances such as IP and MAC addressing.
- Walrus Storage – particular to Eucalyptus based platforms, stores the machine images and snapshots for the cloud network.
- Storage Controller – provides storage for the instances running on the cloud to use.
- Cloud Controller – the overall cloud management system. Provides the web interface to users to facilitate requesting instances. Provides the network/cloud administrator with interfaces (graphical & command line) to manage the cloud infrastructure. Monitors and maintains data regarding usage and availability of resources in the cloud and the overall state of the cloud network {{110 Anonymous}}

To illustrate how these elements fit together, a diagram of a generic cloud structure is provided on the following page:

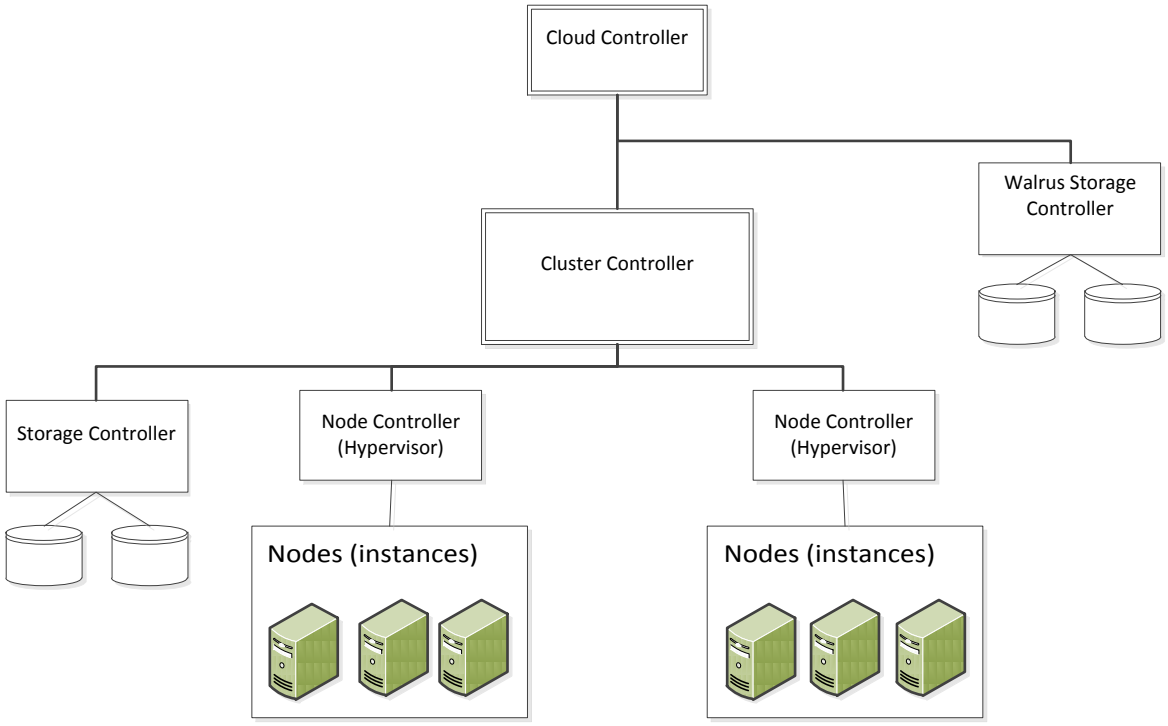


Figure 1 - physical structure of a cloud

1.1.5 Security Concerns Surrounding Cloud Computing

Cloud computing could be seen as the perfect solution to an organisation's information needs, however, there are drawbacks to be considered. The structure of the cloud, where more than one consumer is sharing the same resources can present considerable security risks to its users. {{63 Ristenpart, T. 2009}} This has led to a lack of confidence amongst potential customers {{16 Subashini,S. 2011}} Security is a concern commonly discussed in cloud computing literature Three main areas of concern exist: attacks upon the cloud launched from the internet, attacks upon a client launched from another client and an insider attack launched from an employee of the cloud company {{18 Barbour,Tracy 2011}} . Although cloud providers are constrained by laws such as the Data Protection Act, {{97 Information Commissioners Office 2011}},the onus is on the user to ensure that the cloud provider they choose is competent at managing security on their network.

Recently, the subject of information security has gained more and more of a high profile in the media. Industrial espionage may be the main concern for businesses; however the use of malicious attacks has escalated so much nowadays that even government intelligence agencies are attacking each other's resources and opening up new battle fronts - leading to the term "cyber-warfare." {{20 Corera, Gordon}}This highlights the seriousness of the situation how vital it is to know just exactly how business computing assets and resources are protected.

1.1.6 Intrusion Detection Systems

To address the concerns and issues surrounding cloud security, a cloud provider must create a multi-faceted approach to their network security. A combination of methods is used to defend computing infrastructures against attack usually consisting of elements such as firewalls, anti-virus applications, efficient methods to maintain up to date patching, the education and training of staff and intrusion detection systems (IDS), {{56 Krutz, L. R. 2010}}

There are a number of different types of Intrusion Detection Systems, these are: network based, network behaviour analysis and host based. This report will discuss two – network based and network behaviour. Network Based IDS monitor the flow of data within a network segment and the activity of protocols for suspicious behaviour. Network Behaviour Analysis IDS examine packets on a network for suspicious behaviour and analyse traffic for behaviour which does not fall within 'typical' behaviour it has learned for that network. {{71 Balzarotti,D. 2006}} These methods should therefore be capable of identifying common attacks such as a denial of service. These can exist in many forms, for example by fragmenting packets which when reassembled at their destination produce a packet too large for the receiving system to process and consequently cause a freeze or crash of the system rendering the service unavailable to users.

Three main approaches are used by IDS to detect threats. These are signature based, anomaly based and stateful protocol analysis, {{76 Mutz, D. 2005}} Most IDS use some combination of the 3.

Signature based analysis operates when the IDS compares the signatures of data traversing the network with the signatures of known threats. Accuracy standards of detection are excellent with known threats but this system is only effective when continually updated with new threat signatures that become known, {{77 Wang, Ke. 2004}}. It is however useless at detecting so far unknown threats or threats that consist of more than one event.

Anomaly based detection techniques analyse the 'habits' of the network. An accepted range of network traffic 'behaviour' is declared to it and any behaviour deviating from the 'norm,' is considered to be suspicious, {{78 Mazzarielo, C. 2010}} This type of IDS detection tends

to be successful but its success relies heavily on being given accurate profiles of network behaviour to work with in the first instance.

Stateful protocol analysis concentrates on the examining of protocol activity with the IDS being given profiles of acceptable types of protocol behaviour. As with anomaly based detection, these are very effective when configured accurately according to the protocol behaviour, but use a lot of resources. However, if an attack is staged against the network which does not deviate in terms of protocol behaviour the attack will pass thru the IDS undetected. {{17 Scarfone, Karen 2007}}

Thus, as can be seen from the previous paragraphs, IDS can detect a variety of malicious behaviour but they are not completely failsafe - three varieties of detection methods, a combination of accurately configured profiles and almost constant updating of signatures are required to compose a relatively effective mode of detection. In addition, when configuring IDS profiles for network and protocol behaviour, great care must be taken to stipulate what is considered a threat and what is not. All IDS generate alerts called false negatives and false positives. False negative occurs where a genuine threat is identified as being harmless and a false positive generates an alert where none exist{{17 Scarfone, Karen 2007}}, {{79 Owen, D.}}

This project concentrates on evaluating cloud platforms, investigating the methods used by IDS and detection rate achieved when they are faced with a Denial of Service type attack attempting to traverse the cloud network.

1.1.7 Denial of Service Attacks

Denial of Service attacks can be staged by a variety of methods. To generalise, their methods reduce or prevent legitimate access by users to the system they target. Methods used include bombarding the target system with traffic to the point that the system becomes overwhelmed and rendered unavailable to users and taking advantage of TCP/IP processes {{21 Krutz, Ronald 2007}}.

An integral part of the TCP/IP process is to break down or fragment data packets when they are too large to transmit on certain media present on a network, on arrival at their destination, the packets are reassembled using flags and sequence numbers, {{82 Kurose, J. 2008}} Fragmentation attacks take advantage of this process and use packets larger than the maximum permitted size of 65,536 bytes which results in the destination host crashing when the packet is reassembled, thus rendering the system unavailable to legitimate users, {{80 Ptacek, T. 1998}}

A ‘SYN flood’ attack sends high levels of synchronisation packet requests in an attempt to establish communications with a target computer. This attack takes advantage of the TCP Handshake – a client initiates communication with a server with a TCP SYN packet, the

client receives acknowledgement of the connection request from the server and ultimately a connection is established between the two. SYN flood attacks work by triggering an acknowledgement from the server which then sets up a buffer queue for these messages until an ACK is received back from the client. If no ACK in received, as in this case, the queue starts to fill up and become overwhelmed preventing it from responding to legitimate user requests. A possibility exists that it can crash the system, {{21 Krutz, Ronald 2007}}

1.2 PROJECT OUTLINE AND RESEARCH QUESTION

1.2.2 Project Outline

Krutz & Vines, {{21 Krutz, Ronald 2007}} state that fragmenting an IP datagram to disguise the contents of TCP/IP packets and the TCP SYN flood attack are both examples of attacks which can be used to evade detection by IP filtering devices. In consideration of the stated concerns over security provision in cloud system computing, this report focuses on one aspect of the overall security features which should be operating within a cloud environment – the Intrusion Detection System – and strives to evaluate the detection abilities of an open source IDS to an attack launched upon the cloud system it is resident upon.

The reasoning behind this project is that although many different procedures can be set in place to secure a network, if an organisation must have contact outside its own cloud environment (which the vast majority must) it has to have openings (ports) in its security framework to facilitate this. These openings, although vital, present a weakness; this project tries to establish whether IDS are effective at helping to mitigate these weaknesses, {{64 Bellovin, S. 2004}}.

This project shall be an experiment which will take the form of a small open source cloud system running an open source IDS. Fragmentation type attacks will be launched at the system and data from the IDS logs examined for its ability to detect these attacks under varying conditions of operation.

1.2.3 Research Question

Taking the project outline stated previously into consideration, the following Research Question has been formed:

"Creating a Eucalyptus Cloud Computing Environment and Evaluating the Ability of the Snort Intrusion Detection System to Detect Denial of Service Attacks Within It"

1.3 AIMS AND OBJECTIVES

1.3.1 Project Aim

The aim of this project is to establish what level of intrusion detection open source applications can provide to cloud platforms, and what level of exploit, if any, can evade detection by them. This experiment will be run on a physical experimental cloud network. The logs of the IDS will be examined to deduce how many attacks are being detected when the cloud is running and an exploit gets launched towards the cloud server and the intrusion detection system itself.

1.3.2 Project Objectives

The objective of the secondary research or literature review was to obtain greater understanding of the project subject material in order to facilitate decision making towards, and the development of, the experiment, this involved:

- Investigate and evaluate a small range of open source Cloud Computing platforms. From that evaluation, decide upon the most suitable platform to be used for the experiment and justify that decision.
- Identify typical topologies used within a cloud platform and create a topology that will be suitable for the experiment
- Investigate and evaluate open-source IDS to understand fully what they do and what their capabilities are. Gain a greater understanding of their methods and composition. Identify potential weaknesses or vulnerabilities. Make an informed decision as to which IDS would be most suitable for the experiment and justify this decision.
- Examine further the methods of signature based, anomaly based and network behaviour analysis techniques to establish exactly what they do and identify ways in which they can successfully be evaded.
- Research common Denial of Service techniques and from that research decide upon a suitable attack to test the IDS and be able to justify this decision.
- Research ethical hacking tools and identify one which would be suitable to launch the intended denial of service attacks

The objectives to be addressed by the primary research or experiment part of this project are listed next:

- Construct a simulated public cloud platform and configure it to run and launch instances
- Install and configure the open source IDS within the cloud and install the latest available rule set for it
- Make a final selection of which exploits to use. Build on previous skills gained within the BSNE programme to do this effectively.
- Launch the selected exploit towards the cloud controller server
- Observe performance of the cloud server and network when the attacks are launched for reduced performance capabilities by posing as a host upon a client network and requesting access to applications residing within the cloud. IDS will be observed in terms of performance and network will be observed for signs of attack - for example: slowing of performance and an inability to provide access to the cloud. This performance data will be gathered for analysis.
- Examine the logs of the IDS for reports of attacks observed and prevented and also the lack of information regarding any attacks which may have passed undetected
- Establish what the detection abilities of the IDS are
- Establish whether more data and activity on the network causes a drop in detection rates
- Present findings and conclusions in the Final Report for the project and discuss them.

1.4 HYPOTHESES

I. By ensuring that all the applications have been patched according to the developer's instructions in an up to date manner, the IDS should detect the vast majority, if not all of any exploits launched at the experimental cloud system.

Justification: Surveying many of the publications and articles used in this project, for example, Krutz & Vines Cloud Security (2010) and Hamouda & Glauert,(2012) will inform the reader that IDS are an effective defence against attack when maintained according to the developer's instruction and kept up to date in terms of signatures or accurate in terms of anomaly detection. IDS do form an important part of any security strategy for a cloud or network and will be effective in detecting attacks.

II. Examination of the IDS audit logs and observations of the cloud network performance will produce results proving that some attacks were successful and evaded the IDS.

Justification: In their document, 'Intrusion Detection Systems,' the Information Assurance Technology Analysis Center (IATAC) which provides the United States Department of

Defense with technical information regarding Information Systems, it is stated that, “Over-reliance on IDS can become a problem especially when commercial IDS vendors overhype features in the race to sell products on the market. Sometimes IDS capabilities claims are over exaggerated and should be tested with scepticism. Administrators should thoroughly check IDS output and use competent judgment when analyzing reports”, {{84 Tzeyoung, Max. Wu. 2009}} This suggests that although an important part of a security strategy, users must be aware of their weaknesses as well as strengths.

