ENHANCING SECURITY CONCERNS IN CLOUD COMPUTING VIRTUAL MACHINES

(CASE STUDY: CENTRAL BANK OF SUDAN)

SAMAH SABIR MOHAMED HASSAN

MSc, INFORMATION AND COMMUNICATION TECHNOLOGY

AL-MADINAH INTERNATIONAL UNIVERSITY

JUNE 2014

ENHANCING SECURITY CONCERNS IN CLOUD COMPUTING VIRTUAL MACHINES

(CASE STUDY: CENTRAL BANK OF SUDAN)

By

SAMAH SABIR MOHAMED HASSAN

Thesis Proposal Submitted to Faculty of Computer & Information Technology

Al-Madinah International University

in Fulfillment of the Requirements for the Degree of

MASTER OF SCIENCE IN INFORMATION AND COMMUNICATION TECHNOLOGY

Certification of thesis work

PERMISSION TO USE

In presenting this thesis in fulfillment of the requirements for a postgraduate degree from Al-Madinah International University, I agree that the University Library make it freely available for inspection. I further agree that permission for copying of this dissertation in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor or, in his absence by the Dean of Faculty of Finance & Administrative Sciences or the dean of Postgraduate Studies. It is understood that any copying or publication or use of this dissertation or parts thereof for financial gain shall be given to me and to Al-Madinah International University for any scholarly use which may be made of any material from my dissertation.

Request for permission to copy or make other use of materials in this thesis, in whole or in part should be addressed to:

Dean of Faculty of Computer & Information Technology or the Dean of Postgraduate Studies

40100

11th floor –Plaza Masalam

Sec 9, Shah Alam

Malaysia

Abstract

Cloud computing like virtualization has been attracting a lot of attention lately. Many organizations have already virtualized their environment and are planning on adopting cloud computing. Moving to the cloud from a virtual environment is easier than a physical one due to the fact that Virtualization is considered as the foundational element of cloud computing and helps deliver on the value of cloud computing. However, the risks associated with virtualization when moving to the cloud from a virtual environment are problematic for many companies.

The negative effects of these risks on the adoption of cloud computing is what led us to conduct a research project with two objectives. The first objective is to investigate and highlight what the risks associated with current virtualization environment of Central bank of Sudan are most disturbing. The second objective is how to evaluate these risks and which approaches can be used to reduce these risks. The approaches of risk reduction can consist of people, process, and technology based controls.

Based on a review of literature on the risks of virtualization, interviews and questionnaires with virtualization experts in different organizations an overview of the most worrying risks was created. The results indicate that data management, external attacks, security training and awareness are the top three of the most worrisome risk of CBOS. These risks are discussed in detail along with the approaches taken to reduce these risks.

This thesis however did bear some limitations due to the scattering of relevant literature and websites. Also there is the problem related to the embargo which made it impossible to contact any vendors for information on possible sources of existing methods, so the overview of existing methods cannot be exhaustive.

Keywords: Virtual machines, Risks, Cloud Computing, Virtualization

Acknowledgements

The research process is by no mean an isolated activity and I am grateful to all those who helped me in completing my research work. First and foremost, I would like to thank Dr. Shadi Hillies, my supervisor, for his valuable input, guidance and timely support. Thank you for never saying no to any of my enquiries.

I am much obliged to my friends, Mohamed Mahmoud Abkam and Elrasheed Babikir for extensive proof-reading of my thesis draft and guiding me in regards to my grammatical errors. They deserve my deepest gratitude for being so kind and helpful. I would like to thank all the interview and questionnaire participants who kindly shared their views, ideas and knowledge with me. Without their support, I would have never been able to achieve the outcome I did with this research work.

Samah Sabir Mohamed

June 2014

.

Dedication

Commitment, effort, and dedication were fundamental elements for the completion of my master thesis, but even more was the support of my family. To my father Dr. Sabir Mohamed Hassan whom is my idol for his endless support and encouragement throughout the years. To my mother, husband and children for their love and patience today I dedicate them this important professional achievement because without their presence, support, and comprehension I would have not achieved my goal. I love you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

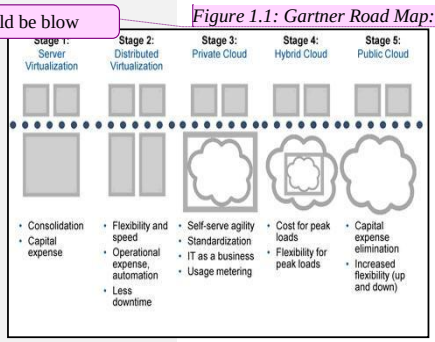
1.0 INTRODUCTION

Virtualization has become one of the most attractive and widely used technologies today. The ability to share resources of a single physical machine between several isolated virtual machines (VM) enables more optimization in hardware utilization. Also virtual machine offer the ease of management and migration compared to its physical counterpart. However, adding another abstraction layer between hardware and software raises new security challenges.

In today's global software markets every business needs to play a major role and respond faster to the changes that are happening in the software market based on customer demands and the growth opportunities. For this to occur we need have a flexible infrastructure that can be upgraded to the current changes in the market. Virtualization is a key element in cloud computing, because it is really an entry point to a much longer evolution that will lead to cloud computing thus changing technology architectures, management tools, operational processes, customer relationships, funding models and nearly everything along the way. The path from virtualization to cloud computing is achieved through five stages Server Virtualization, Distributed Virtualization, Private Cloud, Hybrid Cloud and Public Cloud (Figure 1.1) (Bittman, 2011).

Comment [L1]: Title should be blow

Figure 1.1: Gartner Road Map: From Virtualization to Cloud Computing



Source: Gartner (March2011)

Comment [L2]: Problem statement should be clear.

1.0.1 Problem Statement

Now we are in the middle of a technology hype cycle called cloud computing. According to the Gartner Group (Smith, 2013) we are at the peak of inflated expectations. Despite the media hyping cloud computing, there can still be

tremendous benefit to many who adopt a cloud computing strategy. This benefit exists for industry, government and the general public alike.

As a result, virtualization and virtualization security have gone through major transforms in the recent years. Virtualization and its unique architecture have many characteristics and advantages over traditional non-virtualized machines. However, these new characteristics create new vulnerabilities and possible attacks on a virtualized system. This has caused a widespread of concern regarding virtualization security. Since Cloud computing, is an umbrella term that encompasses virtualization. There are certain issues to address when adopting virtualization in any environment, there are additional security concerns that arise when using virtualization to support a cloud environment. Moving to the cloud from a virtual environment can be complicated because there are many risks which are associated with virtualization. Poor knowledge about the risks and a lack of good methods to mitigate these risks reduces the speed at which companies adopt cloud computing in the future (Chow, et al., 2009). Most likely the initial reaction of people would be to avoid moving to the cloud. This represents a general lack of understanding but at the same time can be a valid concern.

Comment [L3]: What is the differences between Aims and Objectives

1.0.2 Objective and Aims

This research aims to investigate and highlight what the risks associated with current virtualization environment of Central bank of Sudan are, how to evaluate them and which approaches can be used to reduce these risks.

1.0.2.1 Objectives

The specific objectives of his research is to determine what the virtualization security risks are when moving to the cloud from a virtual environment, how to evaluate these risks and which approaches can be used to reduce these risks. These approaches may be existing approaches which are available and can be applied or entirely new approaches may be found. This will assist Central bank of Sudan as well as other organizations in making their decisions on whether they are ready to move to the cloud from a virtual environment or not.

1.0.3 Research Questions

In order to determine which risks this thesis needs to focus on. We will first determine what the virtualization security risks are the question by answering the first research question which is:

- What are the risks / challenges of virtualization?

Next we will need to determine what are the most important virtualization risks and because they are many it is not possible to cover all the risks. Therefore, only the three most critical risks will be chosen according to customer prospective. This will lead us to the second research question which is:

- What are the most critical risks of virtualization?

The answers to the second question will lead us to the third research question which is:

- Are there existing approaches which are used to reduce this risk?

If the answer to question three is no we will answer a fourth research question which is:

- Are there existing approaches from outside the virtualization domain which can be which can be used to reduce the risk?

If the answer to question four is no, we will check if it is possible to find new solutions and what these solutions are. These questions will be answered for each risk individually.

Comment [L4]: I think this statement not match with the above questions, also the research questions not match the research objectives.

1.0.4 Significance of the Study

Almost every organization today depends on technology for running its business efficiently and effectively in one way or another. This dependency along with the rapid growth of the internet has lead organizations to incorporate virtualization in their data centers to fully utilize their hardware resources in order to achieve the required scalability, availability and performance. As organizations move toward virtualizing more of their servers and data center infrastructure, they need specialized protective technologies that match this environment.

There are several important security concerns that need to be addressed when considering the use of virtualization for cloud computing. These concerns are many but the major concerns are (Winkler, 2011):

a. There is a possibility of compromising the virtual machine (VM) hypervisor. If the hypervisor is vulnerable to exploit, it will become a primary target. At the scale of the cloud, such a risk would have broad impact if not otherwise mitigated. This requires an additional degree of network isolation and enhanced detection by security monitoring.
b. The nature of allocating and de-allocating resources such as local storage associated with VMs. During the deployment and operation of a VM, data is written to physical memory. If it's not cleared before those resources are reallocated to the next VM, there's a potential for exposure.
c. The theoretical technique for limiting traffic flow between VMs would be to use segregation to gather and isolate different classes of VMs from each other. VMs could be traced to their owners throughout their lifecycle. They would only be collocated on physical servers with other VMs that meet those same requirements for colocation.
d. When considering the security issues with VMs, it's important to recognize that this technology is not new. Several products have undergone formal security evaluations and received certification. What this means in practical terms is that several VM technology vendors have taken pains to obtain independent and recognized security certification.

Comment [L5]: Most of the above points not related with risk, also is it all form the above reference, how far these points from the case in bank od Sudan

Moving to the cloud from a virtual environment comes with many risks. But how big are these risks? And how can they be mitigated? Companies that want to move a part of or maybe all of their environments into the cloud often have these questions, while they can be very hard to answer. Because of this organizations are hesitant to move their current virtual environment to the cloud. This hesitation is causing a great delay in the adoption of cloud services.

It can be concluded that the uncertainty about the risks of virtualization forms a barrier to cloud adoption. This barrier can be gradually removed by making organizations aware of what these risks are and using effective approaches to reduce the risks.

1.0.5 Scope of the Study

This thesis discusses, improving or introducing several approaches to reduce these risks using technology. Due to the fact that there are many risks in Virtualization not all will be covered. A selection of three risks will be made and these will be the focus of this research. A search will be made for approaches that already exist will be made to reduce these risks. If not found other approaches will be mentioned if they will reduce these risks. If not it will also be stated.

Comment [L6]: What type of Technology?

Comment [L7]: Why? What is the support for that?

Comment [L8]: This statement confuse, so the research will not cane with new approach only focus on exist approaches.

1.1 CLOUD COMPUTING

This chapter outlines the benefits and challenges of cloud computing and virtualization. It is divided into two parts, first it begins with the history of clouds, definition of cloud computing based on NIST definition, the different types of computing services available, the key characteristics of cloud , benefits & limitations of cloud computing. Next there will be the history & definition of virtualization, Classification of virtualization, advantages & challenges and then virtualization security. The main focus of this chapter will be on the challenges and risks of virtualization that may occur when moving to the cloud from a virtual environment.

Comment [L9]: Stand for what?

Comment [L10]: This statement deference from first statement above.

1.1.1 History of Cloud Computing

Even though you might have heard about Cloud computing just recently, the concept behind it has been around for some time now. In the early '60s and '70s, most people used a centralized computing model, typically consisting of supercomputers located behind the glass walls of an internal data center. These supercomputers, with all the software, storage devices, printers, etc. were quite expensive, typically costing millions of dollars. The 1980s brought the growing demand for increasingly more powerful and less expensive microprocessors and personal computers, paving the way for low costs and simplicity. Grid and Utility Computing came into play in the early 1990s as the Internet and the World Wide Web exploded into the general computing world moving from centralized, client-server models to Internet-based computing. Application Service Providers (ASP) took the next step in the late 1990's creating the first wave of Internet-enabled applications. An ASP would license a commercial software application to multiple customers. This made it possible for companies to outsource some of their IT needs such as servers and software, saving those companies the time and money spent on everyday IT management (Stark, 2012) .

Time has passed and the technology caught up with the ideas. Therefore in 1999 Salesforce started delivering applications to users using a simple website. The applications were delivered to enterprises over the Internet, and this way the dream of computing sold as utility started being reality. Later in 2002 Amazon started Amazon Web Services, providing services like storage, computation and even human intelligence. However, only starting with the launch of the Elastic Compute Cloud in 2006 a truly commercial service open to everybody existed. The year 2009 marked a

key turning point in the evolution of cloud computing, with the arrival of browser based cloud enterprise applications, with the best known being Google Apps (Blaisdell, 2011).

Today all large companies offer Cloud Computing within a secure environment. Microsoft offers Windows Azure, and Oracle and HP offers cloud computing, and is fast becoming the acceptable way to go. Cloud computing will continue to grow as long as there is a demand for increased data.

1.1.2 What is Cloud Computing

There are many definitions to cloud computing but for this research I prefer to use the NIST definition (Figure 1.2) because it is simple to understand and reflects the IT market. (Mell & Grance, 2011) NIST states that Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

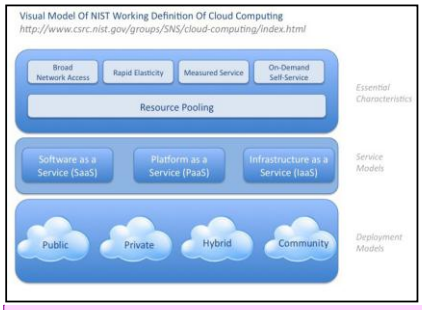


Figure 1.2: The NIST cloud computing definition framework

Comment [L11]: Figure not clear

1.1.3 Characteristics of Clouds

NIST has also defined the Cloud to have five key characteristics: Measured Service, Elasticity, Resource Pooling, On Demand Self Service and Broad Network Access. All are described in (Table 1.1) below.

Table 1.1-Cloud computing characteristics

Characteristic	Description
On-demand self-service	IT is used as service and is readily available on demand without requiring manual intervention.

Broad network access	The service is made available via a network independently of the user end device. The network connection must be of sufficiently high performance and available for that particular service.
Resource pooling	The provider makes the necessary resources available to multiple consumers using technologies such as virtualization and multi-tenancy.
Rapid elasticity	The resources necessary can be provisioned rapidly and released without manual intervention when no longer needed.
Measured Service	A service consumed must be measurable in terms of the re-sources used. In this way, consumption-based billing becomes possible. Also known as "pay as you go" or "pay-per-use."

Source: Based on "The NIST Definition of Cloud Computing" by P. Mell and T. Grance, Special Publication 800-145 (National Institute of Standards and Technology, Gaithersburg, MD, Sept. 2011).

1.1.4 Service Models

Service models are the type of services which the cloud can provide to customers/organization (Figure 1.3).There are three service models IaaS (Infrastructure as a Service), PaaS (Plat-form as a Service), and SaaS (Software as a Service).The type of service received from service providers depends on the service model that has been chosen by the customer.

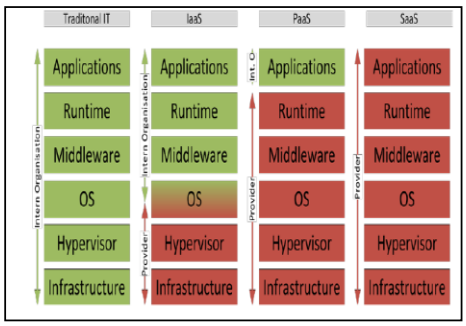


Figure 1.3: Service models

Comment [L12]: What is the deference in colors in the table.

Comment [L13]: What is the relation between this and the risk or the objective of the research?

1.1.4.1 Infrastructure as a Service (IaaS)

This service model provides to the customer with raw storage space, computing, or network resources in which the customer can run and execute an operating system, applications, or any software that they choose. The customer however does not manage or control the cloud infrastructure but can control their operating systems, storage, deployed applications, and may have limited control of some networking components (e.g. host firewalls). Examples of IaaS providers are Amazon, Go Grid and Flexiscale.

1.1.4.2 Platform as a Service (PaaS)

In the PaaS model, the cloud provider provides the customer with the hardware and allows customers to deploy consumer-created or acquired applications created using programming languages and tools that are supported by the service provider. However the customer does not manage or control the cloud infrastructure and this includes network, servers, operating systems, or storage, but has control over their deployed applications and maybe applications hosting environment configurations. Examples of PaaS providers are Google App Engine, Microsoft Windows Azure and Force.com.

1.1.4.3 Software as a Service (SaaS)

In the SaaS service model the customer uses the cloud provider's applications running on a cloud infrastructure. These applications can be accessed from different client devices through a thin client interface such as a web browser. The customer using this model does not manage or control the cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the some exceptions of limited user specific application configuration settings. Examples of SaaS providers are Salesforce.com, Rack space and SAP Business by Design.

1.1.5 Types of Clouds

The different infrastructure deployment models are distinguishing by their architecture, the location of the datacenter where the cloud is realized, and the needs of the cloud provider's customers (Xuefeng, 2012). The three most common types of clouds are Public, Private and Hybrid.

1.1.5.1 Public Cloud

In a public cloud companies can store and manage data and computer programs in a shared IT infrastructure. You share server resources with other businesses in a safe and secure location. Each company's data and applications are separate, so no one can see or access other people's information. You "rent" the amount of space you need, as you need it. All backups, upgrades and maintenance are included in the rental agreement. The public cloud comes with some risks in the areas of security, uptime and performance. There is less direct control over who has access to what, because you're not the only tenant storing data at that location. If you share a network with others, bandwidth can slow down as the number of users increases (Taylor, 2011). The factor of public clouds is described below in (Table 1.2).

