NATIONAL UNIVERSITY OF RWANDA

FACULTY OF APPLIED SCIENCES

MSc IN ICT

OPTION: COMPUTER SCIENCE

NETWORK SECURITY ANALYSIS USING BAYESIAN ATTACK GRAPHS

Research submitted in partial fulfillment of the requirement for the award of Master's Degree in ICT

Presented by **Jean Luc MINEGA**

Supervisor: Dr Felix K. AKORLI

Huye, July 2013

DECLARATION

I declare that, this project work entitled, “Network Security analysis Using Bayesian Attack Graphs” is original and has never been submitted to any University of other Institution of Higher Learning.

It is my own research whereby other scholar’s writings were cited and references provided.

I thus declare this work is mine and was completed successfully under the supervision of

Dr Felix AKORLI

Jean Luc MINEGA.

ACKNOWLEDGEMENT

Our sincere thanks go first to the almighty God for his help and guidance; I also acknowledge with gratitude the contributions of Dr Felix Akorli for having accepted to supervise this thesis despite his enormous responsibilities.

I am also very grateful to our parents, relatives, different families and friends for their valuable support out the years of our education.

We would not forget to appreciate the company and friendship from all members of New Generation Rwanda and my classmates.

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

In this research, we study and analyse the National University of Rwanda (NUR) Network based on Vulnerability found there. A review on Bayesian Networks contributes to analyze and quantify information security risks caused by various threat sources on the network. We utilize existing network in attack graphs and individual vulnerability metrics, such as CVSS, and apply probabilistic reasoning to produce a sound risk measurement. The NUR network has many host interconnections and network privileges could be gained in many ways. This factor leads to cycles in an attack graph, which must be identified and properly treated when measuring risk to prevent distortion of the results. By using NESSUS for simulation, we analyze different parameters for the vulnerability of the system and the attack graphs path were being done, considering different servers and the risk of attacks. This research identifies and describes security problems in the NUR Network that may lead to different types of attacks. Such security problems include flooding attacks, security vulnerabilities in parser implementations, and attacks exploiting vulnerabilities at the signaling application level. A qualitative analysis of these security flaws and their impacts on NUR network is presented.

CHAPTER 1: GENERAL INTRODUCTION

As recent explosive usage of Information and Communication (ICT), the implementation of the Internet facilities in particular is seen as a competitive advantage in the communication between people and the centralization of data across the world. Computers are connected to network equipments to access the Local Area Network or the Internet and offer various services to customers on demand.

Most networks in use today are far from the system administrators to effectively ensure the security and the integrity of services and data of their elements. It is therefore important for system administrators to analyze, inspect and monitor any risk of intrusion or attack of their systems.

Information security means protecting information systems from unauthorized access, use, disclosure, disruption, modification, or destruction [1]. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information.

Defending against an insider who attempts to misuse his access privileges is one of the most significant problems facing network security. An authorized insider can violate a system security policy for several reasons and in a multitude of ways but not all violations are true threats [2].

To carry out enterprise security analysis, graphical models capturing relationships among vulnerabilities and exploits have become the main- stream approach [3]. An attack graph illustrates possible multi–stage attacks in an enterprise network, typically by presenting the logical causality relations among multiple privileges and configuration settings. Such logical relations are deterministic: the bad things will certainly happen in their worst forms as long as all the prerequisites are satisfied, and no bad things will happen if such conditions do not hold. While it is important t o understand such logical relations, the deterministic nature has limited their use in practical network defense, especially when the graphical models are to be used in real-time intrusion response [4].

1.1 Purpose

The purpose of this research is to analyze the National University of Rwanda (NUR) network in term of Network Security using Bayesian Network (BN). The NUR network is the first computer network in the Rwanda in term of number of users, network equipments and network services.

Due to his complexity, some vulnerability across the network has been reported. The BN will facilitates to establish the risk Analysis using attack graphs and the graphic representation of the joint probability distribution function over a set of variables.

1.2 Objective of Thesis

The goal of this study is to analyze network security vulnerability using BN which will contribute to understand the properties of its behavior and its usability to help the identification of possible attacks NUR may face. To emphasize the need for good security management, its aims are to identify the problems associated with security management and to show how NUR can solve those problems by:

- Analyze security risks which imply vulnerability at NUR network.
- Analyze the security architecture of NUR network.
- Dynamic Bayesian Network (DBN) - based model to incorporate relevant temporal factors, such as the availability of exploit codes or patches, into attack graph-based security metrics.

1.3 Research questions

RQ1.How can a complex network model be reduced into a simple one for analysis in terms of vulnerability?
RQ2.How does the Bayesian Network-based attack graph contribute to analyze the network security?
RQ3.What is the appropriate probabilistic graphical model for network security?

1.4 Organization of the work

This thesis is divided and organized as follows:

- The first chapter deals with introduction.
- The second chapter gives the background of the study, network security, Bayesian theorem and Bayesian Network.
- The third chapter describes different methodologies used to accomplish this research.
- The fourth chapter describes the results and analyses data collected in this research.
- The lastly, the sixth chapter gives a conclusion and answers to research questions and gives some recommendations for further improvement.

CHAPTER 2: Network Security Overview and Bayesian network

The terms information security and computer security are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information. However, there are some subtle differences between them [5]. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms [6].

Computer systems use multiple levels of software to abstract the complex operations of the computer such as video output, keyboard input, network and hard drive access. These hardware abstractions are managed by the software in the Operating System (OS). The OS uses hardware drivers to control the various hardware components. The OS also has Application Programming Interface (API) that other software applications use to access the hardware.

The OS offers the layers of security. Even if the OS can be secure, if an attacker has gained access to the OS, he can then take control of the application where the OS is trying to secure. The network security is a continuous process that needs vigilant people.

The growing of the network environment in Rwanda emerge new challenges It is possible to eliminate some of these vulnerabilities by modifying the software, or through other configurations or restrictions to limit access to unauthorized users or applications. Every computer system relies on hundreds of applications, components, libraries, drivers, files and configurations. All of which can become a target once a vulnerability is found. New methods of attacking a computer system are being created each day, and as new vulnerabilities are being discovered in existing software systems. Even when software systems are modified to eliminate a known vulnerability, the modifications can potentially introduce new vulnerabilities. Thus the never ending search for security will continue. Computer with vulnerabilities to a network attack can be exploited by any computer with access to the network. Protecting the system from network attacks becomes important. Some methods used to protect computer systems from network- based attacks include: limiting the number and type of network services being provided, restricting access to specific computers and services with a firewall, restricting access to specific user accounts, keeping OS and network software patched and updated. These restrictions can help protect a computer system on the network, but at the cost of limiting operations to a defined set of trusted users and network systems. In addition, there may be new vulnerabilities that will be discovered. There may be new applications that are not yet installed that can introduce new types of vulnerabilities and may not be compatible with this restrictive firewall solution. Once an

attacker accesses the network beyond the firewall, the protection it provided can be reduced to null.

2.1 Threats, Vulnerabilities, and Attacks

Before starting this section, it is required to review TCP/IP basics and the seven-layer OSI model because, many of the attacks operated takes advantage of some of the vulnerabilities from the TCP/IP protocol suite.

a. **Protocols**

A protocol is a rule or a set of rules and standards for communicating that computers use when they send data back and forth. Both the sender and receiver involved in data transfer must recognize and observe the same protocols. To exchange data, the sending and the receiving computers, also called hosts, must agree on what the data will look like. When one host is sending another host a whole bunch of 1s and 0s, both hosts have to agree on the meaning and placement of each 1 and each 0. Part of the information that is sent represents addresses and part is data—each host has a unique address, just as you have a unique address on your street. And just like a letter being delivered to your address, data is delivered to the appropriate host based on its address. The hosts that send the information must understand how to find the correct address among the data so that the data can be routed to its destination. When hosts begin communicating with each other, they first must agree on what protocols to use. This is similar to two people who are going to have a conversation: They have to agree on which language to use and what the rules for the conversation will be. They must agree on who will talk first, how to address the other, how to acknowledge that the information is understood, and how to finish or close the conversation [7]

b. The OSI Reference Model

The OSI reference model is a seven-layer model that was developed by the International Standards Organization (ISO) in 1978. The OSI model is a framework for international standards that can be used for implementing heterogeneous computer network architecture. The OSI architecture is split into seven layers from top to bottom [8].

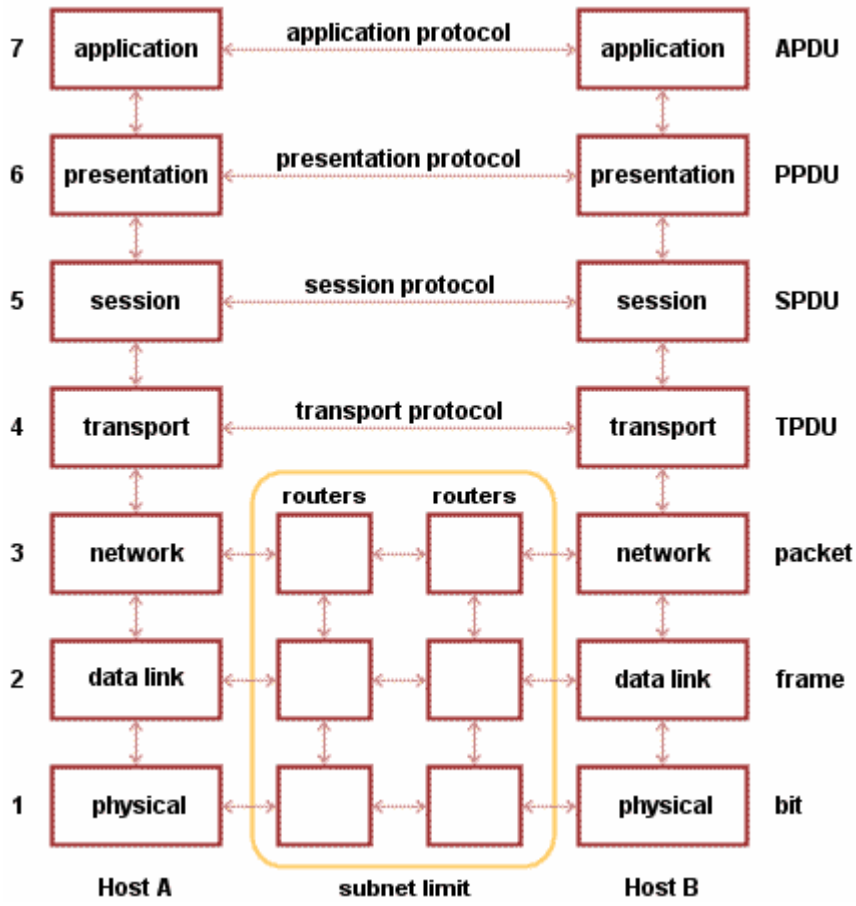

Figure 1: OSI model

Reference: Fundamentals of Network Security, John E. Canavan, Artech House, Boston

The physical layer addresses the physical link and is concerned with the signal voltage, bit rate, and duration. The data link layer is concerned with the reliable transmission of data across a physical link. In other words, getting a signal from one end of a wire to the other end. It handles flow control and error correction. The network layer handles the routing of data and ensures that data is forwarded to the right destination. The transport layer provides end-to-end control and constructs the packets into which the data is placed to be transmitted or "transported" across the logical circuit. The session layer handles the session set-up with another network node. It handles the initial handshake and negotiates the flow of information and termination of connections between nodes. The presentation layer handles the conversion of data from the session layer, so that it can be "presented" to the application layer in a format that the application layer can understand. The application layer is the end-user interface. This includes interfaces such as browsers, virtual terminals, and FTP programs. [9].

c. **TCP/IP**

Transport control protocol is a suite of protocols that can be used to connect dissimilar brands of computers and network devices. The largest TCP/IP network is the Internet. The Internet was developed by the U.S. DOD under the auspices of the Defense Advanced Research Project Agency (DARPA) when DOD scientists were faced with the problem of linking thousands of computers running different operating systems. The Defense Advanced Research Project Agency (DARPA) is a small organization within the Pentagon, but its impact on technology in general and on data communications in particular has been huge. For all practical purposes, DARPA's programs and funding created the Internet. You can think of the TCP/IP suite as the lifeblood of the Internet. The TCP/IP suite has become widely adopted, because it is an open protocol standard that can be implemented on any platform regardless of the manufacturer. In addition, it is independent of any physical network hardware. TCP/IP can be implemented on Ethernet, X.25, and token ring, among other platforms [10].