The rest of this report consists of a Literature Review – where a more in depth review of cloud computing and the security concerns surrounding it is conducted, the Methods Section – which sets out to describe in detail the experiment associated with this project and the justification for using an experimental approach, the Results Section - which illustrates the findings of the experiment once it was conducted and the Final Discussion and Conclusions – which will discuss and critically analyse the results of the experiment, its limitations and possibilities for further research areas. The results will be compared to the hypotheses and hopefully provide some answer to the questions they raised

2.0 LITERATURE REVIEW

The Literature Review focused on the characteristics of Cloud Computing and set out to first investigate and explain its characteristics. Network security and defence methods were researched and in particular Intrusion Detection Systems – the methods that they use and the role they play in defending a network.

2.1 CLOUD COMPUTING

2.1.1 Overview of Cloud Computing

There is still a lot of debate about an exact definition of cloud computing, different services elicit different definitions {{62 Bhaskar,et al 2010}. This report focuses on the concept of Infrastructure as a Service cloud framework and all material refers to that model of computing unless specifically stated.

Put simply, the cloud is a collection of computers (servers and PCs) connected together. This group of resources provides increased computational power, access to applications and stored data delivered over an internet connection. This approach has moved away from the 'traditional' idea of an organisation installing applications on servers that they own which are then accessed by users via their private organisational network. Public cloud providers rent their resources out to multiple clients; this means that the equipment used will host a multi-tenanted environment containing the virtualised machines, applications and data of many organisations. The simplicity of this model is that information stored on the cloud can now be accessed from any geographical location providing internet access is available, {{55 Miller, Michael 2009}}.

Mell & Grance (2011) in their 'Final Version of NIST Cloud Computing Definition' published by the National Institute for Standards and Technology give what is currently regarded as a definitive classification of cloud computing. They set out what its core characteristics should be and give definitions of its various platforms and deployments.

2.1.2 The Essential Characteristics of the Cloud

Five characteristics are listed as crucial to defining a cloud network, these are listed below:

1. On-demand self service – user can access resources without prior contact with provider

2. Broad network access – the cloud must be accessible by a variety of devices from pc to mobile phone to tablet etc via standard procedures and mechanisms

3. Resource Pooling – resources within the network are pooled via virtualisation to provide services to more than one client, resources are allocated and re-allocated dependent on demand. There is no control by the client as to the location of the resources they use.

4. Rapid Elasticity – users can expand or decrease resources as required and according to demand at any time.

5. Measured service – services such as processing, using storage etc are metered and the consumer is charged according to usage.

These characteristics must be present on an infrastructure or be provided by an infrastructure before a system can be considered to be a cloud.

Cloud computing can be provided in different service models for different purposes:

Service Models of Cloud Computing

- Infrastructure as a Service – in this instance, resources such as hardware, processing and storage power are rented by an organisation from a cloud provider. The organisation will use these resources to run applications and store data on.
- Software as a Service – the cloud operator provides access to and use of software applications via an internet connection
- Platform as a Service – cloud customer creates their own application and deploys them onto the cloud infrastructure

Deployment Models of Cloud Computing

- Public Cloud – the cloud is operated by a cloud provider and many different clients or organisations pay to access and use the services provided
- Private Cloud – a cloud infrastructure owned or leased by one private enterprise, access is provided to company employees and possibly other authorised personnel according to company security policy
- Community Cloud – a cloud run for a set of organisations linked by purpose e.g. a cloud run by NHS which could provide access to hospital staff, General Practitioners, pharmacists etc
- Hybrid Cloud – a combination of any of the above listed. An example could be a private enterprise using their private cloud for standard computing requirements and renting space on a public cloud when extra capacity is required.

{{2 Mell,P. 2010}}

The emergence and popularity of cloud computing can be put down to several technological advances that have happened alongside each other: the ability to accurately monitor and charge for services used, increased data transfer rates, virtualisation, service orientated

architecture and service management {{90 Rhoton,John. 2011}} this commonality of development has facilitated the growth in uptake of cloud computing in its present form.

Businesses investigating a feasibility study of cloud computing discover that major reductions can be made to costs by adopting this model. It is far more economical to have a third party maintain infrastructure and employ the staff to do it than to pay for the outlay yourself. Many famous names in the computing world such as IBM, HP, VMware, Google, & Amazon have fully developed strategies for cloud computing which are now in wide use by business clients. Open source application communities have also produced their own cloud platforms which are available for use free of charge, or users can opt to purchase a license which will provide technical support for the application. Notable examples of cloud technology organisations are Eucalyptus and Open Nebula

2.1.3 Open Source Cloud Computing Platforms

Cloud platforms such as those listed previously work within the Infrastructure as a Service framework and in general provide a central user interface with which to manage the components of the cloud infrastructure such as storage, network etc. These platforms facilitate the process of provisioning virtual machines to cloud users. Virtual machines of a desired configuration and of any number can be initialised according to the needs of the client, these are spawned somewhere on the infrastructure but the details of physically where become unimportant to the user whose main concern is service needs being met. {{92 Sempolinski, Peter. 2010}}. Typically the use of these platforms is within an organisation's private cloud although they do feature in hybrid clouds where an organisation's private cloud uses the facilities of a public cloud. Open source is a term used for applications which are free to users, their source code is freely available for users to modify to their own requirements and developers are encouraged to contribute and make improvements to the application.

Eucalyptus Cloud Platform

Eucalyptus is an open-source platform created by the Department of Computer Science at the University of California at Santa Barbara, {{93 Anon,}} Eucalyptus grew from a research project on cloud computing and is now available in a corporate and open-source form. Eucalyptus is the most widely used cloud platform for private IaaS clouds and was specifically designed for private or hybrid cloud systems, {{eucalyptus.com}}. It has been described as offering an open source answer to Amazon's EC2 commercial cloud {{92 Sempolinski, Peter. 2010}}. The Eucalyptus website provides detailed support documentation for installation and help forums for troubleshooting – this is important to

consider with regards to the set up of the experiment. Another factor to consider is that the more widely used an open-source applications is, the higher the level of debugging and development has been performed due to the amount of people using the application.

Open Nebula

Most cloud platforms have their development roots in the United States, but Open Nebula is a European development. Is is fully open source, with no commercial version available. The most distinctive feature of Open Nebula is the level of customisation which is provided not only to administrators but also users, (Sempolinski& Thain, 2012) It permits users to request specific configurations of resources upon the cloud network which provides great flexibility but also makes it more suited for private clouds – where the users are known to the cloud administrators. Its documentation states that it is most suited to the private cloud and focuses on the task of data centre virtualisation. In the true style of an open source application, it is designed not to be hardware or software dependent (Open Nebula, 2012)

2.1.4 The Perceived Weakness of Cloud Computing

Business and IT managers could be forgiven for thinking that the Cloud model is the answer to many problems facing their businesses at the current time. Adopting the cloud can provide huge cost savings after an initial outlay – it passes the responsibility for accommodation of infrastructure and employment of staff to maintain it to the cloud provider, {{3 Armbrust,M. 2010}}

However, organisations cite concerns over security in the cloud as a major put-off from adopting cloud computing, {{94 Sarno, D. 2011}} It may seem that concerns would apply to lesser known companies with little experience in managing such an infrastructure but unfortunately, even very high-profile cloud providers have been affected by security breaches such as Amazon - whose cloud servers were used by an attacker to penetrate the Sony Playstation network in 2011 – crippling it in a highly publicised manner and giving the attackers access to users personal data {{95 Galante, J. 2011}} As Onwubiko (2010), states in his article Security Issues to Cloud Computing, “This new model of service (cloud computing) offers tremendous reduction in operating cost; unfortunately, it has also introduced a set of new and unfamiliar risks.”

The features that can make cloud computing seem like an attractive proposition are the same features that cause concern about security, for example – the ability to scale dynamically up or down in the provision of resources to a client – concerns are expressed as to whether this is at the expense of security, {{96 Treacy, B. 2009}}. Studies have also proven that access can be gained by creating virtual machine instances from one account to access virtual machines

belonging to another account holder within the same cloud environment, {{63 Ristenpart, T. 2009}}

Consideration must be given to that of the activities of those whom the cloud is shared with. The cloud is of use to businesses and governmental organisations but also to criminals. Organisations could find themselves in a position where their virtualised machines are residing on devices alongside organisations or individuals intent on exploiting cloud clients and resources for criminal purposes such as data theft, fraud, hacktivism and terrorism {{54 Biggs, S: Vidalis, S 2009}} Organisations are also charged with taking responsibility for protecting the data that they store and work with. Laws such as the Data Protection Act 1998 in the United Kingdom, {{97 Information Commissioners Office 2011}} and the The Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the United States, {{98 US Dep't of Health & Human Services, . 2011}}.

2.1.5 Methods and Practises to Enable a Secure Cloud Environment

Given the security concerns within the cloud, it is reasonable to conclude that a comprehensive and effective security strategy is critical for organisations to apply to their cloud network. The elements of a cloud security system should include the following:

- Firewalls
- De-militarised zones
- Intrusion detection systems on network and hosts
- Anti-virus software
- Monitoring of network via audit logs
- Educating employees to spot suspicious activity within the system or attempts at Social Engineering

{{82 Kurose, J. 2008}}

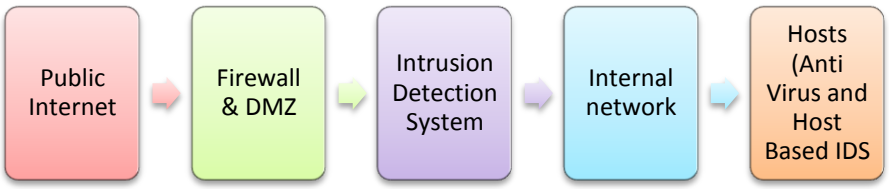


Figure 2 the sequence of network security elements

Figure 2, gives a representative picture of where each element of network security hardware/software should be positioned in relation to each other

2.2 INTRUSION DETECTION SYSTEMS

2.2.1 Background

Intrusion Detection Systems (IDS), monitor the comings and goings of traffic on the network thus allowing network administrators or security personnel to identify attacks, {{59 Simpson, Michael 2006}}. They monitor for violations of the network's security policy. Violations can take the form of 'viruses,' unauthorised access by strangers and already authorised personnel attempting to maliciously escalate their privileges. The events that an IDS will pick up on not only include malicious attempts to access but also erroneous ones where attempted access has been a mistake due to typing the wrong address of where a user wishes to connect to. {{17 Scarfone, Karen 2007}}.

A decision must be taken by the cloud provider regarding the type of IDS to be used. IDS can be host based (on network servers or database servers within the network) or network based sitting on the network side of the firewall of the perimeter network. A host based IDS will monitor events within the operating system and applications on the host, whereas those that are network based monitor or examine packets traversing the area of the network they have been situated in {{73 Boyce, C.A.P. 2004}}. Upon detection, good IDS should be capable of providing the following information:

- What type of event happened
- Where in the network did it happen
- When did it happen
- Who or what was it that attempted the attack

IDS can detect an intrusion by observing it in progress or recognizing and reporting its occurrence from results after it has happened, {{99 Allen, J. 2000}}. The methods that they use to do this fall into two main categories - Signature Based Detection and Anomaly Based Detection. The following paragraphs discuss the main characteristics of each.

There are four main component blocks which constitute an IDS:

Sensor the front end of the IDS and perform the actual monitoring of traffic and behaviour on the network

Monitor collates the information sent from the sensors and in some types of IDS can analyse the information and find activity that the sensors did not, make comparisons between data received from sensors and signatures or behaviour profiles, produces alerts

Resolver receives alerts from the monitor, decides upon the action to be taken e.g. logging, reconfiguring, notifying user

Console the user interface of the IDS, installed on an ordinary pc. Facilitates configuration of IDS and analysis of data.

{{100 Verwoerd, T. 2001}}

2.2.2 Signature Based Detection

Signature based detection methods are designed to detect attacks by looking for specific patterns that will identify an already known attack {{75 Champion, T. 2001}}. When a match to a known signature is found the traffic containing it is dropped or blocked. The weakness of signature based detection is that they cannot defend against variations in the pattern of an attack or unknown 'zero-day' attacks. On their own, signature based IDS are quite ineffective. They cannot understand the complexities of many application and network communications. No correlation can be made between requests sent and responses. Also, when multiple events constitute one attack, the IDS cannot relate the present request with a past request and therefore the attack goes undetected. Signature based systems work on similar practices to that of anti-virus software, {{56 Krutz, L. R. 2010}}.

2.2.3 Anomaly Based Detection

Anomaly based detection is designed to distinguish accepted levels of behaviour from those that are not. A profile of 'typical' network activity is built over a specified period of time. This includes observed levels of CPU activity, logins, level of traffic etc, {{59 Simpson, Michael 2006}}. The longer the observation period of the network, the more accurate a profile will be produced - as this will give indications of peaks and lows of activity. When the profile is complete, it is used by the IDS to compare expected behaviour against actual behaviour – significant deviation from the profile will result in an alert being triggered, Profiles can be of a static or dynamic nature. Static profiles will remain unchanged which means it will eventually become out of date and inaccurate unless reconfigured manually by an administrator. Dynamic profiles adjust as subsequent behaviour change occurs. This however creates a weak point should the IDS be observing malicious behaviour whilst it creates or adjusts its dynamic profile and thus views it as 'normal.' ({{17 Scarfone, Karen 2007}}

Because of the complexity of computing activities of most organizations it is extremely difficult to achieve accuracy with profiles, for example - incidents that occur once a month such as file transfer activity may not be observed during the construction of the profile and therefore appear as a violation when they commence. Difficulty in achieving and maintaining up to date and accurate signatures and profile information is borne out in the problem of False Positives and False Negatives, {{88 Mell, P. 2010}}

False positives occur when an IDS detects an authorised action and deduces that it must be hostile activity. This will most likely have been caused by behaviour upon the network deviating markedly from the information held upon the network behaviour profiles. A false negative is a malicious intrusion which manages to bypass the IDS without detection.

