

Polytechnic of Namibia



School of Information Technology

Department of Computer Systems and Networks

TITLE:

**IPV6— NETWORK SECURITY IN POLYTECHNIC OF NAMIBIA
NETWORK**

Presented by: Mercy Bere, 200731939

Supervisor: Dr. K. Thomson

Acknowledgements

First and foremost I would like to thank the Almighty Lord, who has given me life and who has been guiding me and showing me the light along the way since birth. Philippians 4:13: “I can do all things through him who strengthens me.”

I want to thank my darling husband for supporting me all the way

I would also like to thank Dr. Kerry Thomson and Professor Hippolyte N. Muyingi for guiding me along the way. I would also like to thank Polytechnic of Namibia’s Bureau of Computer Services for giving me a testing platform.

I want to express my appreciation to my colleagues especially Fungai Bhunu- Shava and Meke Shivute for their comments and useful criticisms and support. Finally I would like to thank Cephas Pahla for his help in configuring the IPv6 Network.

Abstract

Increasing demand for IP addresses on the IPv4 address space made the introduction of a new addressing scheme with more addresses inevitable. IPv6 was designed to address the issue of small address space in IPv4. In addition to increasing the address space IPv6 is presumably supposed to increase the security of networks. However, does IPv6 really improve network security? Based on the IPv6 design, it can be argued that IPv6 does improve network security to some extent. IPv6 was designed in such a way that every IPv6 node should support Internet Protocol Security (IPSec), an Internet security standard for protecting communications over IP. The implementation of IPv6 networks is still in its infancy and thus many of its security aspects still need to be thoroughly reviewed and possibly contrasted with highly pertinent IPv4 security issues. Despite its firm security based design structure, research has established that IPv6 may also be susceptible to some of the common IPv4 networks attacks, such port scan attacks, man-in-the-middle attacks and denial of service attacks, as well as to other attacks that are IPv6 specific such as misuse of ICMPv6 and fragmentation attacks. Therefore it can be argued that IPv6 networks are also susceptible to network attacks. However to what extent is IPv6 susceptible? In order to research this, a live IPv4 network was tested for network security and compared to a emulated IPv6 network. As will be discussed in this research, it was found out that both IPv4 and IPv6 networks are susceptible to many types of network attacks.

Table of Contents

Acknowledgements.....	i
Abstract.....	ii
Table of Contents.....	iii
List of Figures	vi
List of Tables	vi
List of Acronyms.....	vii
Chapter One - Introduction.....	1
1.1 Introduction to IPv4 and IPv6	1
1.2 Background	2
1.3 Problem statement	4
1.4 Research Methodology	4
1.5 Summary	6
1.6 Thesis outline	6
Chapter Two – Network Attacks	8
2.1 Introduction	8
2.2 IPv4 Network Attacks.....	10
2.2.1 Reconnaissance Attacks.....	11
2.2.2 Access attacks	11
2.2.3 Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks	12
2.2.4 Fragmentation attacks	12
2.2.5 Network attacks common to both IPv4 and IPv6 networks	13
2.3 Threats in IPv6 Networks	17
2.3.1 Misuse of ICMPv6 and multicast.....	17
2.4 Summary	17

Chapter Three – Network testing	19
3.1 Introduction	19
3.2 Network Security Testing.....	19
3.2.1 Log Reviewing	20
3.2.2 File Integrity Checking.....	20
3.2.3 Penetration Testing.....	20
3.6 Summary	26
Chapter Four -Testing PON Network using Penetration Testing	27
4.1 Introduction	27
4.1.1 Why use Penetration Testing?	27
4.1.2 PON Acceptable ICT Use Policy	28
4.2 Available Information.....	29
4.3 Testing Constraints	31
4.3.1 Time	32
4.3.2 Risk Issues (production and island networks).....	32
4.3.3 Confidentiality.....	32
4.4 Penetration Test Scope	33
4.5 Testing Procedure	33
4.5.1 Information Gathering/foot printing	33
4.5.2 Discovering vulnerabilities	33
4.5.3 Result documentation.....	33
4.6 Summary	33
Chapter Five - Results and Analysis	35
5.1 Introduction	35
5.2 IPv4 production network results.....	35
5.2.1 Scope.....	35
5.2.2 Information Gathering	36
5.2.3 Vulnerability Detection	41

5.3. IPv4 Vulnerability Analysis	46
5.4 IPv4 Network Test Conclusions	47
5.5 IPv6 Island Network results	47
5.5.1 Information Gathering	48
5.5.2 Vulnerability detection	50
5.6 IPv6 Network Test Results analysis	53
5.7 Summary	53
Chapter Six – Conclusions	54
6.1 Summary of the Research	54
6.2 Findings	54
6.3 Recommendations for IPv6 Security	55
6.4 Limitations to the Research	56
6.5 Further Research	56
6.6 Conclusion	57
Chapter Seven – References	59
Appendix A : IPv6 Test Island Routers and Switch Configurations	64
Appendix B: Penetration Test Agreement	67
Appendix C: Acceptable ICT Use Policy	69
Appendix D: DoS Email	73
Appendix E: Typical Nessus Scan Results	74
Appendix F: Typical Nessus Scan Report	74

List of Figures

Figure 2.1: OSI Reference Model Adapted from Deal 2008	9
Figure 2.2: Network Attack Statistics.....	10
Figure 2.3 IPv6 Header Format	15
Figure 2.4 IPv6 Extension Header Chaining	16
Figure 4.1 PON Production Network	30
Figure 4.2 IPv6 Island Network	31
Figure 5.1 ITS Server Nmap scan.....	36
Figure 5.2 Oracle Database Listener Check	38
Figure 5.3 IT Server Nmap Scan	39
Figure 5.4 Staff E-mail Server Nmap Scan	40
Figure 5.5 Verifying Users on E-mail Server.....	40
Figure 5.6 ITS Server Vulnerabilities	42
Figure 5.7 Staff E-mail Server Vulnerabilities	44
Figure 5.8 IT Server Vulnerabilities	45
Figure 5.9 IPv6 Web and Mail Server.....	49
Figure 5.10 Staff VLAN PC	50
Figure 5.11 IPv6 mail and Web Server Nessus Scan vulnerability risk factors	51
Figure 5.12 IPv6 user PC vulnerability risk factors.....	52

List of Tables

Table 2.1 Network Attack Summary	18
Table 3.1 Penetration Testing Tools	26
Table 5.1 ITS Server Medium Risk Factors	43
Table 5.2 PON email server high and medium risk factors.....	44
Table 5.3 IT server high and medium risk vulnerabilities	46
Table 5.4 Nessus Vulnerability Scan Summary	47
Table 5.5 Medium risk vulnerabilities on IPv6 mail and web server	51
Table 5.6 Medium Risk Vulnerabilities on IPv6 user PC	52

List of Acronyms

AAA – Accounting, Authorization, and Accounting protocol

ARP – Address Resolution Protocol

CVSS – Common Vulnerability Scoring System

DoS – Denial of Service

DDoS – Distributed Denial of Service

DNS – Domain Name System

FDDI – Fiber Distributed Data Interface

FTP – File Transfer Protocol

HTTP - Hypertext Transfer Protocol

HTTPS- Hypertext Transfer Protocol Secure

ICMP – Internet Control Message Protocol

ICMPv6 – Internet Control Message Protocol version 6

ICT – Information and Communication Technology

IDS – Intrusion Detection System

IIS – Internet Information Services

IKE – Internet Key Exchange

IMAP – Internet Message Access Protocol

IP- Internet Protocol

IPS – Intrusion Prevention System

IPsec – Internet Protocol Security

IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

IT – Information Technology

ITS – Integrated Tertiary Service

LAN- Local Area Network

LDAP – Lightweight Directory Access Protocol

MTA – Message Transfer Agent

MTU – Maximum Transmission Unit

NAT - Network address translation

ND – Neighbour discovery

NFS –Network File System

NIST – National Institute of Standards and Technology

OS- Operating System

PDA – Personal Digital Assistant

PIX – Private Internet eXchange

PON - Polytechnic of Namibia

PPP – Point-to-Point Protocol

RA – Router Advertisement

RARP – Reverse Address Resolution Protocol

RFC – Request for Comment

RFID – Radio Frequency Identifiers

SLIP – Serial Line Protocol

SMB – Server Message Block

SMTP – Simple Mail Transfer Protocol

SNMP – Simple Network Management Protocol

SQL – Structured Query Language

SSH-1 – Secure Shell version 1

TCP - Transmission Control Protocol

TCP/IP – Transmission Control Protocol/Internet Protocol

TFTP – Trivial File Transfer Protocol

UDP – User Datagram Protocol

UPS – Uninterruptible Power Supply

VLAN – Virtual Area Local Network

VNC – Virtual Network Computing

Wi-Fi - popular name for WLAN

WLAN - Wireless Local Area Network

Chapter One - Introduction

This chapter introduces IPv4 as the Internet Addressing Protocol that has been in use since the inception of the Internet. As a result of the fact that the Internet has grown tremendously, IPv4 addresses are no longer enough to cater for all users that need it. IPv6, therefore, was introduced to address the problem of this address shortage. Additionally, it is seen that besides catering for address shortage, IPv6 was designed with security in mind.

1.1 Introduction to IPv4 and IPv6

IPv4 was specified in 1981 on an experimental basis to connect computers in a way that is fault tolerant in connecting links. It was not anticipated that it would be used on a worldwide basis for connecting millions and millions of computers. IPv4 uses a 32 bit field address space. This means that it allows for 2^{32} (4, 294,967,296) different addresses. This huge number of IPv4 addresses was estimated to be large enough to allow all users to have IPv4 addresses if they wished even though all of these addresses are not available for use. Some of the IP addresses have been set aside for private networks, testing, multitasking and other special uses (Lammle, 2011). The exact number of computers that are currently connected on the Internet is not known and with technologies such as Network Address Translation (NAT) knowing the number of computers with IPv4 installations becomes virtually impossible. NAT is a representation of many private IPv4 addresses by one public IPv4 address. This technology was mainly introduced because organisations do not have enough public IP addresses for all the computers in their organisations to connect to the Internet. However, IPv4 addressing is no longer required just for computer installations. IPv4 is now being used in technologies such as RFID, home appliances like televisions, PDAs, mobile phones and automobiles. It is clear that the addresses available are not enough to cater for all the individuals and services that will require a public IPv4 address in the future (Choudhary, 2009). As such IPv6 was specified in 1995 to resolve the problem of depleting IPv4 address.

IPv6 has a 128 bit address space which translates to 2^{128} addresses. The big address space in IPv6 is thought to be enough to cater for all the emerging uses of IP like RFID, PDA, televisions and so

on. Although IPv6 was designed to cater for depleting addresses, it was also designed with security in mind (Caicedo & Joshi, 2009). Improving network security was a critical issue in the development of IPv6. When IPv4 was designed security was not a design concern. As security became a concern of IPv4 networks a number of security solutions such as firewalls and intrusion detection systems were developed but IPv4 networks are still susceptible to many types of attacks as will be shown in the next chapter.

1.2 Background

The Polytechnic of Namibia (PON) is an educational institution that is slowly migrating from IPv4 to IPv6. This process commenced in December 2009. The institution has about one thousand two hundred and fifty public addresses, which, according to the network manager, are not enough to cater for all the connections that the PON requires in order to effectively connect all the PON personnel, students and remote servers to the Internet using public addresses. The complete migration from IPv4 to IPv6 is expected to take a period of at least three years.

Currently the physical network at PON consists of 2 core multilayer switches, 9 distribution layer switches, more than 97 access layer switches and more than 2000 workstations. The network also consists of 6 main servers and 2 routers that are connected to the Internet. Another router in the resource centre is used for redundancy purposes. The network has more than 3000 IP devices, and this number is growing rapidly with each passing year. Firewalls and Intrusion Detection Systems (IDS) are implemented within the core layer switches. The PON network is segmented into about 40 Virtual Local Area Networks (VLAN). The VLANs are designed in such a way that only the relevant services are provided to the relevant users. Enhanced data protection is provided by controlling the access rights of different network users. (C. Mouton, Personal communication, September 9, 2010)

In order to enhance the security of the IPv4 network, PON deployed two firewall modules in the core network layer. The Cisco Private Internet eXchange (PIX) is the firewall module implemented on the switches. This firewall module regulates the flow of traffic between different security zones and prevents unauthorized access to the networks' resources, such as servers and other network services. The firewall also controls intra-VLAN traffic. The firewalls primarily filter traffic

at the network and transport layers, i.e. at layers 3 and 4. There is also an intrusion detection module in the main core switch. This enables the inspection of traffic at the application layer. For wireless connections, the 802.1X standard is used for authentication. By using 802.1X only authenticated devices get access to the network. Also in use is the Authentication, Authorization, and Accounting (AAA) protocol. It works by specifying who can access the network, how they can access it, and tracking what they did while they were connected. As a result of inadequate funding, the PON has yet to completely phase out some of its legacy network devices such as the old routers and switches which do not support the IPv6 addressing system. Also, due to lack of knowledge as to how the implementation of IPv6 will affect the network security in terms of susceptibility to attacks, the migration will be implemented in a very cautious manner so as not to compromise the security of the PON Internet users (C. Mouton, Personal communication, September 9, 2010). This means that when IPv6 is rolled out it will be done so in one part of the network, observe the effects to network security. After being satisfied with how that part of the network is behaving in terms of security then deploy IPv6 in another part of the network until all parts of the network are configured with IPv6.

Computer network security involves ensuring confidentiality, integrity and availability of digital information and network resources. It is very important to protect the user data, the shared network files that are normally kept on network servers and the other common resources that can be accessed from the Internet. The IPv4 addressing scheme does not have in built security mechanisms. IPv4 originated from ad hoc experiments designed to ensure that computers connected in a way that was resilient to connection faults (Choudhary, 2009). The exponential growth of the Internet was accompanied by an inundation of computer network attacks. As the various types and severity of network attacks increased, so did the techniques for the mitigation of these attacks. Thus it could be said “current IPv4 users are greatly benefiting from twenty years of effort spent identifying and addressing security issues” (Rowe & Gallaher, 2006). However, this is not the case with the evolving IPv6 networks. Rowe & Gallaher, (2006) believe that as IPv6 becomes more and more prevalent, so will its security issues as many network attackers will be paying more attention to its vulnerabilities. This is indeed true because since the inception of IPv6, many successful experimental attacks on IPv6 networks have been carried out

(Zhao-wen, 2007). Therefore, similar to what happened with IPv4 mechanisms to protect networks, many IPv6 protocols aimed at protecting the IPv6 networks are also evolving. However, even though there are many 'candidate' protection mechanisms that are being proposed, the majority of them still need to be tested.