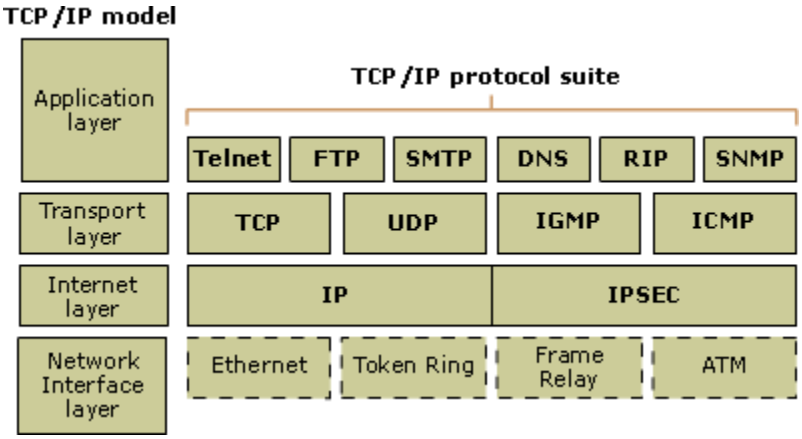

Figure 2: TCP/IP model

Reference: Fundamentals of Network Security, John E. Canavan, Artech House, Boston

2.2.1 Threats

A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system. This can take any form and can be malevolent, accidental, or simply an act of nature. [11].

2.2.1.1 Physical threats

a. Physical attacks against systems

Sometimes, the most apparent attack paths get ignored in favor of what is "in vogue." In a lot of ways, that is what is happening in the information security world. Certainly, cyber attacks and hackers and worms are very real threats. But we can't ignore those attacks that are targeted against physical computing infrastructure and so must factor in other threats to these assets. One example of this kind of threat is apparent with today's multinational corporations. Information security professionals may disregard the threat of physical attacks when attempting to thwart the hack attack coming from the other side of the world, but entities with facilities in countries with diverse geopolitical ideas may have a serious physical threat from employees who can tap networks or steal hard drives. [12]

b. Physical attacks detected by systems

The power of software is in its ability to consistently process large amounts of data and identify nuggets of information in an efficient and effective manner. The challenge of physical threat monitoring is always in identifying an attack before it occurs, or determining the likelihood of a problem in advance. Applying the power of software creates an opportunity to more effectively protect a company. A monitoring system can identify that something is wrong. A physical threat monitoring system that has links to the software can do more. It can identify the same problem and then provide information about the cause of that failure: temperature, air flow, or water existence in the physical facility. The decisive benefit comes from the existence of a secure camera in the room that can send images back through the wires to an operations console. [13]

2.2.1.2 Threats to Networks

Network security threats can be divided into 2 groups: external versus internal and unstructured versus structured threats.

2.2.1.2.1 Internal threats

Most of the time, internal threats are from the administrators of the system. According the Computer Security Institute (CSI) study has found that, of the 70 percent of the companies that had security breaches, 60 percent of these breaches come from internal sources. Some of these securities breaches were malicious in intent; others were accidental.

2.2.1.2.2 External threats

External threats can occurred from externals partners: individuals or organizations that do not have authorized access to the network indeed. The partners access the network through Internet or dialup access servers. The external threats can be either amateurish or from an expert people.

2.2.1.3 Unstructured threats

Unstructured threats are from an amator IT and don't target a specific host, network or organization. A good security solution easily should thwart this kind of attack. Many tools accessible on the Internet can be used to discover weaknesses in a company's network.

2.2.1.4 Structured threats

Structured threats occurred in the effort to gain access a specific target. These threats can be the result from individuals or a group with the purpose to commit fraud, destroy or alter records, or simply to create destruction.

2.2.2 Vulnerability

Vulnerability is an inherent weakness in the design, configuration, implementation, or management of a network or system that renders it susceptible to a threat. Vulnerabilities are what make networks susceptible to information loss and downtime. Every network and system has some kind of vulnerability [14]. There are four primary causes for network security threats:

2.2.2.1 Technological Weaknesses

Computer and network technologies have basic security weaknesses in the following areas:

- TCP/IP
- Operating System
- Network equipments like switches, routers, firewalls etc...

2.2.2.2 Configuration Weaknesses

Many security problems are often caused by the following configuration weaknesses:

- Unsecured accounts

- System accounts with weak passwords
- Misconfigured Internet services
- Misconfigured network equipments

2.2.2.3 Security Policy Weaknesses

Security problems can be caused by security policy weaknesses:

- Lack of a written security policy
- Politics – politics clash and staff conflicts
- Frequent replacement of personnel
- Software and hardware installation/changes do not follow policy
- Lack of Disaster recovery plan

2.2.2.4 Human Error

Human/user error is a large cause of breaches of network security. If staff tells confidential information to friends, family or other coworkers, security has been breached. Unauthorized access to networks can be gained in many different ways:

- Accident
- Ignorance
- Workload
- Dishonesty

The common methods of attacks are:

- Reconnaissance: Discovering information about the intended target
- Vulnerabilities Analysis: Identifying potential ways of attacks
- Exploitation: Attempting to compromise the system by employing the vulnerabilities found through the vulnerabilities analysis.

2.3.1 Classification of network attacks

An attack is a specific technique used to exploit network vulnerabilities. Generally, network attacks can be categories into two groups: active or passive.

2.3.1.1 Active Attacks

This type of attack requires the attacker to be able to transmit data to one or both of the parties, or block the data stream in one or both directions. It is also possible that the attacker is located between the communicating parties. In this case the attacker can stop all or parts of the data sent by the communicating parties. This attacker can try to take the place of the client or server when the authentication procedure has been performed. Without integrity checks of the received data, the server will not detect that the origin of the data is not the authenticated person [15].

2.3.1.2 Passive Attacks

A passive attack is an attack where an unauthorized attacker monitors or listens in on the communication between two parties, in which the malicious nodes do not transmit in the network, but can receive packets transmitted between legitimate nodes. A malicious node can successfully receive a packet from a transmitter if it is within the transmitter's transmission [16]

2.3.2 Types of Attacks

The types of attacks of attacks found here are five:

2.3.2.1 Network Enumeration or Reconnaissance

Before gaining access to a network, we should know the topology of the network first. Every piece of information helps to obtain the structure of target network; we specifically scan the target network to obtain a list of hosts and to map the target network to understand its architecture and what kind of traffic (TCP, UDP, and IPX) is allowed. The goal of scanning the target network is to start with no information and gather as much data as possible about the target network and systems. The information collected helps to identify potential exploits.

Network enumeration is the process of discovering the information over the traffic. This process is performed largely over the Internet using readily available software and publicly accessible repositories of information. Most of the information obtained in this step is freely available and legal to obtain. However, many companies control who tries to get this information since it may indicate an imminent to an attack. [17]

Reconnaissance attacks can consist of the followings:

- Internet information queries
- Ping sweeps
- Port scans
- Packet sniffing

2.3.2.1.1 Internet information queries

Internet information means to determine IP addresses and all the details of any organization, corporation, firms or entities. Free Internet tools or commands such as the nslookup, ipconfig and whois utilities are used to easily determine the IP address and all the details assigned to a given corporation or entity. Once Internet Information is identified, the intruder uses ping sweeps methods – ping (fping, gping) to determine active IP addresses.

2.3.2.1.2 Ping sweeps

Ping sweeps is intended to discover whether specific Internet Protocol addresses in the network are associated with active computers. Legitimate network management technique can be part of network discovery. To control the usage of address space allocations, the address registries that allocate the addresses may scan organizations to see if they are using all their space. A scarce resource with IPV4.

Once the IP addresses are discovered, the intruder used a port scans to determine which network services or ports are active on the network.

2.3.2.1.3 Port scans

Applications using TCP and UDP are assigned port numbers by IANA in the TCP and UDP packet headers. Certain ports are well known and pre-assigned to common protocols, as listed in the table below (IETF RFC 1700, 1994). Some examples: Web servers listen for HTTP requests on TCP port 80. The other ports may be used dynamically as needed.

Port	Description
TCP 20	FTP data
TCP 21	FTP control
TCP 23	Telnet
TCP 25	Simple Mail Transfer Protocol
TCP 53	Domain Name System
TCP 80	HTTP
UDP 161	Simple Network Management Protocol
TCP 179	Border Gateway Protocol

Figure 3: Some well known ports

An attacker is almost always interested to know which ports are open or services are active on a potential target. An open port means that the target will be listening on that port. Scanning is often targeted to the vulnerabilities of a specific service. However, probing every possible port manually would be very tedious. A port scanner is a tool for sending probes to a set of specific ports to see which ports is open.

2.3.2.1.4 Packet sniffing

Sniffing is a passive attack that attempts to exposes the confidentiality of data. It might be considered part of reconnaissance (example: sniffing to learn passwords) prefacing an attack but can just as well be argued to be an attack to gain access to information.

Sniffers traditionally used by network administrators for traffic monitoring and LAN troubleshooting have also been one of the most commonly used attack tools over the years. On a LAN, every host sees the entire traffic broadcast on the LAN medium, but normally ignore the packets that are addressed to other hosts. A sniffer program puts the network interface of a host into promiscuous mode to capture all packets seen on the LAN medium. Thus, the sniffer can eavesdrop on everything transmitted on the LAN including user names, passwords, DNS queries, e-mail messages, and all types of personal data.

Two common uses of sniffing are:

- Information gathering: network intruders can identify usernames and password or all information carried in a packet.
- Information theft: can occur as data is transmitted over the internal or external network.

2.3.2.2 Hacking

A Hacking or access attack is the ability for an intruder to gain access to a device for which the intruder does not have an account or a password. Entering or accessing systems usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked. Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information.

2.3.2.3 Spoofing Attacks

Spoofing is a method of attacking a network in order to gain unauthorized access. In a spoofing attack, the intruder sends messages to a computer indicating that the message has come from a trusted system. To be successful, the intruder must first determine the IP address of a trusted system and then modify the packet headers to that it appears that the packets are coming from the trusted system. In essence, the attacker is fooling (spoofing) the distant computer into believing that they are a legitimate members of the network. The goal of the attack is to establish a connection that will allow the attacker to gain root access to the host, allowing the creation of a backdoor entry path into the target system.

There are mainly FOUR types of Spoofing Attacks. They are:

- IP Address Spoofing
- ARP Poisoning
- WEB Spoofing
- DNS Spoofing

2.3.2.4 Dos/DDoS Attacks

A Denial-of-Service (DoS) attack is designed to hinder or stop the normal functioning of a web site, server or other network resource. There are various ways for hackers to achieve this. One common method is to flood a server by sending it more requests than it is able to handle. This will make the server run slower than usual (and web pages will take much longer to open), and may crash the server completely (causing all websites on the server to go down). Denial of service (DoS) is when an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users.

DoS attacks involve either crashing the system or slowing it down to the point that it is unusable. But DoS can also be as simple as deleting or corrupting information. In most cases, performing the attack involves simply running a hack or script. For these reasons, DoS attacks are the most feared.

It is important to note the difference between a DDoS and DoS attack. If an attacker mounts an attack from a single host it would be classified as a DoS attack. In fact, any attack against availability would be classed as a Denial of Service attack. On the other hand, if an attacker uses a thousand systems to simultaneously launch smurf attacks against a remote host, this would be classified as a DDoS attack.

A DoS attack can be perpetrated in a number of ways. The five basic types of attack are:

1. Consumption of computational resources, such as bandwidth, disk space, or processor time
2. Disruption of configuration information, such as routing information.
3. Disruption of state information, such as unsolicited resetting of TCP sessions.
4. Disruption of physical network components.
5. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

2.3.2.5 Malicious Code (Malware) Attacks

The primary vulnerabilities for end-user workstations are malicious code attacks.

Malware, short for malicious software - is a special kind of software program or file deliberately designed to perform an unauthorized and often harmful action in a computer system. Malware includes viruses, worms, torjan horses, crimeware, adware, spyware etc... It was once sufficient to call something a 'virus' or 'trojan horse', but infection methods and vectors evolved and the terms virus and trojan no longer provided a satisfactory definition for all the types of rogue programs that exist.

Malicious software can be inserted onto a host to damage or corrupt a system, replicate itself, or deny access to networks, systems, or services.

2.4 Social engineering

Social Engineering is the act of tricking computer users into performing actions or revealing private and confidential information, e.g. passwords, email addresses, etc, by exploiting the natural tendency of a person to trust and/or by exploiting a person's emotional response. Phishing, Scamming, Spamming are some techniques used for Social Engineering.