Table 1.2- Public Cloud Factors

Public Cloud (Amazon EC2 Public Cloud (Amazon EC2)		
Factor	**Advantage**	**Disadvantage**
Scalability	• Easily scalable within minutes to accommodate growth • Storage is scalable as well • Easy to switch between performance categories	• Higher cost per hour becomes aggregated with additional computing resources • Scaling up for better performance can multiply cost by a factor of 2 or more • Fixed level of CPU and RAM per category
Per hour computing costs*	• Cost equation is easy and transparent • OpEx rather than CapEx plus staff costs	• Costs are subject to change at whim of provider • Costs are per instance – no scalability within an instance • Data transfer is on a per GB rate ($.10) • Storage costs are in addition to computing costs, on a per GB rate
Reliability & Risk Management		• No control over where systems are located or whether redundancy or failover strategy exists (probably doesn't) • Public Cloud infrastructures are

		notoriously unreliable (see History of Cloud Failures) • No uptime guarantees provided by Amazon

Source: Based on (Group, 2011) . [Per hour computing costs for purchased/leased systems are based on a 3 year analysis]*

1.1.5.2 Private Cloud

In a private cloud computing solution, you'll supply your own hardware, and likely co-locate it at a data center (Teter, 2011). This is referred to as a "dedicated" environment, meaning no aspect of it is shared with any other organization. The private cloud offers increased control and flexibility over access and security, and it can accommodate more customization than the public cloud. The risks associated with the private cloud are no different than the current risks most companies have today (Taylor, 2011). The factor of public clouds is described below in (Table 1.3).

Table 1.3- Private Cloud Factors

Private Cloud (Co-located Data Center)		
Factor	**Advantage**	**Disadvantage**
Scalability	• If virtualized, can scale nearly as quickly as cloud computing. • No additional cost, within virtualized processor and storage capacity • CapEx costs can be converted to OpEx through leasing options • Equipment is owned at end of term • Performance scaling is incremental – can scale out, up, and within easily • Environment can easily support mixed higher and lower performance machines • Easily maintain like environment for development and testing	• For purchase, must amortize costs
Per hour computing costs*	• Generally speaking, hardware & software costs generate lower per hour computing costs when calculated over 3 year term • Can purchase or lease • Equipment is owned at end of lease term	
Reliability & Risk Management	• Can easily increase level of support if needed • Systems are designed for high	

	reliability: To maximize uptime, systems include redundant hot-swappable fans and can be configured with redundant hot-swappable power supplies. • Using a Sun StorageTek Host Bus Adapter (HBA),internal SAS disk drives can be configured for RAID 0, 1, 1E, 10, 5, 5EE, 50, 6, and 60. • Disk drives are also hot-swappable. • Four integrated Gigabit Ethernet ports enhance network availability and can be installed in failover configurations. • On-board system management tools encourage proactive remote. • Monitoring and intervention.	

Source: Based on (Group, 2011). [Per hour computing costs for purchased/leased systems are based on a 3 year analysis.]*

1.1.5.3 Hybrid

It is a combination of public and private cloud computing environments, where some data resides in the private cloud environment and some – perhaps less sensitive data – resides in the public cloud. Hybrid clouds are usually a combination of on- and off-premise (Teter, 2011).

1.1.6 Benefits of Clouds

The Cloud as it is called by experts has many tremendous benefits these benefits are such as; economies of scale resulting in low-costs of IT infrastructure, low maintenance costs and low IT administration costs. Other benefits are, improved of performance as a result of having access to dynamic and scalable computing, memory and storage capabilities based on demand. Cloud computing also offers easier data monitoring, quick incident response, and low costs to undertake security measures. Easier group collaboration, universal access to computing resources and the removal for the need for specific devices or hardware in-house are also benefits that can be accrued from cloud computing (Shimba, 2010). According to (Wu, 2011) there are five key benefits of using cloud computing:

- Ease of management

The maintenance of the software, hardware and general infrastructure to support storage is drastically simplified by an application in the cloud. Applications that take advantage of storage in the cloud are often far easier to set up and maintain than deploying an equivalent service on premise. At the customer site, often all that is needed to manage your storage implementation is a simple web browser leaving the headaches to the service provider.

- Cost effectiveness

For total cost of ownership, cloud computing is a clear winner. Elimination of the costly systems and the people required to maintain them typically provides organizations with significant cost savings that more than offset the fees for cloud computing. The costs of being able to provide high levels of availability and the scalability an organization needs are also unmatched. The economies of scale achieved by data centers simply can't be matched by all but the very largest of organizations.

- Lower impact outages and upgrades

Typically cloud computing provides cost effective redundancies in storage hardware. This translates into uninterrupted service during a planned or unplanned outage. This is also true for hardware upgrades which for the end user will no longer be visible.

- Disaster preparedness

Offsite storage isn't new. Keeping important data backed up off site has been the foundation of disaster recovery since the inception of the tape drive. Cloud computing services not only keep your data off premise, but they also make their living at ensuring that they have redundancy and systems in place for disaster recovery.

- Simplified planning

Cloud computing solutions free the IT manager from detailed capacity planning. Cloud-based solutions are flexible and provide storage as needed. This eliminates the need to over provision for storage that may be needed to meet.

1.1.7 Limitations of Cloud Computing

Due to the various benefits Clouds provide many organizations find it to be an attractive alternative to their current computing resources which depending on the size of the organization can be very costly and tedious to maintain. Unfortunately despite all the benefits of cloud computing there are enormous limitations and security risks that cannot be ignored and have made many organizations hesitant on whether to trust Cloud computing for to host their systems and data or not. What is important is to make customers aware of the risks of deploying Cloud computing.

According to (Xuefeng, 2012) the limitations or challenges of Cloud computing are:

- Interoperability and Portability (Lock – in)

Interoperability and portability present another open research problem for the researcher. Interoperability is the way how different clouds would communicate. It refers to the ability of customers to use the same parameters-management tools, server images etc. with a variety of cloud computing providers and platforms e.g. Amazon and Google are two clouds. Using the same image of Windows from Amazon on Google without any change is called interoperability. This would require Google to understand Amazon language.

Portability refers to the ability to move application and its data from one cloud to another. Portability could be achieved by removing dependencies on the underlying atmosphere. A portable components (application, data) could be moved and reused regardless of the provider, platform, operating system, location, storage etc. without being modified e.g. if the old cloud environment is Windows and new cloud environment is Linux then an application running on old cloud would be able to run on new cloud without being changed is called portability.

- Development of New Architecture

Presently, almost all of the cloud computing services are implemented in large commercial data centers and they are operated in old centralized manner. This design has its benefits i.e. Economy of scale and high manageability, yet it has some limitations i.e. High energy consumption and initial cost of investment. Most of the researchers have an inclination towards using voluntary resources to host cloud applications. This model of cloud computing in which using voluntary resources, or a

Comment [L14]: Need some explanation?

mixture of both dedicated and voluntary resources are very economical and it suits such applications as scientific computing. However, despite its advantages, yet this architecture has open research challenges as well, which are heterogeneous resources management, incentive scheme for such architecture.

- Availability of Service and Limited Scalability

Since many systems have been crashed on cloud like Amazon so using only one CCSP services can result in a drawback as when a shutdown event happens on a cloud the service disappears and user cannot find that service. CCSP promise to provide infinite scalability for customer but due to the fact that millions of users are now migrating to cloud computing so such promise is not fulfilled. The challenge of availability and scalability presents another research area for the researcher to find an optimum solution for these problems.

Comment [L15]: ???

- Lack of Standards

Every cloud provider has his own standards and user is not given any comparative performance measurement facility by which he can compare standards and performance of different clouds using some cost per service metric. It is still needed that cloud computing should be standardized, and a lot of research work is still needed to meet the required level of standardization.

Comment [L16]: What are these standards and what the effect of this point on using Cloud Computing

- Security and Privacy

The main hurdle in the fast adoption of cloud is the security concerns of the customers. Although due to the presence of modern techniques of security the chances of security flaws are reduced but still, when worms and hackers attack a system, mayhem is created within a few hours. It is necessary that the applications and architectures should be secluded and the mechanism of security must be apposite, surfacing and adoptive. A lot of research work is done, going on and still needed to be carried out in the area of cloud security. Trust and Privacy are some other potential areas of research in cloud computing.

- Reliability

Comment [L17]: Is this Means that reliability is disadvantage of Cloud

Availability of connection to cloud network is again an issue. User is not sure if he will remain connected to cloud network and keep on doing his work at any time as

connections do break. The connections to cloud services are secure or not and the migration of data to cloud computing is in safe environment and as per needed speed or not. Cloud itself is reliable enough to be migrated to? So reliability is another challenge yet to be resolved.

- Governance and Management

Many organizations started providing cloud services using their own data centers, thus trying to govern and bring monopoly in cloud computing. Governments, organizations and users must need to work together to resolve this issue.

- Metering and Monitoring

Organizations using cloud services must monitor the performance of services. Services providers must provide means to measure and monitor their services across standard parameters.

- Energy Management in Cloud

The primary requirement of the cloud computing is the management of heterogeneous resources across a distributed computing environment. It is obvious that from the user point of view all these resources are on at all times. If this is the case, then, it is highly inefficient in terms of the requirement for the energy consumption. A lot of research has been carried out in developing energy efficient equipment and utilize this equipment in building data centers to be energy efficient. On the other hand, fewer efforts have been put to model and exhibit a potential which allows various, distributed clouds infrastructure to use a policy which demonstrate to be as energy efficient as possible. The research work is needed to be carried out in the area of virtualization not only in system but network resources as well to minimize the energy consumption.

- Denial of Service

Another burning issue and a challenge that is faced by the researcher working in the area of cloud is the denial of service (DoS) in cloud computing. As a matter of fact cloud offers the allocation of resources dynamically, so what will be the response of the cloud when it is under a heavy denial of service attack? Is it necessary to build a DoS protection into cloud, or it will be handled on the internet level as it is dealt with

presently? This also poses another challenge for the researcher. By updating the security devices used today to make it work in a Cloud environment can improve security in the Cloud but the real challenge is in protecting the Cloud environment itself.

1.2 Virtualization

With the rapid growth in technology companies and advances in cloud computing, it has become very common for companies to incorporate virtualization in their data centers in order to fully utilize their hardware resources. According to a research done by Nemertes Research, nearly 93% of the organizations it surveyed in 2009 have deployed virtualization in their servers (Ritter, 2009). However, despite the various benefits that come with the adoption of virtualization, also new challenges and vulnerabilities arise.

1.2.1 History of Virtualization

Virtualization's history stretches back to the 1960s. Back then, the mainframe was king. But despite the computing power it offered, mainframes were rather inflexible. Only one operator could use it at a time. The operator would feed the mainframe a program, the computer would do its thing, and then the results would be output back to the operator. In order to process two jobs, each task would have to be batched into its own workload.

It's true that batching solved most users' needs but there was a need to develop new hardware that could handle more than one user at a time. IBM created the S/360-67 with its CP/CMS paradigm. CP stood for Control Program and CMS for Console Monitor System. (CMS is also synonymous for Cambridge Monitor System and Conversational Monitor System.) The CP ran on the mainframe, and it created virtual machines that ran the CMS. In addition to serving more than one user at a time by sharing the hardware resources of the mainframe, the CMS allowed the user to interact with the computer rather than simply feed it a program and wait for results.

During the 70s and 80s the course of computing changed and there was a new movement towards distributed computing, which is networking computers together. This led to the birth of server farms and the internet. Even techniques used for high availability and disaster recovery, such as failover clustering and mirroring were developed due to distributed technologies. The problem was that this new movement came at a cost, and virtualization did not make quite as many leaps forward until the 1990s.

In 1998, VMware introduced a new kind of virtualization for x86 processors .This achievement was significant because x86 processors did not meet the standard requirements for virtualization. VMware's programming allowed multiple operating systems to utilize the processor in a safe, efficient manner. In 2001, VMware entered into the Enterprise market with two products, ESX Server and GSX Server. GSX Server was installed on top of an existing operating system installation, such as Windows Server. ESX Server ran directly on the server hardware (AKA: bare metal) in lieu of a traditional operating system (Velic, 2011).

Today there are many kinds of virtualization such as Hardware Virtualization, Desktop Virtualization and Storage Virtualization. (Figure 1.4) below is a timeline that describes the development of virtualization.

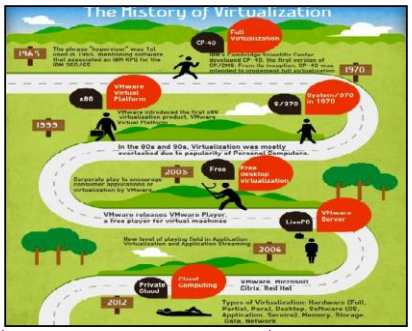


Figure 1.4: Virtualization Timeline

Comment [L18]: Can you explain

1.2.2 What is Virtualization?

As with cloud computing there are many definitions to virtualization but for this research I prefer to use the Oracle definition because it is simple to understand. Virtualization is "the ability to run multiple virtual machines on a single piece of hardware. The hardware runs software which enables you to install multiple operating systems which are able to run simultaneously and independently, in their own secure environment, with minimal reduction in performance. Each virtual machine has its own virtual CPU, network interfaces, storage and operating system" (Oracle, 2009).

Comment [L19]: In the research avoid to use I you prefer to us we

Comment [L20]: Is there is another definition? You should mention

1.2.3 Types of Virtualization

Comment [L21]: Need More details

There are many types of virtualization but the four basic types Process virtualization, Server virtualization, Network virtualization and Storage virtualization (Studnia, Alata, Deswarte, Kaâniche, & Nicomette, 2012). A brief description will be given for

all four but for the purpose of this thesis the focus will be on server virtualization and it will be covered with more details:

- Process virtualization

Virtualizing this layer consists in providing an interface between an application and the underlying system. This allows creating an application without concerning about the specifications of the operating system it will run on, as long as they possess the required virtualization layer. The Java Virtual Machine is an example of process virtualization.

- Server virtualization

Virtualization is applied to the hardware. This allows many Operating systems to run simultaneously on a physical machine. Server virtualization hides the physical nature of server resources, including the number and identity of individual servers, processors and operating systems, from the software running on them.

- Network virtualization

VPNs (Virtual Private Networks, which enable the interconnection of distinct private networks through a public infrastructure such as the Internet) and VLANs (Virtual LANs, distinct local networks sharing the same physical infrastructure) are examples of network virtualization.

- Storage virtualization

Storage virtualization melds physical storage from multiple network storage devices so that they appear to be a single storage device.

1.2.3.1 Server virtualization

Server virtualization can be implemented in three ways which are:

- Interacting with the hardware
- Interacting with the operating system
- Interacting through a hypervisor (program dedicated to the management of virtual machines)

For the purpose of this thesis the focus will be on hypervisors. These hypervisors are often categorized within two groups (Studnia, Alata, Deswarte, Kaâniche, & Nicomette, 2012) :

- Type 1: Type 1 managers are installed directly above the hardware and run with the highest level of privileges (Figure 1.5). Xen and VMware ESX are examples of type 1 hypervisors.
- Type 2: Type 2 managers are installed above an operating system, like any other program (Figure 1.6). QEMU and Virtual Box are examples of type 2 hypervisors.

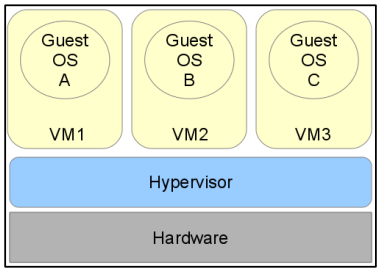


Figure 1.5: Type 1 hypervisor

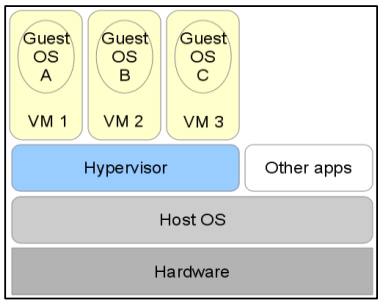


Figure 1.6: Type 2 hypervisor

Also hypervisor based virtualization consists of three major techniques: full-virtualization, paravirtualization and emulation.

Comment [L22]: This title and below under which header

❖ Full-virtualization

In this case, one or more unmodified operating systems (called “guests”) are unaware that it is being virtualized. The hypervisor will handle all OS-to-hardware requests on demand and may cache the results for future use. In this instance, the virtualized OS is completely isolated from the hardware layer by the hypervisor. This provides the highest level of security and flexibility as a broader range of operating systems can be virtualized (Hill, 2012).

- Paravirtualization

The guest OS needs to be engineered in such a way that it knows that it is virtualized. The kernel of the operating system is adjusted to replace instructions that cannot be virtualized with methods that interact directly with the hypervisor. Value for paravirtualized environments comes in the form of lower overhead and optimized operations. Paravirtualization is typically seen in Linux environments with the Xen kernels included, although it is more and more common to find Full Virtualization vendors, including some paravirtualization drivers, in their latest products (Hill, 2012).

- Emulation

Like full virtualization, emulation allows unmodified operating systems to run. However, in that case, the resources seen by the guest OS are completely simulated by software. This allows executing an operating system compiled on an architecture different from the architecture of the host. This has been used in the past but is difficult to do and offers low performance, QEMU is an example of an emulator (Studnia, Alata, Deswarte, Kaâniche, & Nicomette, 2012).

1.2.4 Characteristics of Virtualization

Comment [L23]: Is this characteristics only those which affect the security or its general

The four fundamental characteristics that affect security in virtualized systems are: new management layer, concentration, variable state, and mobility (Ritter, 2009).

- The new management layer

It is essentially a layer created by the hypervisor. Since the hypervisor manages all VMs that run on the physical machine, it possesses administrative rights to all the virtualized components. For a virtualized data center or cloud, the information attackers seek is almost always in the VMs. Thus, by taking control of the hypervisor or the host OS that the hypervisor runs on, the attacker will be able to compromise most if not all of the VMs, posing significant threat to the entire data center or cloud.

- Concentration

Is the characteristic that a plethora of VMs will run on the same physical machine, since the main purpose of virtualization is to fully utilize the physical resources or hardware available. It is an issue directly related to the new management layer created by virtualization. If one physical machine only runs one VM, then compromising the

machine is no different than damaging one server that runs on the VM. However, due to concentration, taking control of one VM on the machine can also potentially let the attacker gain access to other VMs as they run on the same physical machine, thus greatly increase the damage done.

- Variable state

Is how each VM can be on, off, suspended, or in some customized state despite that the underlying hardware is still running. Due to this characteristic, many new security complexities are introduced dealing with virtualized systems. Some of the examples are access control to VMs in different states, data integrity of the VMs, and policies to change the state of VMs.

- Mobility

Is the unique trait of virtualization that allows VMs to move from one physical machine to another without moving any hardware? Due to the ease at which VMs are transported across machines, security issues regarding networking and integrity when transporting VMs will become prevalent as VMs can be moved between machines in the same data center, another data center, or even clouds. This is an issue not present in non-virtualized environments, as movement of non-virtualized systems only requires moving the physical media. Also, the security boundary for each VM is very difficult to maintain as they can easily move between different infrastructures (KarenScarfone, MurugiahSouppaya, & PaulHoffman, 2011).