1.3 Problem statement

Although there are many possibilities as to how IPv6 networks can be secured against network attacks. Many of these suggestions have not been sufficiently tested to prove their effectiveness (Convery & Miller, 2004). As the PON is migrating to an IPv6 addressing scheme it is vital that the recommended solutions for IPv6 security vulnerabilities be tested. The aim was to determine whether the suggested solutions are adequate for protecting the IPv6 computer network at the PON.

Thus it was the aim of this research to:

- Conduct a literature study to identify the network attacks that:
 - are considered most threatening to the PON computer network
 - could occur most frequently
 - could interrupt daily operations at the PON
- Design an experiment to test the security vulnerabilities of both the current IPv4 network of the PON,
- Design an experiment to test the security vulnerabilities of the proposed IPv6 network in an emulated environment.
- Establish the susceptibility of both the IPv4 and IPv6 network environments to various network attacks

1.4 Research Methodology

Research Methodology is a high level framework (road map) on how to conduct a research (O'leary, 2010). Research methodology provides the approach that can be taken to legitimise a research (O'leary, 2010). Research Methodologies can be grouped into many categories depending on the discipline in which they will be applied. In the Information Technology (IT) disciplines there are several types of methodology that can be applied; some of the

methodologies being: Design Research, theoretical research, experimental research, quantitative research, qualitative research, case study, action research, etc. Although these methods are used in the IT disciplines it does not mean they are used exclusively for IT they may be applied in other research disciplines as well.

In this research the experimental research methodology was used. In this type of research conclusions are based on measurements observed. Experimental research methodology can be further divided into two categories. The first one being the formal experiment in which observations are made in a controlled environment maybe in a lab or testing a physical island network. Usually in the formal experiment one variable is controlled to find its effect on other dependent variable(s). The second category of experimental research methodology is a field experiment in which, the researcher makes observations or takes measurements in an uncontrolled environment, for example testing a real world network.

According to O’leary, 2010 when a researcher conducts an experiment, they need to decide or define the following some of the following

- Dependant and independent variables – identifying the main focus of the study and deciding on which variables will be manipulated to cause effect on the dependant.
- Assessment of change – ways to determine whether the manipulation of the independent variable affects the dependant variable
- Research setting – where the research will conducted; natural setting or laboratory
- Number of participants
- Number of variables – deciding on how many variables will be manipulated
- Control of the environment – finding a balance between working with a real world scenario and the need to control the environment.

Research methodologies have methods or techniques that are used to collect and analyse data. In this research, document analysis and observation were used. Document analysis was used to identify network attacks in IPv4 and IPv6 networks. Tools like Nmap and Nessus vulnerability scanner were used to observe the effects of changing the IP version from 4 to 6. Further, Nessus Vulnerability scanner was used to analyse the effect on network security.

To summarise the dependant variable was network security and the independent variable was IP. The research was conducted on real network and an emulated network for the IPv6 part. Only IP version was manipulated there were no other independent variable considered. The network acted as its control because it was subjected to the conditions of IPv4 and IPv6 configurations.

1.5 Summary

This chapter gives an overview of the evolution of IPv4 which was designed without the foresight that the Internet would grow exponentially. As such, the number of IPv4 addresses that can be used by Internet users is coming to an end. Further it was seen that the number of network attacks is increasing with the increase of Internet size. Therefore, there is need to for the introduction of IPv6 which has an address space of 2^{128} and built in security mechanisms. The addresses available in IPv6 are thought to be large enough to cater for all perceived Internet connections in the near future. In addition it was outlined how the PON is migrating to IPv6 and the need for thorough testing of the IPv6 security vulnerabilities in order for the PON to maintain its current network security status or to better it. The way in which the testing will be conducted was also outlined.

1.6 Thesis outline

This thesis has 6 chapters; each chapter has a brief introduction, the core and a summary. The first, which is this chapter, gives an introduction and the problem statement.

Chapter two introduces the types of network attacks prevalent in IPv4 networks the predecessor of IPv6. In addition network attacks that can be carried out in IPv4 and IPv6 networks are outlined. Further, the chapter describes attacks that are possible in IPv6 networks. Each identified attack is described in some detail as to how it can be carried out it.

Chapter three describes various network testing procedures and tools that are available and their capabilities which leads to chapter four which; describes the penetration test used to test both IPv4 and IPv6 networks in this research. Further the testing steps that were used for testing are also outlined. Chapter five outlines the results of the penetration tests and the effects of implementing current IPv6 security measures to the PON network.

Chapter six summarizes the thesis and concludes the research. In addition, further work related to thesis is outlined.

Chapter Two – Network Attacks

2.1 Introduction

IPv6 has a 128 bit address space which translates to 2^{128} addresses. The big address space in IPv6 is thought to be enough to cater for all the emerging uses of IP for ubiquitous computing like RFID, PDAs – mobile 3g and 4g devices, televisions and so on (Choudhary, 2009, & Radhakrishnan, et al , 2007). Although IPv6 was designed to cater for depleting addresses it was also designed with security in mind (Caicedo& Joshi, 2009). Improving network security was a critical issue in the development of IPv6. When IPv4 was designed security was not a design concern (Choudhary, 2009). As security became a concern of IPv4 networks a number of security solutions such as firewalls, intrusion detection systems were developed but IPv4 networks are still susceptible to many types of attacks (Rowe and Gallaher, 2006). This is due to the ability of the attackers to exploit vulnerabilities in its design. IP is part of a group of protocols called TCP/IP on which the Internet is based. The TCP/IP is based on a generic model called the Open Systems Interconnect (OSI) reference model which is used to describe how information is transferred from one networking component to another (Deal, 2008). The OSI protocol suite has 7 layers as illustrated in figure 2.1 below.

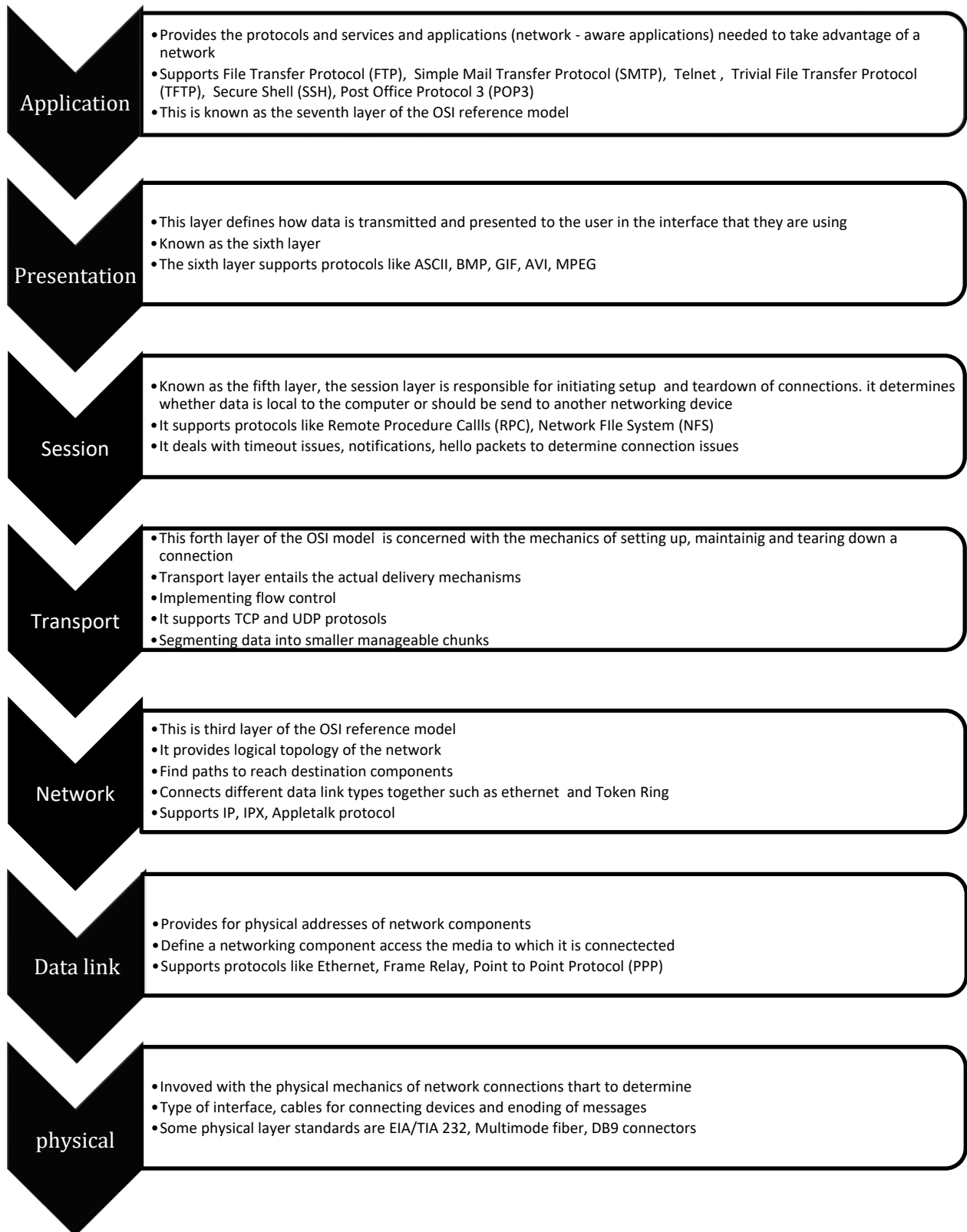


Figure 2.1: OSI Reference Model Adapted from Deal 2008

As shown above, IP is part of the Internet layer of networking protocols. Attackers exploit the vulnerabilities in the different levels of the TCP/IP protocol. An example is a ping sweep attack at layer three. Another example is the man-in-the-middle attack in which attackers place themselves in the middle of a communication channel in order to read and/or modify the information passing through. Some of the more common attacks in IPv4 networks are explained in more detail in the next section

2.2 IPv4 Network Attacks

Figure 2.2 below illustrates how network attacks have increased tremendously from 2008 to 2011. The figure shows the growth of network attacks worldwide. The data is collected by Kaspersky Security network from user computers. Total numbers of network attacks per year were collected and were used to draw the graph below.

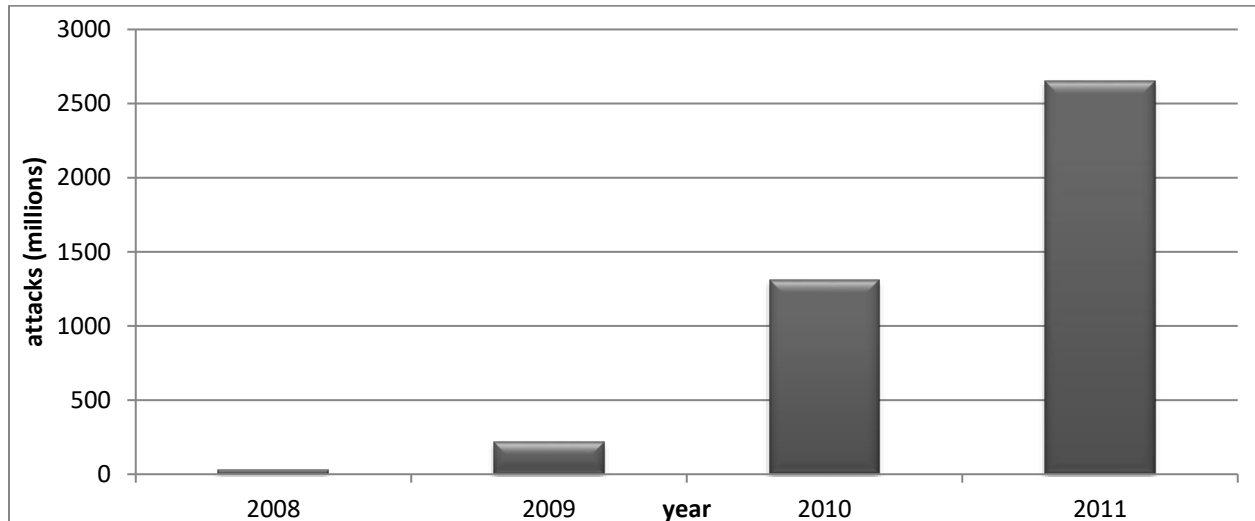


Figure 2.2: Network Attack Statistics.

Adapted from Kaspersky Security Bulletins; 2008, 2009, 2010 and 2011

There are several types of attacks against networks which are usually categorized as follows:

2.2.1 Reconnaissance Attacks

Reconnaissance is about gathering information about the target network. It involves determining active hosts, OSs and the services and ports running on those active hosts. Examples of reconnaissance attacks are:

- Ping Sweeps or Internet Control Message Protocol (ICMP) sweep. This is a network scanning procedure that establishes which IP addresses are in use in a network. A ping sweep is carried out by sending ICMP echo requests to hosts on the network. If any of the chosen addresses is active, the address returns an ICMP echo reply. Once the attacker knows which IP addresses are active, they can focus their attacks on the hosts with the IPs that returned an ICMP echo reply (Paquet, 2009).
- Packet sniffers are programs or devices that monitor packets traversing the network. Packet sniffer programs show data such as passwords and the actual data inside files such as word processing documents (Whitman & Mattord, 2005).
- Port scans are used to identify hosts and devices, the services active and operating systems on the identified hosts and devices. Each service is associated with a known port number. Port numbers enable the communication channels being used by network services offered by one device to be identified. (Whitman & Mattord, 2005).