• Phishing

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to attract the unsuspecting public. Phishing is typically carried out by e-mail or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

• Masquerading (Identity Theft)

Masquerading is the malicious theft and consequent misuse of someone else’s identity to commit a crime. Identity theft often involves cracking into a system to obtain personal information, such as credit card numbers, birth dates, and social insurance or social security numbers of targets and then using this

information in an illegal manner, such as buying items with the stolen identity or pretending to be someone else of higher professional status in order to gain special privileges. Identity theft is one of the fastest-growing crimes around the globe.

• Scamming

Scamming is the process of defrauding a person or group by gaining their confidence using some fraudulent tricks/game/scheme. Confidence men exploit human characteristics such as greed and dishonesty, and have victimized individuals from all walks of life.

• ***Spamming***

Spamming is the act of sending a message or advertisement to a large number of people who did not request the information, or to repeatedly send the same message to a single person.

Spam is the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. Spam is an unspecified, unsolicited (unwanted) bulk email like the physical junk mail delivered through the post. It is sent out in mass quantities by spammers who make money from the small percentage of recipients that actually respond. Spam is also used for phishing and to spread malicious code.

2.5 Bayesian Network

2.5.1 Bayesian Theorem

Bayesian probabilities began with the English mathematician Reverend Thomas Bayes whose discovery of the theorem that now bears his name was published posthumously. Bayes' Theorem is simply a manner to calculate probability of one event occurring based on whether another event has occurred. Suppose that both *A* and *B* are events, and that *P*(*A*) and *P*(*B*) represent the probability that events *A* and *B* occurred respectively. Then Bayes' Theorem is as follows:

Figure 4: Hypothesis and evidence

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \qquad (2.1)$$

where:

***P*(A|B)** is the posterior probability that the hypothesis is true

***P*(B|A)** is the prior knowledge

The formula (1) above summarizes the Bayesian theorem.

Or if the event is in some manner affected by any other events, then its probability distribution is governed by the truth of these events using Bayes' Theorem. The probability distributions that exist before any evidence is added are known as the *priors*. By linking all of the events together that affect each other, a *Bayesian Network*, or a *Belief Network (BN)* is created. When you discover "evidence" about the probability that certain events have occurred, Bayes' Theorem calculates the probability that other events in the network have occurred. In this manner Bayesian Networks calculate probabilities based not only on the priors, but on known evidence as well.

Bayes' Theorem is the only consistent way to modify our beliefs about events given the evidence about what has actually occurred. This highlights one of the strengths of Bayesian probabilities over other statistical methods, the inferences made are based on the actual occurring data, not on all possible data sets that might have occurred but didn't. As a result, once created, Bayesian networks are powerful tools that can be used to make predictions based on the pieces of evidence that are known. One caveat that should be addressed here is that, like all decision making analysis tools, the predictions and conclusions drawn are based on the user input. Therefore, the value of the output is only as reliable as the accuracy of the input. Bayesian Networks are no exception to this.

2.5.2 Bayesian networks

Bayesian networks (BN) also known as Bayesian belief network (BBN), probabilistic network (PN) is a directed acyclic graph (DAG), where each node represents a random variable and is associated with the conditional probability of the node given its parents.

The probability of an event occurring given that another event has already occurred is called a conditional probability. The probabilistic model is described qualitatively by a DAG. The vertices of the graph, which represent variables, are called nodes. The nodes are represented as circles containing the variable name. The connections between the nodes are called arcs, or edges. The edges are drawn as arrows between the nodes, and represent dependence between the variables. Therefore, for any pairs of nodes indicate that one node is the parent of the other so there are no independence assumptions. Independence assumptions are implied in Bayesian networks by the absence of a link.

The BN represents a factorization of a joint distribution [18].

Bayesian network can be described by:

- a directed acyclic graph which is the structure of BN that enables one to reflect dependencies between components of the system in question.
- conditional probability table (CPT) for each node with a positive input degree. CPTs describe the relation between a given node and its parents.

Bayesian Networks have many applications, these include the usage in network security analysis, computational biology, bio-informatics, medical diagnosis, document classification, image processing, image restoration and decision support systems.

As summary the BN can be defined as follow:

- Bayes net is a DAG
- Nodes are random variables
- Link $X \longrightarrow Y$ intuitively means: X has direct influence on Y
- For each node: probability table quantifying effects of parent nodes

There are four main types of reasoning in Bayesian networks [19]:

- causal reasoning ($A \longrightarrow \mathbf{E}$)
- diagnostic reasoning or evidential reasoning ($A \longleftarrow B$)
- inter-causal reasoning
- mixed type reasoning

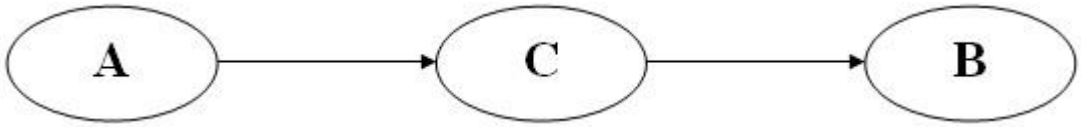

Figure 5: Diagnostic reasoning

The figure 5 shows the diagnostic reasoning with the arrival of clue B one wants to calculate the probability of hypothesis A being true. That means one sees the evidence and looks for most probable causes. Evidential reasoning is deducted from causes and effects phenomena, given an observed phenomenon, one tries to explain it by the presence of other phenomena. Causal reasoning concentrates on deriving

effects from causes, given an observed phenomenon, one is engaged by it to expect the presence of other phenomena, which have the role of its effects.

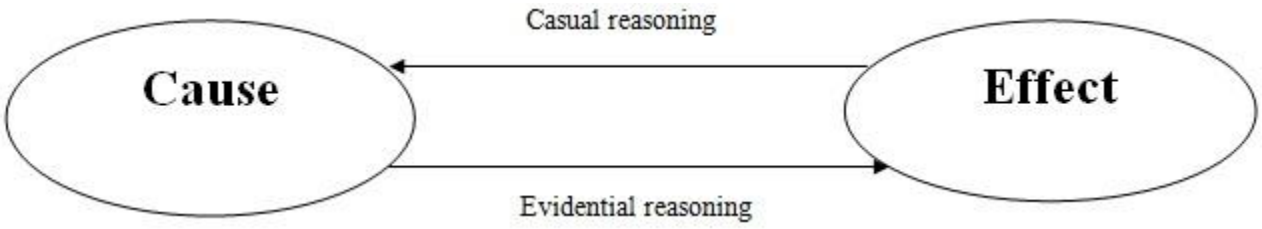

Figure 6: Causal and evidential reasoning

2.5.4 Causal Bayesian networks

A BN becomes a causal model if each of the arrows in the DAG can be given a causal interpretation. Each arrow then represents direct causality. Indirect causality is based on paths that always follow arrows. In many practical applications one can interpret network edges as signifying direct causal influences with the exception of artificial nodes created only to improve calculations and accuracy. One has to remember that causal networks are always Bayesian and BN are not always causal [21]. Only causal networks are capable of updating probabilities based on interventions, as opposed to observations in Bayesian. As it was mentioned earlier causality is represented by arcs in BN [22]. During the construction of such a network one has to be careful not to inverse conditional probabilities (arcs): $P(A|B) \neq P(B|A)$.

2.5.5 Bayesian Network Assumptions

Assumption in Bayesian networks is represented in the form of direct connections between probabilistic variables. The variables need to fix the conditional probability of a given variable and their direct parents. All other relations can be computed based on the simple dependencies.

2.5.5.1 Independence of variables based on graph structure

The independent variables are nodes with no direct connection in a DAG. It means that when there is no direct link between two nodes in BN, variables represented by these two not-connected nodes are independent.

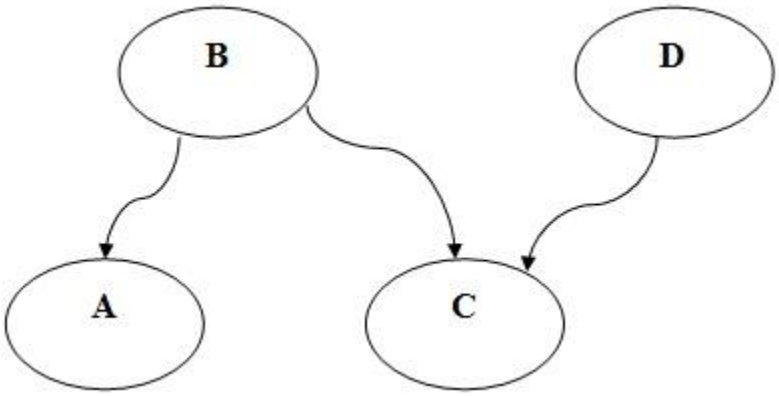

Figure 7: Independent variables

2.5.5.2 Reasoning rules

Suppose a probability of X_1 and X_2 with condition "cond", the reasoning rules are follows:

a. Probability of conjunction: p(X1 ∧ X2 | Cond) = p(X1 | Cond) * p(X2 | X1 ∧ Cond)
b. Probability of a certain event: p(X | Y1 ∧ ... ∧ X ∧ ...) = 1
c. Probability of impossible event: p(X | Y1 ∧ ... ∧ ~X ∧ ...) = 0
d. Probability of negation: p(~X | Cond) = 1 – p(X | Cond) . If condition involves a descendant of X then use Bayes' theorem: If Cond0 = Y ∧ Cond where Y is a descendant of X in BN

   then p(X|Cond0) = p(X|Cond) * p(Y|X∧Cond) / p(Y|Cond)

e. Cases when condition Cond does not involve a descendant of X:

   (a) If X has no parents then p(X|Cond) = p(X), p(X) given

   (b) If X has parents Parents then:

$$p(X \mid Cond) = \sum_{S \in possible\_states(Parent)} p(X \mid S)\, p(S \mid Cond) \qquad (2.2)$$

2.5.6 Bayesian inference

Bayesian inference (BI) uses a prior probability over hypotheses to determine the probability of a particular hypothesis given some observed evidence.

BI extends probability to the areas where one deals with uncertainty not only repeatability. This is possible thanks to Bayesian interpretation of probability, which is distinct from other interpretations of probability as it permits the attribution of probabilities to events that are not random, but simply unknown [23].

During the reasoning process using BI the evidence accumulates and the degree of confidence in a hypothesis ought to change. With enough evidence, the degree of confidence should become either very high or very low. BI uses an estimate of the degree of confidence (the prior probability) in a hypothesis before any evidence has been observed which results in a form of inductive bias. Results will be biased to the a-priori notions which affect prior P(X) node probabilities, CPTs and consequently the whole reasoning process.

2.5.6.1 Inference algorithms

Inference algorithms fall into two main categories:

- exact inference algorithms:
  - based on elimination
  - based on conditioning
- approximation inference algorithms:

Exact algorithms are structure-based and thus exponentially dependant on the network treewidth, which is a graph-theoretic parameter that measures the resemblance of a graph to a tree structure [23]. Approximation algorithms reduce the inference problem to a constrained optimization problem and are generally independent of treewidth. Loopy belief propagation is a common algorithm nowadays for handling graphs with high treewidth [24].

2.5.6.2 Bayesian inference example

This example is based on computer failure diagnostics. There are two possible hardware failures a RAM failure where part of the chip is broken and stores inaccurate data and a CPU failure when the processor overheats and causes the whole system to crash. One can see two possible evidences a Blue Screen of Death (BOD) or a system hang. Each of the causes can result in BOD or hang. The overall structure of the network is presented in figure below.

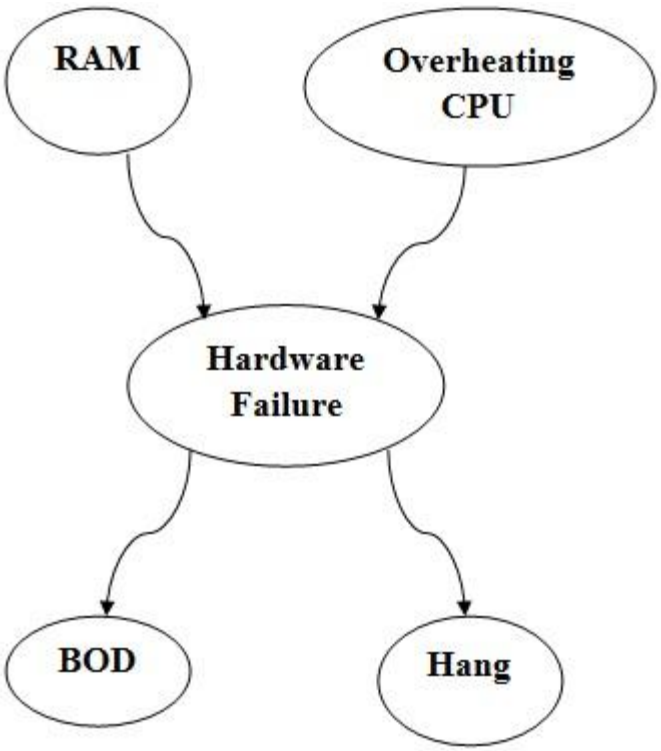

Figure 8: Inference example network

2.5.7 Conditional probability table

The conditional probability table $\mathbf{P_{A|B}}$ describes the probability of B given A.