1.2.5 Benefits of Virtualization

Deploying virtualization offers substantial benefits. According to an article written by Jack Wallen, the ten most prominent advantages of virtualization are (Wallen, 2013).

- Less heat buildup

Millions of dollars have gone into the research and design of heat dissipation and control in the data center. But the cold, hard fact is all of those servers generate heat. The only way around that is to use fewer servers. How do you manage that? The answer would be to virtualize your servers and you're using less physical hardware. Use less physical hardware and you generate less heat. Generate less heat in your data center and a host of issues go away.

- Reduced cost

Comment [L24]: I don't agree? Can you prof.

Hardware is most often the highest cost in the data center. Reduce the amount of hardware used and you reduce your cost. But the cost goes well beyond that of hardware, lack of downtime, easier maintenance, less electricity used. Over time, this all adds up to a significant cost savings.

- Faster redeploy

When you use a physical server and it dies, the redeploy time depends on a number of factors: Do you have a backup server ready? Do you have an image of your server? Is the data on your backup server current? With virtualization, the redeploy can occur within minutes. Virtual machine snapshots can be enabled with just a few clicks. And with virtual backup tools like Vaeem, redeploying images will be so fast your end users will hardly notice there was an issue.

- Easier backups

Not only can you do full backups of your virtual server, you can do backups and snapshots of your virtual machines. These virtual machines can be moved from one server to another and redeployed easier and faster. Snapshots can be taken throughout the day, ensuring much more up-to-date data. And because firing up a snapshot is even faster than booting a typical server, downtime is dramatically cut.

- Greener pastures

Let's face it: If you're not doing your part to help clean up the environment, you're endangering the future. Reducing your carbon footprint not only helps to clean up the air we breathe, it also helps to clean up your company image. Consumers want to see companies reducing their output of pollution and taking responsibility. Virtualizing your data center will go a long way toward improving your relationship with the planet and with the consumer.

- Better testing

What better testing environment is there than a virtual one? If you make a tragic mistake, all is not lost. Just revert to a previous snapshot and you can move forward as if the mistake didn't even happen. You can also isolate these testing environments from end users while still keeping them online. When you've perfected your work, deploy it as live.

- No vendor lock-in

One of the nice things about virtualization is the abstraction between software and hardware. This means you don't have to be tied down to one particular vendor, the virtual machines don't really care what hardware they run on, so you're not tied down to a single vendor, type of server (within reason of course), or even platform.

- Better disaster recovery

Disaster recovery is quite a bit easier when your data center is virtualized. With up-to-date snapshots of your virtual machines, you can quickly get back up and running. And should disaster strike the data center itself, you can always move those virtual machines elsewhere (so long as you can re-create the network addressing scheme and such). Having that level of flexibility means your disaster recovery plan will be easier to enact and will have a much higher success rate.

- Single-minded servers

With Single-minded servers there is a single point of failure, you have services competing with resources as well as with each other. Those all-in-ones are purchased to save money. With virtualization, you can easily have a cost-effective route to separating your email server, your web server, your database server, etc. By doing this, you will enjoy a much more robust and reliable data center.

- Easier migration to cloud

With a move to virtual machines, you are that much closer to enjoying a full-blown cloud environment. You may even reach the point where you can deploy VMs to and from your data center to create a powerful cloud-based infrastructure, but beyond the actual virtual machines virtualized technology gets you closer to a cloud-based mindset, making the migration all the more easy.

1.2.6 Challenges of Virtualization

Even though Virtualization technologies offer many benefits the addition of a new layer of software introduces new security concerns. Garfinkel and Rosenblum have given a list of challenges raised by virtualization that are discussed below (Garfinkel & Rosenblum, 2005).

- Scaling

Virtualization enables quick and easy creation of new virtual machines. Therefore, security policies of a network (setup, updates...) have to be flexible enough to handle a fast increase in the number of machines.

- Transience

With virtualization, machines are often added to or removed from a network. This can hinder the attempts to stabilize it. For example, if a network gets infected by a worm, it will be harder to find precisely which machines were infected and clean them up when these machines exist only during brief periods of time on the network. Similarly, infected machines or still vulnerable ones can reappear after the infection was thought to be wiped out.

- Software lifecycle

The ability to restore a virtual machine in to a previous state raises many security concerns. Indeed, previously patched vulnerabilities (programs flaws, deactivated services, older passwords, etc...) may reappear. Moreover, restoring a virtual machine into a previous state can allow an attacker to replay some sequences, which renders obsolete any security protocol based on the state of the machine at a given time.

- Diversity

In an organization where security policies are based on the homogeneity of the machines, virtualization increases the risk of having many versions of the same system at the same time on the network.

- Mobility

A virtual machine is considered like any other file on a hard drive. It can be copied and moved to another disk or another host. This feature, cited as a benefits of virtualization, also adds security constraints because guaranteeing the security of a virtual machine becomes equivalent to guaranteeing the security of every host it has been on.

- Identity

Usual methods used to identify machines (like MAC addresses) are not necessarily efficient with virtual machines. Moreover, mobility increases even more the

difficulties to authenticate the owner of a virtual machine (as it can be copied or moved).

- Data lifetime

A hypervisor able to save the state of its VMs can counter the efforts made by a guest to delete sensitive data from its memory. Indeed, there may always be a backup version of the VM containing the data.

1.3 RISK MANAGEMENT

Organizations operate in a world of uncertainty and every project or activity has its risks. These risks may have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes (ISO, 2013).Therefore Risk management is considered as an important part of planning for an effective business.

Risk management is a process used to identify, assess, and prioritize risks of different kinds. According to ISO 31000 risks are defined as "the effect of uncertainty on objectives" (ISO, 2013).

Risks may occur for many reasons such as uncertainty in financial markets, threats from project failures, legal liabilities, credit risk, accidents, natural causes and disasters and sometimes for an unpredictable root-cause. There are a number of risk management standards, including those developed by the Project Management Institute such as the International Organization for Standardization (ISO), the National Institute of Science and Technology, and actuarial societies. In addition to the above there are also many documents provided by different companies on the best practice that should be used depending on the product such as the six-step virtualization risk assessment process by VMware (Shackleford, 2011).

Many different methods are used to manage risks but in order to manage risk effectively it is you should (1) to identify and assess the threats to the objectives, (2) to determine the vulnerability of critical assets to these threats, (3) to determine the risk, (4) identify methods to reduce those risks and (5) prioritize the risks.

The process of risk management consists generally of Risk identification, Risk assessment and Risk treatment.

1.3.1 Risk Identification

Risk identification is the first step in the risk management process. It provides the opportunities, indicators, and information that allow an organization to determine risks that could potentially prevent the program, enterprise, or investment from achieving its objectives.

There are many tools and techniques for Risk identification such as brainstorming, Checklist analysis, SWOT analysis, Expert judgment and scenario analysis. More detail on these as well as other techniques is found in (Clarizen, 2013).

Comment [L25]: What?

1.3.2 Risk Assessment

Risk assessment is the second step in the risk management process. It builds on the risk information generated in the identification step, converting it into decision-making information, thus assessing the probabilities and consequences of risk events if they are realized. The results of this assessment are then used to prioritize risks to establish a most-to-least-critical importance ranking. Ranking risks in terms of their criticality or importance provides insights to the project's management on where resources may be needed to manage or mitigate the realization of high probability/high consequence risk events.

In order to be able to determine how big or small a risk is, the probability and the impact have to be determined. It is sometimes possible to calculate the exact impact of a risk and determine the probability based on statistical data from comparable activities. However, generally this is very hard to do because there is not enough hard data and experience with comparable activities to calculate the probability. In these cases the impact and probability will have to be estimated using other methods. There are many different formulae for risk assessment but the most widely used formula is:

Comment [L26]: What is the support of this formula

Risk = Rate (or probability) of occurrence x Impact of the event

1.3.3 Risk Treatment

Risk treatment is the third step in the risk management process and is the process of selecting and implementing of measures to modify risk. Once a risk is identified and assessed different techniques can be used to manage the risk such as avoiding, optimizing, transferring or retaining risk.

Reducing a risk can be done by a combination of people, process and technology. People need to be aware, trained and accountable. Structured and repeatable processes are needed. Technology can be used to continually evaluate the risk and the associated controls, and to monitor and enforce rules which reduce the risk (Microsoft, 2010).

1.3.4 The risks of virtual machines

This thesis focuses on using different approaches to reduce the biggest risks of virtual machines based on a case study of Central Bank of Sudan which is built on VMware. What are these risks?

To answer this question we will examine the security of the VMware Virtual Infrastructure which has been broken down into components.

1.3.4.1 VM Kernel

The VM kernel is the core software that runs the virtual machines and manages the allocation and utilization of hardware resources among them. Due to the high security which was included in the virtual infrastructure design, attacks at this level would have to be very sophisticated. An example would be a denial of service attacks at the CPU of the server or the virtual memory. Thus, because the VMKernel is so complex it is less likely that it would be the main objective of hackers.

1.3.4.2 Virtual Machines

All virtual machines are isolated thus providing a secure environment for them to run. For example, a user on a virtual machine's guest operating system cannot bypass the level of Segregation and gain access to other virtual machines. However, the security of every virtual machine is to be handled with individually exactly as we would with a physical server and make sure to apply the latest operating system patches and security updates, apply security configuration standard to the operating system and Run antivirus software and keep it updated.

Comment [L27]: Stand for what

1.3.4.3 ESX Server Service Console

The Service Console provides a local management interface to the ESX kernel. Anyone with access to the Service Console would have full control of the virtual machines on that host. Access to the Service Console is protected by authentication and encryption by default.

However, security could be enhanced by allowing connections only to the internal trusted network, not allowing connections to the Internet, Use the 'iptables' program within the Service Console to restrict network access to a more granular level, Apply

VMware best practice to configure the Service Console and Monitor configuration files for integrity and unauthorized tampering.

1.3.4.4 ESX Server Virtual Networking Layer

The virtual networking layer in an ESX server allows the virtual machines and Service Console to interact with other systems in the network and includes virtual network adapters and the virtual switches. The virtual adapters are the interfaces to the network. As for the virtual switches they are similar to Ethernet switches and forward packets to the appropriate virtual machine. To enhance the security of this layer you should use VLANs to prevent network attacks, Use separate physical network adapters for virtual machine zones to ensure that the zones are isolated, Label all virtual networks to prevent confusion and Use virtual switch security profiles to help prevent MAC address spoofing attacks.

1.3.4.5 Virtual storage

Virtual machines use virtual hard disks to store its operating system, applications, and data. A virtual disk is a file that resides in data stores and may be deployed on a local storage device or a network storage device. At this VMware level attacks are unlikely to occur.

1.3.4.6 Virtual Center

VMware Virtual Center is an infrastructure management software that provides a single point of control for the virtual datacenter and is composed of the following components:

1. Virtual Center Management Server: Service that interacts with the VMware ESX Servers.
2. Virtual Center Database: Database storing infrastructure information about the physical servers and virtual machines.
3. Virtual Infrastructure Client: Applications used to connect remotely to the Virtual Center Management Server.
4. Virtual Center Agent: Used to connect VMware ESX Servers with the Virtual Center Management Server.
5. Virtual Infrastructure Web access: Used to manage virtual machines via web.

The Virtual Center can be secured by Avoiding the use of the Windows Administrator account to run Virtual Center installation, instead use a dedicated Virtual Center administrator account; ensure the minimum necessary privileges are assigned to Virtual Center administrators; Restrict network access to the Virtual Center to only the ESX Server Service Console and VI Clients; Install the Virtual Center database on a separate server and apply security standards; archive and retain the Virtual Center Server host's local file system for troubleshooting and debugging purposes.

1.3.5 The risks that will be addressed in this thesis

This thesis discusses what the virtualization security risks are when moving to the cloud from a virtual environment, how to evaluate these risks and which approaches can be used to reduce these risks. These approaches may be existing approaches which are available and can be applied or entirely new approaches may be found. Risk reduction methods for three of the most important risks which are data management and protection, external attacks and security training and awareness will be covered.

When dealing with security there is no one-size-fits-all solution to security. Therefore a combination of people, process and technology controls may be used to reduce the risk depending on what the risk is.

1.3.5.1 Data Management

This category deals with the handling of sensitive data such as credentials as well as virtual machine data itself ranging from RAM, BIOS, and the virtual disks and can be split into two parts.

1. In virtual systems we are concerned about data flowing from within the guest and across the network and about data stored within the guest. An example of this would be database server storing credit card information. The number one concern would be how the credit card numbers are stored in the database and transmitted over the network. These concerns are no different from that of same database if it were running on a physical machine. The technological solutions in use today which are relevant in this environment would be hashing, encryption, and protocols such as the Secure Sockets Layer (SSL). In virtualization you may be require you to enable more network services or software components than expected such as web enabled products

and providing remote connectivity access to guests or hosts. All such services and components will also require protection and therefore needs to be understood properly so that solutions are configured appropriately to maintain data protection.

2. Virtual disks are stored as files on the host and most of them store their data in plain text. Thus, allowing attackers whom already have access to these files to be able to easily read the information on it. therefore it is very important to consider the security of the virtual disk files .These are not the only threats, there are others such as injection of malware such as a keystroke logger, into the virtual disks as well as into the contents of RAM and the BIOS information for the guest. To resolve such risks some organizations may consider using strong access controls and encryption for their sensitive files on the host. This can be achieved by using add-ons which are available from the virtualization vendors themselves or by using similar software provided by a different vendor. In the end the appropriate technology to use depends on who you are trying to defend the organization from. This may be an external attacker who steals the virtual machine files or user on the same physical host.

Virtualization can also add new channels of network traffic that could come under attack. Therefore, it is important to understand which protocols used by the virtualization vendors are secure and which are not and what networks these flow over. In some cases, the data protection may not be turned on by default and it is important to understand the implications of this.

Virtualization technologies are becoming an essential element of modern data centers for both large and small organizations. Over time the immense growth of data along with the increasing number of virtual machines lead to the need for an effective means of data management and protection. The shift to virtualization and exceedingly demanding operations requirements have made it necessary to update traditional data protection techniques.

1.3.5.1.1 Data Protection Challenges

There are many challenges to data protection such as:

a. Dwindling Resources: The increased level of server consolidation and high virtual machine density has resulted in a limited number of physical resources that are mainly dedicated to production needs. This means that there is the

potential for neglect when it comes to data management tasks and that large amounts of data must be protected with less storage resources.

b. Unprotected Data: While virtual machines are regularly being created there is the concerning possibility that these devices are not being backed up. Manually applying data protection policies is still a current practice and is a very time-consuming and inefficient method of securing huge amounts of data.
c. Recover Points Deficiencies: Data backed up by sparse intervals is not a sufficient means to maintain optimal levels of data recovery capabilities. With the deployment of critical applications, recovery Point Objectives have shifted from daily to hourly points. This is necessary in order to reduce the amount of data loss in the case of any unexpected disruption to the system. However, it can be challenging to put frequent recover points in place without hindering productivity.
d. Lack of Application Defense: The transfer of critical applications to a virtual setting makes it essential to ensure that they have an equivalent level of protection and recovery capabilities as they would have with a physical server.
e. Limited Restore Granularity: Restoring individual files from the data store of a virtual machine is vital for adequate application uptime. However, traditional means make it necessary to remount the whole virtual machine data store before sifting through the contents to find a single file. This method requires too many resources and a large amount of time to be truly effective.

1.3.5.1.2 Approaches to Data protection

Many businesses use traditional backup approaches such as doing a complete backup of their data on weekends and intermittent backup during the week. Relying on traditional backup approaches in virtualized environments can be complex and time-consuming. There are many data protection approaches such as:

1. A protection approach that uses a tiered system: This type of process focuses on specific recovery objectives and is based on data requirements. An organization may choose to focus on a single recovery type or multiple types, which can include operational recovery, disaster recovery or regulatory recovery. Organizations will benefit from using more aggressive means to protect their more valuable data while scaling back resources on less

significant information. Such a system provides extra security to critical information and decreases costs on data that has less value to the organization. In order to reduce the quantity of data that requires protection inactive data should be transferred to a content storage platform.

There are many advantages to the use of application-specific protection protocols such as (Smith M. , 2014):

a. Creating copies of only strictly necessary information.
b. The ability to restore at a granular level
c. Making use of the automated recovery of applications
d. Saving changes as they take place, which makes it possible to recover data from any point in time.
e. Increased control over applications and their protection

2. Traditional host-based agent: To implement this approach, organizations first need to install a licensed backup on each server. Then the backup software (on the dedicated backup server) initiates the backup of all servers through the agents. This method is considered suitable when each server is running one application, but is inefficient and costly when dealing with virtualized servers.
3. Service console-based agent: In this method the backup is executed by an agent running on the VMware Service Console. It can leverage VMware snapshots for crash consistency and back up the entire VM file (VMDK) but there's no file-level restore, and it still requires processing by the ESX (VMware virtualization) server.
4. Consolidated backup proxy agent: This method takes advantage of the VMware Consolidate Backup (VCP) proxy, which removes processing chores from the ESX server. It uses a single agent running on the proxy server rather than an agent on every VM thus, improving manageability of IT resources. It enhances recovery by recovering individual files from an image-level backup without having to recover the entire image first. It also allows volume-level backup and recovery for VMware environments and includes other options such as including the ability to perform incremental delta block image-level backup to expedite backup operations, save storage capacity, and enable single-pass, full VM recovery.

5. Intelligent advanced host-based agent: This method eliminates up to 90% of the requirements of traditional backup agents by because an agent with snapshot and deduplication capabilities works in conjunction with a data deduplication backup repository to store only unique data blocks.
6. Event-based data protection: This method provides replicated data protection with rollback capabilities using Continuous Data Protection (CDP) with on-demand consistency point generation. This method has low server overhead which allows scaling to hundreds of servers. It has both failover and failback features and can replicate data across any distance.

Every organization is different and there is no single backup and recovery solution that fits all. The choice of a solution depends on the level of recovery needed, how much VM performance impact can be accepted, and the capacity and infrastructure requirements.

1.3.5.1.3 Discussion

This chapter covered what data management and protection is the challenges and approaches that can be taken to reduce its risk. CBOS consists of an environment which uses a SAN storage system and proper backup software which is used to back up there application data. There is no backup for the virtual machines which is considered as a major risk.