2.2.2 Access attacks

Access attacks include all forms of unauthorized access to computer resources. Access gained is used to carry out unauthorized and/or illegal activities. Examples of access attacks are:

- Man-in-the-middle attacks: An attacker is in between legitimate entities that are communicating in order to, eavesdrop, reroute, delete, read or modify the data that passes between the two parties (Whitman & Mattord, 2005).
- Buffer overflow: According to Paquet, (2009) a buffer overflow which usually occurs when programs such as C and c++ are not used correctly is a program that writes data beyond its allocated memory buffer and according to Whitman & Mattord (2005) it occurs when a buffer is sent data that it cannot handle resulting in an application program error. As a result

program control data that often is found in memory locations next to the data may execute arbitrary software which maybe be damaging to the host.

- Password Attack: This is a type of attack in which brute force is usually used to discover user accounts and/ or passwords. This attack is usually executed by choosing specific accounts to attack and then using a list of possible passwords. Just like in the packet sniffer attacks once the information is obtained the attacker would use the information to log into the network. Once in the network they have the same privileges as the user whose account has been compromised. If the privileges are sufficient the attacker can install other malicious programs (Paquet, 2009).

2.2.3 Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks

A Denial of Service (DoS) attack is when an attacker sends a large number of requests to a server, usually by using a spoofed IP address. The large amount of requests cause the target system to operate very slowly and, as a consequence, the attacked server becomes unavailable for legitimate requests (Paquet, 2009). On the other hand Distributed Denial of Service DDoS involves sending a large number of requests to a server from different sources at the same time which also results in the server becoming unavailable for legitimate requests (Whitman & Mattord, 2005).

2.2.4 Fragmentation attacks

Fragmentation is breaking down an IP datagram from a network which has big MTU into smaller packets that can be transmitted over media with smaller MTU (RFC 791, 1981). The packet will be reassembled at the other end. In order for the datagram to be reassembled successfully a fragment must be labelled with an identifier and it must know its placement, amount of data it carries and if there are any other fragments that follow it (Anderson, 2001). All this information is placed in the fragment header (RFC 791, 1981).

When routers receive fragments they apply filtering rules to the first fragment and all other subsequent fragments will be treated the same without being checked (RFC 1858, 1995). The tiny fragments attack and the overlapping fragment header can be carried by exploiting this router

behaviour. Tiny fragments attack forces the fragments to be so small so much that not all TCP header information is in the first fragment. Thus, filtering rules might not be applied correctly because there is insufficient header information.

RFC 791, 1981 specifies a reassembly algorithm that allows overwriting any overlapped portions of previously-received fragments. Thus, if the first packet has information that allows it to be forwarded, the fragments that follow which might have overlapping data that will modify TCP header information like destination port will also be forwarded even though they might not have been if all the TCP values had been filtered (RFC 1858, 1995).

Ping of Death is another example of a fragmentation attacks. In this attack an ICMP packet larger than 65535 bytes (maximum ICMP size) is transmitted in small fragments. The destination device might crash or hang because after reassembling the packet it will fail to handle the large ICMP packet. These types of attacks can also be a header manipulation attacks. Fragmentation attacks can be executed as access or DoS attacks.

All the network attacks (reconnaissance, access and DoS) detailed above are possible in both IPv4 and IPv6 networks (Kim et al, 2007 & Radhakrishnan et al, 2007). The only difference might be in how they are executed.

2.2.5 Network attacks common to both IPv4 and IPv6 networks

In the previous sections network attacks that have been plaguing IPv4 networks were explained. The next section highlights how the attacks in the previous section maybe carried out in IPv6 networks

2.2.5.1 Reconnaissance

Network sizes in an IPv4 network are much smaller than the size of a typical IPv6 network so it would seem that scan attacks would not happen in IPv6 networks (Zhao-wen, 2007). This implies that if an attacker had no clue as to which IPv6 addresses are in use in a network then the task of finding active hosts will be very difficult (Convery & Miller, 2004). But, usually, for ease of

configuration, special multicast and unicast addresses for routers and servers are typically used like all routers (FF05::2) and all DHCP servers (FF05::3) which makes it easier for an attacker to find important resources in a network (Convery & Miller, 2004)

2.2.5.2 Access attack

Man-in-the-middle attacks are also possible through the exploitation of the neighbour discovery (ND). ND is used by IPv6 nodes to learn about link-layer addresses of the opposite end of the local link, to identify unreachable local nodes and to resolve duplicate IP addresses (Zhao-wen, 2007). All ND tasks outlined above are possible by neighbour caches which are updated through ND and trusting nodes on the local links. Thus a rogue device can without a problem construct fake ND messages, counterfeit the other node and become man-in-the-middle (Zhao-wen, 2007)

2.2.5.3 Fragmentation related attacks

IPv6 intermediary nodes do not perform fragmentation. Fragmentation is only at the source nodes (RFC 2460). Zagar & Grgic, (2009) explain that a discovery process determines the maximum transmission unit (MTU) to use during a given session and that the minimum recommended MTU size for IPv6 is 1280 octets. It is good security practice to drop all fragments less than 1280 octets unless it is the last packet in the flow (Zagar & Grgic, 2009). By means of fragmentation an intruder can send small packet fragments that are able to bypass security monitoring devices in between the source device and destination device because the security devices do not reassemble fragments as they are intermediary devices (Zagar & Grgic, 2009). By sending a large number of these small packets an intruder can cause an overload of reconstruction buffers on the destination device which can potentially cause the device to crash (Zagar & Grgic, 2009). This can be a form of denial of service. But in general DoS and DDoS can still also be carried out on IPv6 networks in same way they are carried out in IPv4

2.2.5.4 Header manipulation attacks

A typical IPv6 header is shown in Figure 2.3 below.

Version <i>4 bits</i>	Traffic class <i>8 bits</i>	Flow label <i>20 bits</i>	Payload length <i>16 bits</i>	Next header <i>8 bits</i>	Hop limit <i>8 bits</i>	Source address <i>128 bits</i>	Destination address <i>128 bits</i>
---------------------------------	--	--	--	--	-----------------------------------	---	--

Figure 2.3 IPv6 Header Format

In IPv4 optional internet information is found in the header and a router must process them if they are present whereas in IPv6 they are placed in-between the IPv6 header and the upper layer header. Each extension header is identified by a distinct next header value. Six extension headers are defined namely Hop-by-Hop Options, Routing, Fragment, Destination Options, Authentication and Encapsulating Security Payload. RFC 2460, 1999 specification states that each extension header should occur only once except the destination options header which should occur at most twice in an IPv6 header. The specification also states that even though each extension header should occur only once each IPv6 node must accept and attempt to process extension headers in any order and occurring any number of times in the same packet, except for the Hop-by-Hop Options header which is restricted to appear immediately after an IPv6 header only (RFC 2460, 1999). Several extension headers can be used in one packet. This means that one extension header points to another which can point to another. This results in a string of extension headers between the IPv6 header and the transport layer header. If an IPv6 packet is encapsulated in another IPv6 with its own extension headers then the string of extension headers can repeat (Choudhary, 2009). Figure 2.4 exemplifies the chain of pointers that can be formed by the next header option. Such actions pose security threats because the routing headers will be used to circumvent access controls that are based on destination addresses (Zagar & Grgic, 2009). Also an attacker will intentionally use a lengthy sequence of headers to make it difficult for the security devices to inspect transport layer headers (Choudhary, 2009). This means that if many extension headers are embedded in a packet then by using this vulnerability many such packets might be sent to a device which might initiate DoS attacks. In

addition if an IPv6 header is encapsulated in another then data with malicious content will be able to pass through firewalls.

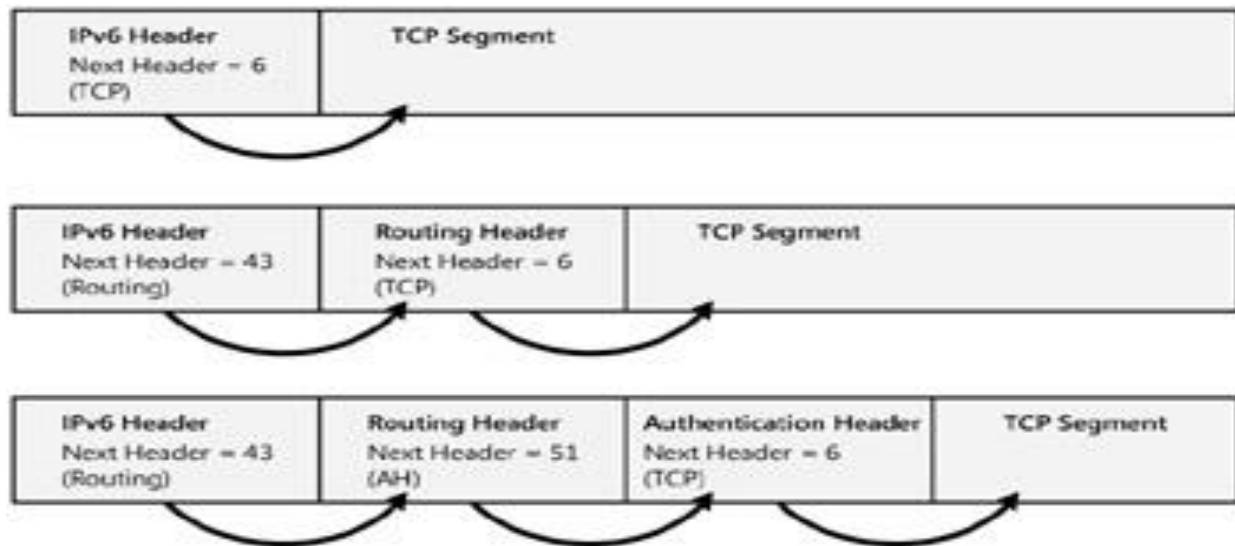


Figure 2.4 IPv6 Extension Header Chaining

(Davies, 2008)

2.2.5.5 Other attacks

It is also useful to note that even though these attacks exist, most attacks occur at the application level (Kim et al, 2007). Examples of application level attacks are web application attacks, viruses and worms. For example few worms have already been detected in IPv6 networks like the slapper worm of 2002 which targeted Apache web servers. (Hogg & Vyncke, 2009). Though, worms and viruses that use scanning to locate vulnerable hosts may find propagation difficulties in IPv6 due to the fact that it might be difficult to scan IPv6 networks (Convery & Miller, 2004).

Network attacks that do not target the network layer in the TCP/IP model will occur in the same manner in either of IPv4 or IPv6. At the network layer most attacks that are rampant in IPv4 are still possible in IPv6.

2.3 Threats in IPv6 Networks

In addition to the threats that are the same with those in IPv4, IPv6 networks are susceptible to misuse of ICMPv6 and multicast attacks.

2.3.1 Misuse of ICMPv6 and multicast

Neighbour discovery uses five types of ICMPv6 messages namely Router Solicitation, Router Advertisement, Neighbour Solicitation, Neighbour Advertisements and Redirect message. A 'packet too big' is a type of ICMPv6 message required for the MTU discovery. Therefore, a few ICMPv6 message types must be allowed in order for the IPv6 network to work properly. ICMPv6 specification also allows an error notification response to be sent to multicast addresses. Zagar & Grgic, (2009) suppose that if a packet was to be sent to a multicast address; an attacker could cause multiple responses from the pool of multicast nodes to target a victim in this case with the spoofed source of the multicast packet

2.4 Summary

Security should be a primary concern of network administrators, whether the network uses IPv4 or IPv6. In this section it has been highlighted that both IPv4 and IPv6 are at the internet layer of the TCP/IP protocol suite. By exploiting Internet layer vulnerabilities attacks may target other layers like the application and transport layers. In addition, some common IPv4 networks and IPv6 network attacks were explained. Attacks common in both IPv4 networks and IPv6 networks were outlined. Table 2.1 below summarises the attacks identified to plague IPv4 and Ipv6 networks in this chapter.

Network Attack	Originating layer	Impact	Possible in IPv4	Possible in IPv6	Does it affect other layers
Ping Sweep	Layer 3	Identification of IP addresses	Yes	Yes	No
Packet sniffing	Layer 2-7	Captures all information about traffic in a network	Yes	Yes	Yes
Port Scan	Layer 4	Services running	Yes	Yes	No
Mai-in-the-middle	Layer 7	Modification ,rerouting and/or deletion of data in transit	Yes	Yes	yes
Buffer overflow	Layer 7	Application program errors	Yes	Yes	Yes
Password Attack	Layer 7	Unauthorised access	Yes	Yes	No
DoS	Layer 7	Limited or no access to networked resources	Yes	Yes	Yes
Fragmentation attacks	Layer 3	DoS	Yes	Yes	Yes
Header manipulation	Layer 3	Circumventing access control	No	Yes	Yes
Virus	Layer 7	DoS	Yes	Yes	Yes
Worms	Layer 7	DoS	Yes	Yes	Yes
Misuse of ICMPv6 and multicast	Layer 3	DoS	No	Yes	No

Table 2.1 Network Attack Summary

Chapter Three – Network testing

3.1 Introduction

The objective of the research was to find out if there is a difference in network security levels between IPv4 and IPv6 configured networks at PON. The PON network was tested for security in its current state of configuration, which is utilizing IPv4, and then emulated an IPv6 network and also tested for security. From the results obtained, it was determined if implementing IPv6 makes a network more secure. In order to test the network, the appropriate method of testing must be chosen. The following section highlights some of the possible network testing techniques that can be used.

3.2 Network Security Testing

Network Security Testing involves assessing a network for vulnerabilities that exist within the network. It involves subjecting a network to different probes or audits that determine whether the network is secure or that determine the level of security in comparison to a theoretical ideal secure network. Network Security Testing encompasses testing and verification of network-related security controls on a regular basis to find facts about the integrity of an organization's network associated systems (NIST Special Publication 800-42, 2003). After testing a network for security, it should be possible to identify the vulnerabilities and the risks that are associated with those vulnerabilities. Vulnerabilities in a network must be known because they can be exploited and used to gain access into network by unauthorized persons.