A	**B**	***P*(A|B)**
Y	Y	0.7
N	Y	0.3
Y	N	0.01
N	N	0.99

Conditional probability table is a right stochastic matrix which means that each row consists of non-negative real numbers and is summing to 1.

2.6 Markov Networks

Markov network are based on undirected graphical models. This model is useful in modeling a variety of phenomena where one cannot naturally ascribe directionality to the interaction between variables. Furthermore, the undirected models also other a different and often simpler perspective on directed models, both in terms of the independence structure and the inference task.

A representation that implements this intuition is that of an undirected graph. As in a Bayesian network, the nodes in the graph of a Markov network graph H represent the variables, and the edges correspond to some notion of direct probabilistic interaction between the neighboring variables.

The remaining question is how to parameterize this undirected graph. The graph structure represents the qualitative properties of the distribution. To represent the distribution, we need to associate the graph structure with a set of parameters, in the same way that conditional probability distribution (CPD) were used to parameterize the directed graph structure. However, the parameterization of Markov networks is not as intuitive as that of Bayesian networks, as the factors do not correspond either to probabilities or to conditional probabilities.

The most general parameterization is a factor:

Let defines D a set of random variables, a factor to be a function from Val(D) to IR^{+}. Let H be a Markov network structure. A distribution $\boldsymbol{P_H}$ factorizes over $\boldsymbol{H}$ if it is associated with:

- a set of subsets $D_1,...,D_m$, where each Di is a complete subgraph of $\boldsymbol{H}$
- factors $\pi_1[D_1],...,\pi_m[D_m]$,

Such as:

Where:

This is an unnormalized measure and

$$Z = \sum_{X_1,\ldots,X_n} \tilde{P}(X_1,\ldots,X_n) \tag{3.1}$$

is a normalizing constant called the partition function. A distribution P that factorizes over ***H*** is also called a Gibbs distribution over ***H***.

Note that this definition is quite similar to the factorization definition for BN, there, to decomposed the distribution as a product of CPDs. In the case of Markov networks, the only constraint on the parameters in the factor is non-negativity.

2.6.1 Independencies in Markov Networks

As in the case of Bayesian networks, the graph structure in a Markov network can be viewed as encoding a set of independence assumptions. Intuitively, in Markov networks, probabilistic influence flows along the undirected paths in the graph, but is blocked if the condition on the intervening nodes. We can define the sets:

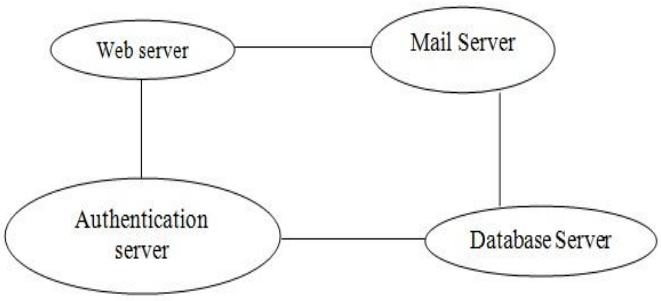

Figure 9: A simple Markov network describing the network services status.

The local Markov properties are associated with each node in the graph and are based on the intuition that we can block all influences on a node by conditioning on its immediate neighbors.

2.6.2 Inference as Optimization

The methods that fall into an optimization framework are based on a simple conceptual principle: define a target class of easy distributions Q, and then search for a particular instance Q within that class which is the best approximation to P_F. Queries can then be answered using inference on Q rather than on P_F. The specific algorithms that have been considered in the literature differ in many details.

However, most of them can be viewed as optimizing a target function for measuring the quality of approximation.

computing the so-called M-projection Q of P_F the argmin $D(P_F|Q)$ is actually equivalent to running inference in PF. Somewhat surprisingly, as show in the subsequent discussion, this does not apply to the so-called I-projection: we can exploit the structure of PF to optimize argmin $D(P_F|P_F)$ efficiently, without running inference in PF.

An additional reason for using relative entropy as our distance measure is based on the following result, which relates the relative entropy $D(Q|P_F)$ with the partition function Z:

(3.2)

2.6.3 Exact Inference as Optimization

Before considering approximate inference methods, the illustration the use of variation approach to derive an exact inference procedure. The concepts we introduce The goal of exact inference here will be to compute marginal of the distribution. To achieve this goal, we will need to make sure that the set of distributions Q is expressive enough to represent the target distribution P_F. Instead of approximating P_F, the solution of the optimization problem transforms the representation of the distribution from a product of factors into a more useful form Q that directly yields the desired marginals

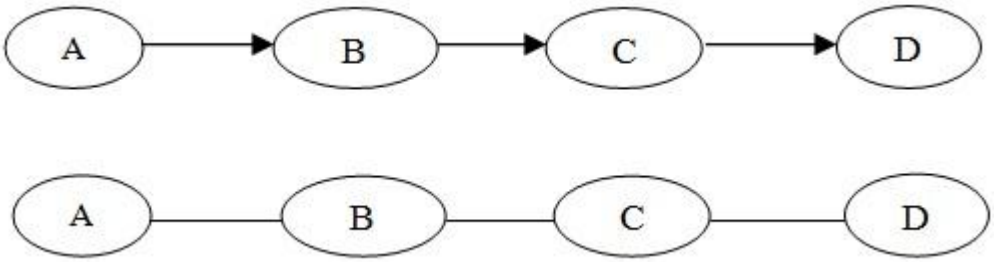

Figure 10: Chain-structured Bayesian network and equivalent Markov network

2.7 RESEARCH METHODOLOGY

2.7.1 Overview

According Arbnor and Bjerke an appropriate methodology is crucial for conducting a good and trustworthy analysis in research. It helps to create high quality in knowledge, make our research reach deeper, clear to the methodological root of knowledge. The research design can reflect our assessment of the nature of knowledge we are planning to generate using this specific approach [25]. Applying this approach in connection with the applied theories attempt to answer and solve the problems cleared out by the research questions. Data collection is an essential component to conducting research. Data collection is a complicated and hard task. O'Leary says "collecting credible data is a tough task, and it is worth remembering that one method of data collection is not inherently better than another" [26] Therefore, which data collection method to use would depend upon the research goals and the advantages and disadvantages of each method.

2.7.2 Qualitative research

Qualitative researchers are interested in understanding the meaning people have constructed, that is, how people make sense of their world and the experiences they have in the world. [27]. Qualitative research is a situated activity that locates the observer in the world. It consists of a set of interpretive, material practices that makes the world visible. These practices transform the world. They turn the world into a series of representations, including field notes, interviews, conversations, photographs, recordings, and memos to the self. At this level, qualitative research involves an interpretive, naturalistic approach to the world. This means that qualitative researchers study things in their natural settings, attempting to make sense of, or to interpret, phenomena in terms of the meanings people bring to them. [28].

The advantages of doing qualitative research include:

- ✓ flexibility to follow unexpected ideas during research and explore processes effectively
- ✓ sensitivity to contextual factors
- ✓ ability to study symbolic dimensions
- ✓ increased opportunities:
    - ➢ to develop empirically supported new ideas and theories
    - ➢ for in-depth and longitudinal explorations

- for more relevance and interest for practitioners.

2.7.3 Quantitative research

Quantitative research focuses on gathering numerical data and generalising it. Sampling variability reflects the amount of confidence you can have about how well your sample has captured the characteristics of the population influenced by sample size [29].

Characteristics of a quantitative research:

- Researcher has a clearly defined research question to which objective answers are sought
- All aspects are carefully and precisely designed before data collection
- Data are in the form of numbers and statistics
- Project can be used to generalise concepts more widely, predict future results or investigate causal relationships

The considerations in quantitative research are:

- Study Design
- Data Collection
- Data analysis
- Reporting your results

2.7.4 Interviews

Interviewing is a process to collect data as well as to gain knowledge from individuals. Interviews is an interchange of views between two or more people on a topic of mutual interest, sees the centrality of human interaction for knowledge production, and emphasizes the social of research data. Interviews are ways for participants to get involved and talk about their views. In addition, the interviewees are able to discuss their perception and interpretation in regards to a given situation. It is their expression from their point of view. The interview is not simply concerned with collecting data about life: it is part of life itself, its human embeddedness is inescapable [30].

There are many reasons to use interviews for collecting data and using it as a research instrument [31]:

- ❖ There is a need to attain highly personalized data.
- ❖ There are opportunities required for probing.
- ❖ A good return rate is important.
- ❖ Respondents are not fluent in the native language of the country

There are many types of interviews which include:

- structured interviews
- unstructured interviews
- non-directive interview.

a. Structured interviews

A structured interview is sometimes called a standardized interview. The same questions are asked of all respondents. Corbetta states structured interviews are interviews in which all respondents are asked the same questions with the same wording and in the same sequence. It would be ideal if questions can be read out in the same tone of voice so that the respondents would not be influenced by the tone of the interviewer [32]

b. ***Unstructured interviews***

This type of interview is non-directed and is a flexible method. It is more casual than the aforementioned interviews. There is no need to follow a detailed interview guide. Each interview is different. Interviewees are encouraged to speak openly, frankly and give as much detail as possible
Usually the interviewer has received virtually little or no training or coaching about the interview process and has not prepared much. The interviewers ask questions that respondents would be able to express their opinions, knowledge and share their experience [33].

The strengths of unstructured interviews are no restrictions are placed on questions. It is useful when little or no knowledge exists about a topic. So, background data can be collected. Unstructured interviews are flexible and the researcher can investigate underlying motives. The drawbacks of unstructured interviews are that they can be inappropriate for inexperienced interviewers.

The interviewers may be bias and ask inappropriate questions. Also, respondents may talk about irrelevant and inconsequential issues. Consequently, it may be difficult to code and analyze the data.

c. ***Non-directive Interviews***

The structured and semi-structured interviews are somewhat controlled by the researcher who has set the issues and questions. In non-directive interviews there are no preset topics to pursue. Questions are usually not pre-planned. The interviewer listens and does not take the lead. The interviewer follows what the interviewee has to say. The interviewee leads the conversation.

The interviewer does not know which direction the interview will take. Non-directive interviews have their origin in dynamic psychology and psychotherapy with the objective to help patients reveal their deep-seated and subconscious feelings. The strengths of non-directive interviews are to find the deep-seated problem and the subconscious feelings. On the other hand, the drawbacks are that there are no directions or issues to explore which can cause some problems in coding and analyzing the data [34].

2.7.5 Literature Review

Relevant literature was reviewed in order to explore potentially relevant different network protocols and techniques. In the review, a number of networks at the national were considered. Additionally, interviews activities helped to identify relevant topologies.

To answer the research questions and achieve the final goal of our research, we employed also quantitative method. Where we collected data on NUR network, data were collected using measurement and vulnerability scanner tools at NUR.

In the beginning, the researcher used literature review to collect required information from books, papers, article and then conducting survey interviews, where unstructured interview with the experienced professionals of the domain working in network operating center (NOC) at NUR, to verify and crosscheck the finding of literature review and provide details that will help in analysis. Case study method will be used to collect data on NUR network, which will be analyzed to see network vulnerabilities.

Table 1: RQ with methodology to answer them

Research question	**Method(s)**
RQ1	Literature review + Interviews with the Network and System Administrators at NUR and case study method
RQ2	Literature review, unstructured interview
RQ3	Literature review

CHAPTER 3: DATA COLLECTION

The proposed framework for data collections is relating components that can be used to design DAG that are adaptive to the Bayesian environment. Some tools have been used: NMAP a Network Mapper to detect all the open ports associated to their respective services and Nessus, vulnerability scanner software was deployed in the network to collect the potential vulnerabilities from servers with. The collected vulnerabilities are grouped into different category according the standard of information security vulnerabilities names called common vulnerabilities and exposures (CVE). Besides of tools other parameters have taken in consideration that can be source of vulnerability: Technological Weaknesses, Configuration Weaknesses, and Security Policy Weaknesses.