In order to reduce this risk, appropriate backup software to backup and restore the virtual machines. The software chosen as method to reduce this risk was Veeam Backup. This conclusion was reached after thorough research and according to 2013 virtual Server survey (Wendt, 2013) which consisted of a comparison between three software applications which are Veeam, Appsure and Netbackup (Table 1.4). The chosen software was not tested on the actual environment but on a production environment that was setup specifically for this thesis.

Table 1.4- Comparison between Symantec, Veeam and Dell

Product	Overall Score	Backup Technology	Management	Restore	Support
Symantec NetBackup 7.5	83.00	40.50	24.50	10.00	8.00
Veeam Backup & Replication 6.5	55.00	28.00	16.00	8.00	3.00
Dell AppAssure 5.2	47.50	20.50	14.00	9.00	4.00

Overall Scores Rankings		Backup Technology Scores Rankings	
Recommended	41.59 – 46.00	Recommended	81.28 – 87.50
Excellent	69.38 – 81.37	Excellent	34.69 – 41.58
Good	57.46 – 69.37	Good	27.78 – 34.68
Basic	39.50 – 57.45	Basic	13.50 – 27.77

According to Gartner report 2014 (Figure 1.7) and based on user reviews, if the software solution will be implemented in a complete virtual environment with no physical servers then Veeam would be the best option. If the environment is mixed with both physical and virtual servers and a single backup solution is required then Appsure would be a more appropriate choice. More details regarding Veeam can be found in http://www.veeam.com and Appsure can be found in http://software.dell.com.

Figure 1.7: Magic quadrant for enterprise backup software and integrated appliances

Whether CBOS decide to use Vaeem backup software or not it is recommended that they follow the top 10 best practices of backup Replication for VMware and Hyper-V (Davis, 2011).

1.3.5.2 External Attacks

With any new technology there will always be threats and security concerns associated with it and virtualization is no exception. The majority of the threats tend to be external where external sources try to gain unauthorized access to your organization networks using the Internet or any other networks.

One of the major risks of virtualization is the hypervisors, or VM managers, which is the core of a virtualization platform. Therefore a hacker with control of the hypervisor could control any virtual machine running on the physical server. There are many types of attacks some may traditional threats where most organizations have had more experience dealing with and others may not. According to a recent article by Penetration Testing Lab (Younger, 2013) some of the top security threats surrounding virtualization are:

a. VM sprawl: VMs are easy to deploy, and many organizations view them as hardware-like tools that don't merit formal policies. This has led to VM sprawl, which is the unplanned proliferation of VMs. Attackers, can take advantage of poorly monitored resources. More deployments also mean more failure points, so sprawl can cause problems even if no malice is involved.
b. Hyper jacking: Hyper jacking takes control of the hypervisor to gain access to the VMs and their data. It is typically launched against type 2 hypervisors that run over a host OS although type 1 attacks are theoretically possible. In reality, hyper jackings are rare due to the difficulty of directly accessing hypervisors. However, it is considered as a real-world threat, and administrators should take the offensive and plan for it.
c. VM escape: A guest OS escapes from its VM encapsulation to interact directly with the hypervisor. This gives the attacker access to all VMs and, if guest privileges are high enough, the host machine as well. Although few if any instances are known, experts consider VM escape to be the most serious threat to VM security.
d. Denial of service: These attacks exploit many hypervisor platforms and range from flooding a network with traffic to sophisticated leveraging of a host's own resources. The availability of botnets continues to make it easier for attackers to carry out campaigns against specific servers and applications with the goal of derailing the target's online services.

e. Incorrect VM isolation: To remain secure and correctly share resources, VMs must be isolated from each other. Poor control over VM deployments can lead to isolation breaches in which VMs communicate. Attackers can exploit this virtual drawbridge to gain access to multiple guests and possibly the host.
f. Unsecured VM migration: This occurs when a VM is migrated to a new host, and security policies and configuration are not updated to reflect the change. Potentially, the host and other guests could become more vulnerable. Attackers have an advantage in that administrators are likely unaware of having introduced weaknesses and will not be on alert.
g. Host and guest vulnerabilities: Host and guest interactions can magnify system vulnerabilities at several points. Their operating systems, particularly Windows, are likely to have multiple weaknesses. Like other systems, they are subject to vulnerabilities in email, Web browsing, and network protocols. However, virtual linkages and the co-hosting of different data sets make a serious attack on a virtual environment particularly damaging.

1.3.5.2.1 Methods to Mitigate Risk

Several steps to minimize risk can be taken. The main step is to accurately characterize all deployed virtualization and any active security measures beyond built-in hypervisor controls on VMs. This should include anti-virus, intrusion detection, and active vulnerability scanning. Other additional step should be considered (Younger, 2013).

1. VM traffic monitoring: Monitoring the VM backbone network traffic is very critical. Conventional methods will not detect VM traffic because it is controlled by internal soft switches. However, hypervisors have effective monitoring tools that should be enabled and tested.
2. Administrative control: Secure access can become compromised due to VM sprawl and other issues. Therefore, it's crucial to make sure that authentication procedures, identity management, and logging are ironclad.
3. Customer security: It is important to make sure that protection outside of the VM is in place for customer-facing interfaces such as websites.
4. VM segregation: Strengthening VM security through functional segregation in addition to normal isolation is important. An example of his would be to create separate security zones for desktops and servers.

5. VM Patching server hardening: It is important to make sure to protect your VMs by installing all recommended security patches and to close all ports not in use and disable any unwanted features.

1.3.5.2.2 Discussion

External attacks are one of the biggest risks that face any organization especially financial ones. According to CBOS environment the most major risks which may result in external attacks are lack of VM patching and use of security tools. The current virtual environment is running on VMware version 4.1 and has been never been patched. For this particular situation the best option is to upgrade to version 5.5.

Regarding the security tools none have been used and the current security infrastructure is not virtual aware and needs to be replaced with new equipment that is virtual aware. This is not any easy process and may take time. Currently to reduce this risk it is recommended to use Retina virtual security scanner.

This decision was reached after extensive research and study of user reviews and surveys and vulnerability tool assessments by Gartner (Kavanagh, 2013), SC magazine (Stephenson, 2013) and InfoSec (Bakar, 2014). Both Nexpose and Retina were installed and tested in a testing environment prepared for this study. Based on this test Retina was recommended for CBOS. Sample reports of Retina can be found in Appendix C.

1.3.5.3 Security Training and Awareness

Every organization's security goal is to lock down their infrastructure as tightly as possible while maintaining a productive and fluent environment. These controls are often technical solutions that have to be properly implemented and maintained. This type of mentality gives a false sense of security and leaves an organization vulnerable to one of the greatest risk which is human nature. Security awareness training is very crucial because one of the greatest threats to information security could actually come from within your organization. Inside 'attacks' have been noted to be some of the most dangerous since these people are already quite familiar with the infrastructure. It is not always disgruntled workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee (CTG, 2008).

One of the best ways to make sure company employees will not make costly errors in regard to information security is to perform company-wide security-awareness training. There are other reasons that security awareness training occurs some more productive and strategic than others:

1. Limit Corporate Liability: If an organization doesn't make very clear to employees what they can and cannot do using corporate technology assets, they cannot terminate employees for doing the wrong thing. Too much of today's awareness training content is built as a warning to justify termination. This kind of training is built by lawyers expressly to enable them to prosecute employees if needed.
2. Compliance Mandate: This is implemented in many government organizations, which are expected to follow NIST 800-50 to comply with FISMA and build a security training program. Unfortunately compliance requirements rarely create sufficient urgency to address the original goals behind the regulation.
3. Protect Information: Some organizations perform security awareness training to actually train employees about security. Imagine that. For example, administrators must understand how to harden a given virtualization installation. Security requirements might often define a higher bar than default installations can provide. In this case they need to know what not to click and why. They need to learn who to call when they think something is wrong. How to protect their mobile devices, which increasingly contain sensitive data and access. This content is typically built by the security team (or under their watch).

Some of the more important items to cover in your security awareness training are your organization's security policy, data classification and handling, workspace and desktop security, wireless networks, password security, phishing, hoaxes, malware, file sharing and copyright (University of Tennessee).

1.3.5.3.1 Methods of Training

Security awareness training can be performed in a variety of ways that can be utilized individually or in co-ordination with each other. These methods can consist of a more thorough classroom-style training, creation of a security-awareness website, pushing

helpful hints onto computers when they start up and/or e-mailing helpful hints on a weekly or monthly basis, and utilizing visual aids like posters.

a. Classroom-Style Training

Utilizing a classroom setting for security-awareness training can offer the benefit of lecture-based and interactive learning as well as the availability of someone to answer questions in real time. There can also be a question and answer period after the materials are presented as well as contact information distributed for questions that might pop up afterward. Some companies offer both live and web-based training and utilize a variety of methods such as role-playing and simulation games so the interaction is more two-way than one-way. Other organizations offer videos, web-based training, and live trainers. The methods used are by no means limited (Dublin, 2006).

b. Security Awareness Website

Another way of implementing a security awareness program is through the creation of a security awareness website. This website could consist of different sections with the different areas that cover for example malware, hoaxes, file sharing and copyright, etc.

c. Helpful Hints

Using helpful hints and tips is more of a supplement to the training, whether its classroom style or online. Helpful hints can consist of tips and reminders that are pushed to user screens when they log in (e.g. "Never keep your password in a place that can be accessed or viewed by anyone besides yourself."). Reminders can be as simple as reminding someone to change their password or run their virus scan.

d. Visual Aids

Visual aids are another item that should not be used as the lone source of security awareness training, but more as a supplement. An example is to create a series of catchy password security posters. The first one saying to change them often, the second saying to not leave passwords lying around and the last one saying to not share them with friends.

e. Promotions

Security tips can appear on flyers distributed across the user base and some organizations could even go so far as to hand out pencils or key chains with a catchy security-related phrase or reminder (e.g. “Unexpected attachments can mean unexpected chaos: Please do not open them”).

1.3.5.3.2 Discussion

Proper training and security awareness is important for any organisation. CBOS has invested thousands to build and secure its current IT infrastructure. Its true investment on technical training has been made but unfortunately when it comes to security this is not enough.

After a few interviews with CBOS users it was found that their knowledge of the importance of security was weak. Also using social engineering I was able to obtain some confidential information such as passwords and use accounts. Therefore there is an enormous need to work on security awareness for CBOS users. In this attempt a presentation of the importance of security and how they can be a part of the awareness program was conducted for managers in coordination with CBOS IT staff which was complete success. Also visual aid using screens located in different parts of the building was used to show tips and reminders of the importance of security. Also tips and hints were used on the intranet of the organization.

CHAPTER TWO

Comment [L28]: This review general, should be specific on the research area and the case, also should be sorted by date.

2.0 LITERATURE REVIEW

Virtualization is a staple technology of cloud computing. IBM pioneered it in 1960s (Armbrust, 2009) to fully utilize their hardware resources with timesharing and multiprogramming techniques. These techniques led to the adaptation of virtualization. Virtualization is "the ability to run multiple virtual machines on a single piece of hardware. The hardware runs software which enables you to install multiple operating systems which are able to run simultaneously and independently, in their own secure environment, with minimal reduction in performance. Each virtual machine has its own virtual CPU, network interfaces, storage and operating system" (Oracle, 2009).These resources can be made available to the users on demand through the internet. Virtualization's unique architecture has many characteristics and advantages over traditional non-virtualized machines. However, with virtualization benefits comes the need for virtualization security (Garber, 2012)

Many solutions to the vulnerabilities of virtualization have been developed or are in the process of being developed. Most of the solutions target either the virtualization architecture itself or the infrastructure. Many of these solutions have already been utilized by some virtualization security companies in their products to combat the vulnerabilities that are present.

Enormous benefits can be gained from moving to cloud computing. That is why it is very important for organizations to be aware of current risks of their virtual systems and how to address them. Therefore, most of the previous work has focused on the challenges and risks of virtualization that may occur when moving to the cloud from a virtual environment and the approaches used to overcome them. It would also be an advantage to experiment and validate the use of approaches chosen to overcome a specific risk. In this, study a similar setup to that of CBOS which is built on VMware will be used to perform the validation test.

2.0.1 Related Work

A closely related literature is (Studnia, Alata, Deswarte, Kaâniche, & Nicomette, 2012) where the authors discussed virtualization vulnerabilities such as Scaling,

Transience, Software lifecycle, Diversity, Mobility, Identity, Data lifetime listed by (Garfinkel & Rosenblum, 2005).

The author addressed these vulnerabilities with the use of good policies. Even so attackers were still able to exploit flaws the system and perform an attack. Examples of these attacks are detecting a virtualized environment, identifying the hypervisor, breach in the isolation, accurate targeting of VMs in a cloud and virtual machine based rootkits. Each example was explained in detail and to avoid such attacks and improve security VM monitoring and isolation Enforcement were used.

(Zheng, 2011) On the other hand focused on risks related to attacks which may occur on the hypervisor such as attacks on hypervisor through host OS and attacks on hypervisor through guest OS.

These attacks are considered the most well-known vulnerabilities in virtualization and exploit mainly the architecture. There are other forms of risks which are related to characteristics and infrastructure of virtualization and they are; Virtual library check-out, Migration attack and Encryption attack.

Many researches have been done in the field of virtualization security. (Sabahi, 2012) discussed the threats and attacks that can occur in virtualization. The threats discussed were Virtual machine level attacks and Communication in virtualization and the attacks were DDoS attacks and Client to client attacks.

The author described the risks in detail and to overcome these risks proposed virtualization architecture to secure the cloud.

A similar methodology approach was also used by Anton den Hoed in his research which aimed to find out which data privacy related risks are causing the most concerns and which technology based methods can be used to reduce these risks and had a positive contribution (Hoed, 2012).

Virtualization will continue to being widely implemented, however, the question is whether there's been adequate consideration for possible security threats. One reason may be because many security professionals are uninformed about the security risks of virtualization. On the other hand, those that are aware are challenged because they lack the authority to ensure that adequate measures are implemented at the IT infrastructure and operations level according (Mnovellino, 2013). Also most of the

concentration of security of virtualization has been on external risks therefore much more consideration should also be done to internal risks.

The above mentioned literatures have highlighted in them many different virtualization security risks that are present and the approaches used to overcome them. Such literature will be used to look for solutions to overcome the risks that may be found in CBOS current virtual environment.

CHAPTER THREE

Comment [L29]: This chapter very brief you the student should give all details about his work

3.0 METHODOLOGY

This research will use exploratory design because this research targets identifying the security risks associated with virtualization and moves on towards addressing the most important risks in order to significantly identify the appropriate approaches to overcome them. Thus, it is not certain what the final outcome would be.

The data collection methods that will be used in this research are qualitative and quantitative. The instruments that will be used for data collection will be interviews and questionnaires.

The steps that are to be followed for data collection and analysis for this research are:

1. To form an overview of the risks of virtualization by finding and analyzing relevant literature.
2. The overview of the risks of virtualization formed in step one will be used to prepare interviews and questionnaires which will be performed with approximately fifty IT experts in CBOS (Central Bank of Sudan), SUDATEL (Sudan Telecommunication Company) and NTC (National Telecommunication Corporation).
3. A search will be done for approaches currently available at this moment to reduce the risk using books, articles, journals and internet sources.
4. If no approaches to reduce the risk are found I will try to create a new approach.
5. A test for the chosen approaches will be done in a testing environment which will be setup similar to that of CBOS to see whether the approaches chosen have reduced the risk entirely, partially or not at all.

Comment [L30]: What does this means

Comment [L31]: Same as before

The steps for data collection and analysis that have been stated above in this research are represented in (Figure 3.1).

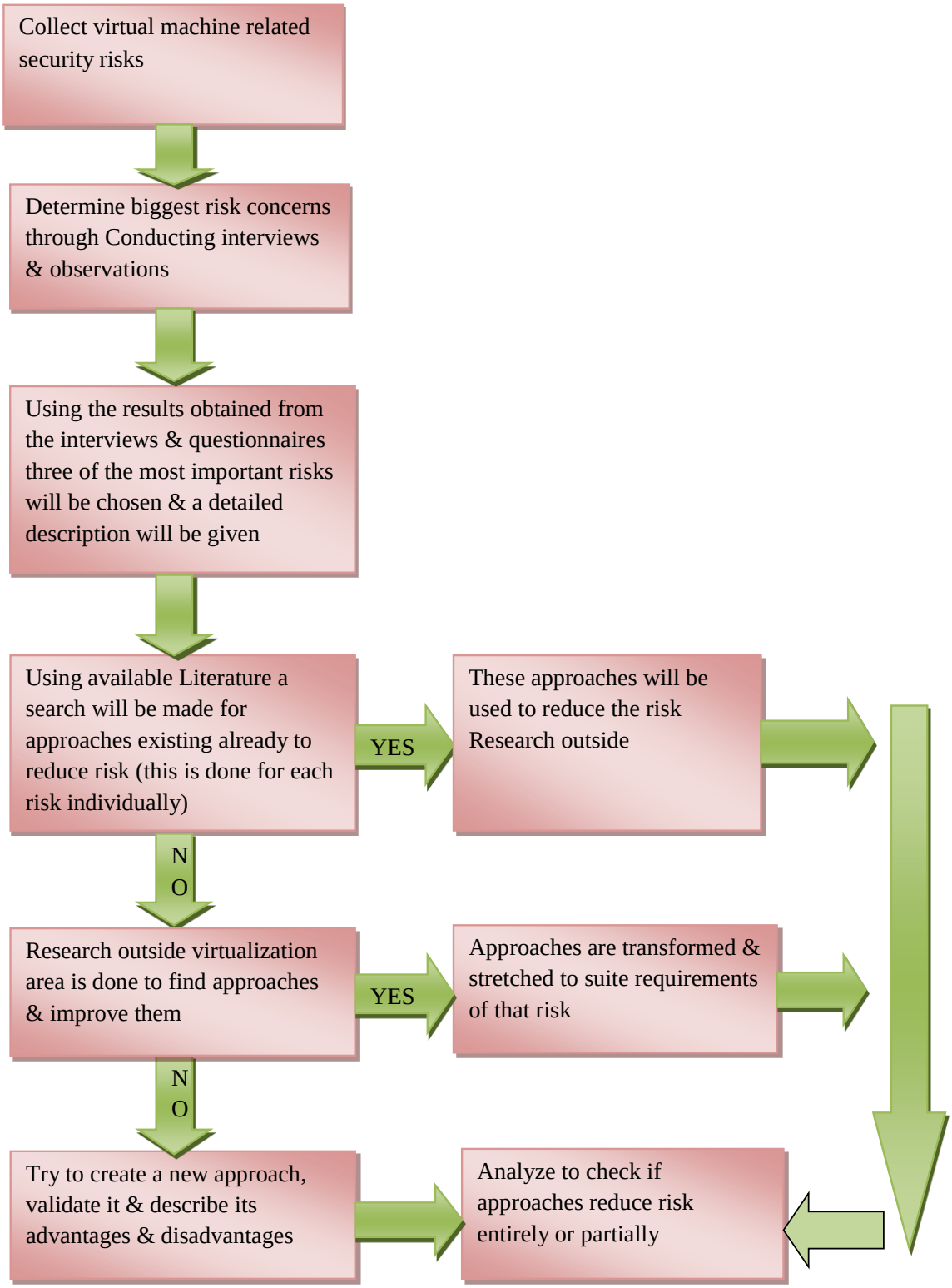


Figure 3.1: Methodology Steps

CHAPTER FOUR

4.0 RESULTS AND DISCUSSION

The objective of this research is to determine what the virtualization security risks are when moving to the cloud from a virtual environment, how to evaluate these risks and which approaches can be used to reduce these risks. These approaches may be existing approaches which are available and can be applied or entirely new approaches may be found. Identifying which risks are the most important was achieved by using interviews and questionnaires with virtualization experts working in different organizations. An overview of the risk of virtualization domain was required as a basis for the interviews and questionnaires before they could begin. A result analysis flowchart is represented in (Figure 4.24). Now we will begin by answering the first research question.