There are various types of testing that can be conducted as part of Network Security testing, which include, but not limited to: (NIST Special Publication 800-42, 2003) Network Scanning

- Vulnerability Scanning
- Password Cracking
- Log Reviewing
- Integrity Checkers
- Penetration Testing

All the testing methods listed above will be discussed in the next sections. Network Scanning and Vulnerability Scanning which are incorporated in Penetration Testing will be discussed in section 3.2.3. Password cracking has been described in section 2.2.2. Log reviewing and File Integrity Checking will be discussed next.

3.2.1 Log Reviewing

NIST Special Publication 800-42, (2003) says that system logs generated from IDS logs, server logs or any other logs that collect audit data on systems may be used to identify deviations from the organizations security policies. Since it is cumbersome to manually go over system logs, it is recommended to use automated tools to summarize the log contents.

3.2.2 File Integrity Checking

Wiles and Reyes (2007) state that file integrity checkers are tools that prove that files have not been altered. These tools can be used by network security testers to check whether files have been altered. Process Monitor on Windows 7 and Server 2003 SP1 are examples of File integrity checkers. NIST Special Publication 800-42, (2003) mention that file integrity checkers are usually embedded in IDS systems

3.2.3 Penetration Testing

Penetration Testing is the process of evaluating the security posture of a network (Cunningham, et al, 2007). Penetration testing is a security testing is al all inclusive technique that aims to find vulnerabilities and network security threats (Duan, Zhang & Gu, 2008). With Penetration Testing one can evaluate the security flaws and vulnerabilities in a network. A Penetration Test aims to demonstrate that if the network characteristics, its environment and its state are considered as is then one would be able to violate the site security policy (Bishop, 2003). Therefore, a Penetration Test confirms whether the current security measures are effective, or not. Penetration Testing involves network scanning, vulnerability detection and exploiting the vulnerabilities in order to gain access to the network.

Depending on the information available to the tester, the Penetration Test may be classified as white box, black box testing or grey box testing. White box testing is when the tester is given complete information about the network including network diagrams, some IP addresses, source

code, etc. This might be an employee in the organization Black box testing assumes there is no prior knowledge about the network before beginning the test. Thus the tester needs to ascertain the network location and assets before beginning the test. This is usually how the malicious attacker begins. Grey box testing is when the tester has partial information about the network at hand. (Harper, Harris, Ness, Eagle, Lenkey, Williams, 2011). In addition a penetration test maybe classified as internal or external. An internal penetration test aims to evaluate the security posture of the network using resources that are within the network. An external penetration test aims to evaluate the security posture of a network from outside the network. An internal penetration test aims to: (Cole, 2009)

- Obtain unauthorized connection and access to the network
- Determine the network architecture
- Identify the OS
- Identify OS vulnerabilities
- Obtain protected information from the network and its associated resources
- Evaluate response of any installed intrusion detection systems
- Determine if there are any unauthorized items connected to the network

While external Penetration Testing which strives to find security holes within a network from outside the network boundary aims to:

- Determine the network OS
- Determine OS vulnerabilities
- Obtain unauthorized entry to the internal network
- Gather information about the internal network
- Obtain information stored on internal network resources
- Test the external intrusion detection system (IDS)
- Test the firewall

Thus a penetration test maybe classified as one of the following; Internal –white box, Internal – grey box, Internal – black box, External – white box, External – grey box or External- black box. A

penetration test generally follows three steps, namely Network Scanning, Vulnerability Detection and Vulnerability Exploitation.

3.2.3.1 Network Scanning

The first step in Penetration Testing is Network Scanning. Network scanning is about gathering information about the target network. It involves determining active hosts, OSs and the services and ports running on those active hosts (Orebaugh, & Pinkard, 2008). Network Scanning is comprised of: (Orebaugh, & Pinkard, 2008).

- Network Mapping: Sending messages to a host that will generate a response if the host is active. For example ping sweeps discussed in section 2.2.1 which determine that a host is active if it replies an ICMP echo request.
- Port Scanning: Sending messages to a specified port to determine if it is active
- Service and Version Detection: Sending specially crafted messages to active ports to generate responses that will indicate the type and version of service running
- OS Detection: Sending specially crafted messages to an active host to generate certain responses that will indicate the type of operating system running on the host

Furthermore, current network scanners can hide their source address, bypass firewalls and provide reports based on their findings (Orebaugh, & Pinkard, 2008). Nmap is an example of Network Scanning software.

3.2.3.2 Vulnerability Detection

The second step in Penetration Testing is Vulnerability Detection. Vulnerability is defined as a programming error or misconfiguration that can give unauthorised users access to network resources (Rogers, 2008). A vulnerability scanner can be used for vulnerability detection by confirming that vulnerabilities exist in a network (Beaver, 2010). These scanners do not exploit the vulnerabilities but simply identify settings that verify that vulnerabilities exist (Seagren, 2007). Examples of vulnerability scanning software are Nessus, X-Scan and QualysGuard

3.2.3.3 Vulnerability Exploitation

The final step in Penetration Testing is Vulnerability Exploitation. After identifying the vulnerabilities in the system the next step is to find ways in which the security loopholes can be

used to penetrate the network. Beaver, (2010) highlights that after identifying security holes you can then do all or some of the following; gain further information about the host and its data which was not obtained in the first step of Penetration Testing. The tester may obtain a remote command prompt, start or stop certain services or applications, capture screen shots, access sensitive on the compromised host. Further, using the compromised host, the tester can launch another type of DoS attack, access other systems, disable logging or other security controls, send an e-mail as the administrator and perform SQL injection attacks. Finally the tester can upload a file proving victory. An example of software that be used to exploit vulnerabilities is Metasploit.

In order to carry Penetration Tests successfully the tester needs to use some tools in order to be able to do network Scanning, Vulnerability Detection and Vulnerability Exploitation.

3.2.3.4 Penetration Testing Tools

There are many tools that can be used to perform Penetration Testing. Penetration Testing tools may include techniques and software. Software products consist of both commercial and free software. Commercial products include; Core Impact, QualysGuard and Internet Scanner. Free tools for penetration testing that are available include Wireshark, Nmap, Metasploit, Nessus and Cain and Abel, etc. Due to lack of funds to purchase commercial products free tools were explored. In addition many free software tools such Nessus and Metasploit are among the best security testing tools (Sectools.org, 2006). Below is a list of the free penetration test tools that were explored in greater detail

3.2.3.4.1 Wireshark

WireShark is a network protocol analyser. It is used for network troubleshooting, analysis, software and communications protocol development, and education. It runs on most computing platforms such as Windows, Unix and Linux (Orebaugh, 2007; Sanders, 2011). It is used by network administrators to troubleshoot network problems, by network security engineers to examine security problems, by developers to debug protocol implementations and by students to learn the TCP/IP protocol (Wang, Xu and Yan, 2010).

3.2.3.4.2 Network Mapper (Nmap)

Nmap is an open source utility for network exploration and security auditing and systems and network administrators use it for network inventory, managing service upgrade schedules, and monitoring host or service uptime (Lyon, 2009). Nmap works by creating IP packets from scratch and sending them to determine hosts, services (application name and version) those hosts are offering, operating systems and OS versions that they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics (Lyon, 2009; Orebaugh, & Pinkard, 2008). Initially it was intended for scanning enterprise networks, but it works well with single hosts (Lyon, 2009).

3.2.3.4.3 Metasploit

Metasploit project is an open source computer project for penetration testing. Metasploit webpage states that Metasploit helps security and IT professionals detect security issues, verify vulnerability mitigations, and that it is able to manage expert-driven security assessments. It provides information about security vulnerabilities and uses the exploit code to abuse the target system or compromise it. According to Gregg, (2008) the following basic steps are taken in exploiting a system using Metasploit: First Step is to choose and configure an exploit. An exploit is code that will enter the target system by using its vulnerabilities. There 300 exploits for windows and Linux. Secondly verify that the targeted host is susceptible to the chosen exploit. The third step is to choose and configure a payload and unlike step one this code will be executed on the compromised system. The forth step is choose a technique that hides the payload from being detected by an IPS. The fifth and final step is to execute the exploit

3.2.3.4.4 Nessus

Nessus is a free open source vulnerability scanner. Nessus is able to do high-speed detection, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of network security posture (Tenable Network Security, 2011). Nessus is not only able to detect vulnerabilities but it is also able to determine the level of risk the vulnerability poses for an organization (Rogers, 2008).

3.2.3.4.5 Cain and Abel

Cain & Abel is used to retrieve many kinds of passwords for Microsoft Operating Systems by sniffing the network (Montoro, 2011). It is able to crack encrypted passwords using Dictionary, Brute-Force (Montoro, 2011). In addition, it can be used for “Cryptanalysis attacks, recording of VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analysing routing protocols” (Montoro, 2011). Cain and Abel is able to: (Montoro, 2011)

- Recover passwords and credentials from various sources.
- Allow ARP poison routing which enables sniffing on switched LANs and Man-in-the-Middle attacks.
- Analyse encrypted protocols such as SSH-1 and HTTPS
- Capture credentials from a wide range of authentication mechanisms.
- Monitor routing protocols authentication and extract routes,
- Crack password/hash calculators, several specific authentications, hashing algorithms, etc using dictionary and brute-force crackers

3.2.3.4.6 NetStumbler

NetStumbler is a Windows tool for finding open wireless access points. It is used to detect wireless local area networks, list all the Wi-Fi networks, their signal strength and whether they are password protected or not (Norman, 2011). It is also able to discover unauthorized access points and find locations with poor coverage in your WLAN (Norman, 2011).

Following is table that summarises the Penetration Testing tools discussed in section 3.2.3.4

Tool	Category	Features	Platform	IPv6	IPv4
Wireshark	Network sniffer	Network troubleshooting Network analysis	Windows Unix Linux	yes	yes

		Software and communications protocol development			
Nmap	Network scanner	Finding open ports Determining OSs Determining services	Windows Unix Linux Mac OS	yes	yes
Metasploit	Vulnerability exploitation	Compromise target systems	Windows Linux	yes	yes
Nessus	Vulnerability scanner	Detect vulnerabilities Determine vulnerability risk level	Windows Linux Mac OS	yes	yes
Cain and Abel	Vulnerability exploitation	Determine passwords	Windows	yes	
NetStumbler	Network Scanning	Detect wireless networks Detect Access points	Windows	yes	

Table 3.1 Penetration Testing Tools

3.6 Summary

Network testing is a fundamental step in evaluating the security status of an organization. A network security test is essential to any system or network administrator because it informs the administrator about the security loopholes in the networks. Testing a network involves many parameters like network scanning, log reviewing, file integrity checking, penetration testing, etc.

Chapter Four -Testing PON Network using Penetration Testing

4.1 Introduction

To test for IPv4 and IPv6 network security differences Penetration Testing was chosen because it would give results better suited for giving differences in network security, as will be discussed in this chapter. A further factor was that most of the tools that were required to conduct a penetration test were free. The tests were conducted on the PON IPv4 production network and on an IPv6 island network that emulated the PON IPv4 logical topology. This chapter will discuss how the Penetration Tests were carried out. The PON Acceptable ICT Use Policy is discussed because it is used as the benchmark for showing when vulnerability has been successfully exploited.

4.1.1 Why use Penetration Testing?

A penetration test can never prove the non-existence of vulnerabilities but, rather their existence. The aim was to show that vulnerabilities do exist in both IPv4 and IPv6 but what needed to be ascertained was whether there was any difference in the risk levels associated with those vulnerabilities. In addition penetration testing was used because according to Budiarto, et al, (2004) a penetration test:

- Confirms whether the current security measures are effective, or not
- Identifies the types of information available to the attacker and whether such information is hazardous or not depending on the different testing scenarios.
- Helps to identify the information that is exposed to the public or the Internet world.
- Is an effective method as it is “proof of concept” that the measures taken to secure the network are not effective.
- Penetration testing helps to identify and narrow down security risks

Penetration Testing was thus chosen because it would confirm whether the ‘Acceptable ICT Use Policy’ of the PON is effective in the IPv4 and IPv6 networks. It would show which information is available to unauthorised users and it would help the PON network administrators identify the

vulnerabilities in the IPv4 network and the kind of vulnerabilities they would be exposed to once they implement IPv6 in their network.

4.1.2 PON Acceptable ICT Use Policy

The PON has an Acceptable ICT Use Policy which identifies confidential information as the following; Institution corporate strategies, strategic planning, trade secrets, customer lists, student records, payroll, personal and research data. The Policy also states that one is prohibited from “accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access” (Acceptable ICT Use Policy).

Thus, using penetration testing the network both the IPv4 and IPv6 networks were tested to check whether the following could be determined through use of tools:

- Identify hosts, open ports, operating systems, and services
- Determine vulnerabilities
- Exploit vulnerabilities by:

4.1.2.1 Reading confidential information

Institutional corporate strategies, strategic planning information, student records and payroll are some of the information that the PON recognizes as confidential. Using the penetration test we wanted to test if it was possible to gain access to any of the information recognized as confidential. After accessing the confidential information, test to determine whether it could be edited or printed.

4.1.2.2 Change data stored in the system

This would be used to see whether someone who has unauthorised access can escalate their rights and be able to change any of the information stored in the PON systems.

4.1.2.2 Impersonate a User

Impersonating a user in this case meant that we would pretend to have credentials of an authorized user and then gain access to the system.

Finding vulnerabilities and exploiting them does not mean that the penetration testing was successful because the ‘said’ vulnerabilities might be accepted in the network being tested. Thus,

the PON Acceptable ICT Use Policy which highlights what should not happen in PON network was used to measure whether the Penetration Tests were successful.

4.2 Available Information

The test that was carried out was an internal- grey box test because the testers had complete knowledge of the test IPv6 island network and some information as to how the PON network is setup and which devices are in the network. Island network means that the IPv6 network was not connected to any network. To test IPv4 network security we used the PON live network and for IPv6 network security an island network was used. The PON production network diagram and the IPv6 island network diagram are shown below.