A malicious attack which attempts to elude the system and be viewed as a false negative is the Fragmentation Attack. This method fragments or splits the packets containing an attack into multiple smaller packets which in themselves contain only part of the attack and therefore only part of its signature, these can pass by the IDS undetected - the packets are reassembled at their destination at which point they execute the attack. The research of IDS capabilities for the purposes of this report concerns the abilities of fragmentation attack to evade the detection of an IDS, {{79 Owen, D.}}

It can be concluded that the configuration of an accurate and effective IDS is a highly complex task. This leads to the purpose of this project which is to ascertain how effective they can be given the complexity of not only their successful operation but also the complexity of their surroundings in a cloud network.

2.2.4 Snort

An open source Intrusion Detection and Prevention System (IDPS), Snort can execute real-time traffic analysis and packet logging within IP networks. A popular open source IDPS, Snort claims to have over 400,000 users and claims to be the most used IDPS worldwide. Snort performs 3 main roles – packet sniffing, packet logging and as a fully functioning NIDPS. Its creator's website claims that it ranks in first place frequently when compared to other IDPS, {{68 Anonymous}}. Like most open source applications, Snort is reviewed and tested not only by its own developers but also a community of experienced developers worldwide. A search of popular computing sites will also reveal favourable reviews of Snort,{{69 Ahronovitz,M. 2010}}. Snort utilises signatures for known attacks and rules as a method of detecting zero day attacks. Rules focus on detecting the presence of vulnerability within a system as opposed to a signature which uses comparative methods to spot known exploits.

2.2.5 Suricata

Suricata is developed and promoted by the Open Security Information Foundation and funded partly by the United States Department of Homeland Security. It describes itself as an open source IDPS. Suricata is a rule based system that uses rule sets created by other organisations to monitor networks and detect attacks. It can utilise some features of Snort such as the rule set produced by the Snort Vulnerable Research Team but also rule sets produced by such organisations as Emerging Threats,{{69 Ahronovitz,M. 2010}}. Suricata was first released in 2010, Snort first appeared in 1998. Suricata was developed to increase processing capabilities due to the advancement of multi-core processing. Suricata can operate what is termed a 'multi-threaded' processing (more than one core), whereas Snort is perhaps seen as less efficient in respect to this as it operates single threaded (one core). If consideration is paid to current manufacturing of processors being primarily multi-core, this could be perceived as a weakness in the case of Snort,{{67 Day,D.J. 2011}}.

2.3 SECURITY THREATS IN CLOUD COMPUTING

2.3.1 Denial of Service Attacks (DoS)

DoS attacks prevent legitimate users from accessing network resources, {{59 Simpson, Michael 2006}}. An Denial of Service attack's purpose is not to access specific data or cause damage to it but rather to attempt to cause as much disruption to the service provided by the network as is possible, although in some cases it may be used as a distraction in the first part

of an attack to establish a vulnerability prior to launching a secondary attack. Virtualised environments such as clouds have an increased risk of denial of service due to the virtualised machines residing on a host, this means the virtual machine is at risk but also other virtual machines residing on the host and the host itself and its resources all become susceptible to the attack. The procedures used to allocate resources in a virtualised environment are in themselves complex meaning that the measures used to prevent denial of service attacks have to adapt to this complexity too,{{56 Krutz, L. R. 2010}}. Denial of service attacks exist in many forms – all have the intention of preventing authorised users from gaining access to a system and using its resources – but there are different methods to do this.

2.3.2 TCP SYN Flood

One method is to exploit the TCP-SYN-ACK handshake process by creating so many half-open connections that bona-fide users can no longer gain access to the system, {{64 Bellovin, S. 2004}}. When a computer receives a SYN packet, it sets up a buffer queue for these messages until an ACK is received back from the client. If no ACK in received, as in this case, the queue starts to fill up and become overwhelmed preventing it from responding to legitimate user requests{{21 Krutz, Ronald 2007}}.

2.3.3 Fragmentation Attacks

A necessary part of transmitting data packets over an IP network involves fragmentation. The IP protocol is not media-dependent which means traffic can traverse a variety of media to get to its destination e.g. fibre optic, copper wire and wireless. Different media however have different maximum packet sizes that can be transmitted upon them. Fragmentation is the process of breaking a data packet down into smaller size pieces to enable certain media to carry the traffic. Each type of media has a maximum transmission unit (MTU) which may be smaller than the original size of the packet. When a packet arrives at the router on a network with a smaller MTU size, it fragments the packet and forwards it. When the packet has traversed the network, it is reassembled at its destination to its original size using information from flags and fragmentation offset details. {{65 Dye, M.A. 2008}}

A malicious fragmentation attack exploits this process in an attempt to crash a target system. An oversized IP packet in excess of 65,536 Bytes is created by the attacker. Packets of this nature are larger than the maximum IP packet size permitted to be transmitted. Therefore it must be split into smaller packets or ‘fragments.’ When the packet has been fragmented and the fragments sent across a network to its destination, the destination host reassembles the packet which is too large to be processed and causes the operating system to freeze or crash.{{21 Krutz, Ronald 2007}}.

2.3.4 Understanding the Threat

To gain insight into the seriousness of the security issues relating to any computer network and the importance of the security thereof, an inspection of newspapers, TV or current affairs based websites will, at the time of writing produce multiple reports regarding what is termed 'Cyber-crime.' In one example, the UK government reported that cybercrime was costing the UK £27 billion a year – this was forecast as a mid-range estimate and may well have been higher. Businesses most at risk were drug manufacturers, chemical producers, IT and electronics companies, {{60 Anonymous 17 February, 2011}}. Aside from the commercial impact on national economies, the situation has become so serious in terms of international espionage and warfare that the US Army are now recruiting what it terms to be "a world class, cyber-warrior force," and nations are launching attacks against each other's stock exchanges and commercial concerns such as airlines, {{61 Watts, Susan 26 January, 2012}} .

Cyber-crime now encompasses areas of international espionage and warfare. The most notable and widely publicised example of an exploit in recent times has been the Stuxnet worm. This is an exploit targeted at the interface between a computer program and the mechanical processes it controls in equipment manufactured by Siemens.

Suspicion exists that this worm has been created by a governmental organisation due to the resources which would have been required to create it. Its intended target appears to be the nuclear development project in Iran, although approximately 50-100,000 computers in Iran, and surrounding countries appear to have been infected with it. This could be dismissed as out of the realms of consideration for a small to medium sized business, however, the technology present in Stuxnet works on a wide variety of industrial equipment and is now there to be copied by criminals, terrorists or hacktivists who have their own agenda and targets where attacks are concerned, {{66 Chen,T.M. 2010}}.

2.3.5 The Role of the IDS

What has Stuxnet got to do with businesses considering cloud adoption? It is an illustration of how prevalent and serious the issue of malicious attempts to access information systems and cause damage is at the time of writing. A worm created by an intelligence agency designed to damage infrastructure of another country contains material that is of an exceptionally high standard – and it is now available for use by smaller criminal organisations. Falling prey to a 'hacker' is no longer being subject to the mischief of a school or university student – it has the potential to dictate whether an organisation can still be open for business and maintain its trustworthy reputation with its customers.

The role of the IDS in relation to this issue is that it should be part of a multi-faceted and effective security strategy employed to defend against the exploits that are current at the time of writing and those that have yet to be discovered or even developed.

A network or cloud system security strategy is only as strong as its weakest link. An ineffective IDS which fails to declare true positive events will render a security system ineffective leaving the system open and vulnerable to attack. This report aims to demonstrate the role that IDS have within a cloud system in terms of keeping it secure, and although not the sole element of defending a cloud system, it is an integral part which the success of that security depends upon.

3.0 METHODS

This chapter will introduce and describe the practical research component of this project which was experiment based. It discusses the selection of the applications used and why they were selected and the reasons behind the development of the experiment which was conducted to investigate the questions raised in this report – how an IDS performs within the complicated environment of a cloud platform.

3.1 THE USE OF OPEN SOURCE PRODUCTS

Many commercial variations of cloud computing platforms are available; these include offerings from the large well known computing companies such as HP, VMware, IBM and Oracle. However there are huge cost implications to consider and also the possibility of having to commit to vendor hardware to facilitate the cloud platform and being locked into contracts for certain periods of time.

Open source platforms offer the possibility for enterprises, (particularly small to medium sized businesses), to create and manage their own cloud systems on existing resources providing a far more cost effective and flexible solution. Developer communities provide support for open source software as with Eucalyptus and Open Nebula to guide users on installation and configuration (see https://help.ubuntu.com/community/UECsupport). An open source application should provide a cost effective, flexible and well supported solution to any small or medium sized business which is looking to explore the implementation of cloud computing within their own infrastructure.

3.2 CHOICE OF OPEN SOURCE CLOUD PLATFORM

An investigation was conducted into the properties of four open source cloud computing platforms to evaluate the most suitable and relevant platform to use. Many open source platforms are available for use, the four which were evaluated were Nimbus, Open Nebula, Open stack packaged as Ubuntu Cloud Infrastructure (UCI) and Eucalyptus packaged as Ubuntu Enterprise Cloud (UEC).

An evaluation of the platforms was performed with consideration given to:

- Suitability for purpose – a small, experimental private cloud similar to that used by businesses to evaluate cloud platforms before adopting them
- Installation and troubleshooting support available in terms of manufacturer's site and user-forums
- Ease of use

3.2.1 Nimbus

Nimbus is described as a 'scientific' cloud aim at providing computing power to those who wish to share cluster time {{92 Sempolinski, Peter. 2010}} and not so much a cloud liable to be used by everyday enterprises, as the focus of this project lies with how businesses would protect their cloud system for commercial practises, Nimbus was ruled out.

3.2.2 Open Nebula

Open Nebula is a European developed cloud platform used by organisations such as Cern and KPMG. It provides a high level of customisation to its administrators (e.g. the shared file system which stores all of the configuration files) and users who are allowed to request specific memory, processor and disk resources. However, the drawback of this feature is that it is easy to make a mistake and jeopardise the running of the cloud platform {{92 Sempolinski, Peter. 2010}} The writer also found less technological support available than for Eucalyptus and in some instances the help available was in Spanish which is possibly due to the location of the Open Nebula labs in Madrid.

3.2.3 Openstack

Openstack is one of the newest open source cloud platforms to be released at the time of writing. Launched in July 2010, it is a collaborative project between NASA and the web-hosting/cloud platform provider Rackspace. A consequence of its relative newness in the open-source field is that compared to Eucalyptus, there is a lack of clear documentation and user forums available to support first time users and those wishing to use Openstack for research purposes. According to Dr Steve Thorn of Edinburgh University, in an evaluation of Openstack that he produced for the UK Engineering Task Force, "Not all documented features work as advertised and it would be challenging to deploy and maintain a production quality system at this time." He goes on to state in his conclusions that due to the rapid

deployment of Openstack, documentation is not always up to date with the software and that it "...does not make a stable base for deploying and maintaining a stable production infrastructure at present," {{106 Thorn, Steve, Dr 2011}} Openstack is utilised by some well known companies such as AT & T at the moment, however, as a result of the writer's own research, experience regarding the configuration of Openstack, (in the form of Ubuntu Cloud Infrastructure) and taking into account Dr Thorn's conclusions, Openstack was judged as being unsuitable for the purposes of this project.

3.2.4 Eucalyptus

Eucalyptus is commonly described as an open source version of the Amazon Elastic Cloud (EC2). It is the most widely used platform for private, on premise clouds, {{103 anonymous}}. In terms of research and assessment, Eucalyptus features as the most widely used platform for this purpose. Eucalyptus describes itself as designed for industry. Private companies with high numbers of users and machines benefit from the scalability of the system. It's popularity comes from the fact that it is designed to be easy to install and in addition to its scalability, it can be also be used effectively on very small configurations for the purposes of research, proving it to be highly versatile {{104 Sempolinski, Peter 2012}} Its use of the industry standard Amazon EC2 interface in the form of Euca2ools is what makes it different from most other open source platforms. {{102 Khan,I. 2011;}} Although all open source cloud platforms have a level of unresolved issues - Eucalyptus does not provide a high level of customisation of its system due to the focus on compatibility with EC2. High levels of customisation were not deemed a necessary requirement relation to this experiment and as stated in the review of OpenNebula this can actually cause more problems than solve them. In conclusion, the decision was made to use Eucalyptus because it provided a realistic platform which is already widely used in actual enterprise cloud networks – this gives it an accurate 'real-world' quality that some of the other platforms could not provide. Its widespread use in a variety of forms – be it business or research is also proof of its fitness for purpose. The UEC form of Eucalyptus also provides troubleshooting support available to the first time user via Ubuntu Documentation and related user forums. It was judged that Eucalyptus (UEC) would provide the best opportunity and support for a successful experiment amongst the four platforms evaluated.

3.3 CHOICE OF IDS

Snort Intrusion Detection System has become the industry standard for signature based NIDS {{107 Kohlenberg, Tony 2007}}. An open source Intrusion Detection and Prevention System (IDPS), Snort can execute real-time traffic analysis and packet logging within IP networks. A popular open source IDPS, Snort claims to have over 400,000 users and claims to be the

most used IDPS worldwide. Snort performs 3 main roles – packet sniffing, packet logging and as a fully functioning NIDPS. Its creator's website claims that it ranks in first place frequently when compared to other IDPS, {{68 Anonymous}}. Like most open source applications, Snort is reviewed and tested not only by its own developers but also a community of experienced developers worldwide. A search of popular computing sites will also reveal favourable reviews of Snort,{{69 Ahronovitz,M. 2010}}. Snort utilises signatures for known attacks and rules for detecting zero day attacks. Rules focus on detecting the presence of vulnerability within a system as opposed to a signature which uses comparative methods to spot known exploits. It is for these reasons that Snort was chosen as the IDS for this experiment.

3.4 CHOICE OF ETHICAL HACKING SOFTWARE

Whilst carrying out research a suitable packet generator with which to craft an attack, a few open source applications were found. Some such as 'PDos' were designed for distributed denial of service attacks and many were designed for network performance analysis such as NetscanTools Basic Edition. According to the author, Hyenae can be used for low level Ethernet attack scenarios, {{109 Richter, Robin 2011}}. Hyenae is a simple program and is packaged with comprehensive instructions on how to use it. It provides many varieties of attack vector such as ARP-Request flood, ICMP Smurf attack and TCP-SYN attack – all varieties of Denial of Service attacks. It has been designed to show vulnerabilities of a network. After successful trialling by the writer, it was judged to be fit for the purposes of this experiment.