Q1. What are the risks / challenges of virtualization?

Comment [L32]: In this chapter should be no reference it's the researcher part.

The latest security reports from PCI (PCI, 2011), SANS (Hietala, 2009) , Computer and Electronics Security Applications (Studnia, Alata, Deswarte, Kaâniche, & Nicomette, Survey of Security Problems in Cloud Computing Virtual Machines, 2012), MacAfee (Hau, 2007) , Beyond Trust (Trust, 2013) and Trend Micro (Reis, 2013) were used to provide the overview of the risk of virtualization which was used as a guidance in structuring the interviews and questionnaires. Before starting an interview the interviewees were presented with the overview of the risk of virtualization and they were asked to answer the questions. The interviews covered administrators and operators from Central Bank of Sudan. As for the questionnaires they covered experts from other organizations which ranged from commercial banks to specialized companies in this field were sent by email. Information gathered will be used to answer the second research question.

Comment [L33]: Questionnaires should be adopted, and should be done as a pilot test on sample. There is no a pilot test and how did you chose the sample on which hypothesis.

Q2. What are the most critical risks of virtualization?

The number of times a risk was classified as one of the most important risks was based on the result of the interviews and questionnaires which is represented in (Figure 4.23). Even though it will not be discussed in this research, overall it was indicated that policies is a very important source of worries for most organizations.

When it comes to policies nothing changes significantly from the physical world. Current best practices are still relevant even though virtualization adds new components and considerations the basic security threats do not change. An example of this is provisioning accounts on the host. This should be handled with very carefully because providing a user with access to the host can be a potentially very powerful privilege over the guest. Therefore it is a good idea to link authentication to the host to existing identity management solutions such as Active Directory. It is always better for organizations to use the capabilities of their existing technologies to bring virtualization into the current infrastructure.

Three different risks were chosen for further research based on the results of the interviews and questionnaires.

First data management and protection because the results indicate that it is a big problem with many uncertainties. It is important to consider the security of the virtual disk files because virtual disks are stored as files on the host, especially if deployed on mobile computers or in untrustworthy physical environments.

The second risk is external attacks. Some of these attacks have already been covered in previous chapters. There are many types of external attacks and all cannot be covered in this research. Therefore, in addition to those already stated in previous chapters only most recent possible security threats in virtualized environments that are emerging will be highlighted here. According to an article by (Mnovellino, 2013) there are possible security threats in virtualized environments that are emerging which are:

Comment [L34]: This result chapter

1. The first is called the Blue Pill. This occurs when a virtual machine masquerades as a hypervisor by installing itself on a host machine. As a result, resource allocations and interactions between virtual OS instances are controlled by the virtual machine acting as an imposter.
2. The second is called SubVirt, which is a VM rootkit that positions itself on the physical machine. It then monitors and records the activity of the VM. As a result, it disguises when the system is compromised and also may involve other threatening programs like spyware or keystroke loggers.
3. The third threat is Denial-of-Service. This is a virtual machine infrastructure attack that allows a single or multiple VMs to consume all of the resources

that are contained within the host machine. Thus, these resources would not be available for other VMs.

4. The last threat is a Trojan. In this case, a hacker compromises the virtual machine manager, which allows them to control the applications and operating systems that are found on the machines, which is generally not addressed by antivirus software.

The third risk chosen for further research is security training and awareness. When it comes to security most organizations focus significant attention on technology their When assessing our customers' security implementations we often find significant attention focused on technology at the expense of the people. It is extremely important that people are properly trained about any new technology and its importance in order to be able to understand and plan for any change in process that may be brought about by the new technology.

Q3. Are there existing approaches which can be used to reduce this risk?

Large parts of Q3 have already been answered in the discussion sections of the previous chapters but for the purpose of this research which is based on a case study for CBOS. This part of the findings will focus on the risks that were specified by CBOS technical staff which were data management, training and awareness and external attacks.

4.0.1 Interviews and Questionnaires: The most important risks

The risk analysis documents of ENISA and PCI as well as latest security reports from SANS ,Computer and Electronics Security Applications ,MacAfee, Beyond trust and TrendMicro resulted in an overview of the most important risks of virtualization. However, it is not possible to cover all these risks in this thesis. Therefore, in order to determine which risks have the highest priority interviews and questionnaires with over thirty experts from eleven different organizations were used. These interviews and questionnaires were prepared using the overview of the top risks prepared earlier.

4.0.1.1 Interview results

Before an interview the interviewee received a document with an overview of the top risks formed from the three different analysis (Table 4.1) and instructions on how to access the risk analysis documents if required. During the interview many questions

were asked but the two main questions were: “In your opinion and based on your experience what are the most well-known virtualization risks?” and the second question is “According to your previous answer number what the three most important risks are (1) being most important? Interviewees were given the possibility to introduce risks which were not on the list. For interviews only CBOS administrators were interviewed since this research is based on case study for CBOS.

During the interviews no new risks were introduced to the list but all interviewees agreed that the most important risks according to their environment are data management, external attacks and lack of proper training & awareness. A copy of the interview questions & answers can be found in Appendix A.

4.0.1.2 Questionnaire results

The information obtained after analyzing the data using SPSS indicated that 65% of the participant’s ages were 25-35 years (Figure 4.1). Most of them have a bachelor degree (Figure 4.2) and 75% have more than five years’ experience (Figure 4.3).

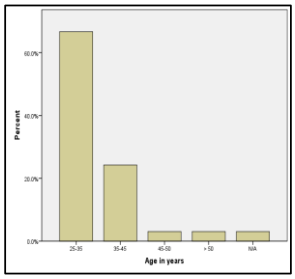


Figure 4.1: Age in years

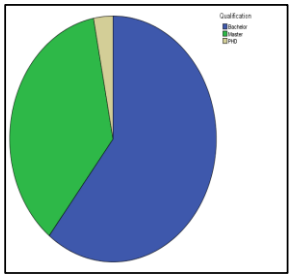


Figure 4.2: Qualification

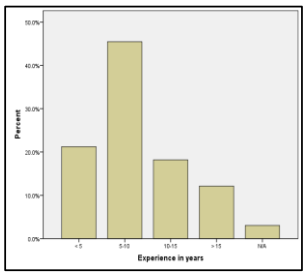


Figure 4.3: Experience in years

The most widely used technology by most of the organizations was VMware Vsphere (Figure 4.4). About 38% of them have 25-100 hypervisors (Figure 4.5) and more than 100 virtual guests (Figure 4.6).

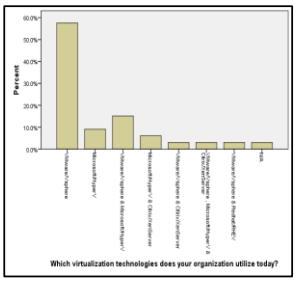


Figure 4.4: Virtualization technologies used

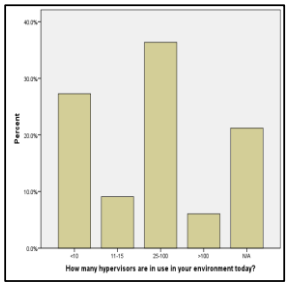


Figure 4.5: No. of hypervisors in current environment

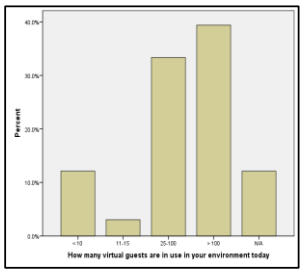


Figure 4.6: No. of virtual guests in current environment

More than half of the participants agreed that they regularly use security tools as a part of their administration (Figure 4.7). The most widely used tools were antivirus and security scanners (Figure 4.8).

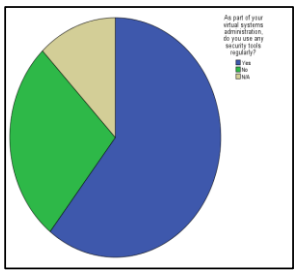


Figure 4.7: Do you use security tools regularly?

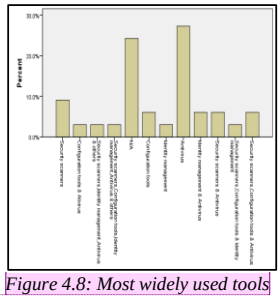


Figure 4.8: Most widely used tools

Comment [L35]: Not clear

Most organizations used SAN as a shared storage (Figure 4.9 and Figure 4.10). Also 60% indicated that their current security components are virtual aware (Figure 4.11). About half of them have virtual environments that meet regulatory compliance (Figure 4.12) and 80% have well trained administrators and operators (Figure 4.13) which is a good indication on the awareness on the importance of virtualization security.

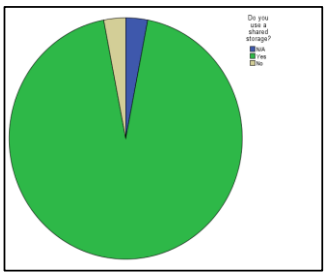


*Figure 4.9: Do you use shared storage***?**

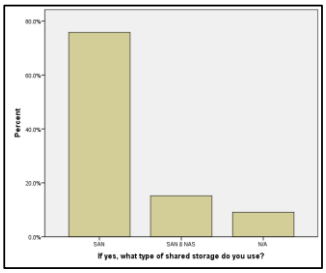


Figure 4.10: Type of shared storage used

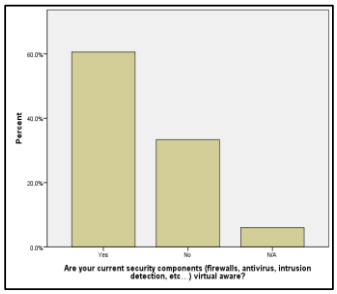


Figure 4.11: Are security components virtual aware?

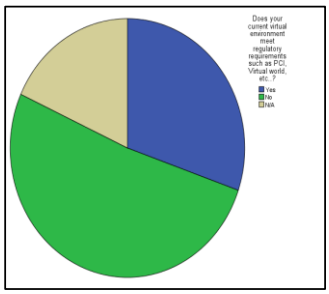


Figure 4.12: Do you meet regulatory compliance?

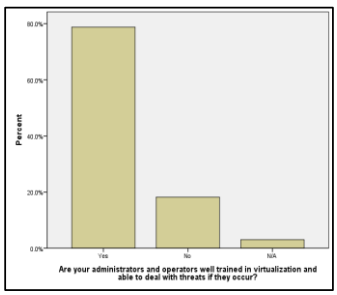


Figure 4.13: Are admins well trained?

Most of the participants believed that the most well-known risks are related to mostly patching and data management (Figure 4.14) and this was due to the fact that about 30% don't patch regularly (Figure 4.15), while 35% don't even know how often they need to perform security scans on virtual machines (Figure 4.16). Many of the

participants also indicated that they monitor their VMs using virtualization monitoring software (Figure 4.17), their inward-facing and outward-facing VMs placed on the same physical servers (Figure 4.18) but their dormant VMs are not scanned regularly for known vulnerabilities (Figure 4.19). This was an indication of poor data management which is considered a big risk.

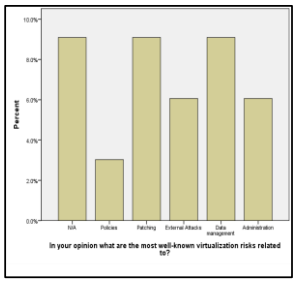


Figure 4.14: Most well-known risks

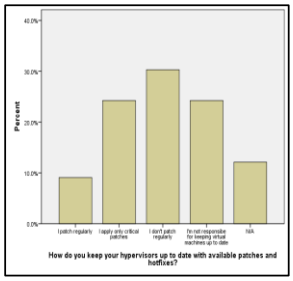


Figure 4.15: Do you patch hypervisors?

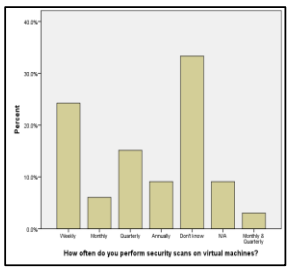


Figure 4.16: How often do you scan VMs?

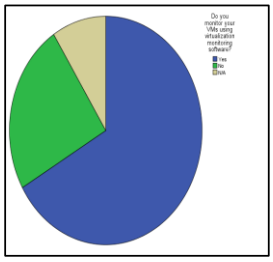


Figure 4.17: Do you monitor VMs?

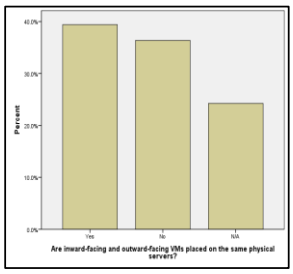


Figure 4.18: Are inward/outward VMs on same server?

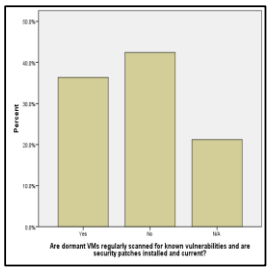


Figure 4.19: Are dormant VMs scanned?

On the other hand most organizations handle the data associated with retired VMs properly (Figure 4.20), backup their VMs (Figure 4.21) and have a backup policy (Figure 4.22).

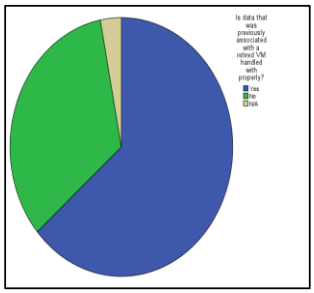


*Figure 4.20: Are retired VMs data handled properly**?***

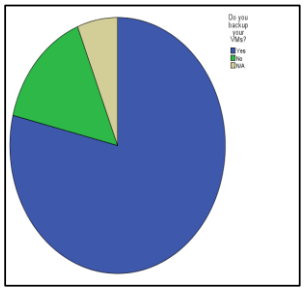


Figure 4.21: Do you backup VMs?

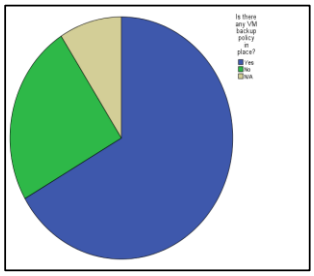


Figure 4.22: Do you have a backup policy?

According to the information gathered by interviews and questionnaires, data management and protection was classified as one of the top risks of virtualization (Figure 4.23). A copy of the questionnaire could be found in Appendix B.

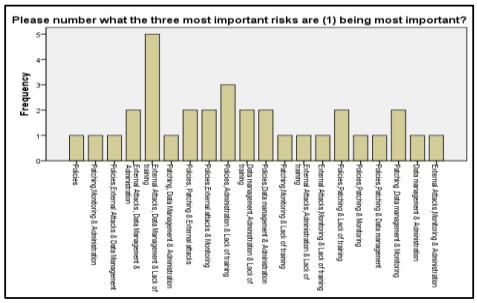


Figure 4.23: Three most important risks

It is important to consider the security of the virtual disk files because virtual disks are stored as files on the host, especially if deployed on mobile computers or in untrustworthy physical environments. However, the security measure implemented by each organization differs from one to another depending on size and business type. Some perform specific audits and implement best practices while others do not.

Another risk which has been mentioned frequently and may occur as the result of improper data management and protection is external attacks.

Virtual systems and networks are subject to the same attacks and vulnerabilities that exist in a physical infrastructure. For example if a vulnerable application from a physical environment is moved to a virtual environment it will still have those same flaws and vulnerabilities.

Table 4.1- The top risks of virtualization according to MacAfee, SANS and Gartner

Gartner (Gartner, 2010)	SANS (Hietala, 2009)	MacAfee (Hau, 2007)
Information Security Isn't Initially Involved in the Virtualization Projects	Misconfiguration of virtual hosting platform	Change control
A Compromise of the Virtualization Layer Could Result in the Compromise of All Hosted Workloads	Separation of duties	Asset tracking and management
The Lack of Visibility and Controls on Internal Virtual Networks Created for VM-to-VM Communications Blinds Existing Security Policy Enforcement Mechanisms	Failure of integration into life cycle management	Patch management
Workloads of Different Trust Levels Are Consolidated Onto a Single Physical Server Without Sufficient Separation	Security awareness	Contingency Planning
Adequate Controls on Administrative Access to the Hypervisor/VMM Layer and to Administrative Tools Are Lacking	Lack of tools and policies	
There Is a Potential Loss of Separation of Duties for Network and Security Controls	VM sprawl	
	Lack of open ecosystem	
	Failure of policy coordination	
	Failure to consider hidden costs	

Security training and awareness is a risk which must be dealt with carefully. Unlike malware and viruses which are external threats and can be reduce by use of technology. Lack of proper security training and awareness is considered as an internal threat. When it comes to security implementations customers usually focus most of their attention on technology at the expense of the people. Therefore, it is extremely important that people are properly trained about any new technology and its importance in order to be able to understand and plan for any change in process that may be brought about by the new technology.