3.1 Types of Vulnerabilities weaknesses

3.1.1 Technological Weaknesses

Computer and network technologies have intrinsic security weaknesses. These include protocol weaknesses, operating system weaknesses, and network equipment weaknesses [35]. Common examples of technological weaknesses are:

- ✓ HTTP, FTP, ICMP and other protocols are inherently insecure
- ✓ OS security holes and problems.
- ✓ Network equipment weaknesses:
- ✓ password protection,
- ✓ lack of authentication,

3.1.2 Configuration Weaknesses

The redundant servers have been found with different type of softwares and version. Those redundants have been upgraded differently by system administrators, so they need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate.
Some configuration weaknesses found are:

- ✓ Unsecured user accounts

- ✓ Easily guessed passwords
- ✓ Misconfigured services
- ✓ Default settings used in running configurations

3.1.3 Security Policy Weaknesses

Security policy weaknesses can create unforeseen security threats. The network may pose security risks to the network if users do not follow the security policy like:

- ➢ Lack of written security policy
- ➢ Politics
- ➢ Lack of continuity
- ➢ Software and hardware installations
- ➢ or installation changes do not follow the policy

3.2 Data collection

The collected data are vulnerabilities from NUR network which were scanned by Nessus vulnerability scanner and grouped into 3 categories according their risks: High, medium and low. Twenty six servers were used to collect Data: 15 located in the LAN and 12 with public IPs. The NOC uses 3 types of OS: Ubuntu 12.04.2, Windows server 2003 and Linux Redhat. The NUR network has 2 parts: the internal network and the DMZ. The collected data are vulnerabilities with 2 standards: Common Vulnerabilities and Exposures and Open Source Vulnerability Database (OSVDB).

3.2.1 Common Vulnerabilities and Exposures (CVE)

Common Vulnerabilities and Exposures (CVE) is a dictionary of common names (CVE Identifiers) for publicly known information security vulnerabilities. CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools [36]. If a report from one of your security tools incorporates CVE Identifiers, you may then quickly and accurately access fix information in one or more separate CVE-compatible databases to remediate the problem.

CVE is now the industry standard for vulnerability and exposure names. CVE Identifiers provide reference points for data exchange so that information security products and services can speak with each other. CVE Identifiers also provides a baseline for evaluating the coverage of tools and services so that users can determine which tools are most effective and appropriate for their organization's needs. In short, products and services compatible with CVE provide better coverage, easier interoperability, and enhanced security. The CVE score the vulnerability into a system called Common Vulnerability Scoring System, CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of vulnerability.

CVSS scores is a free and open industry standard for assessing the severity of computer system security vulnerabilities, and is under the custodianship of the Forum of Incident Response and Security Teams (FIRST). It attempts to establish a measure of how much concern a vulnerability warrants, compared to other vulnerabilities, so efforts can be prioritized. The scores are based on a series of measurements called metrics based on expert assessment. The scores have a range of 0 least severe to 10 critical. Vulnerabilities with a base score in the range 7.0-10.0 are typically categorized as critical, those in the range 4.0-6.9 as major, and 0-3.9 as minor [36].

3.2.1.1 Metric Groups for CVE

The base metric group captures the characteristics of a vulnerability that are constant with time and across user environments. The Access Vector, Access Complexity, and Authentication metrics capture how the vulnerability is accessed and whether or not extra conditions are required to exploit it. The three impact metrics measure how vulnerability, if exploited, will directly affect an IT asset, where the impacts are independently defined as the degree of loss of confidentiality, integrity, and availability. The vulnerability could cause a partial loss of integrity and availability, but no loss of confidentiality[36].

a. Access Vector (AV)

This metric reflects how the vulnerability is exploited. The possible values for this metric are listed in below. The more remote an attacker can be to attack a host, the greater the vulnerability score.

Table 2: Metric Value for Access Vector

Metric Value	Description
Local (L)	A vulnerability exploitable with only *local access* requires the attacker to have either physical access to the vulnerable system or a local (shell) account. Examples of locally exploitable vulnerabilities are peripheral attacks such as Firewire/USB DMA attacks, and local privilege escalations (e.g., sudo).
Adjacent Network (A)	A vulnerability exploitable with *adjacent network access* requires the attacker to have access to either the broadcast or collision domain of the vulnerable software. Examples of local networks include local IP subnet, Bluetooth, IEEE 802.11, and local Ethernet segment.
Network (N)	A vulnerability exploitable with *network access* means the vulnerable software is bound to the network stack and the attacker does not require local network access or local access. Such a vulnerability is often termed "remotely exploitable". An example of a network attack is an RPC buffer overflow.

b. Access Complexity (AC)

This metric measure the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system. Consider a buffer overflow in an Internet service: once the target system is located, the attacker can launch an exploit at will. Other vulnerabilities, however, may require additional steps in order to be exploited. For example, a vulnerability in an email client is only exploited after the user downloads and opens a tainted attachment

c. Authentication (Au)

This metric measure the number of times an attacker must authenticate to a target in order to exploit vulnerability. This metric does not gauge the strength or complexity of the authentication process, only that an attacker is required to provide credentials before an exploit may occur.

The metric should be applied based on the authentication the attacker requires before launching an attack. For example, if a mail server is vulnerable to a command that can be issued before a user authenticates, the metric should be scored as "None" because the attacker can launch the exploit before credentials are required. If the vulnerable command is only available after successful authentication, then the vulnerability should be scored as "Single" or "Multiple," depending on how many instances of authentication must occur before issuing the command.

d. Confidentiality Impact (C)

This metric measures the impact on confidentiality of a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. The possible values for this metric are listed in Table 4. Increased confidentiality impact increases the vulnerability score.

e. Integrity Impact (I)

This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and guaranteed veracity of information.

f. Availability Impact (A)

This metric measures the impact to availability of a successfully exploited vulnerability. Availability refers to the accessibility of information resources. Attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of a system.

3.2.2 Open Source Vulnerability Database (OSVDB).

OSVDB is an independent and open source database created by and for the community. The goal of the project is to provide accurate, detailed, current, and unbiased technical information on security vulnerabilities [37]. OSVDB promotes greater, open collaboration between companies and individuals, eliminates redundant works, and reduce expenses inherent with the development and maintenance of in house vulnerability databases.

Its goal is to provide accurate, unbiased information about security vulnerabilities in computerized equipment. The core of OSVDB is a relational database which ties various information about security

vulnerabilities into a common, cross-referenced open security data source. As of April, 2013, the database catalogs over 90,000 vulnerabilities.

3.2.3 Description of Test Network

The NUR network is shown in figure 12, there are 12 servers on the Demilitarized zone (DMZ) and 15 server on the Interne, and the firewall separating the internal network from external network. The firewall filters and allows the inbound services packets to communicate with the world, but interdicts other packets. In the internal network, connection relation won't be controlled by firewall, so it can be assumed that the internal hosts can make connection with any remote server.

CHAPITER 4: RESULTS AND DISCUSSION

To analyze the network security with BN, we have to consider the level of vulnerability depending on the risk, this will help us to make the CPTs with Integer and Boolean. The collected data are based on most high-level network traffic, such as email, web pages, etc reach a server via a high-level protocol that is transmitted reliably by a TCP stream. The data used in our analysis was the trace acquired at National University ICT Center.

4.1 Vulnerabilities

All of the servers in NUR network have at least one vulnerability that potentially allows for remote exploitation, each of the active applications on different servers accessed by the attacker in the NUR LAN or Internet are sufficient for an attacker to gain control of the server. The figure 12 shows the vulnerabilities, the highest number of vulnerability has the EZproxy which is is a web proxy server used by libraries to give access from outside the library's computer network to restricted-access websites that authenticate users by IP address. This allows library users at home or elsewhere to log in through their library's EZproxy server and gain access to bibliographic databases and the lowest number of vulnerability are on Hotspot server which allows NUR network users to access the NUR-Wireless. The average of vulnerabilities @NUR network is 113.4444444.

Table 3: Number of vulnerabilities at NUR Network

NAMES	DESCRIPTION	NBER OF VULNERABILITIES
Agnes	Hotspot Server	13
Amasimbi	Oracle server	37
Bowie	Ldap server	79
Carey	File server	74
Cher	Virtualization server	27
Denver	Oracle DB server	73
Elton	Repository	35
Elvis	Domain Controller	129
Holiday	Web server	58
Impala	DNS server	56
Intare	VPN server	58
Inyange	VOIP server	44
Inzovu	Firewall	25
Jagger	DHCP	70
John	MIS Appl. Server	421

Kagame	Elearning	47
Kravitz	VNP Router	37
Miller	Backdoor	103
Nyampinga	Mysql Database server	66
Oates	File server for Virtualization	42
Prince	Ezproxy	1117
Rusaro	Monitoring server	48
Sade	OTRS server	62
Salus	Live streaming for Radio	53
Sam	Mail server	129
Springsteen	Apt Repository for ubuntu	69
Watson	Ray server	91
	Total	**3063**
	Average	**113.4444444**
	Max	**1117**
	Min	**13**

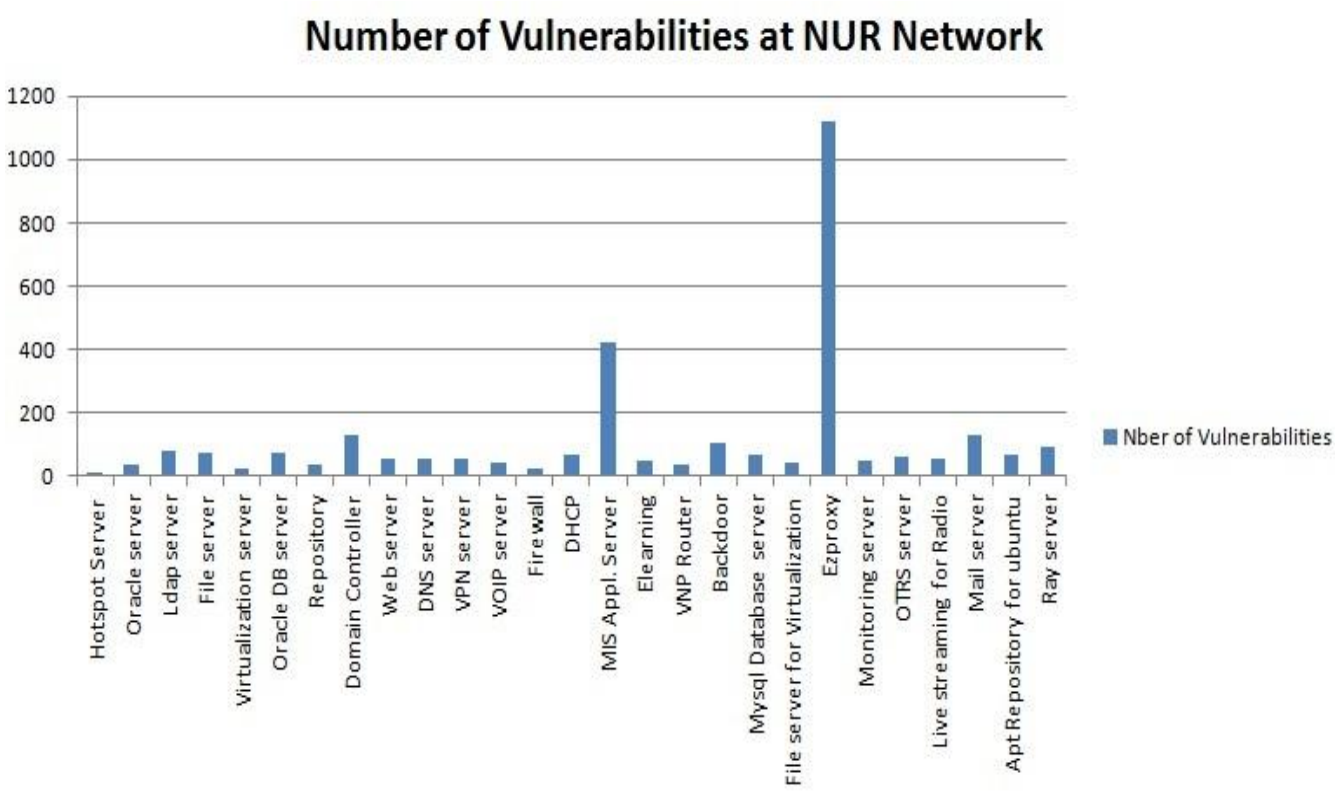

Figure 11: Number of vulnerabilities @NUR Network

Among the 3063 vulnerabilities found @NUR Network, many of them do not represent any risk in the CVSS scoring, it is just the information about the OS used by the servers, the services running by the servers, etc but can represent a risk if an attacker want to gathers those information.