3.5 DESCRIPTION OF THE EXPERIMENT:

3.5.1 Reasoning

The purpose of the experiment and the project as a whole was to evaluate open source cloud platforms and the role and performance of an IDS whilst monitoring a prototype cloud environment. This physical construction in a lab environment was chosen as it is recommended by Snort developers,{{107 Kohlenberg, Tony 2007}} and it best represents the type of environment a user would start with when evaluating both the performance of the cloud platform and the IDS.

The two server cloud environment is the minimum construction recommended for UEC {{108 Ubuntu Community Documentation 2010}}- using four servers for the UEC may have been more accurate for a production environment but as this was an preliminary experimental evaluation the presence of another two servers would have created unnecessary components

which added no research value to the experiment itself. In a production environment, if a user were to find the results of their initial investigation of interest or favourable they would then be expected to create a larger topology to research upon further.

3.5.2 Construction of the Experiment

After consideration, a physical topology was decided upon for the experiment in preference to an experiment which used a simulation application. Reasons to justify this decision are given as follows:

- Using physical hardware simulates a realistic business environment – although virtualisation is part of cloud computing – it is stills run on physical machines – the virtualisation is part of the process not the fabric. Using an experimental framework allows for accurate and more realistic 'real-life' results. The quality of the results could be judged to be more accurate.
- The alternative used by many Networking Students which is OPNET did not support cloud computing systems at the time of experimentation
- Using instances generated upon a commercial cloud would have breached 'conditions of use' of commercial cloud providers due to the presence of a malicious attack being launched against the cloud servers.

The topology was built together gradually in a modular fashion to ensure that the separate components: cloud platform, Snort and Hyenae all worked independently before linking them together in one network. Each application was installed onto the appropriate computer and ran to check configuration before being connected into the topology of the experiment. This methodical approach helps to identify problems to specific areas instead of trying to troubleshoot the prototype network as a whole and is standard practise when installing new systems in a network {{90 Rhoton,John. 2011}}

Configuring a cloud platform or network can be a complex affair {{106 Thorn, Steve, Dr 2011}}. With this in mind the topology used was selected for its simplicity. In a real life scenario, it is likely that an organisation would start with such a topology to investigate initial characteristics of the cloud such as ease of installation, selecting and running instances before perhaps scaling up to see how the platform performed with a larger number of users.

The experiment consisted of creating a topology of two pc's which acted as servers running the UEC (Eucalyptus) cloud platform. These were connected to a switch which also had a pc connected which was running Snort. Outside this network, lay the attack PC which was running Hyenae – a packet generating application that was used to test the reaction of the IDS. On the following page a diagram which illustrates the topology can be seen.

Physical Topology

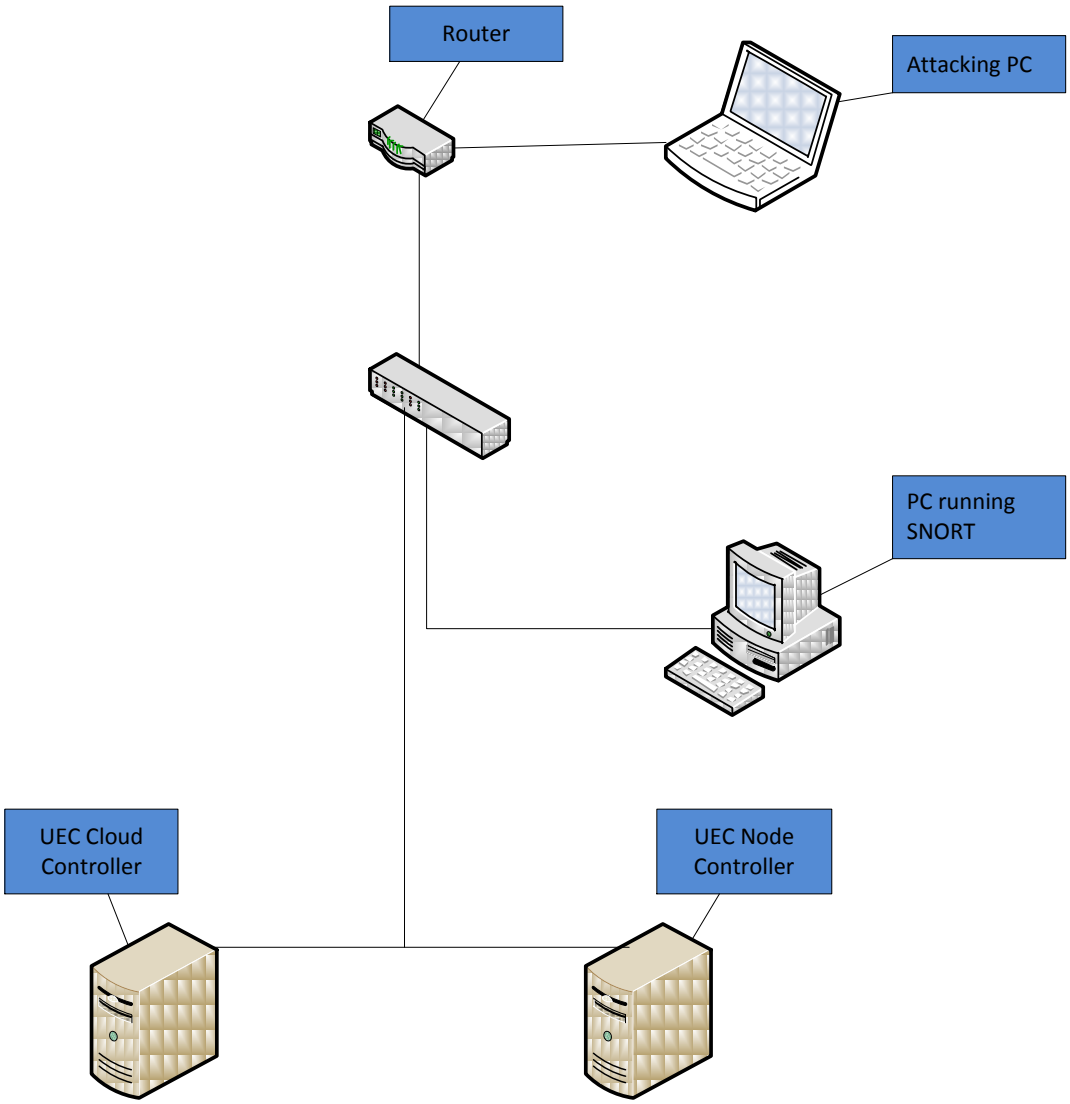


Figure 3 Physical Topology of the Experiment

The technical specifications of the components were:

Netgear DG434GT Router, 2.4 GHz, 108Mbps

1 Netgear 5 port, FS105 Fast Ethernet Switch

1 Acer Aspire 5552 laptop, AMD Athlon II x2 P340 CPU, 4GB RAM, running Ubuntu-10-4-LTS Server (Snort machine)

1 HP G62 Notebook PC, AMD Athlon II P340 Processor, 3GB RAM, running Windows 7 SP1 (attack machine)

1Toshiba Satellite Pro U400 Core 2 Duo 2 GHz - 3 GB Ram, running Ubuntu Enterprise Cloud (Node Controller)

Dell Inspiron 530s PC, Intel Core 2 Duo CPU, 2.83 GHz, 4GB RAM , running Ubuntu Enterprise Cloud (Cloud Controller)

3.5.3 UEC – Ubuntu Enterprise Cloud

As UEC was being used as the platform, it was appropriate to use a topology based on the installation guide published by Ubuntu Community to maintain uniformity. The initial topology for the installation of UEC module follows:

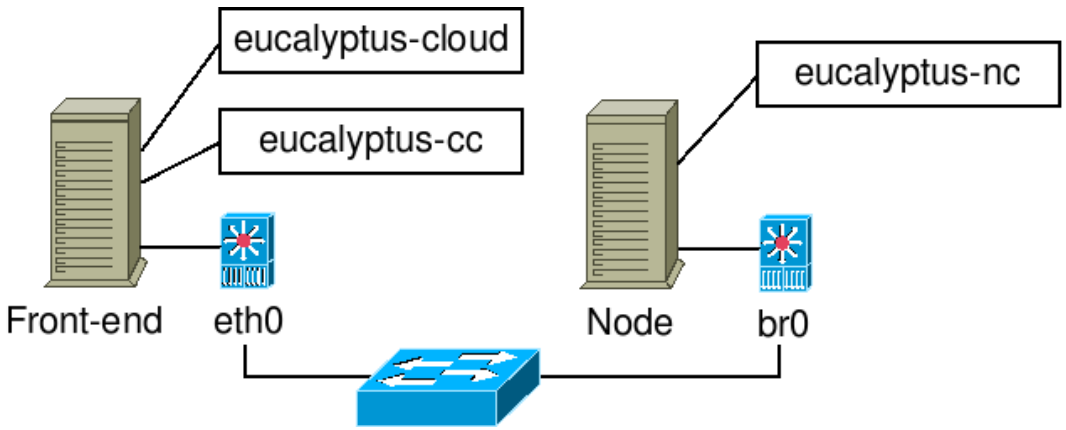


Figure 4 UEC Cloud Experimental Topology {{108 Ubuntu Community Documentation 2010}}

As can be seen from Figure 4, two computers were configured to run Ubuntu Enterprise Cloud, one as the front end performing the role of cloud controller and the second as the node from which the virtual instances are run. The computers were connected together using Cat5 Ethernet cables to the switch, which in turn was connected to the internet via the router.

Full configuration details in the form of an Installation Log are contained in the Appendix of this report. The first PC to be configured was that of the Cloud Controller – this requires to be done first in order that the installation will assume controller status – it performs a search for other nodes before deciding that it is the first on the network and assuming this role, it then prompts the user to confirm this status. Once UEC was installed onto the first PC, Ubuntu desktop was installed to provide a GUI with which to perform administration such as obtaining credentials - which users require to do after installing UEC and are used for verification between the node and cloud controller when sourcing instances. Ubuntu desktop was installed and the Cloud Controller rebooted.

Whilst the desktop was installing on the Cloud Controller, the Node Contoller was installed on the other PC. The node controller detected the Cloud Controller already configured on the network and presented install mode as Node which was selected. The Node Controller installation is much more straightforward than the Cloud Controller and proceeded quickly. Once installed, the Node Controller was rebooted as directed.

The next step was to obtain credentials upon the Cloud Controller which, as stated before, are used to provide verification between node and cloud controller. This was a straightforward process which involved accessing the UEC web interface. Passwords for the administrator account were set and the administrator email was added (users would contact this email to gain access). Credentials were downloaded and unzipped.

Once credentials had been obtained the next task was to install an image. This involved accessing the UEC web interface once again. Under the 'store' tab of the web interface could be found a variety of virtual pc images – images containing a certain operating system such as Ubuntu working to the performance levels of various components such as CPU/RAM etc. A user would select one of these variations when choosing to run an instance from the cloud.

An attempt was then made to launch an instance from UEC. This was done via the command line as per guidance from Ubuntu documentation. A keypair was created to allow login as root to an instance once launched. This only takes place the first time the instance is launched. Port number 22 on the pc was opened and an instance of the image chosen (Ubuntu 10-4 Maverick Meerkat) was run and a connection made to its IP address via a secure shell connection.

3.5.4 Configuration of Snort

After the cloud controller and node were installed and configured to launch instances, the next phase of constructing the experiment was to install Snort on to a pc configured with Ubuntu 10-4-LTS Server. A technical guide to the installation of Snort onto Ubuntu by David Gullet of Symmetrixtech was found and referred to throughout the installation, but the writer had to adjust a certain number of entries to achieve successful installation. The majority of the installation of Snort was done via command line. A Technical Log detailing exact configuration of the server is contained in the Appendix of this report.

Before the installation of Snort itself, a number of packages had to be installed such as Snort Report which would provide a graphic reporting facility. The data acquisition API for Snort which facilitates inter-software communication was downloaded next – this is required to run Snort 2.9.0 and later.

The Snort package was then downloaded, unpackaged and then installed after resolving various issues regarding the correct web address from which to retrieve the files. Obtaining and installing the rules that Snort uses also had difficulties as the author of the guide had not stated that an account had to be set up with Snort and an 'Oinkcode' downloaded before this could be done.

Snort was then configured to output to specific directories in keeping with the installation of Snort Report.

The final package to be downloaded was Barnyard which takes output from Snort's logging files and collects them in a database. This is a useful application as it allows Snort to dedicate more processing to its detection processes whilst Barnyard collates its results.

The network cards were configured: eth0 to sniff packets on the network and eth1 to interact with the network traffic.

Snort was then initialised and started to run.

3.5.5 Installing and Configuring Hyenae

Installing Hyenae was a straightforward process of downloading the application from the Sourcforge website and running the installation on the PC which would perform the role of attacker. The version was Hyenae0.36-1_fe0.1-1_win32. Although Linux variations exist, a Linux OS was not a prerequisite for the attack PC as in real scenarios an attacking PC need not have the same OS as its intended target. Documentation that comes with download file in the shape of a 'Howto' file was consulted for configuration information.

3.6 The Experiment

A number of attacks were devised to test the IDS abilities to monitor the cloud platform and to monitor the IDS itself. These choices were based on an Overview of Testing Intrusion Detection Systems, {{88 Mell, P. 2010}} – a study sponsored by the Defence Advanced Research Projects Agency in the United States. In this document, the authors strive to investigate rigorous methods to establish standards and test the effectiveness of IDS.

To establish connectivity, each machine on the cloud network and the attack PC pinged each other – each action was successful.

Experiment 1 - was based on Section 3.4 of the report "Resistance to Attacks Directed at the IDS." An attack was formulated to send DoS attacks to a variety of ports that the server would be likely to u The attack was created on Hyenae by using the graphical interface to create SYN packets with no limits set on the amount of packets sent – this would create a continual stream of packets being directed towards the target. The Snort machine IP address was entered for the destination.