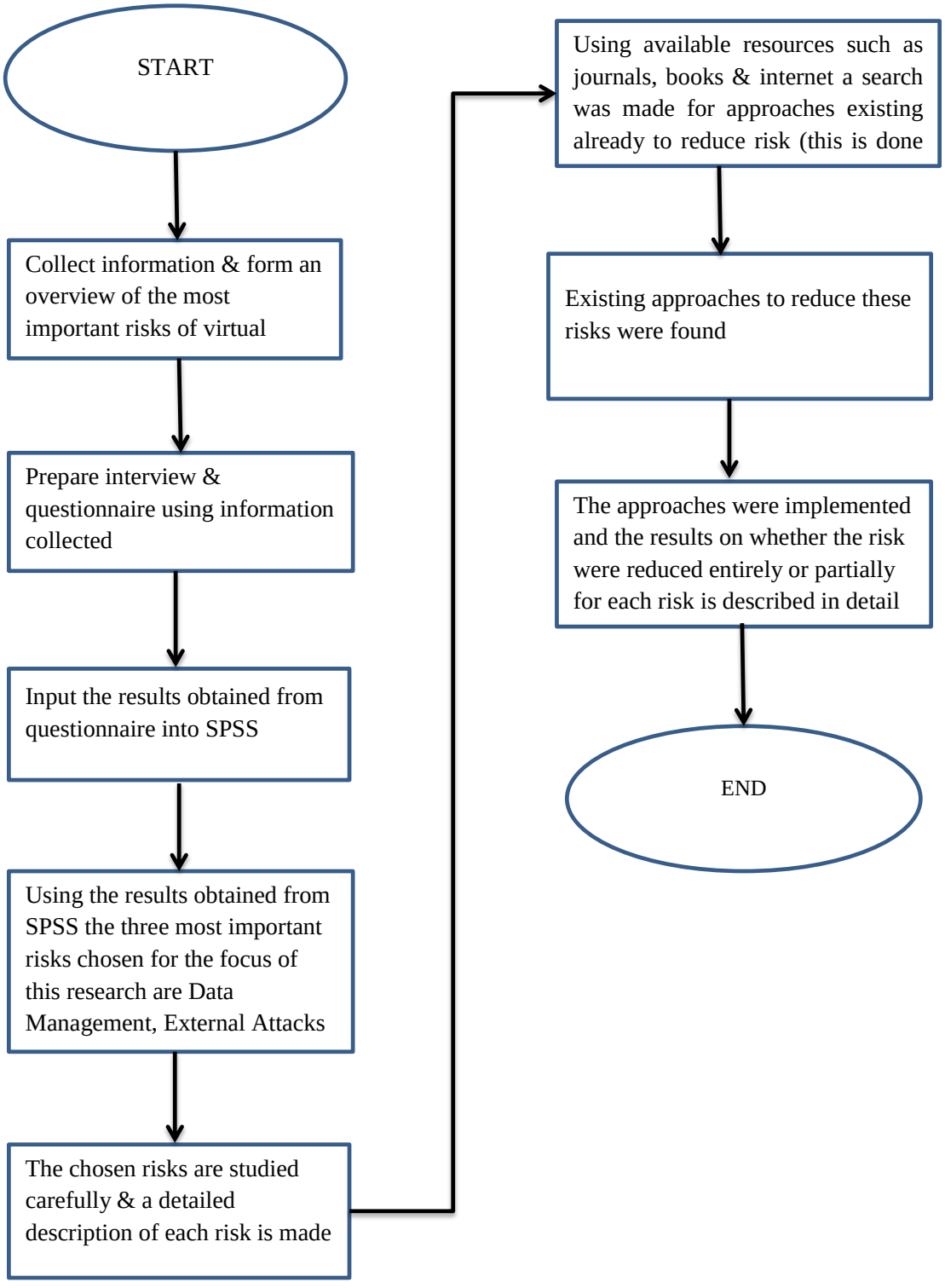


Figure 4.24: Result analysis flowchart

Comment [L36]: Is this methodology or results.

Comment [L37]: Where is the IT fingerprint in this research

Comment [L38]: How did you chose the sample and why, what is the actual size of the case, what level of management been involved and why.

Comment [L39]: The current situation in central bank not mentioned.

Comment [L40]: Where is your contribution in this research

CHAPTER FIVE

5.0 CONCLUSION AND REOMMENDATION

Virtualization technologies can bring many interesting new features such as optimized use of hardware resources, eased restoration and machine migration but they also introduce new means to perform attacks. These attacks may either be directed against virtualized systems or leverage some features related to virtualization in order to take over a system. Therefore, especially if a system is shared between many users, as is the case in cloud computing, strong security of virtual machines is crucial to protect their data and gain the customer's trust. In the above sections we initially describe the basic features of clouds and then covered virtualization in more detail beginning from its history, types, characteristics, benefits and ending with its limitations.

The research on security issues in virtualization is very active today, following a great diversity of possibilities, going from ways to secure popular systems like Xen, KVM or VMware are solutions, to creating new models such as the microkernel-based virtualization. However, even if these solutions are satisfying security-wise, one should still consider the possible issues of their large-scale deployment. Indeed, additional control procedures will cause a decrease in efficiency. Therefore it is important to find the right balance between performance and security according to their needs, keeping in mind that the usage of virtualization technology effectively can lead to efficient usage of cloud computing in the future.

5.0.1 Reflection and Limitations

It was really difficult to validate if the recommended approaches completely overcame the two risks of data management and external attacks because it is not possible to test the chosen software technologies in the real environment.

The discussion of existing methods that are used or can be adapted for virtualization use may not be complete for this thesis. This is because a wide range of sources was needed to perform this research and it is not possible to get complete knowledge required about all the different technologies that exist and can potentially be used to reduce the risk due to embargo on Sudan.

The risks that are covered in this thesis are data management, external risks, security training and awareness. Out of the three risks in my opinion lack of proper security training and awareness seems to be the most critical. The introduction of technology in the banking sector began to flourish in year 2000 when CBOS implemented its first network and since then has been expanding rapidly. Today almost the entire banking sector is completely dependent on technology. All this concentration on the implementation of technology has come at the expense of security.

The lack of proper protection and the increase of BYOD make detecting and preventing the leakage of information even harder. Therefore moving to the cloud from the current virtual environment means that your data is also moved to a location where there is no direct control over it. Therefore additional risks will be added to those already present in the current environment.

Comment [L41]: Some of this references not mention in the research and some mentioned but didn't used

REFERENCES

Armbrust, M. e. (2009). Above the Clouds : A Berkeley View of Cloud Computing. Science.

Bakar, R. A. (2014, April). Vulnerability scanner product reviews. Retrieved from Infosec: http://www.royabubakar.com/blog/2014/04/29/vulnerability-scanner-product-reviews/

Bittman, T. J. (2011, March). The Road Map From Virtualization to Cloud Computing. Retrieved from Easystreet.com: http://easystreet.com/wp-content/uploads/2012/12/Gartner_The-Road-Map-From-Virtualization-to-Cloud-Computing-G00210845_English.pdf?bcsi_scan_b895edbe82a47962=0&bcsi_scan_filename=Gartner_The-Road-Map-From-Virtualization-to-Cloud-Computing-G00210845_Englis

Blaisdell, R. (2011, November). A brief history of cloud computing. Retrieved from RicksCloud: http://www.rickscloud.com/a-brief-history-of-cloud-computing-2/

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., et al. (2009). Controlling data in the cloud: outsourcing computation without outsourcing control. Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 85-90.

Clarizen. (2013, June). Risk Management - Useful Tools and Techniques. Retrieved from Clarizen: https://success.clarizen.com/entries/24127786-Risk-Management-Useful-Tools-and-Techniques

Davis, D. (2011, November). Top 10 Best Practices of Backup and Replication for VMware and Hyper-V. Retrieved from informationweek: http://www.informationweek.com/whitepaper/Hardware/Virtualization-Hardware/top-10-best-practices-of-backup-and-replication-fo-wp1321629893?articleID=191703853

Garber, L. (2012). The Challenges of Securing the Environment.

Garfinkel, T., & Rosenblum, M. (2005). When Virtual is Harder than Real: Security Challenges in Virtual Machine. Proceedings of the 10th conference on Hot Topics in Operating Systems-Volume 10, p. 20.

Gartner. (2010, March). Six Most Common Virtualization Security Risks and How to Combat Them. Retrieved from Gartner: http://www.gartner.com/newsroom/id/1322414

Group, A. S. (2011). Private vs. Public Cloud Comparison Chart. Retrieved May 11, 2013, from Advanced Systems Group: http://www.virtual.com/solutions/cloud-computing/cloud-comparison-chart

Hau, W. A. (2007). Virtualization and Risk – Key Security Considerations for your Enterprise Architecture. Retrieved from MCafee: http://www.mcafee.com/uk/resources/white-papers/foundstone/wp-virtualization-and-risk.pdf

Hietala, J. D. (2009, August). Top Virtualization Security Mistakes (and How to Avoid Them). Retrieved from SANS: http://www.sans.org/reading-room/analysts_program/McAfee_Catbird_Virtualization_Jul09.pdf

Hill, B. (2012, March 12). Intro to Virtualization: Hardware, Software, Memory, Storage, Data and Network Virtualization Defined. Retrieved from Petri IT Knowledgebase: http://www.petri.co.il/intro-to-virtualization.htm#software-virtualization

Hoed, A. d. (2012, October). Technology Based Methods to Reduce The Risks of Cloud Computing. Retrieved from Leiden Institute of Advanced Computer Science: http://www.liacs.nl/assets/Masterscripties/2012-12AntonDenHoed.pdf?bcsi_scan_b895edbe82a47962=0&bcsi_scan_filename=2012-12AntonDenHoed.pdf

ISO. (2013, December). ISO 31000:2009 - Risk management - Principles and guidelines. Retrieved from ISO: http://www.iso.org/iso/catalogue_detail?csnumber=43170

KarenScarfone, MurugiahSouppaya, & PaulHoffman. (2011, January). Guide to Security for Full Virtualization Technologies. Retrieved from NIST: http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

Kavanagh, K. M. (2013, September). MarketScope for Vulnerability Assessment. Retrieved from Gartner: https://www.gartner.com/doc/2586218/marketscope-vulnerability-assessment

Mell, P., & Grance, T. (2011, September). The NIST Definition of Cloud Computing. Retrieved from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Microsoft. (2010, September). A Guide to Data Governance for Privacy, Confidentiality, and Compliance.Part 3: Managing Technological Risk. Retrieved from Microsoft Corp.: http://www.microsoft.com/en-eg/download/details.aspx?id=10985

Mnovellino, C. a. (2013). Virtualization: awareness and security threats. Retrieved from MIT Geospatial Data Center Media:

http://cybersecurity.mit.edu/2013/09/virtualization-awareness-and-security-threats/

Oracle. (2009). Oracle VM Server User's Guide. Retrieved from Oracle: http://docs.oracle.com/cd/E11081_01/doc/doc.21/e10898/intro.htm

PCI. (2011, June). Information Supplement: PCI DSS Virtualization Guidelines. Retrieved from PCI: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

Reis, D. (2013). Cloud & Virtualization Security for Dummies. Hoboken, New Jersey: John Wiley & Sons.

Ritter, T. (2009). Virtualization Security. Retrieved from Trenmicro: http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_nemertes-virt-security.pdf?bcsi_scan_b895edbe82a47962=0&bcsi_scan_filename=wp_nemertes-virt-security.pdf

Sabahi, F. (2012). Secure Virtualization for Cloud Environment Using Hypervisor-based Technology. International Journal of Machine Learning and Computing.

Shackleford, D. (2011, July). A six-step virtualization risk assessment process. Retrieved from TechTarget: http://searchcloudsecurity.techtarget.com/tip/A-six-step-virtualization-risk-assessment-process

Shimba, F. (2010, September). Cloud Computing:Strategies for Cloud Computing Adoption. Retrieved from Dublin Institute of Technology: http://arrow.dit.ie/scschcomdis/1

Smith, D. M. (2013, May). Hype Cycle for Cloud Computing, 2013. Retrieved from Gartner: https://www.gartner.com/doc/2573318/hype-cycle-cloud-computing-

Smith, M. (2014, May). Protecting Your Data in a Virtualized Environment. Retrieved from Software Specialists : http://www.softwarespecialists.com/protecting-data-virtualized-environment/

Stark, C. (2012, March). The History of Cloud Computing. Retrieved from Cetrom: http://www.cetrom.net/blog/the-history-of-cloud-computing/

Stephenson, P. (2013, February). Vulnerability assessment tools. Retrieved from SC magazine: http://www.scmagazine.com/vulnerability-assessment-tools/grouptest/278/

Studnia, I., Alata, E., Deswarte, Y., Kaâniche, M., & Nicomette, V. (2012). Survey of Security Problems in Cloud Computing Virtual Machines. Cloud and security:threat or opportunity.

Studnia, I., Alata, E., Deswarte, Y., Kaâniche, M., & Nicomette, V. (2012). Survey of Security Problems in Cloud Computing Virtual Machines. "Computer and Electronics Security Applications Rendez-vous (C&ESAR 2012). Cloud and security:threat or opportunity.

Taylor, S. (2011, May). Public vs. Private Cloud: Mitigating Risk. Retrieved from OmniVue: http://www.omnivue.net/2011/05/public-vs-private-cloud-mitigating-risk/

Teter, M. (2011, February). Public vs. Private Cloud Comparison. Retrieved from Advanced Systems Group: http://blog.virtual.com/2011/public-vs-private-clouds-comparison

Trust, B. (2013, May). Survey Results: Virtual Insecurity. Retrieved from Beyond Trust: http://img.en25.com/Web/eEyeDigitalSecurityInc/%7B81b03119-b2ea-42e6-9924-13b20d8412fd%7D_BEYONDTRUST_Virtual_Insecurity_Survey_Results.pdf

Velic, M. (2011, December). The History of Virtualization. Retrieved from Matt Velic: http://mattvelic.com/history-of-virtualization/

Wallen, J. (2013, April). 10 benefits of virtualization in the data center. Retrieved from Techrepublic: http://www.techrepublic.com/blog/10-things/10-benefits-of-virtualization-in-the-data-center/3662/#.

Wendt, J. M. (2013). 2013 Virtual Server Backup Software Buyer's Guide. Retrieved from DCIG: http://webdocs.commvault.com/assets/dcig-2013-virtual-server-backup-software-buyers-guide-analyst-report.pdf?dl=1

Winkler, V. (2011, December). Cloud Computing: Virtual Cloud Security Concerns. Retrieved from TechNet Magazine: http://technet.microsoft.com/en-us/magazine/hh641415.aspx

Wu, J. (2011). Recent Advances in Cloud Security. Journal of Computers,Vol.6.

Xuefeng, S. U. (2012). Cloud Computing: a Prologue. International Journal of Advanced Research in Computer and Communication Engineering, 1-4.

Younger, J. (2013, February). Common Virtualization Vulnerabilities and How to Mitigate Risks. Retrieved from pentestlab: http://pentestlab.wordpress.com/2013/02/25/common-virtualization-vulnerabilities-and-how-to-mitigate-risks/

Zheng, M. (2011). Virtualization Security in Data Centers and Clouds. Retrieved from www.cse.wustl.edu: http://www.cse.wustl.edu/~jain/cse571-11/ftp/virtual/index.html

APPENDICES

Appendix A. INTERVIEW QUESTIONS

Al-Madinah International University
Faculty of Computer and Information Technology

Interview Questions

The following are the questions and answers of the interview. Questions were asked after a brief introduction regarding the thesis and an overview of the top security threats of virtualization was given.

1. Which virtualization technologies does your organization utilize today?

The virtualization technology used is VMware version 4.1.

2. As part of your virtual systems administration, do you use any security tools regularly?

No security tools for virtual systems are used.

3. What kinds of tools are you using currently or are being considered?

We are considering monitoring tools but no specific brand has been decided on yet.

4. Do you use a shared storage?

Yes there is a SAN.

5. Has virtualization improved the quality of service in your organization?

Yes it has and hopefully by the end of the year all applications will be running on virtualization.

6. Are your current security components (firewalls, antivirus, intrusion detection, etc…) virtual aware?

No they are not.

7. Is your data encrypted?

Yes there is encryption.

8. Does your current virtual environment meet regulatory requirements such as PCI, Virtual world, etc..?

No regulatory requirements have been met yet.

9. Are your administrators and operators well trained in virtualization and able to deal with threats if they occur?

Yes they have received some training but advanced training is still required.

10. Are virtual assets included as part of regulatory compliance audits and reporting?

There was a security audit but unfortunately the virtual machines were not included.

11. Have you followed any security hardening best practices on your virtual infrastructure?

There is no security hardening best practices that we are aware of because the virtual infrastructure was implemented by a vendor.

12. Do you plan on migrating to a cloud environment within the next two years?

No not for the time being due to embargo.

13. In your opinion what are the most well-known virtualization risks related to?

The most well-known risks are related to Policies, External Attacks, Data management, Monitoring & Lack of training.

14. Please number what the three most important risks are (1) being most important?

Policies	**4**
Patching	
External Attacks	**2**
Data management	**1**
Monitoring	
Administration	
Lack of training	**3**

15. Do you keep your hypervisors up to date with available patches and hotfixes?

No patching has been done.

16. Do you perform security scans on virtual machines?

No security scans have been performed.

17. Do you monitor your VMs using virtualization monitoring software?

There is monitoring software used but it does not monitor virtual machines.

18. Do you ensure that the appropriate security policies are applied to individual VMs as they are moved from one physical host to another?

Yes there are policies in place.

19. Are dormant VMs regularly scanned for known vulnerabilities and are security patches installed and current?

No there is not.

20. Are retired VMs properly removed from the virtual infrastructure?

Yes all retired VMs are deleted.

21. Is data that was previously associated with a retired VM handled with properly?

Yes it is.

22. Do you backup your VMs?

There is no backup for VMs only databases and applications are backed up.

23. If yes what software do you use?

Symantec Netbackup version 7.1.0.3

24. Is there any VM backup policy in place?

No VM backup policy is in place.

Appendix B. QUESTIONNAIRE

Al-Madinah International University
Faculty of Computer and Information Technology

Dear Reader,

I am student at Al-Madinah International University in the field of Information and Communication Technology. I am doing this questionnaire for my master thesis titled: "**ENHANCING SECURITY CONCERNS IN CLOUD COMPUTING VIRTUAL MACHINES"**

If you would be kind enough to answer a few questions then I would be really thankful to you. I can ensure you that the information provided will not be used anywhere else. If you are interested in the result of this research please do not hesitate to contact me by email: **samah_hassan@yahoo.com** . Please send the completed document as soon as possible by latest 22, May 2014 to this email address as an attached file.