The figure 13 shows the CVSS scores, as describe above in the chapter 3, we have critical CVSS scores, major and minor CVSS scores and least severe score.

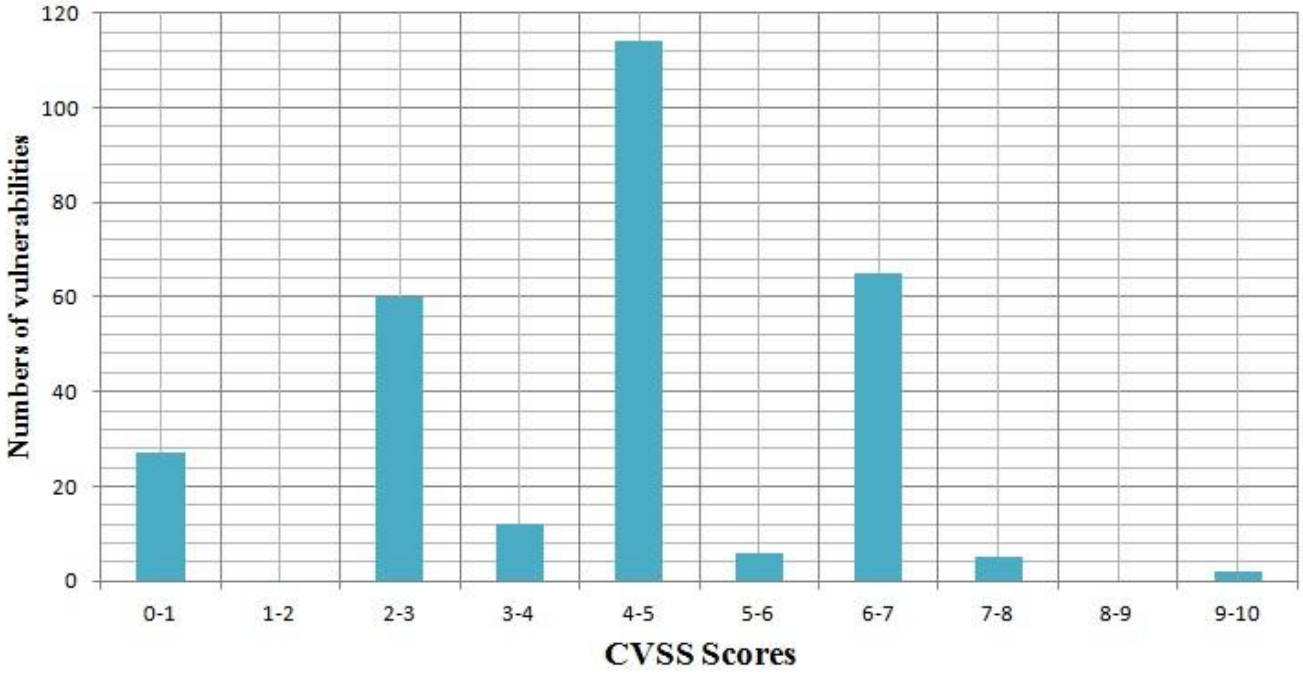

Figure 12: CVSS scores

4.2 Experiment network and Attack Graph Model

Attack graphs model shows how multiple vulnerabilities may be combined for an attack. They represent system states using a collection of security related conditions, such as the existence of vulnerability on a particular host or the connectivity between different hosts. Vulnerability exploitation is modeled as a transition between system states. Due to the complexity of NUR Network, the research has chosen four servers high CVSS scores to establish his experiment; the figure below shows the environment where the researcher carried this study.

Attack graphs provide the cumulative effect of attack steps to show how each of these steps can potentially enable an attacker to reach their goal. However, one limitation of an attack graph is that it assumes that a vulnerability can always be exploited. In reality, there is a wide range of probabilities that different steps can be exploited. It is dependent on the skill of the attacker and the difficulty of the exploit. Attack graphs show what is possible without any indication of what is likely. The researcher present a methodology to estimate the security risk using the CVSS scores of individual vulnerabilities for the reduce part of the NUR network. As describe above, the NUR Network is among the big network in the country, the attack graph of the entire network could difficult for analysis, we choose to

analyse the mail, web server and database server.

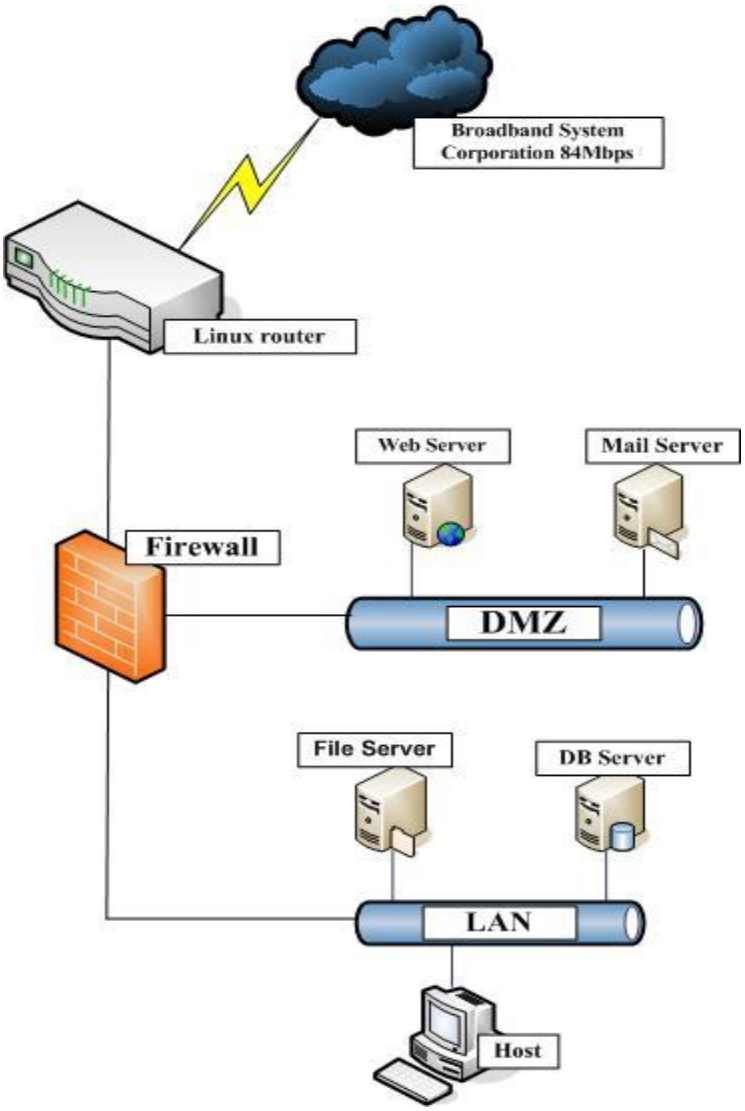

Figure 13: Experiment network

4.2.1 Attack graph for Web server

According the figure 14, there is a firewall that gives access to the Internet according the rules established by the Network and System administrators at NUR. The firewall protects the host in DMZ and only allows external access to ports necessary for the service. In this example, Internet is allowed to access the web server through TCP port 80 and 443 the standard HTTP and HTTPS protocols and ports.

The vulnerability on the Web server has been found, The CVE ID of the discovered vulnerability is

CVE-2004-2320:

Overview:

The default configuration of BEA WebLogic Server and Express 8.1 SP2 and earlier, 7.0 SP4 and earlier, 6.1 through SP6, and 5.1 through SP13 responds to the HTTP TRACE request, which can allow remote attackers to steal information using cross-site tracing (XST) attacks in applications that are vulnerable to cross-site scripting.

Impact:

CVSS Severity (version 2.0):
CVSS v2 Base Score: 5.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:N) (legend)

Impact Subscore: 4.9

Exploitability Subscore: 8.6

CVSS Version 2 Metrics**:**

Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification

These CVSS metrics provide crucial information regarding the pre and post conditions for exploiting the vulnerability. Such information can then be used to construct an attack graph, which shows all possible attack paths in a network. The attack graph for this path is shown in Figure 14.

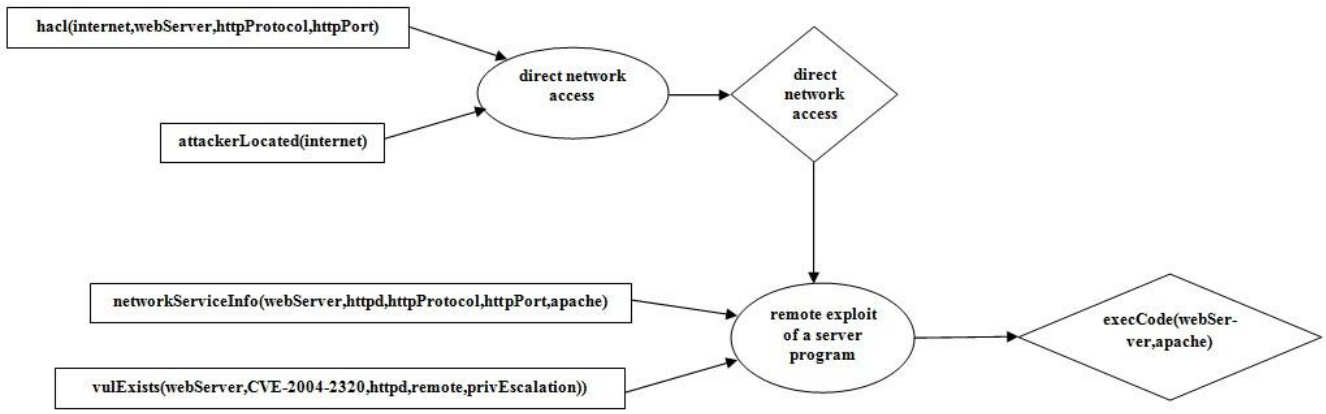

Figure 14: Attack graph for Web server

The figure 14 shows the rectangles that represent configuration of the system, like: the existence of

software vulnerability on a machine (CVE-2004-2320), firewall rules that allow Internet to access the web server through the HTTP protocol and port and services running on a host (HTTPS). The diamond represent potential privileges an attacker could gain in the system, like: code execution privilege on web server execCode(webServer,apache). The elliptical vertices are “attack nodes” which link preconditions to post conditions of an attack like the attack remote exploit of a server program. Its preconditions are: the attacker has network access to the target machine for the specific protocol and port netAccess(webServer,httpProtocol,httpPort), the service on that port is running (networkServiceInfo(webServer,httpd,httpProtocol,httpPort,apache)), and the service is vulnerable vulExists(webServer, CVE-2004-2320,httpd,remote,privEscalation). The post condition of the attack is that the attacker gains the specific privilege on the machine execCode(webServer,apache).