Experiment 2 – The same experiment was sent to the cloud server – to see whether the IDS could detect it – the cloud server had not been hardened against such attacks and therefore would probably accept the connections. Observation would be made of the Cloud Controller for visible signs of an attack such as slowed performance.

Experiment 3 – a version of the 'ping of death' attack was created to represent a fragmentation attack. This was devised to examine the principle of Probability of Detection (Mell et al., 2010). The attack was created on Hyenae to be larger than the maximum permitted size 65,536 and the 'Ignore MTU size' box checked. The IP address of the attack machine was included in the attack profile to enable easier tracking on the IDS logs. With all systems running on the network, the fragmentation attack was launched towards the cloud controller

4. RESULTS

This section recalls the basic procedure involved in the experiment and the results obtained from conducting them

4.1 Experiment No 1:

Attacks Directed Towards the IDS itself

As stated in the Methods section a number of DoS attacks were directed towards a number of TCP ports on the IDS when it was running to establish whether it would be susceptible to attacks. A variety of ports which would be commonly used on the IDS server were selected:

PROTOCOL	PORT NO	REACTION
FTP	20	Actively closed
Secure Shell	22	Actively closed
Secure Socket Layer	1443	Actively closed
Telnet	23	Actively closed
HTTP	80	Actively closed
Apache Tomcat	8443	Actively closed
HTTP Alternate	8080	Actively closed
SQL Services	118	Actively closed
Apache Derby Network Server	1527	Actively closed
MySQL Database System	3306	Actively closed

Table 1 Reaction to Attacks by IDS

From the results of attempting to connect and send a Denial of Service Attack to the Snort Server (IDS), it can be seen that it is resilient towards these types of attacks. In this respect Snort can be judged be capable of resisting Denial of Service attacks

4.2 Experiment No: 2

Experiment 2 was formulated to test the IDS ability to detect an attack on the cloud system. A TCP-SYN attack was sent to the cloud server IP address on via Hyenae. Before even checking the IDS logs a notable difference in performance was observed on the cloud server which was slower in reacting to requests from the user. This at least indicated that the attack had reached its intended target.

On inspection of the IDS logs, in the form of Snort Report, no alerts could be found. The installation of Snort Report as given by its developers - Symmetrixtech was followed but no alerts of attacks which clearly had reached their target could be found. On researching further, this would appear to be a problem which arises commonly, as research on the internet for possible solutions flagged up a number of similar problems{{110 Anonymous}}. Unfortunately and rather disappointingly no solution could be found to this problem. A page was found giving instructions on how to reconfigure Apache and this was followed, however when attempting to reconnect with the Snort Report GUI alerts menu via http to its IP address, an error reported that the file snortreport-1.3.3/alerts.php could not be found. This file was present and accessed via the command line. This configuration issue remained unresolved. This perhaps highlights the problem with open source applications in that the level of support provided may not be adequate when operational issues arise and proves the need for thorough investigation and evaluation before an organisation decides to implement open source products. It also highlights that installation guides are perhaps not read through and tested before publication by developers.

4.3 Experiment No 3

After lengthy investigation, a possible solution was found to the problem of the alerts log. The Snort Report configuration instructions had omitted to advise the user to assign the network address to the snort configuration file. This had meant that the IDS had not originally been actively monitoring the network it had been placed on. After reconfiguring the file, Experiment 2 was rerun. This time the TCP/SYN attack did show up as detected in the Snort logs via the command line interface and could be identified as the TCP/SYN attack from the source address which was used 192.168.1.3 going to the destination address of the cloud 192.168.0.5. The IDS was successful in detecting the attack.

4.4 Experiment No 4

Experiment No 4 adopted the form of a Fragmentation attack. This was devised on the principle of Probability of Detection {{88 Mell, P. 2010}} The attack was crafted upon Hyenae again with the packet size set to 65536 – over the permitted amount and the MTU limit set to be ignored. The attack was launched and once again a dip in performance was detected on the target machine in the form of slower reaction times to requests such as opening the web browser. Examination of the logs indicated the nature of the attack once more had been detected. The IP address of the attack machine was displayed as source with the cloud server IP address as the destination upon the network.

5. DISCUSSION & CONCLUSIONS

This section starts with a brief summary of the project as a whole. Conclusions which can be drawn from the results and their relationship to the original hypotheses with be discussed. Areas of the project which could perhaps have been done better or differently will be suggested in the Limitations section. Finally, discussion will take place regarding any future work which may lead on from what has been conducted in this project, followed by overall conclusions.

Project Summary

Initial research during this project established that cloud computing systems have the potential to considerably reduce business IT costs whilst providing improved services. However, there is currently a lack of user confidence based on security concerns about the cloud.

The project was established to evaluate the features and capabilities of open source cloud platforms and test an intrusion detection system for suitability to this environment. The development of cloud computing has presented organisations with an attractive alternative to the traditional IT approach of buying and running their own private network infrastructures. However, as stated earlier, there have been some notable security breaches within cloud environments which have seen a fall in customer confidence with this particular business model.

This project set out first to evaluate cloud computing platforms, create a simulated cloud platform and then use an IDS to attempt detection of malicious packets within the cloud platform. The results of the experiment proved that the Snort was competent at its task.

5.1 Research Question

As stated throughout this project, although benefits can be gained from adopting the cloud model of computing, security considerations are going to be vital to its success. Intrusion detection systems are a valuable component of a network security policy and this led to the formation of the Research Question:

"Creating a Eucalyptus cloud computing environment and evaluating the ability of the Snort Intrusion Detection System to detect Denial of Service Attacks within it"

5.2 Hypotheses

In 'Hypotheses,' it was stated that sometimes IDS capabilities could be over exaggerated and that IDS should be tested with scepticism, {{84 Tzeyoung, Max. Wu. 2009}}. This statement was made after a study conducted by the Information Assurance Technology Analysis Centre – a government organisation in the United States and is undoubtedly true in relation to some IDS. However, the experiment that was devised for this project, Snort did perform to a high standard in the cloud environment. The results of the experiment support the statement that Snort is the industry standard when it comes to IDS. {{107 Kohlenberg, Tony 2007}} The IDS did detect the attacks which were sent to the targets with a very high detection rate. This would support the argument that Snort is a viable IDS for a cloud environment, bearing in mind that more than one Snort machine would be running in a real cloud environment compared to the single machine of the experiment.

The answers to the Hypotheses are as follows:

I. By ensuring that all the applications have been patched according to the developer's instructions in an up to date manner, the IDS should detect the vast majority, if not all of any exploits launched at the experimental cloud system.

This hypothesis was proved. The IDS was installed with an up to date set of rules which is available to registered users. Every attack that was launched towards the network and the IDS itself was detected.

II. Examination of the IDS audit logs and observations of the cloud network performance will produce results proving that some attacks were successful and evaded the IDS.

According to the results which were achieved from the experiments, Snort managed a 100% detection rate of attacks launched upon the network it resided on. In terms of the experiments carried out for this project, this hypothesis has been disproved. Of the attacks launched at the cloud server – all were detected without fail. Likewise, any attacks launched towards the IDS itself were refused connection.

In comparison to other projects, (Boyce& Zincir-Heywood, 2004) & (Albin& Rowe, 2012) Snort did perform better. This however can be attributed to the level of experimentation perhaps than the abilities of Snort. In the studies quoted, Snort when compared to the Suricata IDS started to drop packets earlier due to its single threaded detection methods as compared to Suricata's multithreaded abilities. In the experiment conducted by Boyce, Snort was outperformed by 3 other IDS when tested for attacks from insider and outsider traffic.

This experiment suggests that Snort is an efficient IDS when placed within a small cloud environment. Other investigations such as (Boyce& Zincir-Heywood, 2004) & (Albin& Rowe, 2012) have been conducted on much more complex networks and produced results suggesting that Snort may not perform as well in these larger environments. However, it is interesting to note that in the report by Albin, Snort was the best performer at catching in some test categories, namely DoS attacks and in the 'Probe' category – the same types of attack as used in this experiment.

The results were slightly different from what was expected. It was imagined that some attacks may have passed the IDS undetected in Hypotheses 2. This was not the case however.

5.3 Limitations

A range of limitations were identified during the progress of the project.

Open source applications are generally written in Linux format and are compiled and ran upon Linux based operating systems. It was felt that the experience of Linux and associated skills of the writer – despite undertaking practise and research in that area - fell short of what would be required of a network administrator who chose to investigate cloud and open source IDS. This affected the quality and depth of the experiments as can be seen from the breakdown given under experiment 2. This could be mitigated in future projects by ensuring

skills are to a high enough standard before proceeding or by using Windows based applications – although it is likely these would have to be proprietary applications which would incur costs.

Due to the time frame involved and the time taken to familiarise with the applications featured in the experiment, only one platform and IDS were examined. A comparative experiment could have been constructed between different cloud platforms and different IDS but this may have required more than one person to be involved in the project to be feasible.

Unfortunately, due to relocation, the Voter lab did not become available till the second week of March. This had an impact on the development of the project as the writer had intended to attempt a 4 server configuration of UEC to perhaps give a more realistic setting but in the end this was not possible. It is uncertain as to whether the 4 server configuration would have run successfully in any case.

Some evaluations of IDS that were read in the research part of the project used simulated 'live' traffic profiles, {{113 Albin, Eugene 2012}} , these experiments were conducted at Post Graduate level in government funded laboratories. It is maybe unrealistic to use experiments such as these at Undergraduate level, but they would have given much more accurate results in the experiment had it been possible.

5.4 Further Research

This has been an initial and therefore basic investigation into the adaptability of Snort towards cloud networks and based on a prototype topology. Further research and development areas on this subject matter are suggested as follows:

Studies could focus on the performance of the IDS on busier cloud platforms with more instances running and higher rates of data present upon the network. Also, the placing of more than one IDS server upon the cloud network and their optimal positioning is worthy of consideration. The next stage which would follow on from this research would be to enlarge the prototype network to a 4 server scenario - with more hosts present on the network and possibly introduce traffic generation profiles on the network whilst staging attacks and monitoring the IDS logs

Another and possibly more realistic investigation could be to run similar evaluations using commercially produced products - although this is dependent on the budget available. To test the ease of use of products that manufacturing companies claim to be the best in the business and to test their performance against said manufacturer's claims. Companies advertise the advantages of their products but are, of course, less likely to highlight weak parts of their developments. Are these products really worth the investment? Do they live up to their manufacturers claims? Or do open source products offer a viable and much less costly alternative – despite their possible complexity?

Cloud platforms are also in a state of rapid development at the moment. Time could be spent on assessing their qualities regarding practical implementation and weighing up the strengths and weaknesses of more than one platform.

As technology advances, bandwidth levels are ever increasing and multiple CPU environments are becoming the norm. It would prove useful to assess the capabilities of another open source IDS – Suricata. This has been billed as the next generation of IDS features multi-threading capabilities to increase inspection rates and appears to outperform Snort in comparative tests {{113 Albin, Eugene 2012}} This area particularly addresses the problem of Snort dropping packets when it becomes overwhelmed by traffic.

IDS can provide a good level of detection capabilities, although they must taken in the context of a security system or policy for a network – they are one component of a whole system and provide little use if not accompanied by elements such as IPS, anti-virus and firewalls. IDS do not provide preventative actions toward an attack - this is a role that must be performed by other components. IDS also produce large numbers of false alarms from packets which are unfamiliar - but not necessarily harmful, and also attacks that are OS/Application specific which offer no threat unless the network runs them. Some current research and development areas are now focussing on developing IDS that have 'knowledge' of their network, assessing whether an attack is dangerous to their network and so far proving to produce far lower incidences of false alarms, {{112 Kruegel, Christopher}} this is definitely an area for further focus – the justification being that the more accurate the logs of an IDS are – the easier it is to identify the real threats and not waste time on false ones.

Similarly, focus could be directed towards Intrusion Prevention Systems which actively respond to attacks when detected upon the monitored network and hence provide a level of proactive protection to an infrastructure.

5.5 Conclusions

In conclusion, this project did prove one hypothesis of those it set out to test – that Snort would be a sensible choice for an IDS to be used upon a cloud computing network. The experiment however, did not work our quite as predicted by the hypotheses in that it detected all attacks with none passing through undetected. The literature review also supports Snort as worthy of consideration for this role.

Snort did pick up all the attacks present on the simple cloud network topology, however, Snort is not a standalone solution to network security, but certainly would provide alert and logging information on attacks that had already managed to breach cloud security. Realistically, in a cloud network, an IDS would be one part of many precautions taken to secure the infrastructure and would reside alongside features such as firewalls and anti-virus to create an all round approach to securing the cloud.

This report may be of use in the future to students wishing to carry out similar research as it contains information about the analysis and configuration of open source applications related to cloud computing and security. Small firms and their IT staff may find it of interest when looking into the possibility of implementing cloud and the security which that requires.

REFERENCES

References of quotations used in the report:

[online]. Available at: http://groups.google.com/group/snortusers/browse_thread/thread/4980bd539ec087ab .

About snort [online]. Available at: http://www.snort.org/ [Accessed 30 January 2012].

BBC news - GCHQ chief reports 'disturbing' cyber-attacks on UK [online]. Available at: http://www.bbc.co.uk/news/uk-15516959 [Accessed 11/1/2011 2011].

Cloud computing and the data protection act. | *enVirtua.com* [online]. Available at: http://envirtua.com/articles/2008/11/26/cloud-computing-and-the-data-protection-act/ [Accessed 2011/10/26 2011].

Eucalyptus beginners guide - UEC edition, 2.0th edn, CSS Corp, United States.

Introducing eucalyptus 2.0 [online]. Available at: http://open.eucalyptus.com/book/export/html/4260 [Accessed 11/14/2011 2011].

Ahronovitz, M. & Amrhein, D. 2010, *Cloud computing use cases* [online]. Available at: http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf [Accessed January 30 2012].

Albin, E. & Rowe, N. 2012, *A realistic experimental comparison of the suricata and snort intrusion detection systems,* US Naval Postgraduate School, Monterey, California.