Very sincerely yours,

Samah Sabir Mohamed
Researcher

PART ONE:

The following questions are about your personal information. Read each question and answer it, making a mark (√) or providing the information requested in the blank spaces.

1. **Name of organization:** _____

2. **Gender:** ☐ Male ☐ Female

3. **Age (in years):** ☐ 25-35 ☐ 35 –45 ☐ 45 –50 ☐ Above 50 years

4**. Qualification:** ☐ Bachelor ☐ Master ☐ PHD

5. **Position:**

☐ Manager ☐ Head of Department ☐ Programmer ☐ Engineer

☐ Administrator ☐ Other (Please specify) _____

6. **Years of Experience:** ☐ Less than 5 ☐ 5 -10 ☐ 10–15 ☐ Above 15 years

PART TWO:

The following questions are about technical information in virtualization. Read each question and answer it, making a mark (√) or providing the information requested in the blank spaces.

1. Which virtualization technologies does your organization utilize today?

☐ VMware/Vsphere ☐ Microsoft/Hyper-V ☐ Citrix/XenServer

☐ Redhat/RHEV

2. How many hypervisors are in use in your environment today?

☐ < 10 ☐ 11-15 ☐ 25-100 ☐ > 100

3. How many virtual guests are in use in your environment today?

☐ < 10 ☐ 11-15 ☐ 25-100 ☐ > 100

4. Does your organization currently use any of the following Application Virtualization technologies?

☐ Microsoft App-V ☐ VMware ThinApp

☐ No Application virtualization Technology

☐ Other (Please specify) _____

5. As part of your virtual systems administration, do you use any security tools regularly?

☐ Yes ☐ No

6. What kinds of tools are you using currently or are being considered?

☐ Security scanners ☐ Configuration tools ☐ Identity management

☐ Antivirus ☐ Other (Please specify) _____

7. Do you use a shared storage?

☐ Yes ☐ No

8. If yes, what type of shared storage do you use?

☐ NAS ☐ SAN

9. Has virtualization improved the quality of service in your organization?

☐ Yes ☐ No

10. Are your current security components (firewalls, antivirus, intrusion detection, etc…) virtual aware?

☐ Yes ☐ No

11. Is your data encrypted?

☐ Yes ☐ No

12. Does your current virtual environment meet regulatory requirements such as PCI, Virtual world, etc..?

☐ Yes ☐ No

13. Are your administrators and operators well trained in virtualization and able to deal with threats if they occur?

☐ Yes ☐ No

14. Are your current administrators and operators well aware of the types of security threats especially the most recent threats?

☐ Yes ☐ No

15. Is high availability used in your current virtual environment?

☐ Yes ☐ No

16. Do you have proper documentation which is updated regularly?

☐ Yes ☐ No

17. Are virtual assets included as part of regulatory compliance audits and reporting?

☐ Yes ☐ No ☐ Sometimes ☐ Don't Know

18. Have you followed any security hardening best practices on your virtual infrastructure?

☐ Yes ☐ No

19. If yes, what was the source of those best practices?

☐ Virtualization vendor ☐ Security vendor ☐ Networking vendor

☐ Other (Please specify) _____

20. Do you plan on migrating to a cloud environment within the next two years?

☐ Yes ☐ No

21. In your opinion what are the most well-known virtualization risks related to?

☐ Policies ☐ Patching ☐ External Attacks ☐ Data management

☐ Monitoring ☐ Administration ☐ Lack of training

☐ Other (please specify) _____

22. Please number what the three most important risks are (1) being most important?

Policies	
Patching	
External Attacks	
Data management	
Monitoring	
Administration	
Lack of training	

☐ Other (please specify) _____

23. How often are existing image templates used for new virtual images?

☐ Often ☐ Rarely ☐ Never

24. Are there any security controls in place that require a security sign off prior to releasing a new virtual image or template?

☐ Yes ☐ No

25. How do you keep your hypervisors up to date with available patches and hotfixes?

☐ I patch regularly ☐ I only apply critical patches ☐ I don't patch regularly

☐ I'm not responsible for keeping the virtual machines up to date

☐ Other (Please specify) _____

26. How often do you perform security scans on virtual machines?

☐ Weekly ☐ Monthly ☐ Quarterly ☐ Annually ☐ Don't Know

27. Are new VMs deployed using an approved security profile and in accordance with established policies?

☐ Yes ☐ No

28. Is the correct OS version installed and patched when deploying new VMs?

☐ Yes ☐ No

29. Do you monitor your VMs using virtualization monitoring software?

☐ Yes ☐ No

30. Do you ensure that the appropriate security policies are applied to individual VMs as they are moved from one physical host to another?

☐ Yes ☐ No

31. Are inward-facing and outward-facing VMs placed on the same physical servers?

☐ Yes ☐ No

32. Are adequate resources available for new VMs deployed on a host machine?

☐ Yes ☐ No

33. Is a capacity analysis conducted prior to deploying new VMs on a host machine?

☐ Yes ☐ No

34. Does a new VM impact the performance and security of other VMs on the host machine negatively?

☐ Yes ☐ No

35. Are dormant VMs regularly scanned for known vulnerabilities and are security patches installed and current?

☐ Yes ☐ No

36. Are retired VMs properly removed from the virtual infrastructure?

☐ Yes ☐ No

37. Is data that was previously associated with a retired VM handled with properly?

☐ Yes ☐ No

38. Do you backup your VMs?

☐ Yes ☐ No

39. Is there any VM backup policy in place?

☐ Yes ☐ No

PART THREE: CONFIRMATION

The following is information below is required for confirmation purposes regarding this thesis only. Kindly provide the information requested in the blank spaces and stamp with organization stamp please.

I _____ certify that the above information is true, complete, and correct to the best of my knowledge.	
Signature	**Date**

Thank you for your help!

Appendix C. RETINA SAMPLE REPORT

Retina Network Security Scanner

Network Vulnerability Assessment & Remediation Management

7/1/2014 - Report created by version 5.19.10.2787

Executive Report

CONFIDENTIAL INFORMATION

The following report contains company confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company's security policy. All copies and backups of this document should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is grounds for termination.

Retina Network Security Scanner

Network Vulnerability Assessment & Remediation Management

7/1/2014 - Report created by version 5.19.10.2787

Report Created By	Report Created For

Retina Network Security Scanner

Network Vulnerability Assessment & Remediation Management

7/1/2014 - Report created by version 5.19.10.2787

Metrics for 'sample test'	
File name:	C:\Program Files (x86)\eEye Digital Security\Retina 5\Scans\sample report.rtd
Audits revision:	2787
Scanner version:	5.19.10
Start time:	7/1/2014 5:55:29 PM
Duration:	0d 0h 17m 10s
Credentials:	Single Use
Audit groups:	All Audits
Address groups:	N/A
IP ranges:	172.60.2.1-172.60.2.254
Total hosts attempted:	254
Total hosts scanned:	4
No access:	2

Retina Network Security Scanner

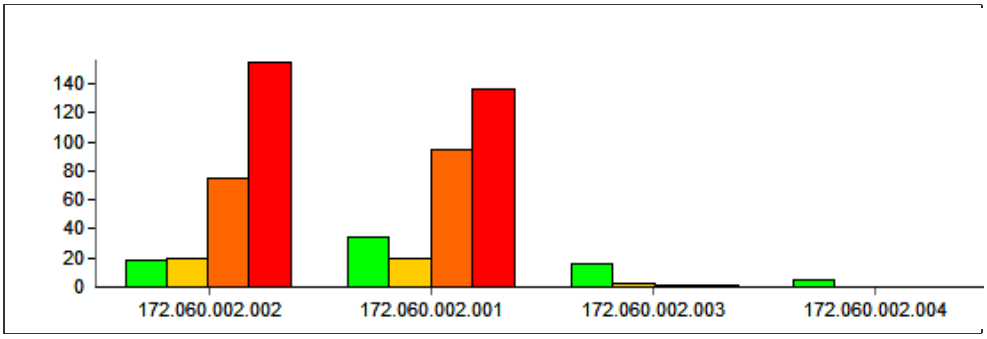
Network Vulnerability Assessment & Remediation Management

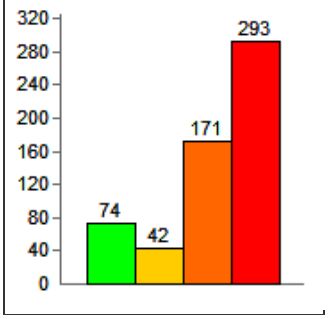
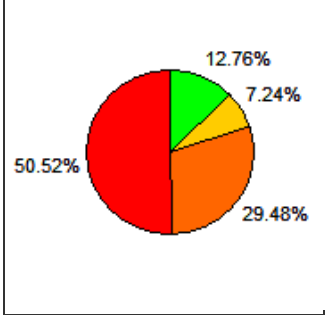
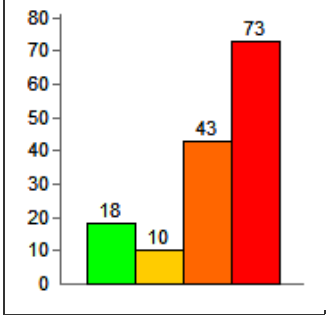
7/1/2014 - Report created by version 5.19.10.2787

NETWORK ANALYSIS RESULTS

Report Summary			
Scanner Name	Retina	Machines Scanned	4
Scanner Version	5.19.10.2787	Vulnerabilities Total	506
Scan Start Date	7/1/2014	High Risk Vulnerabilities	293
Scan Start Time	5:55:29 PM	Medium Risk Vulnerabilities	171
Scan Duration	0h 17m 10s	Low Risk Vulnerabilities	42
Scan Name	sample test	Information Only Audits	74
Scan Status	Completed	Credential Used	Single Use
Vulnerable Machines	4		

Top 5 Most Vulnerable Hosts



Num. of Vulnerabilities By Risk	% of Vulnerabilities By Risk	Avg. of Vulnerabilities By Risk
		

Retina Network Security Scanner

Network Vulnerability Assessment & Remediation Management

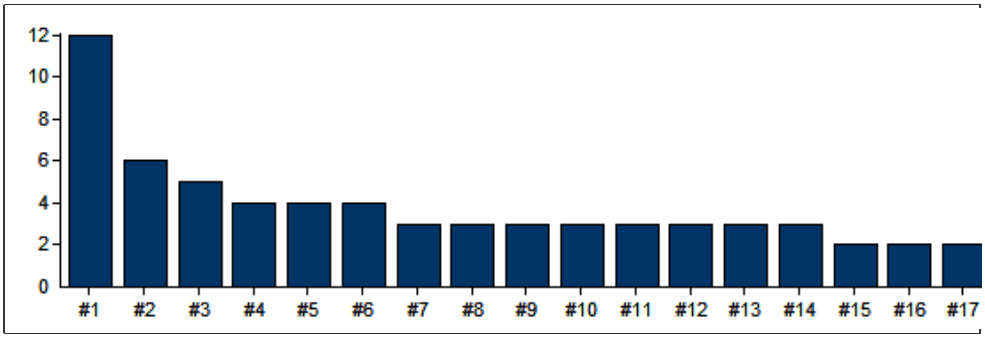
7/1/2014 - Report created by version 5.19.10.2787

TOP 20 VULNERABILITIES

The following is an overview of the top 20 vulnerabilities on your network.

Rank	Vulnerability Name	Count
1.	SSL Weak Cipher Supported	12
2.	SSL Weak Cipher Method Supported	6
3.	User Never Logged On	5
4.	Microsoft Windows Operating System Older Than Newest Major Version	4
5.	DCE/RPC Service Detected	4
6.	Virtual Environment Detected	4
7.	HTTP Methods Detected	3
8.	SSLv2 Detected	3
9.	NetBIOS/SMB Information Disclosure	3
10.	HTTP 1.1 Protocol Detected	3
11.	SSL Certificate Public Key Algorithm	3
12.	SSL Certificate Version	3
13.	Web Server Default Install Page Detected - IIS	3
14.	Microsoft Windows Share Allows Everyone Access	3
15.	Account Lockout Reset Time	2
16.	Account Lockout Threshold - PCI DSS/HiTrust	2
17.	Minimum Password Length	2
18.	DNS Version Detection	2
19.	Microsoft DNS Version Detection	2
20.	CHARGEN service (Simple TCP Services on Windows) - REMOTE	2

Top 20 Vulnerabilities

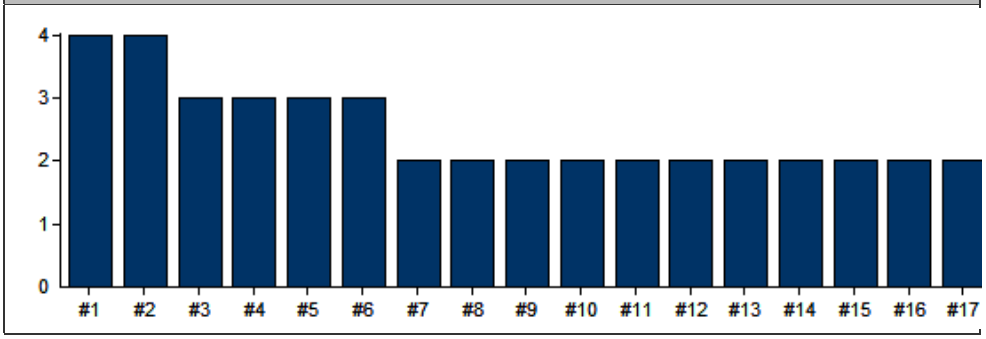

12
10
8
6
4
2
0
#1
#2
#3
#4
#5
#6
#7
#8
#9
#10
#11
#12
#13
#14
#15
#16
#17

TOP 20 OPEN PORTS

The following is an overview of the top 20 open ports on your network.

Rank	Port Number	Description	Count
1.	TCP:135	RPC-LOCATOR - RPC (Remote Procedure Call) Location Service	4
2.	TCP:445	MICROSOFT-DS - Microsoft-DS	4
3.	TCP:80	WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)	3
4.	TCP:139	NETBIOS-SSN - NETBIOS Session Service	3
5.	TCP:443	HTTPS - HTTPS (Hyper Text Transfer Protocol Secure) - SSL (Secure Socket Layer)	3
6.	UDP:137	NETBIOS-NS - NETBIOS Name Service	3
7.	TCP:7	ECHO - Echo	2
8.	TCP:9	DISCARD - Discard	2
9.	TCP:13	DAYTIME - Daytime	2
10.	TCP:17	QOTD - Quote of the Day	2
11.	TCP:19	CHARGEN - Character Generator	2
12.	TCP:53	DOMAIN - Domain Name Server	2
13.	TCP:88	KERBEROS - Kerberos	2
14.	TCP:389	LDAP - Lightweight Directory Access Protocol	2
15.	TCP:636	LDAPSSL - LDAP Over SSL	2
16.	TCP:49153		2
17.	UDP:7	ECHO - Echo	2
18.	UDP:13	DAYTIME - Daytime	2
19.	UDP:17	QOTD - Quote of the Day	2
20.	UDP:19	CHARGEN - Character Generator	2

Top 20 Open Ports



Retina Network Security Scanner

Network Vulnerability Assessment & Remediation Management

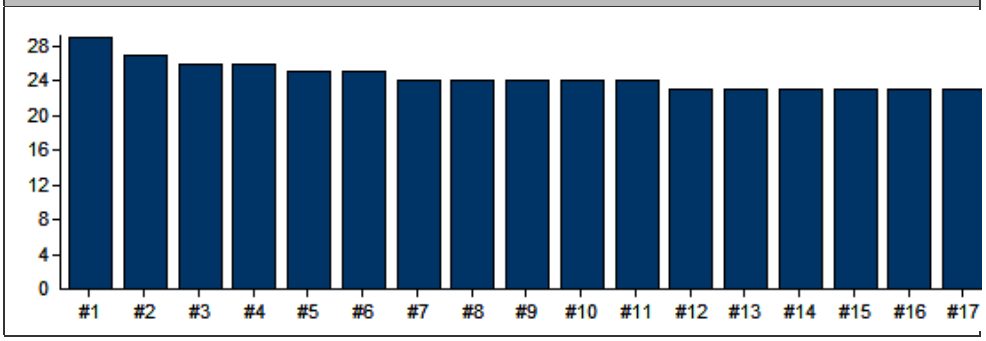
7/1/2014 - Report created by version 5.19.10.2787

TOP 20 RUNNING SERVICES

The following is an overview of the top 20 running services on your network.

Rank	Name	Description	Count
1.	WPDBusEnum		29
2.	lmhosts		27
3.	Browser		26
4.	Dnscache		26
5.	AppIDSvc		25
6.	wudfsvc		25
7.	Dhcp		24
8.	KtmRm		24
9.	RpcSs		24
10.	Schedule		24
11.	SENS		24
12.	AudioEndpointBuilder		23
13.	AudioSrv		23
14.	BFE		23
15.	dot3svc		23
16.	IKEEXT		23
17.	LanmanWorkstation		23
18.	MpsSvc		23
19.	PolicyAgent		23
20.	ProfSvc		23

Top 20 Running Services



Retina Network Security Scanner

Network Vulnerability Assessment & Remediation Management

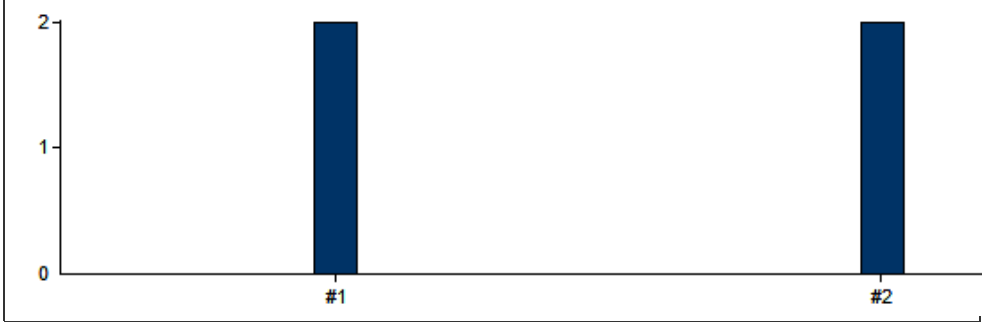
7/1/2014 - Report created by version 5.19.10.2787

TOP 20 OPERATING SYSTEMS

The following is an overview of the top 20 operating systems on your network.