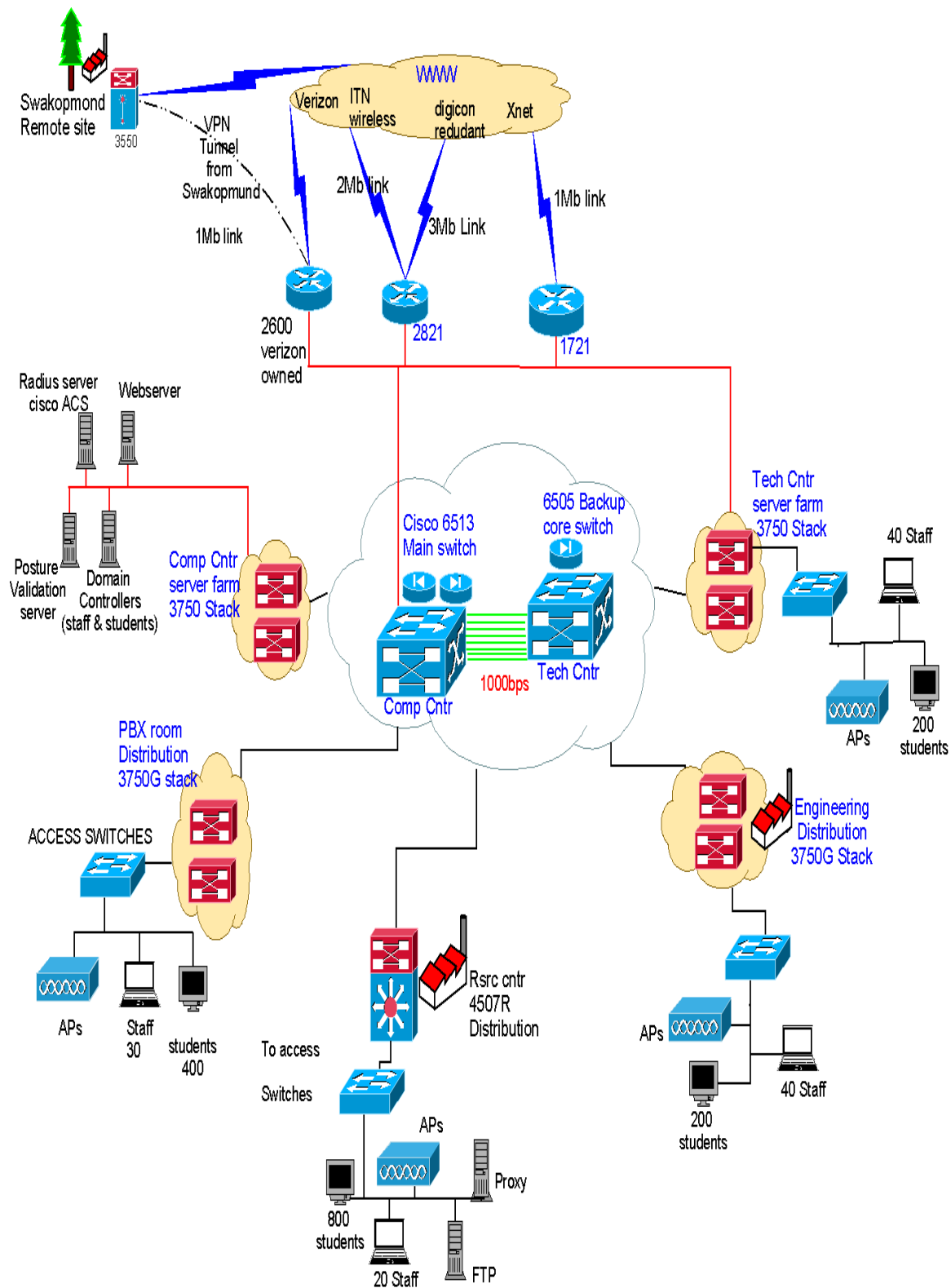


Figure 4.1 PON Production Network

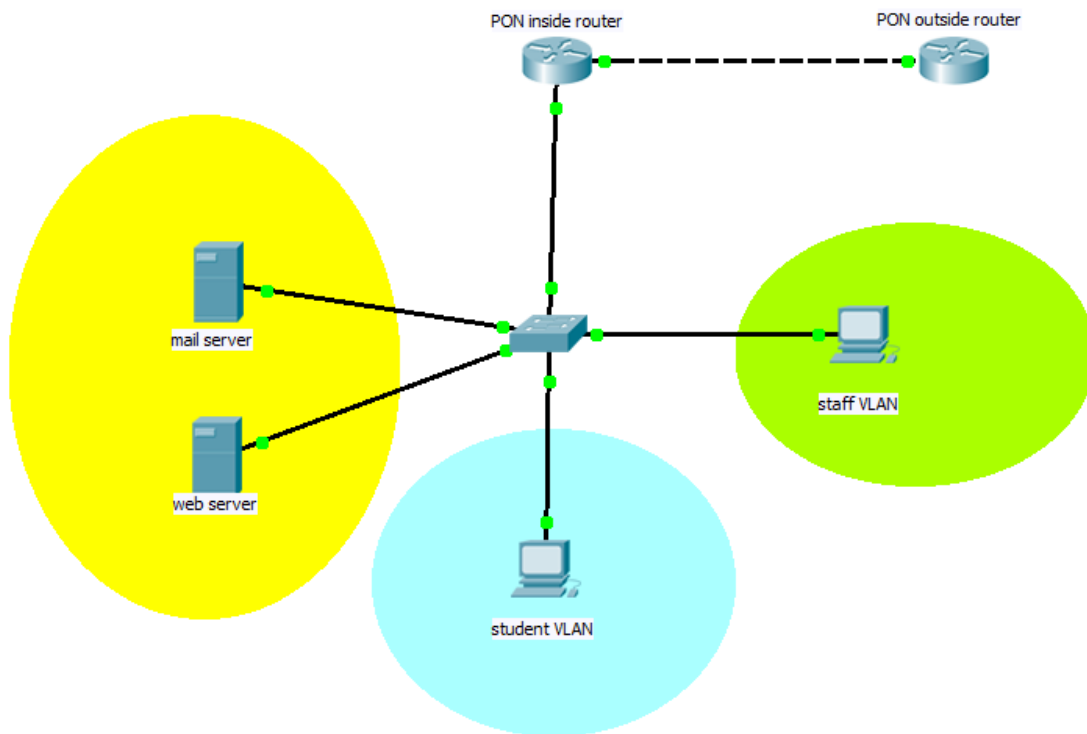


Figure 4.2 IPv6 Island Network

Figure 4.1 shows the PON IPv4 production network. The diagram shows the logical network topology of the PON IPv4 network. Figure 4.1 also shows that there is one central device the cisco 6513 from which servers, access points, and distribution switches connect. It is also the device that hosts the firewall and IPS modules. The IPv6 shown in figure 4.2 network was also designed in a similar manner. The PON inside router a cisco 2811 is the central point which has servers and distribution switches connected to it. Both the IPv4 and IPv6 penetration tests were conducted from the Staff VLANs.

4.3 Testing Constraints

The next section discusses the limitations to the penetration tests that were conducted. The constraints discussed had implications to the outcomes of the research.

4.3.1 Time

Time was a limiting factor to the testing process. In order to utilize the testing tools efficiently, the author needed sufficient time to learn how best to use them. Through this learning process it was also necessary to identify which tool was right for which vulnerability. The time to carry out the experiments was limited because of work and family commitments. Thus, the right tools might not have been chosen for testing also the best testing procedures might not have been followed. Although due care was taken in the time available to know as much as possible about the tools and then choosing appropriately.

4.3.2 Risk Issues (production and island networks)

As some of the systems in PON network are too critical to bring down were only able to find vulnerabilities could only be found not exploited. For example, DoS attacks could not be performed on the live PON IPv4 network. This was communicated to the author via email by the PON network administrator (appendix F). There was not enough insight as to how Metasploit was going to exploit the found vulnerabilities found. As such it was not used to exploit vulnerabilities because it could execute DoS attacks in the PON network. In order to match the results with that of IPv4 the IPv6 island network was also just tested for vulnerabilities. Another limiting factor was that there was no concrete way of saying that the IPv6 test network is a true representation of the PON network as there is no one with a complete network diagram of PON network. The network seen previously is a rough sketch of what the IPv4 network might be looking like. In line with this also was the fact that the test IPv6 network may not be secured as well as the production network or it might be more secured than the production network. There was no way of really saying it is in which state but due care was taken to emulate as much as possible the security controls that exist in the IPv4 production network to that of the IPv6 test network.

4.3.3 Confidentiality

On areas that need consulting with experts in the field of network security, this was not possible because of the agreement signed between the author and the PON Bureau of Computer Services (Appendix D). The agreement did not allow divulging confidential information to any third parties. As a result the authors did not get good advice from the specialists in the field.

4.4 Penetration Test Scope

The penetration tests were used to find out the vulnerabilities that exist in the PON production network and the IPv6 island network and to what extent these vulnerabilities could be exploited. By doing this it could be determined if vulnerabilities exist and their associated risk levels.

Therefore, in order to find out if the above can be achieved in PON network the following the steps were undertaken.

4.5 Testing Procedure

Below are the steps that we followed in order to perform the penetration test. The same procedures were followed for both the IPv4 and IPv6 environments. The steps taken followed those recommended by Whitaker & Newman, (2006)

4.5.1 Information Gathering/foot printing

First thing was to gather the information that was available. At this stage the hope was to get domain names, server names, and IP addresses of hosts. In line with this the testers attempted to get operating systems, and applications running on the active IP addresses by doing a port scan with Nmap. As mentioned earlier the choice of tools were mainly because they were free and Nmap is listed as one of the best scanning tools by Sectools.org, (2006).

4.5.2 Discovering vulnerabilities

After gathering the information and identifying systems in the network, the aim was now to determine the vulnerabilities that exist in the network. The tool that was used to determine the vulnerabilities is Nessus again for the reasons mentioned above. The tool was also used to determine the risk levels associated with the found vulnerabilities

4.5.3 Result documentation

The results obtained from conducting the test are highlighted in the next chapter.

4.6 Summary

This section outlines that to test for network security penetration testing was used. It is explained why penetration testing was chosen and the steps that were followed in order to carry out the tests. In order to mark the success of the penetration tests conducted the Acceptable ICT use

Policy was used. The PON Acceptable ICT Use Policy describes what should happen in the PON network. Limitations that impact on the results obtained were also discussed

Chapter Five - Results and Analysis

5.1 Introduction

This chapter reports on the results obtained from the tests and graphical analysis of Penetration Testing which was chosen as the method to test IPv4 and IPv6 network security. The tests were conducted on the PON IPv4 production network and on an IPv6 island network that emulated the PON logical topology. The chapter will give the details on the results obtained from the information gathering stage and vulnerability detection stages in the IPv4 and IPv6 networks. How the tests were conducted has already been discussed in chapter four, thus this chapter focuses on the actual results obtained. The first section highlights the results in the IPv4 production network which confirmed the network attacks possible in IPv4 as highlighted in chapter two. Further in the chapter, results for the IPv6 Island will follow the IPv4 results and they also confirm network attacks possible in IPv6 as highlighted in chapter two.

5.2 IPv4 production network results

The following section highlights the results obtained from the tests conducted in the IPv4 network. The results were obtained from the reconnaissance scans and vulnerability scans

5.2.1 Scope

The Penetration Test was initially held from the 15th of February 2012 to the 29th of February 2012 and again from 8th of May 2012 to 30 May 2012. The aim of the test was to find any security vulnerabilities that exist in the PON network. The test was conducted using the following IP addresses

- 196.12.10.91 – the ITS server,
- 196.10.12.171 – the PON e-mail server and
- 10.1.4.6 – the server in the IT department.
- In figure 4.1 the ITS server is a module in the 6513 switch, the PON email server is in the server farm and the IT server is part of the access devices in the IT department

The test was targeted to these IP addresses as the researcher was aware of which IP addresses were critical to the PON network. The server with IP address, 196.12.10.91, hosts the Integrated

Tertiary System (ITS). This is a critical system that is used by the PON for student records, by human resources, for inventory and for many operations at the PON. The server with IP address, 196.10.12.171, is the PON staff email server that is used for all internal and external communications. The server with IP address, 10.1.4.6, is the server used in the School of Information Technology for student support. Mostly the IT server is used for reading material and announcements for students. The tests were conducted several times as conditions changed in the production network.

5.2.2 Information Gathering

This section highlights the ports that were found open and the successful telnets using the different ports using Nmap. The findings will be grouped according to each server's IP address.

5.2.2.1 ITS Server Nmap Scan

Nmap is an open source utility for network exploration and security auditing. Nmap works by creating IP packets and sending them to determine hosts, services those hosts are offering, operating systems and OS versions that they are running, etc. The screenshot below shows the initial Nmap port scan result for the device with IP address 196.12.10.91

```
C:\Users\csn>nmap -Pn -sS 196.12.10.91 -O -p 80
Starting Nmap 5.51 < http://nmap.org > at 2012-02-23 10:00 Namibia Standard Time
Nmap scan report for prodintvlapp.polytechnic.edu.na <196.12.10.91>
Host is up.
PORT      STATE SERVICE
80/tcp    filtered http
Too many fingerprints match this host to give specific OS details
OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address <1 host up> scanned in 18.54 seconds

C:\Users\csn>nmap -Pn -sT 196.12.10.91
Starting Nmap 5.51 < http://nmap.org > at 2012-02-23 10:04 Namibia Standard Time
Nmap scan report for prodintvlapp.polytechnic.edu.na <196.12.10.91>
Host is up <0.00045s latency>.
Not shown: 996 filtered ports
PORT      STATE SERVICE
443/tcp   open  https
1521/tcp   open  oracle
7777/tcp   open  cbt
7778/tcp   open  interwise
Nmap done: 1 IP address <1 host up> scanned in 48.01 seconds
```

Figure 5.1 ITS Server Nmap scan

As was discussed in chapter four the initial stages of a penetration test involve gathering information about the network, then particular devices. Getting initial information about the network was not necessary as the researcher had knowledge about the IP addresses used and the critical hosts in the network. Figure 5.1 is an Nmap scan of the 196.12.10.91 (ITS server) server. It was necessary to discover the services running on the targeted hosts in order to find ways in which to obtain entry. From Figure 5.1 it can be seen that, at the time of the scan, four TCP ports were open. An open port means that the service listed is listening or accepting packets for that service. The services listed as running on the ports are https, oracle, cbt and interwise. The results also show that the operating system of the host could not be determined

The telnet to the device using the command **telnet 196.12.10.91** would give results: “Connecting To 196.12.18.91...Could not open connection to the host, on port 23: Connect failed”. This means that there was no access to the device and is as a result of the fact that telnet operates on port 23, which Nmap did not discover as being open. However, if the same command was issued with port 1521 specified, for example **telnet 196.12.10.91 1521**, a blank console was returned which further confirms that Oracle is listening on the port. The connection can also be taken to mean we can establish a TCP/IP connection to the ITS server. Since port 1521 is used by Oracle the researcher used the AppSentry Listener security check tool to find out any additional information about the Oracle service running. The AppSentry Listener is a tool that verifies the security status of the Oracle database listener and Oracle applications (Intergrigy, 2012).