J. Allen, A. Christie, W. Fithen, J. McHugh, J. Picket & E. Stoner. 2000, *State of the practice of intrusion detection technologies.* Carnegie Mellon University, United States.

amazon 2012, *Acceptable use policy* [online]. Available at: http://aws.amazon.com/aup/ [Accessed January 30 2012].

Amazon *Premium support* [online]. Available at: http://aws.amazon.com/premiumsupport/ [Accessed 30 January 2012].

Anon, *What is eucalyptus?*[online]. Available at: http://open.eucalyptus.com/learn/what-is-eucalyptus [Accessed January 25 2012].

Anonymous 17 February, 2011, ***UK cyber crime costs £27bn a year - government report*** [online]. Available at: http://www.bbc.co.uk/news/uk-politics-12492309 [Accessed 28 January 2012].

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., et al. 2010, "A view of cloud computing", *Association for computing machinery.communications of the ACM,* Vol. 53, no. 4, pp. 50.

Balzarotti, D. 2006, *Testing network intrusion detection systems,* Politecnico di Milano.

Barbour, T. 2011, "Cloud computing", *Alaska business monthly,* Vol. 27, no. 6, pp. 36.

Baun, C. & Kunze, M. 2012, "A taxonomy study on cloud computing systems and technologies." in: *Cloud computing methodology, systems and applications,* ed. l. Wang, R. Ranjan, J. Chen & B. Benatallah, 1st edn, CRC Press, Boca Raton, FL, United States, pp. 73-74-90.

S. Bellovin. 2004, *A look back at security problems in the TCP/IP protocol suite.* 20th Annual Computer Security Applications Conference (ACSAC), December 2004.

Bhaskar, P.R., Eunmi, C. & Lumb, I. 2010, "A taxonomy, survey and issues of cloud computing ecosystems." in: *Cloud computing, principles, systems and applications,* ed. N. Antonopoulos & L. Gillam, 1st edn, Springer, London, pp. 21-46.

Biggs, S.V., S 2009, "Cloud computing: The impact on digital forensic investigations, 4th international conference for internet technology and secured transactions (ICITST-2009)", 09 November 2009, .

C.A.P. Boyce & A.N. Zincir-Heywood. 2004, *A comparison of four intrusion detection systems.* Dalhousie University, Halifax, NS.

Braendle, M., Naedele, M., Koch, T., ABB & Vahldieck, R., ABB 2008, "Strictly no admittance", *Power engineering international,* Vol. 16, no. 8, pp. 38.

Burnett, M. 2006, "How I secured one company's network", *Windows IT security,* Vol. 6, no. 10, pp. 6.

Buyya, R., Chee Shin Yeo & Venugopal, S. 2008, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities", *High performance computing and communications, 2008. HPCC '08. 10th IEEE international conference on*, pp. 5.

T. Champion & M.L. Denz. 2001, *A benchmark evaluation of network intrusion detection systems.* (0-7803-6599-2), IEEE,.

Chen, T.M. 2010, "Stuxnet, the real start of cyber warfare? [editor's note]", *Network, IEEE,* Vol. 24, no. 6, pp. 2-3.

Corera, G. *BBC news - GCHQ chief reports 'disturbing' cyber-attacks on UK* [online]. Available at: http://www.bbc.co.uk/news/uk-15516959 [Accessed 11/1/2011 2011].

Day, D.J. & Burns, B.M. 2011, "A performance analysis of snort and suricata network intrusion detection and prevention engines", *The fifth international conference on digital society* Guadeloupe, 23-28 February, 2011, IARIA, , pp. 187.

Dikaiakos, M., Katsaros, D., Mehra, P., Pallis, G. & Vakali, A. 2009, "Cloud computing: Distributed internet computing for IT and scientific research", *IEEE internet computing,* Vol. 13, no. 5, pp. 10.

Dye, M.A., Mcdonald, R. & Rufi, A.W. 2008, *Network fundamentals - CCNA exploration companion guide,* 4th edn, Cisco Press, Indianapolis, Indiana, United States.

Galante, J., Kharif, O. and Alpayev, P. 2011, **Sony network breach shows amazon Cloud's appeal for hackers**, *Bloomberg,* May 16, p. http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html.

Hamouda, S.K. & Glauert, J. 2012, "Security, privacy and trust management issues for cloud computing." in: *Cloud computing - methodology, systems and applications,* ed. L. Wang, R. ranjan, J. Chen & B. Benatallah, 1st edn, CRC Press, Boca Raton, FL, United States, pp. p389-421.

Holstein, M. *How does fragroute evade IDS detection?*[online]. Available at: http://www.sans.org/security-resources/idfaq/fragroute.php [Accessed January 30 2012].

Information Commissioners Office 2011, *Key definitions of the data protection act* [online]. Available at: http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx [Accessed December 30 2011].

Kelion, L. 2012, ***Expect more online attacks, anonymous hackers say*** [online]. Available at: http://www.bbc.co.uk/news/uk-17648852 [Accessed 08 April 2012].

Khan, I., Habib-ur, R. & Zahid, A. 2011, "Design and deployment of a trusted eucalyptus cloud", *2011 IEEE 4th international conference on cloud computing* Washington, DC, United States, 4-9 July, IEEE, , pp. 380.

Khan, I., Rehman, H. & Anwar, Z. 2011, "Design and deployment of a trusted eucalyptus cloud", *Cloud computing (CLOUD), 2011 IEEE international conference on*, pp. 380.

Kohlenberg, T. (ed) 2007, *Snort IDS & IPS toolkit*, 1st edn, Syngress, Burlington, MA, United States.

Kruegel, C. & Robertson, W. *Alert verification - determining the success of intrusion attempts,* University of California, Santa Barbara.

Krutz, L.R. & Vines, R.D. 2010, *Cloud security - a comprehensive guide to secure cloud computing,* 1st edn, Wiley, Indianapolic, Indiana, United States.

Krutz, R. & Vines, R. 2007, *The CEH prep guide: The comprehensive guide to certified ethical hacking,* Wiley,.

Kurose, J. & Ross, K. 2008, *Computer networking - A top down approach,* 4th edn, Pearson, Boston, M.A., United States.

Lippmann, R.P., Fried, D.J., Graf, I., Haines, J.W., Kendall, K.R., McClung, D., Weber, D., Webster, S.E., Wyschogrod, D., Cunningham, R.K. & Zissman, M.A. 2000, "Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation", *DARPA information survivability conference and exposition, 2000. DISCEX '00. proceedings*, pp. 12.

Massicotte, F., Gagnon, F., Labiche, Y., Briand, L. & Couture, M. 2006, "Automatic evaluation of intrusion detection systems", *22nd annual computer security applications conference (IEEE)*2006, .

Mazzarielo, C., Bifulco, R. & Canonico, R. 2010, "Integrating a network IDS into an open source cloud computing environment", *6th international conference on information assurance and security* Atlanta, G.A., United States, IEEE, , pp. 265.

P. Mell, V. Hu, R. Lippman, J. Haines & M. Zissman. 2010, *An overview of issues in testing intrusion detection systems.* (1), NIST, United States of America.

Mell, P. & Grance, T. 2010, "The NIST definition of cloud computing", *Association for computing machinery.communications of the ACM,* Vol. 53, no. 6, pp. 50.

Miller, M. 2009, *Cloud computing - web-based applications that change the way you work and collaborate online,* 2nd edn, Que, Indianapolis, Indiana.

D. Mutz, C. Kruegel, w. Robertson, G. Vigna & R. Kemmerer. 2005, *Reverse engineering of network signatures.* www.iseclabs.org/papers, University of California, Santa Barbara.

Onwubiko, C. 2010, "Chapter 16, security issues to cloud computing." in: *Cloud computing, principles, systems and applications,* ed. N. Antonopoulos & L. Gillam, 1st edn, Springer, London, pp. 271-272-288.

Open Nebula 2012, *About the open nebula project* [online]. Available at: http://opennebula.org/about:about [Accessed 29 March 2012].

Owen, D. *What is a false positive, and why are false positives a problem?*[online]. Available at: http://www.sans.org/security-resources/idfaq/false_positive.php [Accessed January 30 2012].

T. Ptacek. 1998, *Insertion, evasion, andDenial of service: Eluding network intrusion detection.* Secure Networks Inc, United States.

N. Puketza, K. Zhang, M. Chung, B. Mukherjee & R. Olsson. 1996, *A methodology for testing intrusion detection systems.* National Security Agency INFOSEC University Research Program, California, United States.

Rhoton, J. 2011, *Cloud computing explained,* 2nd edn, Recursive Press, United Kingdom & United States (simultaneously).

Richter, R. 2011, *Hyenae - description* [online]. Available at: http://sourceforge.net/projects/hyenae/?_test=b [Accessed 28 March 2012].

Ristenpart, T., Tromer, E., Shacham, H. & Savage, S. 2009, "Hey, you, get off of my cloud", Chicago, Illinois, US, 9-13 November, 2009, Conference on computer and communications security, 2009, Chicago, Illinois, US, pp. 1.

Ros, S. 2009, "Intrusion detection in the cloud", *Dependable, autonomic and secure computing (DASC), IEEE international symposium on,* , pp. 729-734.

Sarno, D. and Rodriguez, S. 2011, Hacker attacks show vulnerability of cloud computing, *Los Angeles Times,* Jun 7, 2011, .

Scarfone, K. & Mell, P. 2007, *NIST IT security: Content / / NIST SP 800-94, guide to intrusion detection and prevention systems (IDPS)*, http://www.nist.org/nist_plugins/content/content.php?content.64 edn.

Sempolinski, P. & Thain, D. 2010, "A comparison and critique of eucalyptus, OpenNebula and nimbus", *2nd IEEE international conference on cloud computing technology and science* Indianapolis, 30 November - December 3 2010, IEEE, United States, pp. 417.

Sempolinski, P. & Thain, D. 2012, "An introduction to open-source IaaS cloud middleware." in: *Cloud computing, methodology, systems and applications,* ed. W. Lizhe, R. Ranjan, C. Jinjun & B. Benatallah, 1st edn, Taylor Francis, Boca Raton, Fl, United States, pp. 133-133-149.

Simpson, M. 2006, *Hands-on ethical hacking and network defense,* 1st edn, Cengage, Boston, M.A., United States.

Subashini, S. & Kavitha, V. 2011, "A survey on security issues in service delivery models of cloud computing ", *Journal of network and computer applications,* Vol. 34, no. 1, pp. 1 <last_page> 11.

Tchifilionova, V. 2010, iNetSec'10 Proceedings of the 2010 IFIP WG 11.4 international conference on Open research problems in network security, Springer-Verlag Berlin, Heidelberg.

S. Thorn Dr. 2011, *An evaluation of openstack for the ETF.* UK Engineering Task Force, University of Edinburgh.

Treacy, B. & Bruening, P. 2009, "Cloud computing - data protection concerns unwrapped", *Privacy & data protection,* [online], Vol. 9, no. 3, pp. 25 January 2012. Available at: http://www.pdpjournals.com/overview-privacy-and-data-protection.

M.W. Tzeyoung. 2009, *Intrusion detection systems.* IATAC, Hendon, VA, United States.

Ubuntu Community Documentation 2010, [online]. Available at: https://help.ubuntu.com/community/UEC/PackageInstall [Accessed March 28 2012].

US Dpt of Health & Human Services, . 2011, ***Understanding health information privacy*** [online]. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html [Accessed December 30 2011].

T. Verwoerd & R. Hunt. 2001, *Intrusion detection techniques and approaches.* Elsevier, New Zealand.

Wang, K. & Stolfo, S. 2004, "Anomalous payload-based network intrusion detection", *Seventh international symposium on recent advances in intrusion DetectionS*, ed. E. Jonsson, Springer-Verlag, Berlin, pp. 203.

Watts, S. 26 January, 2012, ***Call for cyberwar 'peacekeepers' force*** [online]. Available at: http://news.bbc.co.uk/1/hi/programmes/newsnight/9687338.stm [Accessed 28 January 2012].

Wilbanks, L. 2007, "Cybersecurity: Welcome to my world", *IT professional magazine,* Vol. 9, no. 2, pp. 61.

BIBLIOGRAPHY

A list of all the literature and web sites consulted during the progress of the module:

Anonymous, 2011, "CloudPassage delivers elastic cloud server security for the amazon cloud", *PR newswire,* .

[online]. Available at: http://groups.google.com/group/snortusers/browse_thread/thread/4980bd539ec087ab .

About snort [online]. Available at: http://www.snort.org/ [Accessed 30 January 2012].

BBC news - GCHQ chief reports 'disturbing' cyber-attacks on UK [online]. Available at: http://www.bbc.co.uk/news/uk-15516959 [Accessed 11/1/2011 2011].

Cloud computing and the data protection act. | *enVirtua.com* [online]. Available at: http://envirtua.com/articles/2008/11/26/cloud-computing-and-the-data-protection-act/ [Accessed 2011/10/26 2011].

Eucalyptus beginners guide - UEC edition, 2.0th edn, CSS Corp, United States.

Http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1624001 - google search [online]. Available at: http://www.google.co.uk/search?q=http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1624001&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a [Accessed 1/13/2012 2012].

Introducing eucalyptus 2.0 [online]. Available at: http://open.eucalyptus.com/book/export/html/4260 [Accessed 11/14/2011 2011].

Ahronovitz, M. & Amrhein, D. 2010, *Cloud computing use cases* [online]. Available at: http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf [Accessed January 30 2012].

Albin, E. & Rowe, N. 2012, *A realistic experimental comparison of the suricata and snort intrusion detection systems,* US Naval Postgraduate School, Monterey, California.

J. Allen, A. Christie, W. Fithen, J. McHugh, J. Picket & E. Stoner. 2000, *State of the practice of intrusion detection technologies.* Carnegie Mellon University, United States.

amazon 2012, *Acceptable use policy* [online]. Available at: http://aws.amazon.com/aup/ [Accessed January 30 2012].

Amazon *Premium support* [online]. Available at: http://aws.amazon.com/premiumsupport/ [Accessed 30 January 2012].