4.2.2 Attack graph for Database server

Again the figure 13 will facilitates us to make the attack graph on Database server, this server has vulnerability: CVE-2011-3551. The Oracle database is located in LAN, the figure 15illustrate

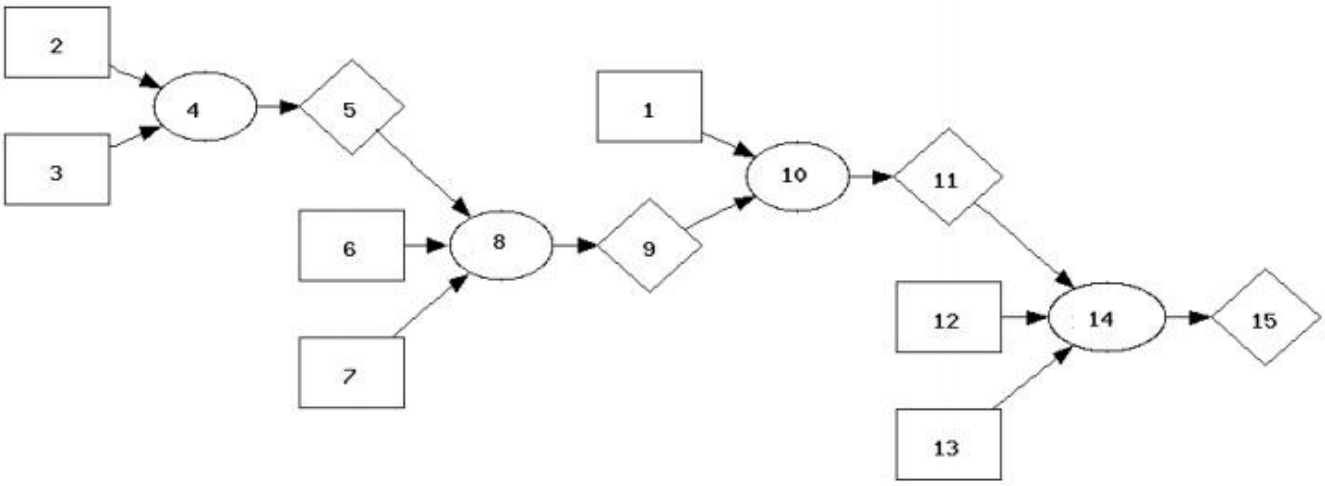

Figure 15: Attack graph for Database and Web server

1: hacl(webServer,dbServer,dbProtocol,dbPort)

2: hacl(internet,webServer,httpProtocol,httpPort)

3: attackerLocated(internet)

4: direct network access

5: netAccess(webServer,httpProtocol,httpPort)

6: networkServiceInfo(webServer,httpd,httpProtocol,httpPort,apache)

7: vulExists(webServer,'CVE-2006-3747',httpd,remote,privEscalation)

8: remote exploit of a server program

9: execCode(webServer,apache)

10: multi-hop access

11: netAccess(dbServer,dbProtocol,dbPort)

12: networkServiceInfo(dbServer,mySQL,dbProtocol,dbPort, superuser)

13: vulExists(dbServer,'CVE-2009-2446',mySQL,remote,privEscalation)

14: remote exploit of a server program

15: execCode(dbServer,superuser)

The figure shows two-stage attack. The attacker can first compromise the web server. Then they can use the web server as a stepping stone to further compromise the database server. The component metric for node 2 is 0.6, since the MySQL vulnerability is easier to exploit than the Apache vulnerability. In this attack graph, since there is only one path to reach the compromises of the Database server, it is easy to see that the cumulative metric for node 1 is the multiplication of the two component metrics on the path: 0.2x0.6=0.12. This is intuitive since the longer the attack path, the lower the risk.

The figure 15 highlights the need to account for security interactions in the specific network to fully understand the risk vulnerability brings to a system. Although the vulnerability on the database server has a high CVSS score (8.5).

4.2.3 Attack graph for Mail server

The mail is among the most exposed server with maximum CVSS score for vulnerability, 10. The CVSS scores funds are:

- CVE-1999-0512: A mail server is explicitly configured to allow SMTP mail relay, which allows abuse by spammers and CVSS v2 Base Score: 10.0 (HIGH)
- CVE-2002-1278: The mailconf module in Linuxconf 1.24, and other versions before 1.28, on Conectiva Linux 6.0 through 8, and possibly other distributions, generates the Sendmail configuration file (sendmail.cf) in a way that configures Sendmail to run as an open mail relay, which allows remote attackers to send Spam email and **CVSS v2 Base Score:**7.5 (HIGH)

❖ CVE-2003-0285: IBM AIX 5.2 and earlier distributes Sendmail with a configuration file (sendmail.cf) with the (1) promiscuous_relay, (2) accept_unresolvable_domains, and (3) accept_unqualified_senders features enabled, which allows Sendmail to be used as an open mail relay for sending spam e-mail and 5.0 (MEDIUM)

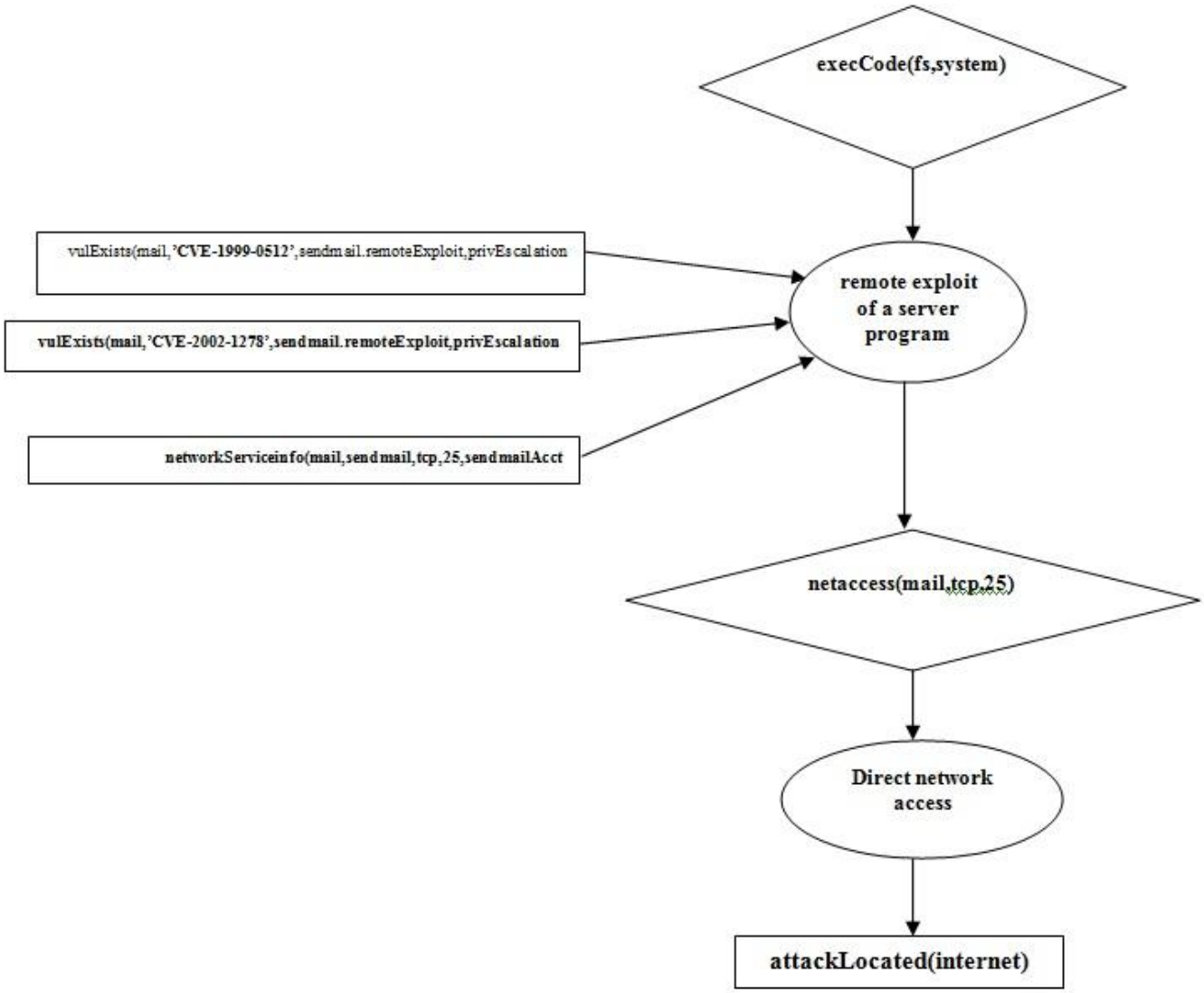

Figure 16: Attack graph for mail server

4.3 Modeling Security Metrics Using Bayesian Networks

This part of the research is very essential, from the vulnerabilities found in NUR, We are going to combine AG results with BN principals. By doing this we are going to establish quantitative values representing the overall network security when considering the combined effect of all known vulnerabilities of a NUR network. This quantitative value will serve as a security metric for measuring the overall security of the network.

4.3.1 Condition Probability Tables construction

4.3.1.1 Web server

From the Web server AG, we are going to allocate quantitative values: let us take the letter X as the vulnerability CVE-2004-2320, CVSS score: 5.8, Y as the preconditions to exploiting vulnerability. The successful exploitation of the vulnerability allows us to the goal state which is the post-condition of vulnerability X. The CPT for each node will be created with the probability value of each node and its conditional dependencies. In this case the Boolean value will be used to determine that the exploit has been successfully performed by the attacker or not, T and F or 1 and 0

X	
T	F
0.4	0.6

Y		
X	T	F
T	0.4	0.6
F	0	1

Figure 17: CPT

The figure 17 can allows us to calculate the joint probability function for the Web server AG and this CPT can help us to verify that the vulnerability has been exploited:

$$P(\mathrm{Y}=\mathrm{T}) = \sum_{\mathrm{X,Y} \in \{\mathrm{F,T}\}} \mathrm{P}\,(\mathrm{Y=T,X}) \qquad (4)$$

= P(Y=T,X=T)+P(Y=T,X=F)

=P(Y=T|A=T)P*P(X=T)+P(Y=T|X=F)*P(X=F)

4.3.1.2 Mail server

In this case, as the mail server has 2 types of vulnerabilities, one of the two has to be exploited by the hacker:

X	
T	F
0.8	0.2

Y	
T	F
0.8	0.2

Z			
X	**Y**	**T**	**F**
F	F	0	1
F	T	0.4	0.6
T	F	0.4	0.6
T	T	0.6	0.6

Figure 18: Case of mail server

$$P(\mathrm{Y}=\mathrm{T}) = \sum_{\mathrm{X,Y} \in \{\mathrm{F,T}\}} \mathrm{P}\,(\mathrm{Z=T,X,Y}) \qquad (5)$$

$$= \mathrm{P(Z=T,X=F,Y=F)+P(Z=T,X=F,Y=T)+P(Z=T,X=T,Y=F)+P(Z=T,X=T,Y=T)}$$

$$=0+0.084+0.084+0.36$$

$$=\mathbf{0.204}$$

This calculation satisfies the intuitive property whereby a security metric should satisfy the concept that as more paths to a goal state exist, the security of the network decreases. This calculation validates the notion and the use of the probabilistic score as a security metric.

4.3.1.3 Conjunctive relationship in the mail server

Successful exploitation of X increases likelihood of exploiting Y (Conjunctive relationship) This case shows that vulnerabilities X and Y are dependant in that successful exploitation of X increases the likelihood of exploiting Y. We show the results of achieving the goal state:

X	
T	F
0.3	0.7

Y		
X	T	F
T	0.5	0.5
F	0.3	0.7

Z			
X	**Y**	**T**	**F**
F	F	0	1
F	T	0	1
T	F	0	1
T	T	0.4	0.6

Figure 19: Conjunctive relationship in the mail server

$$P(\mathrm{Y}=\mathrm{T}) = \sum_{\mathrm{X,Y} \in \{\mathrm{F,T}\}} \mathrm{P}\,(\mathrm{Z=T,X,Y})$$

$$= \mathrm{P(C=T,X=F,B=F)+P(Z=T,X=F,Y=T)+P(C=T,X=T,Y=F)+P(Z=T,X=T,Y=T)}$$

$$= 0+0+0+0.6=\mathbf{0.06}$$

4.3.2 Bayesian Attack Graphs applications

In the graph on the figure 20, an attacker must exploit X or Y, and Z, and A to achieve the goal state. The graph on the figure 21 differs slightly. In order to achieve the goal state, an attacker must execute the same steps as that to the left. However, if the attacker exploits X, he acquires knowledge that will make exploiting A easier and more likely. This is denoted by the likelihood score of 0.4 (when A is not exploited to reach A) and 0.8 when A has been exploited to reach A. This is modeled by the CPTS in the figure 20 and 21. The probability score for reaching the goal state can be calculated with BN inference. This probability score represents the overall security metric for the network being analyzed. Notice in the CPT for the figure 20 that exploiting A implies that exploiting A will be more likely, however, Z must still be exploited.

X	
T	F
0.3	0.7

Y		
X	T	F
T	0.5	0.5
F	0.3	0.7

Z			
X	**Y**	**T**	**F**
F	F	0	1
F	T	0.4	0.6
T	F	0.4	0.6
T	T	0.4	0.6

A		
Z	**T**	**F**
F	0	1
T	0.4	1

Figure 20: CPT Bayesian Attack Graphs applications

X	
T	F
0.3	0.7

Y		
X	T	F
T	0.5	0.5
F	0.3	0.7

Z			
X	**Y**	**T**	**F**
F	F	0	1
F	T	0.4	0.6
T	F	0.4	0.6
T	T	0.4	0.6

A			
X	Z	T	F
F	F	0	1
F	T	0.4	0.6
T	F	0	1
T	T	0.8	0.2

Figure 21: CPT Bayesian Attack Graphs applications

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

This research shows that BNs can be used with AGs as a tool for network security analysis regarding information system networks. The use of our Bayesian AG model with the mechanisms from CVSS is in our opinion an effective and sound methodology contributing towards improving the research into network security field. Threat analysis, producing quantitative risk values, is necessary in order to numerically illustrate risk-impact figures in a distributed computing environment.