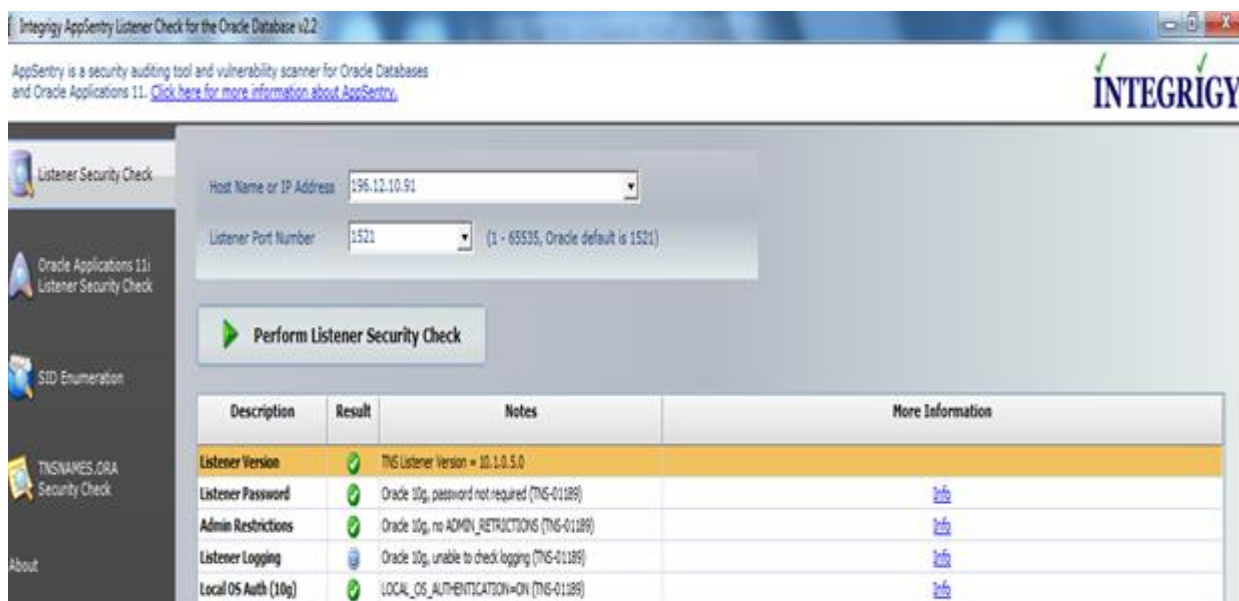


Figure 5.2 Oracle Database Listener Check

It can be seen from Figure 5.2 that no password is set for the Oracle listener and passwords Admin restrictions are not set for the Oracle Database listener. It can also be seen that LOCAL_OS_AUTHENTICATION is set to ON. This means that the listener cannot be managed remotely and thus no further probes could be made.

5.2.2.2 IT Server Nmap Scan

Below is the initial Nmap scan for the device with IP address 10.1.4.6. Figure 5.3 is an Nmap scan of the IT server. As was mentioned in the previous section it was essential to discover the services running on the targeted host in order to find ways in which to obtain access. From Figure 5.3 it seen that, at the time of the scan, 19 TCP ports were open. Some of the services listed are ftp, domain, http, Kerberos –sec, ldap and IIS. Telnet to port 21 was not successful. However, a telnet to port 53, 80, 88 and 139 returned a blank screen which meant that a TCP/IP session could be established. The scans were repeated 3 times on three different days and the scan results were the same.


```
C:\Windows\system32\cmd.exe

C:\Users\csn>nmap -Pn -sT 10.1.4.6

Starting Nmap 5.51 < http://nmap.org > at 2012-02-29 17:10 Namibia Standard Time

Nmap scan report for itstudsrv.itsys.polytechnic.edu.na (10.1.4.6)
Host is up (1.00s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1025/tcp  open  NFS-or-IIS
1027/tcp  open  IIS
1038/tcp  open  mtqp
1048/tcp  open  neod2
1074/tcp  open  warmspotMgmt
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-term-serv

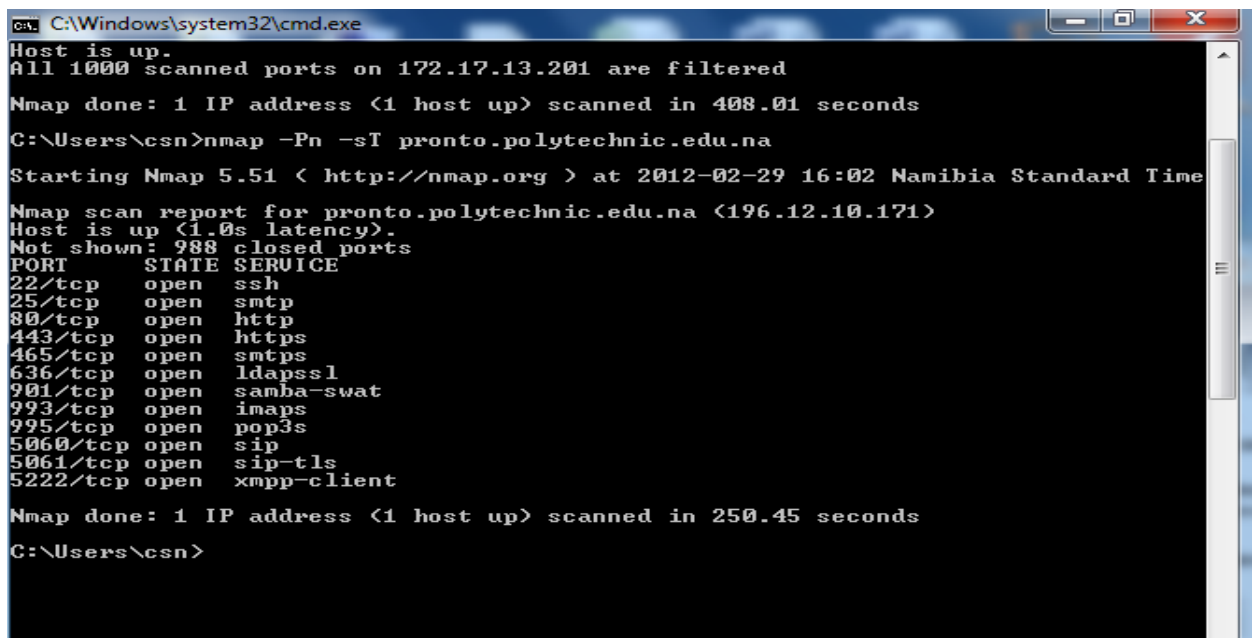
Nmap done: 1 IP address (1 host up) scanned in 225.40 seconds

C:\Users\csn>
```

Figure 5.3 IT Server Nmap Scan

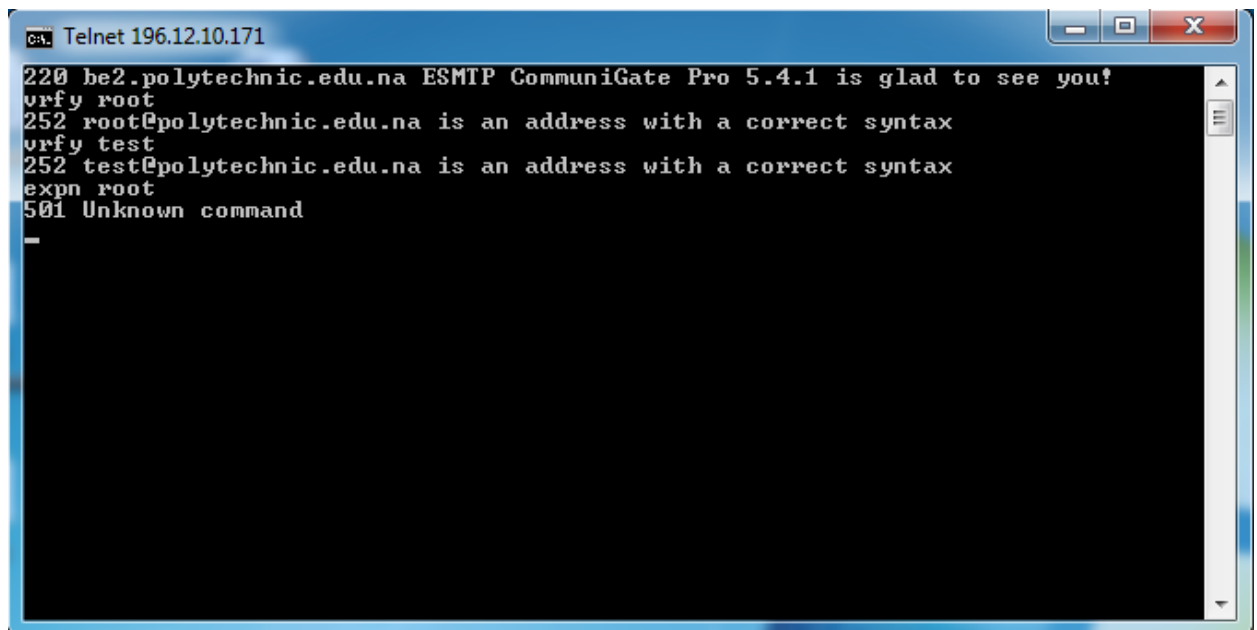
5.2.2.3 PON staff E-mail Server Nmap Scan

Figure 5.4 below shows an Nmap scan of the PON staff E-mail server. When the scan was conducted, 12 TCP ports were open. Some of the services listed are SSH, SMTP, IMAPS, HTTP and SIP. Telnet to port 25 was successful. Repeating the scans yielded the same results as those seen above below in figure 5.4. After gaining access to the server on port 25 the command **vrfy** was used to verify valid users. Two usernames 'root' and 'test', which are common usernames used by system/network administrators were verified as shown in Figure 5.5. Gathering users of a system is also part of information gathering.



```
C:\Windows\system32\cmd.exe
Host is up.
All 1000 scanned ports on 172.17.13.201 are filtered
Nmap done: 1 IP address (1 host up) scanned in 408.01 seconds
C:\Users\csn>nmap -Pn -sT pronto.polytechnic.edu.na
Starting Nmap 5.51 ( http://nmap.org ) at 2012-02-29 16:02 Namibia Standard Time
Nmap scan report for pronto.polytechnic.edu.na (196.12.10.171)
Host is up (1.0s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
443/tcp   open  https
465/tcp   open  smtps
636/tcp   open  ldapssl
901/tcp   open  samba-swat
993/tcp   open  imaps
995/tcp   open  pop3s
5060/tcp  open  sip
5061/tcp  open  sip-tls
5222/tcp  open  xmpp-client
Nmap done: 1 IP address (1 host up) scanned in 250.45 seconds
C:\Users\csn>
```

Figure 5.4 Staff E-mail Server Nmap Scan



```
Telnet 196.12.10.171
220 be2.polytechnic.edu.na ESMTP CommuniGate Pro 5.4.1 is glad to see you!
vrfy root
252 root@polytechnic.edu.na is an address with a correct syntax
vrfy test
252 test@polytechnic.edu.na is an address with a correct syntax
expn root
501 Unknown command
-
```

Figure 5.5 Verifying Users on E-mail Server

This section highlighted the information that was gathered on the different servers using Nmap. What was mostly gathered in this stage were the open ports on the different servers and if any of the open ports could be used for further access.

The next step of the penetration test was to find the vulnerabilities of the ITS, IT and Staff E-mail server. To find the vulnerabilities Nessus Scanner was used.

5.2.3 Vulnerability Detection

This section highlights the vulnerabilities as found by the Nessus Scanner. A 'vulnerability' was defined in chapter three as a programming error or misconfiguration that can give unauthorised users access to network resources. Nessus looks for vulnerabilities and reports on them. The report gives feedback on where the vulnerability was found, the risk of the vulnerability and how it can be resolved. The vulnerability discovered is either reported as a Hole, Warning or Note. A Hole is a severe flaw, a Warning is mild flaw and a Note can be any varied information about the vulnerability. The risk factor is the likelihood of the vulnerability being exploited successfully and the impact the exploit will have after being executed successfully. Risk factors can be classified as being low, high, medium or critical (Rogers, 2008). The classification of the risk factors is based on Common Vulnerability Scoring System (CVSS). CVSS is a model of gauging and elaborating on the effect and features of IT vulnerabilities (Witte, Cook, Kerr & Shaffer, 2012). CVSS has 3 groups each scored from 0 to 10. The 3 groups according to Witte, Cook, Kerr & Shaffer, 2012 are as follows:

- A base group that gives the vulnerability features that are constant over time
- A temporal group that focus on the characteristics of a vulnerability that change over time.
- An environmental group that shows the features of vulnerabilities that are unique to a given organizational environment.

Score is usually based on the Base group but if all are considered then the score is given according to the group with biggest impact (Mell, Scarfone & Romanosky, 2007). This means that if risk factor is measured using the both the base group and the temporal group if the highest risk factor is from the temporal group then the risk factor will be given the score using the temporal group. Nessus Scanner shows which group was used to determine the risk factor.