Anon, *What is eucalyptus?*[online]. Available at: http://open.eucalyptus.com/learn/what-is-eucalyptus [Accessed January 25 2012].

Anonymous 17 February, 2011, ***UK cyber crime costs £27bn a year - government report*** [online]. Available at: http://www.bbc.co.uk/news/uk-politics-12492309 [Accessed 28 January 2012].

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., et al. 2010, "A view of cloud computing", *Association for computing machinery.communications of the ACM,* Vol. 53, no. 4, pp. 50.

Balzarotti, D. 2006, *Testing network intrusion detection systems,* Politecnico di Milano.

Barbour, T. 2011, "Cloud computing", *Alaska business monthly,* Vol. 27, no. 6, pp. 36.

Baun, C. & Kunze, M. 2012, "A taxonomy study on cloud computing systems and technologies." in: *Cloud computing methodology, systems and applications,* ed. l. Wang, R. Ranjan, J. Chen & B. Benatallah, 1st edn, CRC Press, Boca Raton, FL, United States, pp. 73-74-90.

S. Bellovin. 2004, *A look back at security problems in the TCP/IP protocol suite.* 20th Annual Computer Security Applications Conference (ACSAC), December 2004.

Bhaskar, P.R., Eunmi, C. & Lumb, I. 2010, "A taxonomy, survey and issues of cloud computing ecosystems." in: *Cloud computing, principles, systems and applications,* ed. N. Antonopoulos & L. Gillam, 1st edn, Springer, London, pp. 21-46.

Biggs, S.V., S 2009, "Cloud computing: The impact on digital forensic investigations, 4th international conference for internet technology and secured transactions (ICITST-2009)", 09 November 2009, .

Biggs, S. & Vidalis, S. 2009, "Cloud computing: The impact on digital forensic investigations", *4th international conference for internet technology and secured transactions (ICITST-2009)* London, November 9, 2009, .

C.A.P. Boyce & A.N. Zincir-Heywood. 2004, *A comparison of four intrusion detection systems.* Dalhousie University, Halifax, NS.

Braendle, M., Naedele, M., Koch, T., ABB & Vahldieck, R., ABB 2008, "Strictly no admittance", *Power engineering international,* Vol. 16, no. 8, pp. 38.

Burnett, M. 2006, "How I secured one company's network", *Windows IT security,* Vol. 6, no. 10, pp. 6.

Buyya, R., Chee Shin Yeo & Venugopal, S. 2008, "Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities", *High performance computing and communications, 2008. HPCC '08. 10th IEEE international conference on*, pp. 5.

T. Champion & M.L. Denz. 2001, *A benchmark evaluation of network intrusion detection systems.* (0-7803-6599-2), IEEE,.

Chen, T.M. 2010, "Stuxnet, the real start of cyber warfare? [editor's note]", *Network, IEEE,* Vol. 24, no. 6, pp. 2-3.

Corera, G. *BBC news - GCHQ chief reports 'disturbing' cyber-attacks on UK* [online]. Available at: http://www.bbc.co.uk/news/uk-15516959 [Accessed 11/1/2011 2011].

Danford, T. 2003, "Learning to protect a network", *Optimize,* , pp. 74.

Day, D.J. & Burns, B.M. 2011, "A performance analysis of snort and suricata network intrusion detection and prevention engines", *The fifth international conference on digital society* Guadeloupe, 23-28 February, 2011, IARIA, , pp. 187.

Denning, D.E. 1987, "An intrusion-detection model", *IEEE transactions on software engineering,* Vol. SE-13, no. 2, pp. 1-17.

Dikaiakos, M., Katsaros, D., Mehra, P., Pallis, G. & Vakali, A. 2009, "Cloud computing: Distributed internet computing for IT and scientific research", *IEEE internet computing,* Vol. 13, no. 5, pp. 10.

Dong, L.X. & Wang, J.Z. 2003, *Penetration testing - an useful form of computer network security testing,* .

Dye, M.A., Mcdonald, R. & Rufi, A.W. 2008, *Network fundamentals - CCNA exploration companion guide,* 4th edn, Cisco Press, Indianapolis, Indiana, United States.

J. Faulhaber, D. Felstead & P. Henry. 2011, *Microsoft security intelligence report - ZEROING IN ON MALWARE PROPAGATION METHODS.* (Volume 11), Microsoft, Redmond, Washington.

Galante, J., Kharif, O. and Alpayev, P. 2011, **Sony network breach shows amazon Cloud's appeal for hackers**, *Bloomberg,* May 16, p. http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html.

Geiger, R. 2005, "Intelligence behind intrusion protection", *Security technology & design,* Vol. 15, no. 3, pp. 46.

Guilbault, N. & Guha, R. 2009, *Experiment setup for temporal distributed intrusion detection system on amazon's elastic compute cloud,* .

Hamouda, S.K. & Glauert, J. 2012, "Security, privacy and trust management issues for cloud computing." in: *Cloud computing - methodology, systems and applications,* ed. L. Wang, R. ranjan, J. Chen & B. Benatallah, 1st edn, CRC Press, Boca Raton, FL, United States, pp. p389-421.

Hofmann, A. & Sick, B. 2011, "Online intrusion alert aggregation with generative data stream modeling", *IEEE transactions on dependable and secure computing,* Vol. 8, no. 2, pp. 282.

Holstein, M. *How does fragroute evade IDS detection?*[online]. Available at: http://www.sans.org/security-resources/idfaq/fragroute.php [Accessed January 30 2012].

Hwee, O.G. & Kiat, K.W. 2006, *Rate limiting with network monitor approach to counter DDoS attacks in distributed computing environments,* .

Information Commissioners Office 2011, *Key definitions of the data protection act* [online]. Available at: http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx [Accessed December 30 2011].

Kelion, L. 2012, ***Expect more online attacks, anonymous hackers say*** [online]. Available at: http://www.bbc.co.uk/news/uk-17648852 [Accessed 08 April 2012].

Khan, I., Habib-ur, R. & Zahid, A. 2011, "Design and deployment of a trusted eucalyptus cloud", *2011 IEEE 4th international conference on cloud computing* Washington, DC, United States, 4-9 July, IEEE, , pp. 380.

Khan, I., Rehman, H. & Anwar, Z. 2011, "Design and deployment of a trusted eucalyptus cloud", *Cloud computing (CLOUD), 2011 IEEE international conference on*, pp. 380.

Kim, B. 2006, "Protecting agent from attack in grid computing(II)", *Intelligent data engineering and automated learning - ideal 2006, proceedings,* Vol. 4224, , pp. 1174-1181.

Kohlenberg, T. (ed) 2007, *Snort IDS & IPS toolkit*, 1st edn, Syngress, Burlington, MA, United States.

Kruegel, C. & Robertson, W. *Alert verification - determining the success of intrusion attempts,* University of California, Santa Barbara.

Krutz, L.R. & Vines, R.D. 2010, *Cloud security - a comprehensive guide to secure cloud computing,* 1st edn, Wiley, Indianapolic, Indiana, United States.

Krutz, R. & Vines, R. 2007, *The CEH prep guide: The comprehensive guide to certified ethical hacking,* Wiley,.

Kurose, J. & Ross, K. 2008, *Computer networking - A top down approach,* 4th edn, Pearson, Boston, M.A., United States.

Li, Z., Ma, Y., Wang, L., Lei, J. & Ma, J. 2011, "A novel real-time aggregation method on network security events", *Kybernetes,* Vol. 40, no. 5/6, pp. 912.

Lillard, T.V., Garrison, C.P., Schiller, C.A. & Steele, J. 2010, "Chapter 12 - the future of cloud computing." in: *Digital forensics for network, internet, and cloud computing,* Syngress, Boston, pp. 319-339.

Lippmann, R.P., Fried, D.J., Graf, I., Haines, J.W., Kendall, K.R., McClung, D., Weber, D., Webster, S.E., Wyschogrod, D., Cunningham, R.K. & Zissman, M.A. 2000, "Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation", *DARPA information survivability conference and exposition, 2000. DISCEX '00. proceedings*, pp. 12.

Massicotte, F., Gagnon, F., Labiche, Y., Briand, L. & Couture, M. 2006, "Automatic evaluation of intrusion detection systems", *22nd annual computer security applications conference (IEEE)*2006, .

Mazzarielo, C., Bifulco, R. & Canonico, R. 2010, "Integrating a network IDS into an open source cloud computing environment", *6th international conference on information assurance and security* Atlanta, G.A., United States, IEEE, , pp. 265.

P. Mell, V. Hu, R. Lippman, J. Haines & M. Zissman. 2010, *An overview of issues in testing intrusion detection systems.* (1), NIST, United States of America.

Mell, P. & Grance, T. 2010, "The NIST definition of cloud computing", *Association for computing machinery.communications of the ACM,* Vol. 53, no. 6, pp. 50.

Miller, M. 2009, *Cloud computing - web-based applications that change the way you work and collaborate online,* 2nd edn, Que, Indianapolis, Indiana.

Muthuregunathan, R., Siddharth, S., Srivathsan, R. & Rajesh, S.R. 2009, *Efficient snort rule generation using evolutionary computing for network intrusion detection,* .

D. Mutz, C. Kruegel, w. Robertson, G. Vigna & R. Kemmerer. 2005, *Reverse engineering of network signatures.* www.iseclabs.org/papers, University of California, Santa Barbara.

Noh, S., Jung, G., Choi, K. & Lee, C. 2008, "Compiling network traffic into rules using soft computing methods for the detection of flooding attacks", *Applied soft computing,* Vol. 8, no. 3, pp. 1200-1210.

Onwubiko, C. 2010, "Chapter 16, security issues to cloud computing." in: *Cloud computing, principles, systems and applications,* ed. N. Antonopoulos & L. Gillam, 1st edn, Springer, London, pp. 271-272-288.

Open Nebula 2012, *About the open nebula project* [online]. Available at: http://opennebula.org/about:about [Accessed 29 March 2012].

Owen, D. *What is a false positive, and why are false positives a problem?*[online]. Available at: http://www.sans.org/security-resources/idfaq/false_positive.php [Accessed January 30 2012].

T. Ptacek. 1998, *Insertion, evasion, andDenial of service: Eluding network intrusion detection.* Secure Networks Inc, United States.

N. Puketza, K. Zhang, M. Chung, B. Mukherjee & R. Olsson. 1996, *A methodology for testing intrusion detection systems.* National Security Agency INFOSEC University Research Program, California, United States.

Rhoton, J. 2011, *Cloud computing explained,* 2nd edn, Recursive Press, United Kingdom & United States (simultaneously).

Richter, R. 2011, *Hyenae - description* [online]. Available at: http://sourceforge.net/projects/hyenae/?_test=b [Accessed 28 March 2012].

Ristenpart, T., Tromer, E., Shacham, H. & Savage, S. 2009, "Hey, you, get off of my cloud", Chicago, Illinois, US, 9-13 November, 2009, Conference on computer and communications security, 2009, Chicago, Illinois, US, pp. 1.

Ros, S. 2009, "Intrusion detection in the cloud", *Dependable, autonomic and secure computing (DASC), IEEE international symposium on,* , pp. 729-734.

Sarno, D. and Rodriguez, S. 2011, Hacker attacks show vulnerability of cloud computing, *Los Angeles Times,* Jun 7, 2011, .

Scarfone, K. & Mell, P. 2007, *NIST IT security: Content / / NIST SP 800-94, guide to intrusion detection and prevention systems (IDPS)*, http://www.nist.org/nist_plugins/content/content.php?content.64 edn.

Selim, S., Hashem, M. & Nazmy, T. 2011, "Hybrid multi-level intrusion detection system", *International journal of computer science and information security,* Vol. 9, no. 5, pp. 23.

Sempolinski, P. & Thain, D. 2010, "A comparison and critique of eucalyptus, OpenNebula and nimbus", *2nd IEEE international conference on cloud computing technology and science* Indianapolis, 30 November - December 3 2010, IEEE, United States, pp. 417.

Sempolinski, P. & Thain, D. 2012, "An introduction to open-source IaaS cloud middleware." in: *Cloud computing, methodology, systems and applications,* ed. W. Lizhe, R. Ranjan, C. Jinjun & B. Benatallah, 1st edn, Taylor Francis, Boca Raton, Fl, United States, pp. 133-133-149.

Simpson, M. 2006, *Hands-on ethical hacking and network defense,* 1st edn, Cengage, Boston, M.A., United States.

Soh, B.C. & Young, S. 1998, "Distributed computing: An experimental investigation of a malicious denial-of-service applet", *Computer communications,* Vol. 21, no. 7, pp. 670-674.

Stephenson, P. 2011, "Protecting the castle gates", *SC magazine,* Vol. 22, no. 4, pp. 33.

Steve, M. 2008, "Danger in the clouds", *Network security,* Vol. 2008, no. 12, pp. 9-11.

Subashini, S. & Kavitha, V. 2011, "A survey on security issues in service delivery models of cloud computing ", *Journal of network and computer applications,* Vol. 34, no. 1, pp. 1 <last_page> 11.

Tchifilionova, V. 2010, iNetSec'10 Proceedings of the 2010 IFIP WG 11.4 international conference on Open research problems in network security, Springer-Verlag Berlin, Heidelberg.

S. Thorn Dr. 2011, *An evaluation of openstack for the ETF.* UK Engineering Task Force, University of Edinburgh.

Treacy, B. & Bruening, P. 2009, "Cloud computing - data protection concerns unwrapped", *Privacy & data protection,* [online], Vol. 9, no. 3, pp. 25 January 2012. Available at: http://www.pdpjournals.com/overview-privacy-and-data-protection.

M.W. Tzeyoung. 2009, *Intrusion detection systems.* IATAC, Hendon, VA, United States.

Ubuntu Community Documentation 2010, [online]. Available at: https://help.ubuntu.com/community/UEC/PackageInstall [Accessed March 28 2012].

US Dpt of Health & Human Services, . 2011, ***Understanding health information privacy*** [online]. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html [Accessed December 30 2011].

T. Verwoerd & R. Hunt. 2001, *Intrusion detection techniques and approaches.* Elsevier, New Zealand.

Vic (J.R.), W. 2011, "Chapter 10 - operating a cloud." in: *Securing the cloud,* Syngress, Boston, pp. 253-277.