Rank	Operating System Name	Count
1.	Windows Server 2008 R2 (X64), Service Pack 1	2
2.	Windows Server 2008 R2, Service Pack 1	2

Top 20 Operating Systems

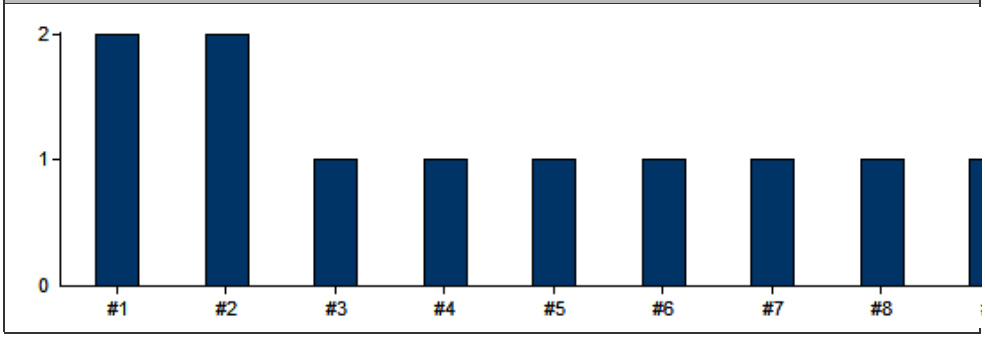


TOP 20 USER ACCOUNTS

The following is an overview of the top 20 user accounts on your network.

Rank	Account Name	Count
1.	Administrator	2
2.	Guest	2
3.	IUSER_RETANON	1
4.	IUSER_RETINA	1
5.	krbtgt	1
6.	samah.hassan	1
7.	user1	1
8.	user2	1
9.	user3	1
10.	user4	1

Top 20 User Accounts

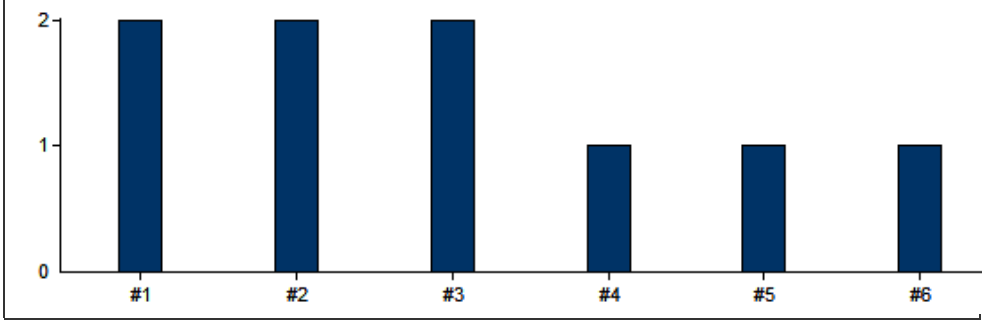


TOP 20 NETWORK SHARES

The following is an overview of the top 20 network shares on your network.

Rank	Share Name	Count
1.	ADMIN$	2
2.	C$	2
3.	IPC$	2
4.	CertEnroll	1
5.	E$	1
6.	NETLOGON	1
7.	SYSVOL	1

Top 20 Network Shares

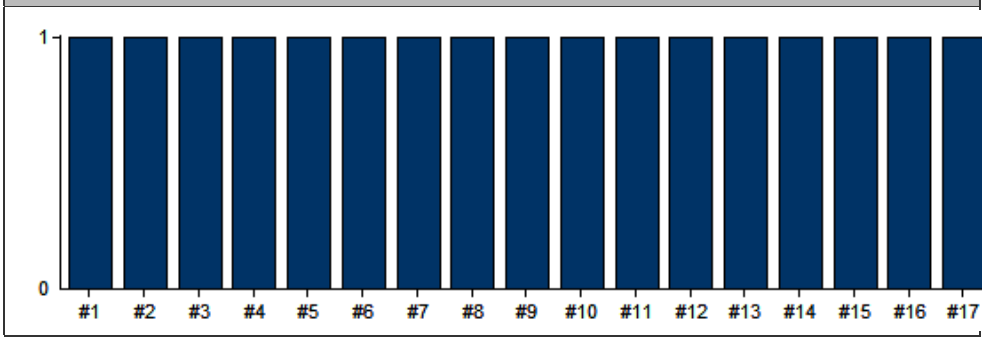


BOTTOM 20 VULNERABILITIES

The following is an overview of the bottom 20 vulnerabilities on your network.

Rank	Vulnerability Name	Count
1.	Microsoft Windows Administrator Group Membership - Vista/2008/7/2008R2	1
2.	Password Does Not Expire	1
3.	DNS Server Enabled - Windows Credentialed	1
4.	IPv6 Protocol Support Detected	1
5.	Adobe Flash Player Multiple Vulnerabilities (20140611) - IE	1
6.	SSL Certificate Domain Name Mismatch	1
7.	SSL Certificate Self-Signed	1
8.	Microsoft (SAMR) Protocol Security Bypass (2934418) - 2923392 - V/2K8 - AD/ADLDS	1
9.	Microsoft .NET and Silverlight Remote Code Execution (2861561) - KB2833957	1
10.	Microsoft .NET and Silverlight Remote Code Execution (2861561) - KB2835393	1
11.	Microsoft .NET and Silverlight Remote Code Execution (2861561) - KB2840628	1
12.	Microsoft .NET and Silverlight Remote Code Execution (2861561) - KB2840642	1
13.	Microsoft .NET Framework 4.0 x64 JIT Compiler Code Execution (2160841)	1
14.	Microsoft .NET Framework Code Execution (2484015) - 4.0	1
15.	Microsoft .NET Framework Information Disclosure (2567951) - 4.0	1
16.	Microsoft .NET Framework JIT Remote Code Execution (2538814) - 4.0	1
17.	Microsoft .NET Framework Multiple Vulnerabilities (2693777) - 4.0 - KB2604121	1
18.	Microsoft .NET Framework Multiple Vulnerabilities (2745030) - 4.0 - KB2729449	1
19.	Microsoft .NET Framework Multiple Vulnerabilities (2745030) - 4.0 - KB2737019	1
20.	Microsoft .NET Framework Multiple Vulnerabilities (2769324) - 4.0	1

Bottom 20 Vulnerabilities



Retina Network Security Scanner

Network Vulnerability Assessment & Remediation Management

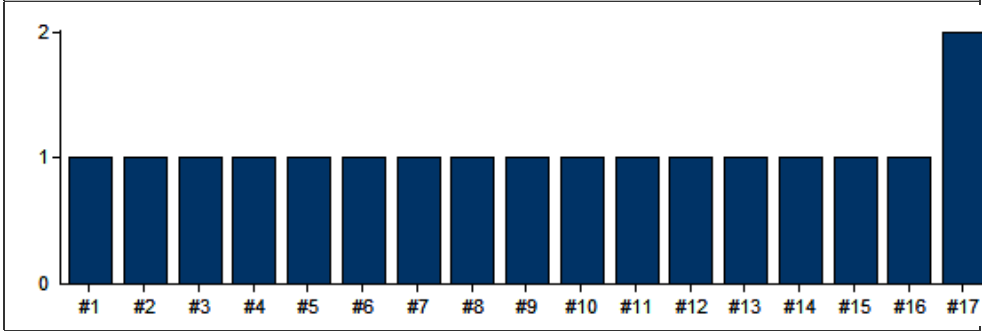
7/1/2014 - Report created by version 5.19.10.2787

BOTTOM 20 OPEN PORTS

The following is an overview of the bottom 20 open ports on your network.

Rank	Port Number	Description	Count
1.	TCP:464	KPASSWD - kpasswd	1
2.	TCP:593	HTTP-RPC-EPMAP - HTTP RPC Ep Map	1
3.	TCP:2012	TTYINFO -	1
4.	TCP:2014	TROFF -	1
5.	TCP:3268	Microsoft Global Catalog	1
6.	TCP:3269	Microsoft Global Catalog with LDAP/SSL	1
7.	TCP:9090	ZEUS-ADMIN - Zeus Admin Server	1
8.	TCP:9875	Portal of Doom	1
9.	TCP:10080	AMANDA - Amanda Backup Util	1
10.	TCP:10443		1
11.	TCP:32000	Generic - Shared service port	1
12.	UDP:9	DISCARD - Discard	1
13.	UDP:88	KERBEROS - Kerberos	1
14.	UDP:138	NETBIOS-DGM - NETBIOS Datagram Service	1
15.	UDP:389	LDAP - Lightweight Directory Access Protocol	1
16.	UDP:500	ISAKMP -	1
17.	TCP:7	ECHO - Echo	2
18.	TCP:9	DISCARD - Discard	2
19.	TCP:13	DAYTIME - Daytime	2
20.	TCP:17	QOTD - Quote of the Day	2

Bottom 20 Open Ports



Retina Network Security Scanner

Network Vulnerability Assessment & Remediation Management

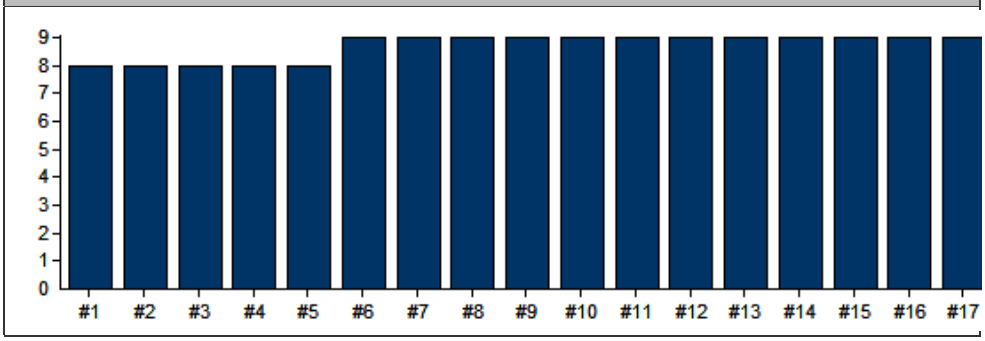
7/1/2014 - Report created by version 5.19.10.2787

BOTTOM 20 RUNNING SERVICES

The following is an overview of the bottom 20 running services on your network.

Rank	Name	Description	Count
1.	aspnet_state		8
2.	CertSvc		8
3.	eEyeUpdateSvc		8
4.	Retina.VMware.ManagementService		8
5.	vspherewebclientsvc		8
6.	AdobeFlashPlayerUpdateSvc		9
7.	DHCPServer		9
8.	DNS		9
9.	eeyeevnt		9
10.	eEyeUpdateSchedulerSvc		9
11.	MSSQL$VIM_SQLEXP		9
12.	MSSQLServerADHelper100		9
13.	RetinaEngine		9
14.	SQLBrowser		9
15.	SQLWriter		9
16.	vCOConfiguration		9
17.	vimPBSM		9
18.	vimQueryService		9
19.	VMwareKdcService		9
20.	vmwarelogbrowser		9

Bottom 20 Running Services



Retina Network Security Scanner

Network Vulnerability Assessment & Remediation Management

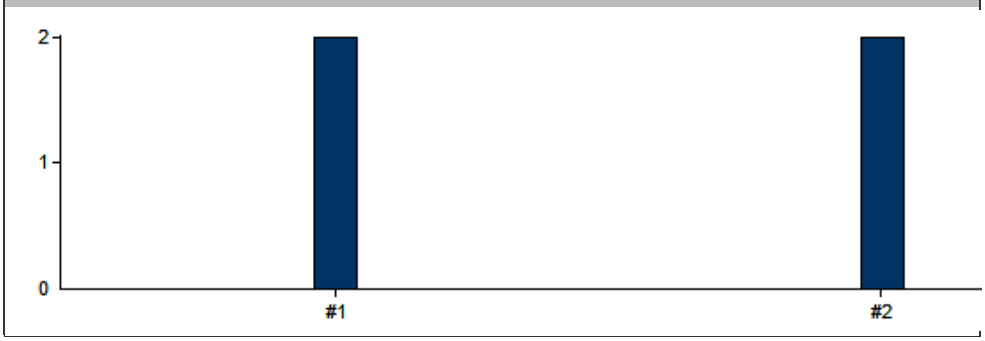
7/1/2014 - Report created by version 5.19.10.2787

BOTTOM 20 OPERATING SYSTEMS

The following is an overview of the bottom 20 operating systems on your network.

Rank	Operating System Name	Count
1.	Windows Server 2008 R2 (X64), Service Pack 1	2
2.	Windows Server 2008 R2, Service Pack 1	2

Botom 20 Operating Systems

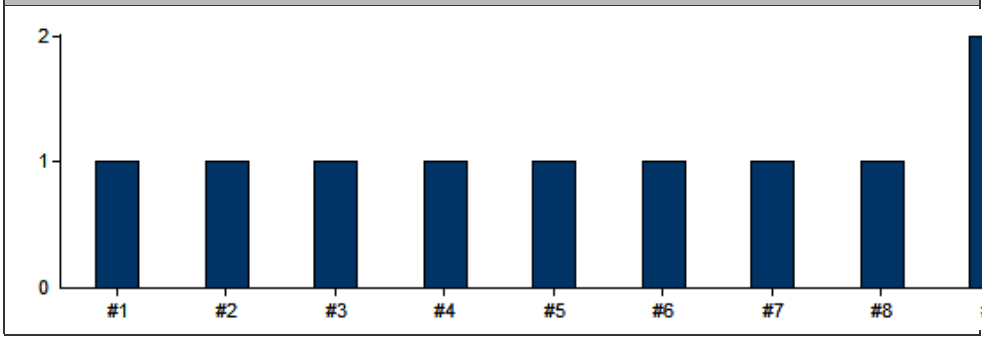


BOTTOM 20 USER ACCOUNTS

The following is an overview of the bottom 20 user accounts on your network.

Rank	Account Name	Count
1.	IUSER_RETANON	1
2.	IUSER_RETINA	1
3.	krbtgt	1
4.	samah.hassan	1
5.	user1	1
6.	user2	1
7.	user3	1
8.	user4	1
9.	Administrator	2
10.	Guest	2

Bottom 20 User Accounts

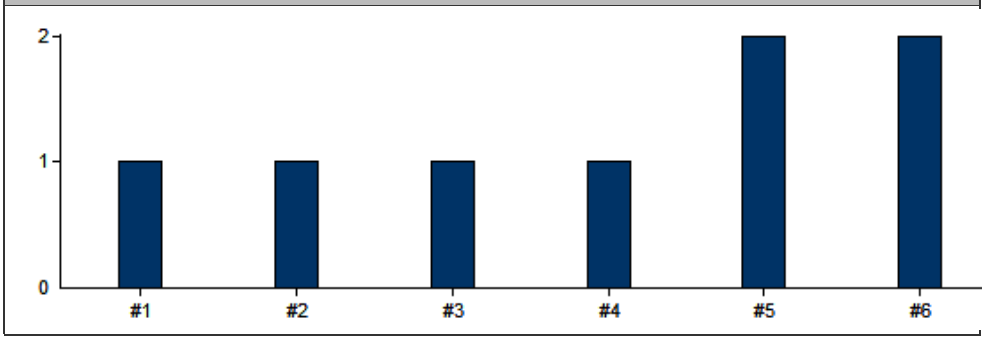


BOTTOM 20 NETWORK SHARES

The following is an overview of the bottom 20 network shares on your network.

Rank	Share Name	Count
1.	CertEnroll	1
2.	E$	1
3.	NETLOGON	1
4.	SYSVOL	1
5.	ADMIN$	2
6.	C$	2
7.	IPC$	2

Bottom 20 Network Shares



GLOSSARY

The following is glossary of common terms used throughout this report.

- **DoS Attack:** A Denial of Service (DoS) attack is a remote attack against a servers TCP/IP stack or services. DoS attacks can saturate a servers bandwidth, saturate all available connections for a particular service, or even crash a server.
- **Exploit:** A script or program that takes advantage of vulnerabilities in services or programs to allow an attacker to gain unauthorized or elevated system access.
- **Host:** A node on a network. Usually refers to a computer or device on a network which both initiates and accepts network connections.
- **IP Address:** The 32-bit address defined by the Internet Protocol in STD 5, RFC 791. It is usually represented in dotted decimal notation. Any device connected to the Internet that used TCP/IP is assigned an IP Address. An IP Address can be likened to a home address in that no two are alike.
- **Netbios:** Network Basic Input Output System. The standard interface to networks on IBM PC and compatible networks.
- **Ping:** A program used to test reachability of destination nodes by sending them an ICMP echo request and waiting for a reply.
- **Port:** A port in the network sense is the pathway that a computer uses to transmit and receive data. As an example, Web Servers typically listen for requests on port 80.
- **Registry:** The internal system configuration that a user can customize to alter his computing environment on the Microsoft Windows Platform. The registry is organized in a hierarchical structure of subtrees and their respective keys, subkeys, and values that apply to those keys and subkeys
- **Risk Level - Info:** Retina may provide additional information about a host that does not necessarily represent a security threat, but may be useful to the administrator in order to better assess the security of the host, or the network at large. These alerts are displayed with the list of discovered vulnerabilities, and are indicated by a green 'I' icon.
- **Risk Level - Low:** A low-risk vulnerability is typically one that only presents a threat in specific and unlikely circumstances. Such vulnerability may provide an attacker with information that could be combined with other, higher-risk vulnerabilities, in order to compromise the host or its users.

- **Risk Level - Medium:** Medium-risk vulnerabilities are serious security threats that would allow a trusted but non-privileged user to assume complete control of a host, or would permit an untrusted user to disrupt service or gain access to sensitive information.

- **Risk Level - High:** A vulnerability is designated as high-risk if it would allow a user who has not been given any amount of trust on a susceptible host to take control of it. Other vulnerabilities that severely impact the overall safety and usability of the network may also be designated as high-risk.

- **Service:** A service is a program running on a remote machine that in one way or another provides a service to users. For example, when you visit a website the remote server displays a web page via its web server service.

- **Share:** A folder, set of files, or even a hard drive partition set up on a machine to allow access to other users. Shares are frequently set up with incorrect file permissions which could allow an attacker to gain access to this data.

- **Sniffer:** frequently attackers will place a sniffer program on a compromised machine. The sole purpose of a sniffer is to collect data being transmitted on the network in clear-text including usernames and passwords.

- **Subnet:** A portion of a network, which may be a physically independent network segment, which shares a network address with other portions of the network and is distinguished by a subnet number.

- **Vulnerability:** A weakness or a flaw in a program or service that can allow an attacker to gain unauthorized or elevated system access.