5.2.3.1 ITS Server Nessus Vulnerability Scans

Below are the results of Nessus scans on the ITS server

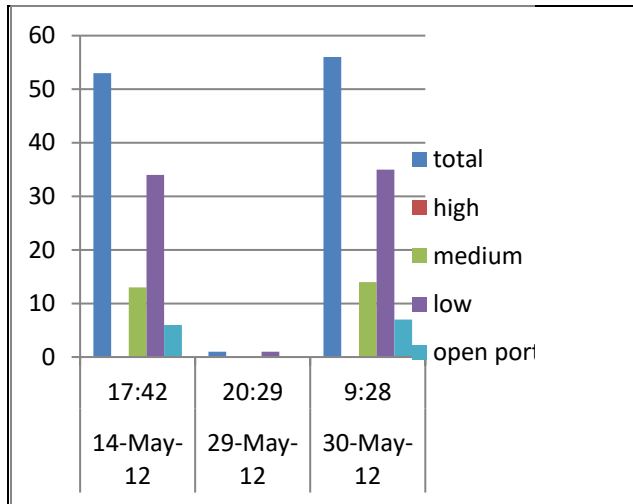


Figure 5.6 ITS Server Vulnerabilities

Referring to Figure 5.6, the following is noted:

- Date indicates the date the test was conducted
- Time indicates the time the test was conducted
- Total highlights the number of vulnerabilities found
- High indicates the number of high risk vulnerabilities
- Medium indicates the number of medium risk vulnerabilities
- Low indicates the number of low risk vulnerabilities
- Open ports – are the number of ports found with vulnerabilities

The graph shows the vulnerability risk factors as categorised by Nessus. In the case of all the risk factors indicated in the graph they were valued using the CVSS base group. This shows that the vulnerabilities

shown here are the same for PON at any given time, given that the configurations have not changed. It is also apparent from the graph that, during the time tested, the Nessus Scanner never detected high risk vulnerabilities on the ITS server. In addition to the risk factors seen in figure 5.6 the following table shows a summary of only the medium risk factors that were discovered in all the reports. Low risk factors were not included in the summary table below because most of them just give information and can be matched with what was discovered using Nmap

Port	Vulnerability	CVSS Score	Exploits	Solution
7779/TCP	HTTP Trace/Track Methods allowed	4.3	available	available
7779/ TCP	Oracle application server portal Authentication bypass	5	available	unknown
7779/ TCP	Apache HTTP server onlyCookie Information disclosure	4.3	available	available
443/ TCP	SSL weak cipher Suites supported	4.3	none	available
443/ TCP	SSL Version (v2) protocol detection	5	none	available
443/ TCP	SSL Medium Cipher Suites supported	4.3	none	available
25/ TCP	Multiple Mail Server EXPN/VRFY Information closure	5	none	available

Table 5.1 ITS Server Medium Risk Factors

From the reports it can be seen that TCP port 7779 had three medium risk factors. One of the problems identified is the vulnerability of HTTP Trace that allows debugging on the server. The base score for the vulnerability is 4.3 and that is classified as a medium risk. Further, the report elaborates that exploits for this vulnerability are available and suggests a solution to mitigate the vulnerability. Another example of the vulnerability detected is that of TCP port 25 which scored a CVSS base score of 5. This vulnerability called Multiple Mail Server EXPN/VRFY Information closure has no known published exploits but a solution on mitigating it is also suggested. All vulnerabilities identified by Nessus Scanner are discussed in a report. Some of them were used to derive table 5.1 above.

On further analysis of the reports, it was seen that the medium risk category overlapped with what Nmap discovered on port 443, though Nmap simply gave the feedback that the port is open. This was the only overlap in the medium risk factor category. Besides the port 443 overlap all the other ports (7777, 7778 and 1521) that were identified by Nmap as open were also found by Nessus and all were classified under low risk categories.

5.2.3.2 PON email server Nessus Vulnerability Scans

Below are the results of Nessus risk factor scans on the PON email server. The labels are the same as those in Figure 5.6.

The scoring was also based on the CVSS base group. The graph looks similar to the one for the ITS server shown in Figure 5.6. As can be seen in both Figure 5.6 and Figure 5.7, the servers have less vulnerabilities after hours.

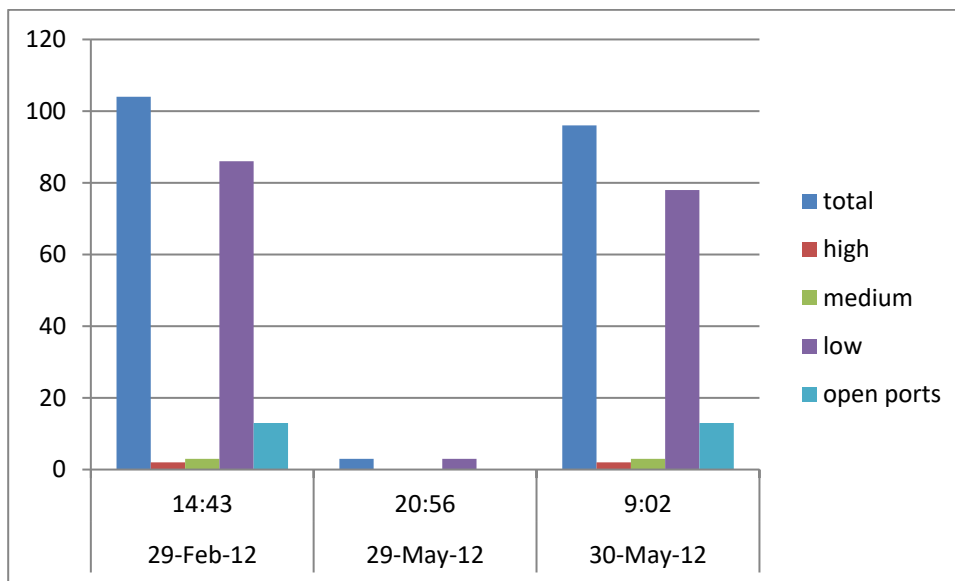


Figure 5.7 Staff E-mail Server Vulnerabilities

Table 5.2 was generated using the reports from the three times the tests were conducted.

Port	Vulnerability	CVSS Score	Exploits	Solution
465/TCP	MTA Open Mail Relaying allowed	7.8	no exploit required	available
443/TCP	Apache WebDAV Module PROPFIND Arbitrary Directory Listing	5	None	available
636//TCP	LDAP NULL BASE Search Access	5	None	available

Table 5.2 PON email server high and medium risk factors

From the reports it can be seen that TCP port 465 had a high risk factor with a CVSS base score of 7.8. This MTA Open Mail Relaying allowed vulnerability allows an unauthenticated remote user to use the mail server to send emails. This is usually targeted by spammers. This vulnerability requires no exploits just getting entry is enough to enable the unauthenticated user to use the mail server like an ordinary

client. Thus no exploits required shown in table 5.2 means that for a vulnerability of such a nature is discovered no further tools or exploits are needed in order to use it for the intruder's purposes. None on the other hand means that an exploit is needed for further access but Nessus Scanner does not know about it or it is not available. Possible solution to this problem was also given in the reports. The other two vulnerabilities shown in the table are medium risk vulnerabilities with no known exploits but the suggestions on mitigating them are available from the reports.

The open ports shown in Table 5.2 were also discovered by Nmap. Besides the three ports shown in Table 5.2, all other ports discovered by Nmap were also discovered by Nessus, but they were classified as low risk vulnerabilities.

5.2.3.3 IT Server Nessus vulnerability Scans

Figure 5.8 shows the results of Nessus risk factor scans on the IT server. The labels mean the same as those shown in Figure 5.6. The scoring was also based on the CVSS base group. This server has quite a number of medium risk vulnerabilities and a few high risk vulnerabilities as can be seen in Figure 5.8. From the detailed Nessus reports the following table could be used in summary.

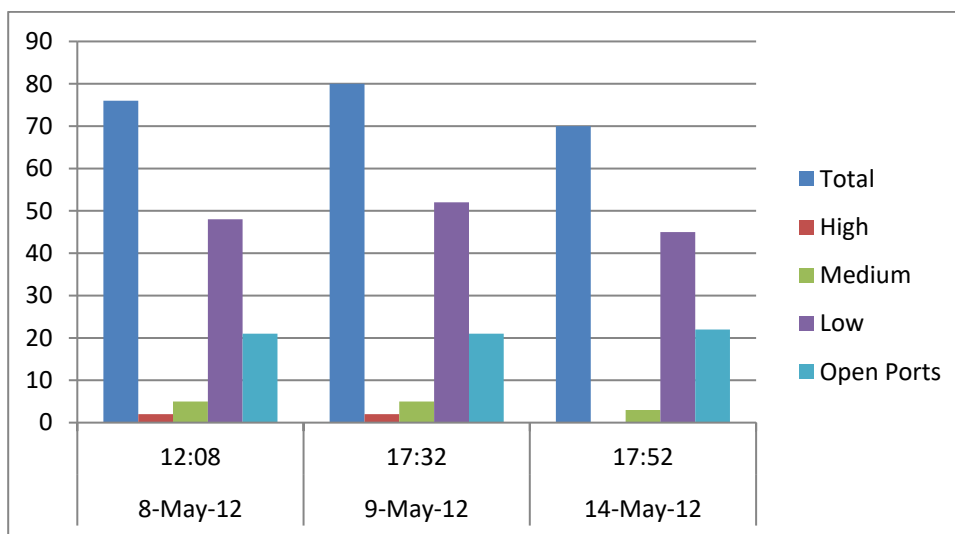


Figure 5.8 IT Server Vulnerabilities

Port	Vulnerability	CVSS Score	Exploits	Solution
445/TCP	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution	10	None	available
445/TCP	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (unauthenticated check)	10	None	available
445/TCP	SMB Use Host SID to Enumerate Local Users Without Credentials	5	Available	N/A
445/TCP	Microsoft Windows SMB NULL Session Authentication	5	Available	available
445/TCP	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials	5	Available	available
3389/TCP	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	5.1	None	available
53/UDP	DNS Server Cache Snooping Remote Information Disclosure	5	None	available
3389/TCP	Terminal Services Encryption Level is Medium or Low	4.3	None	available

Table 5.3 IT server high and medium risk vulnerabilities

The table shows that this server has two critical risk factors with a CVSS base score of 10. These vulnerabilities could cause the server to crash or to be targeted with a DoS attack. These vulnerabilities can be mitigated using the solution suggested by Nessus. We can also see that all these high risk vulnerabilities are on port 445 and that no exploits are needed. An attacker getting to know the vulnerability is all the knowledge the attacker needs to be successful. Additionally we can see from Figure 5.3 and Table 5.3 that there is an overlap with ports discovered by Nmap and the ports associated with their vulnerabilities discovered by Nmap.

Section 5.2 gave an overview of the vulnerabilities that were discovered on the ITS server, the PON staff email server and the IT server. It was seen that the ITS server never has high risk vulnerabilities but the email server and the IT server do sometimes have high risk vulnerabilities. All servers showed that they do have low and medium risk vulnerabilities at any given time.

5.3. IPv4 Vulnerability Analysis

Looking at the Nessus Scan results gathered for the identified servers, it can be observed that there is high total of risks during production hours. PON production time is from 07:30 – 16:30hrs. During this time high risk vulnerabilities were being detected. At any other time the total number of vulnerabilities is relatively low. So from this it be deduced that the servers are most vulnerable during production hours.

The table that follows summarises the results from the Nessus scan for the PON as follows

Time	High risk vulnerabilities	Medium risk vulnerabilities	Low risk vulnerabilities	Open ports
Production hours	≤2	≤14	≤86	≤22
After 18:00	none	none	≤3	none

Table 5.4 Nessus Vulnerability Scan Summary

As was stated earlier in section 5.2.3 risk factor rankings are based on the CVSS base group scores. CVSS scoring is a framework used to rate and expand on the effects and characteristics of IT vulnerabilities. From the results shown in Table 5.4, the PON production network is at the highest risk during production hours and the total number for any type of vulnerability is greater during production hours.

5.4 IPv4 Network Test Conclusions

From the results highlighted above it can be seen that an IPv4 configured network is susceptible to network attacks. In this case the reconnaissance attacks using Nmap scans and Nessus scans were successful. It can be seen from the Nessus reports that an access attack will also be successful in this network. For example, if the Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness were to be exploited then this would be an access attack. Another example would be the MTA Open Mail Relaying allowed vulnerability highlighted in Section 5.2.3.2. The two vulnerabilities; MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check) and MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution vulnerabilities could be used for DoS attacks as was highlighted in the Nessus reports in Section 5.2.3.3. From the results it has been shown that from inside the PON network the devices tested are vulnerable to Reconnaissance, Access and DoS attacks.

The following section will show the results that were obtained in the IPv6 island network in the information gathering and vulnerability detection tests.

5.5 IPv6 Island Network results

The Penetration Test was initially on the 29th of June 2012 and again on 21st of September 2012. The test was repeated because the ones obtained on the 29th of June were insufficient for comparison with

the IPv4 production network results. The aim of the test was to find any security vulnerabilities that exist in the IPv6 island network. Referring to Figure 4.1 the tests were conducted on the

- mail server and web server with IPv6 address fec0:2::4
- the staff PC with IPv6 address fec0:3::2

5.5.1 Information Gathering

Further tests were conducted in the IPv6 island network. The tests were conducted once, as the conditions in the island network were not changing. The island network was configured with feC0:3::0 /64 in the staff VLAN and fec0:2::0/64 was used in the server VLAN.

Due to a lack of equipment, the mail and web server were configured on one device.