Vic (J.R.), W. 2011, "Chapter 4 - securing the cloud: Architecture." in: *Securing the cloud,* Syngress, Boston, pp. 89-123.

Vic (J.R.), W. 2011, "Chapter 6 - securing the cloud: Key strategies and best practices." in: *Securing the cloud,* Syngress, Boston, pp. 153-185.

Vic (J.R.), W. 2011, "Chapter 8 - security criteria: Selecting an external cloud provider." in: *Securing the cloud,* Syngress, Boston, pp. 211-232.

Vic (J.R.), W. 2011, "Chapter 9 - evaluating cloud security: An information security framework." in: *Securing the cloud,* Syngress, Boston, pp. 233-252.

Wang, K. & Stolfo, S. 2004, "Anomalous payload-based network intrusion detection", *Seventh international symposium on recent advances in intrusion DetectionS*, ed. E. Jonsson, Springer-Verlag, Berlin, pp. 203.

Watts, S. 26 January, 2012, ***Call for cyberwar 'peacekeepers' force*** [online]. Available at: http://news.bbc.co.uk/1/hi/programmes/newsnight/9687338.stm [Accessed 28 January 2012].

Wilbanks, L. 2007, "Cybersecurity: Welcome to my world", *IT professional magazine,* Vol. 9, no. 2, pp. 61.

APPENDICES

Configurations of all applications

Tech Log UEC INSTALLATION

Creating the UEC Cloud Controller:

Installation from Ubuntu Server 10.04 installer CD, with a single system serving as the cloud controller with one other node attached.

Insert disk for ubuntu 10-4-LTS
Select English
Select Install Ubuntu Enterprise Cloud
Select United Kingdom for location, do not detect keyboard type-use default UK settings as suggested by Installer
Select Enter hostname UEC-CC
'Select Cloud Installation Mode' – leave blank, this will be the cloud controller
Select Cloud controller
Name the machine: UEC-CC
Accept default time zone London/Europe
Select 'use entire disk and set up LVM'
Select default entry for disk selection – SCSI3
@ 'Write changes to disk?' select yes
Use default volume group amount of 21.2GB
@ 'Write changes to disk?' select yes
Insert user name : student dd
Insert password : 051069
'Use weak password?' – yes
'HTTP proxy?' – leave blank
'How do you want to manage upgrades?' – no automatic updates (experiment is within lab conditions not actual network)
Accept default Eucalyptus cluster name of : cluster1
Insert IP address range : 192.168.1.0-192.16..1.255
Accept system 'mail name' as UEC-CC.localdomain
'Install GRUB boot loader?' : yes

Creating the UEC Node:

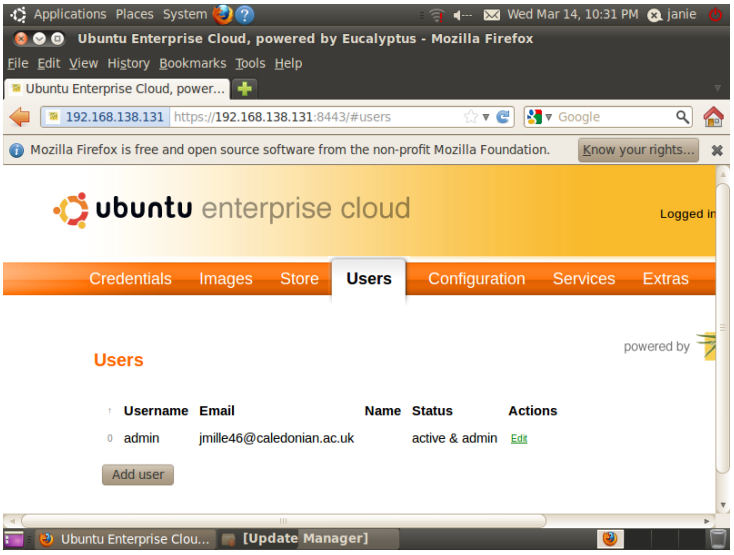
Insert CD, select English as language
Select Install Ubuntu Enterprise Cloud
Name the machine: UEC-NODE
Installation will detect the cluster controller and present the Node installation option, select this option
Confirm the partitioning scheme

Obtaining Credentials:

Install Ubuntu desktop to access web?
Sudo apt-get install ubuntu-desktop
Type: sudo gdm to open up window or reboot using
'sudo shutdown –r now'

In Firefox, in browser, type: https://192.168.138.131:8443
When prompted, add exception,
You are now presented with the UEC login page
Username is: admin
Password is: admin

Configuration page prompts for new password to activate Eucalyptus installation, change password to: 051069
Click submit button at bottom of screen, and screen changes to this:



Click: credentials
Click: download credentials

Go back to cmd line via terminal, and locate file 'euca2-admin-x509.zip' which should be under 'Downloads'

Type: mv euca2-admin-x509.zip ~/.euca
Type: unzip ~/.euca
Install
Euca2ools: sud apt-get install euca2ools
Type: . ~./euca/eucarc
Type: . ~/.euca/eucarc – to validate everything is working ok
  (this didn't work saying eucarc not a directory

Go back to UEC web page on browser and click 'Store' tab, select an image you wish to run:

Store tab would not connect giving an error message:

This is a python fault? And the remedy was found online, sheet attached, updates gained and file edited using vi to insert changes, entries were:

Cd to /usr/lib/python2.6/dist-packages/imagestore/lib

Type: sudo vi fetch.py
Edit at line 142:

```
Curl.setopt(pycurl.SSL_VERIFYPEER, 0)
Curl.setopt(pycurl.SSL_VERIFYHOST, 0)
```

Sudo wget –P /usr/local/share/ca-certificates/ --no-check-certificate https://certs.godady.com/repository/gd-class2-root.crt https://certs.godaddy.com

sudo update-ca certificates

Store tab should work now

Click: image to download – Ubuntu 10-4-lts was downloaded
Click: how to run – after image has downloaded

To Run Instance:

Create a key pair:

```
If { ! –e ~/.euca/mykey.priv }; then
    mkdir –p –m 700 ~/.euca
    touch ~/.euca/mykey.priv
    chmod 0600 ~/.euca/mykey.priv
    euca-add-keypair mykey > ~/.euca/mykey.priv
fi
```

Facilitate access for instances on port 22

```
euca-authorize default –P tcp –p 22 –s 0.0.0.0/0
```

Start to create instances of the image you downloaded:

```
euca-run-instances $EMI –k mykey –t ml.small
```

```
watch –n5 euca-describe-instances
```

- The state of the instance will eventually change to running – it shows pending until it caches

Connect to the instance by typing:

```
IPADDR=$(EUCA-DESCRIBE-INSTANCES | grep $EMI | grep running | tall –nl | awk '(print $4)')
Ssh –I #/.euca/mykey.priv ubuntu@192.168.0.10
```

Snort Installation Tech Log

The technical guide titled 'Snort 2.9.2 and Snort Report 1.3.3 on Ubuntu 10.04 LTS Installation Guide' by David Gullet of Symmetrix Technologies was followed to install Snort.

Download ISO of ubuntu 10-4-LTS(i386)server

Install ubuntu-10-4-server as operating system on the intended Snort machine.

Once server was installed, openssh-server was installed manually via: sudo apt-get install openssh-server

Packages that were required to run Snort and Snort report were added at this point

```
Sudo apt-get install nmap
Sudo apt-get install nbtscan
Sudo apt-get install apache2
Sudo apt-get install php5
Sudo apt-get install php5-mysql
Sudo apt-get install php5-gd
Sudo apt-get install libpcap0.8-dev
Sudo apt-get install libpcre3-dev
Sudo apt-get install g++
Sudo apt-get install bison
Sudo apt-get install flex
Sudo apt-get install libpcap-ruby
```

Mysql server was installed

```
Sudo apt-get install mysql-server
Sudo apt-get install libmysqlclient16-dev
```

Ubuntu was updated using the sudo apt-get update and apt-get upgrade entries

Snort Report Installation

Download Snort Report:

```
Sudo wget http://www.symmetrixtech.com/ids/snortreport-1.3.3.tar.gz
```

Untar the file:

```
Sudo tar zxvf snortreport-1.3.1.tar.gz –C /var/www/
```

Edit the snort report config file with MySQL login password and the location of the libraries for jpgraph

```
Sudo vi /var/www/snortreport-1.3.3/srconf.php
```

Scroll down, press insert key and change $pass = “YOURPASS” to $pass = “051069” ie the password you set for MySQL, then press esc and :wq to save

Getting the Data Acquisition API for SNORT:

```
Sudo wget http://www.snort.org/dl/snort-current/daq-
0.6.2.tar.gz
sudo tar zxvf daq-0.6.2.tar.gz
Cd daq-0.6.2
Sudo ./configure
Sudo make
Sudo make install
```

Get libdnet and install

```
Sudo wget http://libdnet.googlecode.com/files/libdnet-
1.12.tar.gz
Sudo tar zxvf libdnet-1.12.tar.gz
Cd libdnet-1.12/
Sudo ./configure
Sudo make
Sudo make install
Sudo ln –s /usr/local/lib/libdnet.1.0.1 /usr/lib/libdnet.1
```

Downloading Snort and Installation

The correct entry to download Snort was found on the Snort website which gave instructions on how to download from CLI And install on /usr/local/snort

```
Sudo wget http://www.snort.org/dl/snort-current/snort-
2.9.2.tar.gz
```

Untar the file:

```
Sudo tar zxvf snort-2.9.2.tar.gz
Cd snort-2.9.2
Sudo ./configure –prefix=/usr/local/snort
sudo make
sudo make install
sudo mkdir /var/log/snort
sudo mkdir /var/snort
sudo groupadd snort
sudo useradd –g snort snort
sudo chown snort:snort /var/log/snort
```

enter MySQL password to creat the snort database:

```
echo “create database snort;” | mysql –u root –p
```

prompt to enter password: 051069
mysql –u root –p –D snort < ./schemas/create_mysql
create an additional MySQL user for Snort instead of using root:
echo “grant create, insert, select, delete, update on snort.* to snort@localhost identified by ‘050169’” | mysql –u root –p
-reponse is that it asks for password which is also ‘051069’
Type: \c – to end entry
Then type: exit

Downloading Snort Rules

A bit of rooting about had to be done to get the right combination for this, finally on snort.org found details of the entry and the need for an ‘oink code’ the entry is as follows:
Sudo wget https://www.snort.org/sub-rules/snortrules-snapshot-2920.tar.gz/88059568c27e264c7f869d37409076403a32cc5b -O snortrules-snapshot-2920.tar.gz
The response is request for sudo password: 051069
Then,
Sudo tar zxvf snortrule-snapshot-2920.tar.gz –C /usr/local/snort
Sudo mkdir /usr/local/snort/lib/dynamic-rules
sudo cp /usr/local/snort/so_rules/precompiled/Ubuntu-10-4/i386/2.9.2.0/* \
/usr/local/snort/lib/snort_dynamicrules
sudo touch /usr/local/snort/rules/white_list.rules
sudo touch /usr/local/snort/rules/black_list.rules
sudo ldconfig

Snort conf file needed to be edited:

sudo vi /usr/local/snort/etc/snort.conf

scroll down page to approx 16% mark and change the lines to read:

var WHITE_LIST_PATH /usr/local/snort/rules
var BLACK_LIST_PATH /usr/local/snort/rules

scroll down to approx 38% and change to show the following:

dynamicpreprocessor directory /usr/local/snort/lib/snort_dynamicpreprocessor/
dynamicengine /usr/local/snort/lib/snort_dynamicengine/libsf_engine.so
dynamicdetection directory /usr/local/snort/lib/snort_dynamicrules

at the 80% mark, go to this line:
#output unified2: filename merged.log, limit 128, nostamp, \
mpls_event_types, vlan_event_types

and inser underneath it:

output unified2: filename snort.u2, limit 128
(this to send the output of the unified2 files to Barnyard)

press ‘esc’ and type :wq to save and exit

INSTALLING BARNYARD

sudo tar zxvf barnyard2-1.9.tar.gz
cd barnyard2-1.9
sudo ./configure --with-mysql
sudo make
sudo make install
sudo cp etc/barnyard2.conf /usr/local/snort/etc
sudo mkdir /var/log/barnyard2
sudo chmod 666 /var/log/barnyard2
sudo touch /var/log/snort/barnyard2.waldo
sudo chown snort.snort /var/log/snort/barnyard2.waldo

go to barnyard2.conf and reconfigure line to say:

sudo vi /usr/local/snort/etc/barnyard2.conf
At 3% mark on page
config reference_file: /usr/local/snort/etc/reference.config
config classification_file:
/usr/local/snort/etc/classification.config
config gen_file: /usr/local/snort/etc/gen-msg.map
config sid_file: /usr/local/snort/etc/sid-msg.map
config hostname: localhost
config interface: eth1

At the 89% mark on page:
output database: log, mysql, user=snort password=YOURPASSWORD
dbname=snort \
host=localhost

Configure the IP Addresses:

sudo vi /etc/network/interfaces

auto eth1

```
iface eth1 inet static
address 192.168.0.5
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.1.255
gateway 192.168.0.1

auto eth0
iface eth1 inet manual
ifconfig eth1 up
```

press ‘esc’ and :wq to save and exit the file

To refresh networking with the new IPs:

```
sudo /etc/init.d/networking restart
```

Attempt to run Snort:

```
Sudo ifconfig eth0 up –promisc   : will start second NIC card

sudo /usr/local/snort/bin/snort -u snort -g snort -c
/usr/local/snort/etc/snort.conf -i eth1 : starts Snort running
```

From the pc attached to the server running Snort type in browser:

```
http://192.168.1.5/snortreport-1.3.3/alerts.php
```

to view Snort Report

Hyenae Configuration

The application was very straightforward and required the relevant fields such as source pattern (IP and MAC addresses) destination pattern, TCP flags to be set etc, before clicking execute. The application advised when attack was running, if an error had occurred or attack had been sent and completed.

Below is shown a screen shot of the interface of the application.