5.2. Recommendations

This study was limited to BN AG and CVSS, we would like to recommend to future researchers to refine our approach using Dynamic Bayesian Networks to encompass the Temporal domain measurements established in the CVSS.

We suggest the following recommendations to improve the efficiency and effectiveness of traffic network:

- To have an Intrusion Detection System into their infrastructure
- Improve the methodology of logging the Intrusion and documents the past attacks occurred at NUR network
- Run application softwares on compatible OS and versions

REFERENCE

[1] [6] Stallings W., Cryptography and Network Security, 4/E Prentice Hall, 2006.

[2] Using Bayesian Networks for Cyber Security Analysis by Peng Xie*, Jason H Li*, Xinming Out, Peng Liu+, Renato Levy*

[3] Paul Ammann, Duminda Wij esekera, and Saket Kaushik. Scalable, graph-based network vulnerability analysis. In CCS 2002, Washington, DC, 2002 .

[4] Kyle Ingols, Richard Lippmann, and Keith Piwowarski. Practical attack graph generation for network defense. In *22nd*, *Annual Computer Security Applications Conference (ACSAC)*, Miami Beach, Florida, December 2006.

[5] IT Security Review: Privacy, Protection, Access Control, Assurance and System Security by Sattarova Feruza Y. and Prof.Tao-hoon Kim, International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 2, April, 2007

[7] Illustrated TCP/IP: A Graphic Guide to the Protocol Suite by Matt Naugle

[8][9][10][11][15]Fundamentals of Network Security, John E. Canavan , Artech House, Boston

[12][13] Jian Huang; Bastani, F.; I-Ling Yen; Jun-Jang Jeng "Toward a Smart Cyber-Physical Space: A Context-Sensitive Resource-Explicit Service Model", *Computer Software and Applications Conference, 2009. COMPSAC '09. 33rd Annual IEEE International,* On page(s): 122 - 127 Volume: 2, 20-24 July 2009

[14] Ammann P, Wijesekera D, Kaushik S. Scalable, Graph-Based Network Vulnerability Analysis. Proc. of ACM conf. on Comp.& Com. Sec., pp. 217-224, 2002.

[16][17] Secrecy Throughput of MANETs Under Passive and Active Attacks by Yingbin Liang, *Member, IEEE*, H. Vincent Poor, *Fellow, IEEE*, and Lei Ying, *Member, IEEE*

[18] F.V. Jensen, Bayesian Networks and Decision Graphs. Springer, 2001.

[19] J. Jozefowska. Uncertainty modelling 2, bayesian networks, 2005.

[20] [21]Yongning Tang Overlay Fault Diagnosis Based on Evidential Reasoning, Bayesian networks

[22][23][24] A. Darwiche. What are bayesian networks and why are their applications growing across all fields? Communications of the ACM, 53:80–90, December 2010

[23] J. Elkink. Bayesian inference, October 14, 2008

[25] Arbnor and Bjerke. Methodology for Creating Business Knowledge, SAGE Publications Ltd, Dec 22, 2008 - Business & Economics

[26] O'Leary, A. (2004). The Essential Guide to Doing Research. London: SAGE Publications.

[27] Sharan B. Merriam, Qualitative Research and Evaluation Methods. John Wiley & Sons, Apr 6, 2009

[29] Davy, D. ; Valecillos, C., Summary of a literature review of qualitative research in technical communication, Member, IEEE

[S] Louis Cohen, Lawrence Manion, Keith Morrison. Research Methods in Education: 7th Edition

[31] Gray, D. E. (2004). Doing Research in the Real World. London: SAGE Publications.

[32] [33] [34]Corbetta, P. (2003). Social Research Theory, Methods and Techniques. London: SAGE Publications.

[35] McGraw Hill - Hacking Exposed - Network Security, Secrets and Solutions, 3rd Ed

[36] http://nvd.nist.gov/

[37] http://www.osvdb.org/

APPENDIX

Nber	Server Given Name	IP Address	Port opened and services	OS	Description
1	Agnes	192.168.2.46	22/tcp ssh	Ubuntu Precise	Hotspot Server
2	Amasimbi	192.168.2.173	22/tcp ssh 25/tcp smtp 5666/tcp nrpe 9102/tcp jetdirect	Ubuntu Precise	Oracle server
3	armstrong	192.168.2.49	22/tcp open ssh 111/tcp open rpcbind 5666/tcp open nrpe 7007/tcp open afs3-bos 9102/tcp open jetdirect	Ubuntu Precise	Thin Client server
4	Bowie	192.168.2.60	22/tcp ssh 80/tcp http 389/tcp ldap 443/tcp https 636/tcp ldapssl 5666/tcp nrpe 8080/tcp http-proxy 9102/tcp jetdirect	Ubuntu Precise	Loghost and LDAP server
5	Carey	192.168.2.33	22/tcp ssh 80/tcp http 111/tcp rpcbind	Ubuntu Precise	file server

			139/tcp netbios-ssn 443/tcp https 445/tcp microsoft-ds 5666/tcp nrpe 9101/tcp jetdirect 9102/tcp jetdirect 9103/tcp jetdirect		
6	Cher	192.168.2.22	22/tcp ssh 111/tcp rpcbind 5666/tcp nrpe 9102/tcp jetdirect	Ubuntu Precise	Virtualization Server
7	Denver	192.168.2.34	22/tcp ssh 111/tcp rpcbind 1521/tcp oracle 5666/tcp nrpe	RedHat	Oracle DB Server
8	Elton	41.222.244.12	22/tcp ssh 80/tcp http 5666/tcp nrpe 8080/tcp http-proxy 9102/tcp jetdirect	Ubuntu Precise	Repository(Dspace)
9	Elvis	19.2168.2.16	22/tcp ssh 42/tcp nameserver 53/tcp domain 80/tcp open http 88/tcp kerberos-sec	Windows Server 2003	Domain Controller

			135/tcp msrpc 139/tcp netbios-ssn 389/tcp ldap 445/tcp microsoft-ds 464/tcp kpasswd5 593/tcp http-rpc-epmap 636/tcp ldapssl 1025/tcp NFS-or-IIS 1027/tcp IIS 1032/tcp iad3 1049/tcp td-postman 1052/tcp ddt 1287/tcp open routematch 2301/tcp open compaqdiag 2381/tcp open compaq-https 3268/tcp open globalcatLDAP 3269/tcp open globalcatLDAPssl 3389/tcp open ms-wbt-server 9102/tcp open jetdirect		
10	Impala	41.222.244.2	22/tcp ssh 53/tcp domain	Ubuntu Precise	DNS extern/authorative

			80/tcp http 443/tcp https 5666/tcp nrpe 9102/tcp jetdirect		
11	Intare	41.222.244.5	22/tcp ssh 37/tcp time 80/tcp http 443/tcp https 1723/tcp pptp 5666/tcp nrpe 9102/tcp jetdirect	Ubuntu Precise	VPN server
12	Inyange	41.222.244.25	22/tcp ssh 80/tcp http 2000/tcp cisco-sccp 4445/tcp upnotifyp 5666/tcp nrpe 9102/tcp jetdirect	Ubuntu Precise	VOIP server
13	Inzovu	192.168.2.2	22/tcp ssh 179/tcp bgp 2601/tcp zebra 2605/tcp bgpd 5666/tcp nrpe 9102/tcp jetdirect	Ubuntu Precise	FireWall, VLANROUTER and BGP
14	Jagger	192.168.2.14	22/tcp open ssh 37/tcp open time	Ubuntu Precise	DNS/NTP/DHCP/VMPS/LDAP/RADIUS

			53/tcp open domain 80/tcp open http 389/tcp open ldap 636/tcp open ldapssl 5666/tcp open nrpe 9102/tcp open jetdirect		
15	john	192.168.2.35	22/tcp ssh 111/tcp rpcbind 389/tcp ldap 443/tcp https 636/tcp ldapssl 1011/tcp unknown 1049/tcp td-postman 1521/tcp oracle 4443/tcp pharos 4444/tcp krb524 4445/tcp upnotifyp 4446/tcp n1-fwp 5666/tcp nrpe 6003/tcp X11:3 6004/tcp X11:4 6005/tcp X11:5 7777/tcp cbt 7778/tcp interwise	Redhat	MIS Appl. Server

			8888/tcp sun-answerbook 16001/tcp fmsascon		
16	kagame	41.222.244.32	22/tcp ssh 80/tcp http 443/tcp https 5666/tcp nrpe 9102/tcp jetdirect	Ubuntu Precise	Elearning/Moodle MIT Courses
17	kravitz	10.1.0.1	22/tcp open ssh 53/tcp open domain 80/tcp open http 443/tcp open https 5666/tcp open nrpe	Ubuntu Precise	VPN Router
18	Miller	192.168.2.47	22/tcp ssh 80/tcp http 111/tcp rpcbind 139/tcp netbios-ssn 443/tcp https 445/tcp microsoft-ds 631/tcp ipp 2049/tcp nfs 5666/tcp nrpe 9102/tcp jetdirect	Ubuntu Precise	WWW,SVN,TEEAL,GILL,BACKUP,SRS
19	Nyampinga	192.168.2.161	22/tcp ssh 80/tcp http 443/tcp https	Ubuntu Precise	DATABASE server

			3306/tcp mysql 5666/tcp nrpe 9102/tcp jetdirect		
20	oates	192.168.2.20	22/tcp open ssh 111/tcp rpcbind 2049/tcp nfs 5666/tcp nrpe 9102/tcp jetdirect	Ubuntu Precise	Fileserver for Virtualization
21	Prince	41.222.244.18	22/tcp ssh 80/tcp http 81/tcp hosts2-ns 443/tcp https 2065/tcp dlsrpn 2068/tcp advocentkvm 2099/tcp h2250-annex-g 2100/tcp amiganetfs 2103/tcp zephyr-clt 2105/tcp eklogin 2106/tcp ekshell 2107/tcp msmq-mgmt 2111/tcp kx 2119/tcp	Ubuntu Precise	EZProxy server

			gsigatekeeper 2121/tcp ccproxy-ftp 2126/tcp pktcable-cops 2135/tcp gris 2144/tcp lv-ffx 2160/tcp apc-2160 2161/tcp apc-agent 2170/tcp eyetv 2179/tcp vmrdp 2190/tcp tivoconnect 2191/tcp tvbus 2196/tcp unknown 2200/tcp ici 2222/tcp EtherNet/IP-1 2251/tcp dif-port 2260/tcp apc-2260 2288/tcp netml 2301/tcp compaqdiag 2323/tcp 3d-nfsd 2366/tcp qip-login 2381/tcp compaq-https 2382/tcp ms-olap3 2383/tcp ms-olap4		

			2393/tcp ms-olap1 2394/tcp ms-olap2 2399/tcp fmpro-fdal 5666/tcp nrpe 9102/tcp jetdirect		
22	Rusaro	192.168.2.154	22/tcp ssh 80/tcp http 443/tcp https 9102/tcp jetdirect	Ubuntu Precise	Nagios,Cacti,NFSEN,NSDB
23	springsteen	41.222.244.10	21/tcp ftp 22/tcp ssh 25/tcp smtp 80/tcp http 443/tcp https 5666/tcp nrpe 9102/tcp jetdirect	Ubuntu Precise	Apt Repository Ubuntu/Debian
24	Salus	41.222.244.7	21/tcp ftp 22/tcp ssh 25/tcp smtp 80/tcp http 8443/tcp https-alt	Ubuntu Precise	Live Streaming Radio
25	Holiday	41.222.244.13	22/tcp ssh 80/tcp http 443/tcp https	Ubuntu Precise	Web server

			5666/tcp nrpe 9102/tcp jetdirect		
26	Watson	192.168.2.167	22/tcp ssh 111/tcp rpcbind 139/tcp netbios-ssn 445/tcp microsoft-ds 2049/tcp nfs 5666/tcp nrpe 7007/tcp afs3-bos 9102/tcp jetdirect	Ubuntu Lucide	Ray server
27	Sade	41.222.244.24	22/tcp ssh 25/tcp smtp 80/tcp http 443/tcp https 5666/tcp nrpe 9102/tcp jetdirect	Ubuntu Precise	