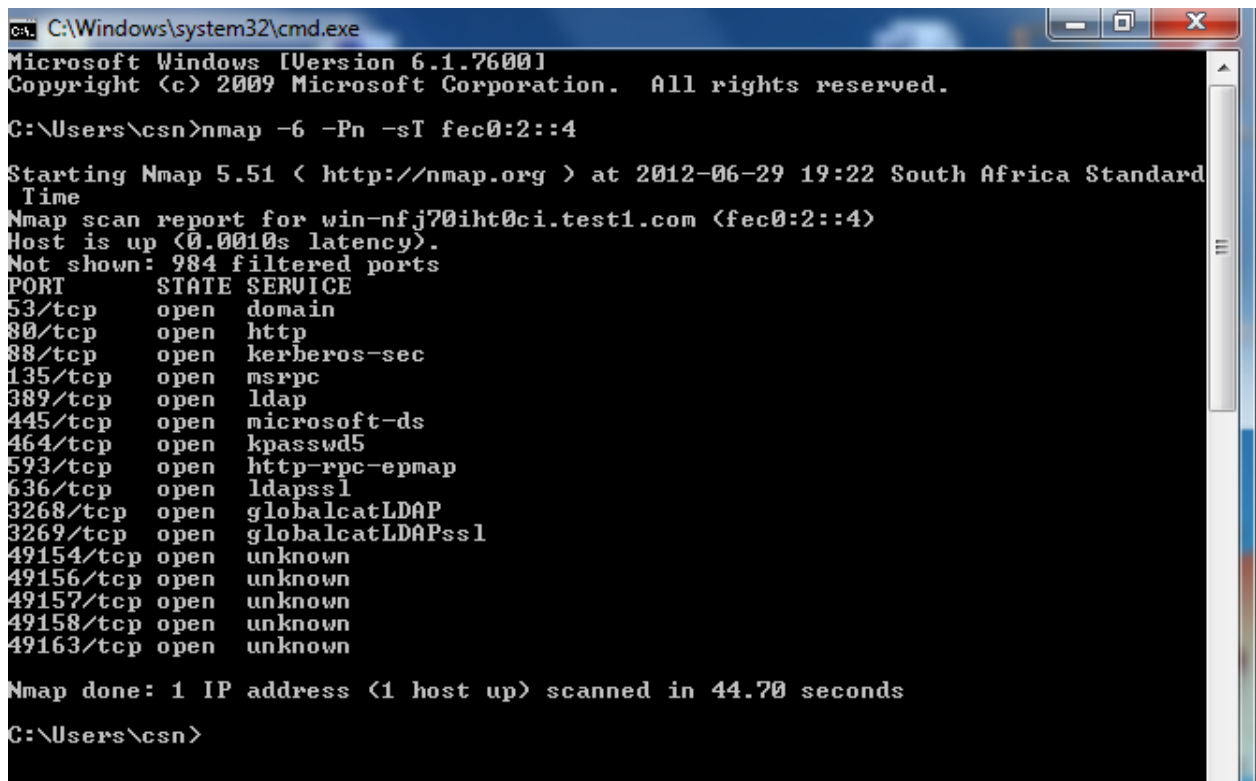
As in the case of the IPv4 Penetration Test; the IPv6 island network Penetration Test had to go through the Penetration Testing stages as discussed in Section 3.2. Thus, the Penetration Test had to go through the information gathering stage, vulnerability detection stage and, finally, the vulnerability exploitation stage. It was not necessary to gather any information about the IPv6 island network as the network was specifically set up for testing purposes. The IPv6 addressing scheme was already known, so the next step was to find which services could be detected by the scanning software. Nmap and Nessus were used in the IPv6 network so that results could be comparable to those of the IPv4 network scans.

The next section highlights Nmap scan results. The findings will be grouped according to the IPv6 address.

5.5.1.1 FEC0:2::4 Mail and web server

Figure 5.9 below is an Nmap scan of the IPv6 mail and web server host. It was also necessary in the IPv6 network to find out the services running on the targeted hosts in order to find ways in which to obtain entry. From Figure 5.9 it can be seen that at the time of the scan 16 TCP ports were discovered. An open port will still have the same meaning. That is to say, an open port is listening for traffic for the service listed. Some of the services listed as running on the ports are HTTP, LDAP, domain and globalcatLDAP.

Telnet to the server using different port numbers would give a blank screen just like in the IPv4 case. This shows that a TCP/IP connection could be established.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\csn>nmap -6 -Pn -sT fec0:2::4

Starting Nmap 5.51 ( http://nmap.org ) at 2012-06-29 19:22 South Africa Standard
Time
Nmap scan report for win-nfj70iht0ci.test1.com (fec0:2::4)
Host is up (0.0010s latency).
Not shown: 984 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp   open  globalcatLDAP
3269/tcp   open  globalcatLDAPssl
49154/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
49158/tcp  open  unknown
49163/tcp  open  unknown

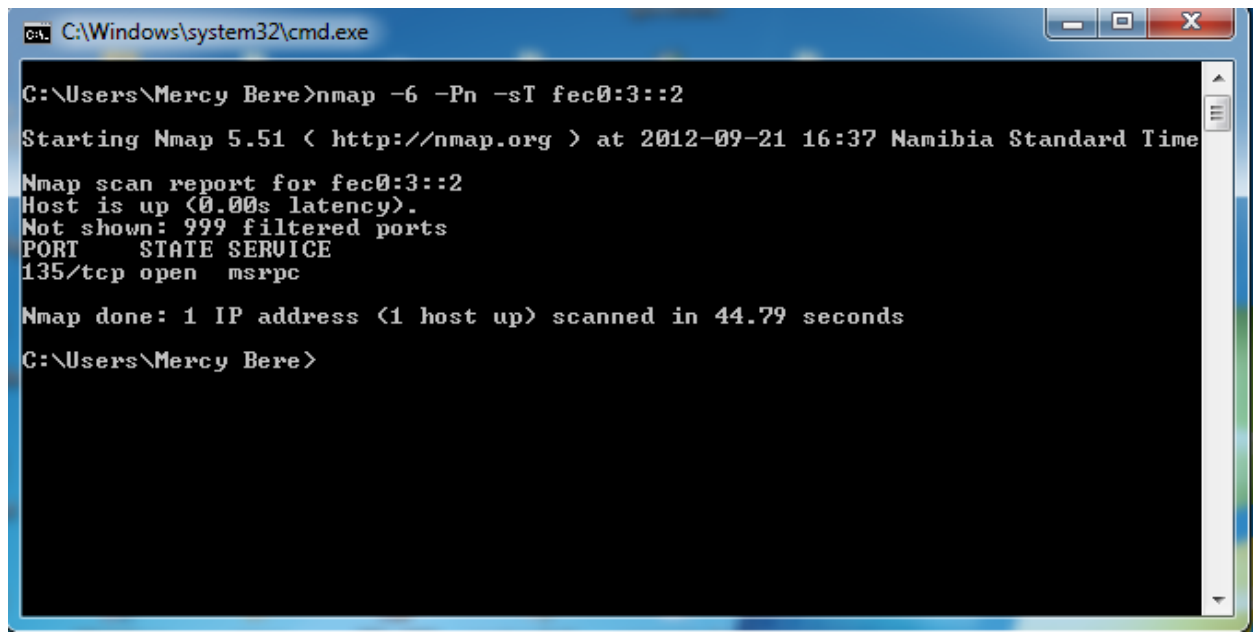
Nmap done: 1 IP address (1 host up) scanned in 44.70 seconds
C:\Users\csn>
```

Figure 5.9 IPv6 Web and Mail Server

The next section shows the results obtained on scanning a user device using Nmap.

5.5.1.2 Nmap Scan of a User PC

In Figure 5.10 below it is seen that the scan yielded 1 TCP port running msrpc. It must be noted that Nmap 5.51 used in the tests does not support IPv6 OS detection. Telnet to the PC on port 135 would give a blank screen.

A screenshot of a Windows command prompt window. The title bar shows the path 'C:\Windows\system32\cmd.exe'. The command prompt shows the user 'Mercy Bere' at 'C:\Users\Mercy Bere' running the command 'nmap -6 -Pn -sT fec0:3::2'. The output shows the Nmap scan report for 'fec0:3::2', indicating the host is up with 0.00s latency, 999 filtered ports, and one open port: 135/tcp (msrpc). The scan took 44.79 seconds.

```
C:\Windows\system32\cmd.exe
C:\Users\Mercy Bere>nmap -6 -Pn -sT fec0:3::2
Starting Nmap 5.51 < http://nmap.org > at 2012-09-21 16:37 Namibia Standard Time
Nmap scan report for fec0:3::2
Host is up (0.00s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrcpc
Nmap done: 1 IP address (1 host up) scanned in 44.79 seconds
C:\Users\Mercy Bere>
```

Figure 5.10 Staff VLAN PC

5.5.2 Vulnerability detection

This section highlights the vulnerabilities as found by Nessus in the IPv6 island network. Nessus works in the same manner as IPv4 vulnerability scans. It looks for the vulnerabilities in the targeted IPv6 hosts or network and returns a report on its findings. The report also gives feedback on the location of the vulnerability the risk factor and how the vulnerability can be resolved. Risk factors are again classified as being low, high, medium or high. Risk factors are based on CVSS scales. The actual value of a risk factor is initially based on the base group, but if all CVSS groups are considered then the score is based on the group with biggest impact.

5.5.2.1 IPv6 Mail and Web Server Nessus Vulnerability Scans

The following section show the results obtained from the Nessus scans on the mail and web server

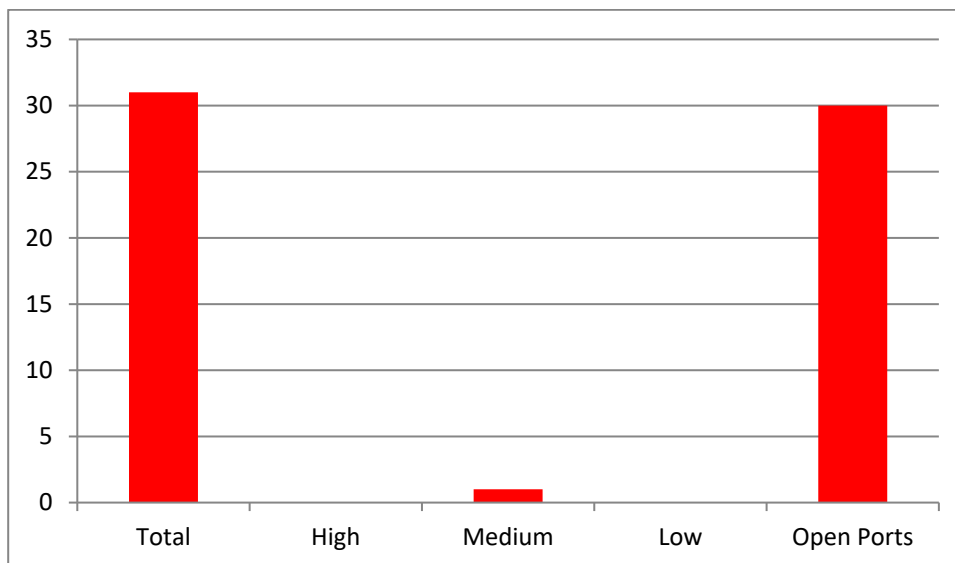


Figure 5.11 IPv6 mail and Web Server Nessus Scan vulnerability risk factors

Referring to Figure 5.6, the following is noted:

- Total highlights the number of vulnerabilities found
- High indicates the number of high risk vulnerabilities
- Medium indicates the number of medium risk vulnerabilities
- Low indicates the number of low risk vulnerabilities
- Info indicates the number of ports open

The graph shows the vulnerabilities risk factors as categorised by Nessus. Risk factors indicated in the graph were valued using the CVSS base group. The server had just 1 medium risk vulnerability. The rest were ranked as ‘information only’ vulnerabilities.

The table below shows the information about the medium risk vulnerability discovered.

Plugin	port	Vulnerability	CVSS Score	Exploits	Solution
11002	53/tcp	DNS server Spoofed Request Amplification DDoS	5	none	available

Table 5.5 Medium risk vulnerabilities on IPv6 mail and web server

From the reports it can be seen that TCP port 53 had the only medium risk factor with a CVSS base score of 5. DNS server Spoofed Request Amplification DDoS means that the server can be used to launch a DDoS attack. A solution to moderate this problem was also suggested. The ports that Nmap discovered were all also discovered by Nessus but besides the one discussed above the rest were classified as low risk vulnerabilities which are seen in the graph as open ports.

5.5.2.2 IPv6 User PC Nessus Vulnerability Scans

The following section show the results obtained from the Nessus scans on a user Pc

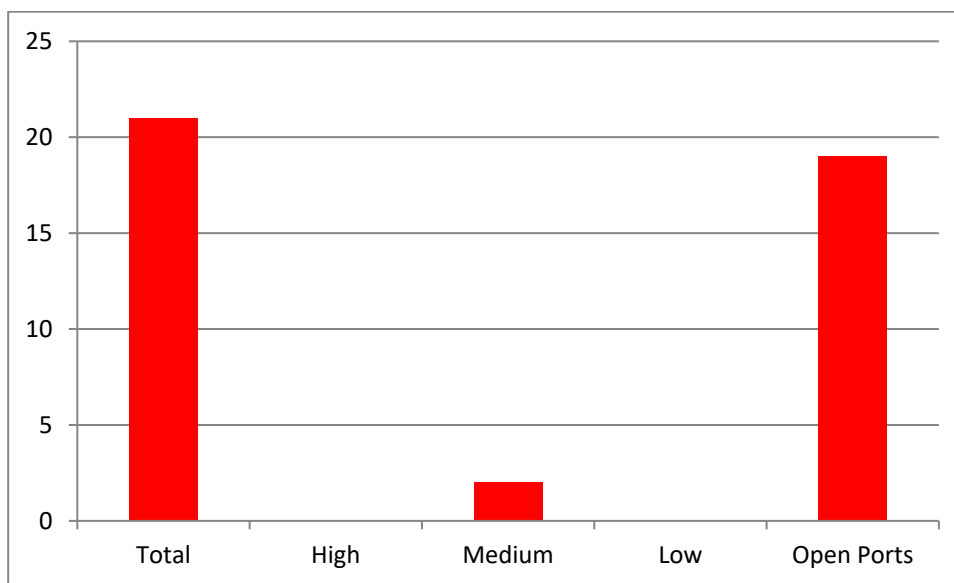


Figure 5.12 IPv6 user PC vulnerability risk factors

The meaning of the labels is the same as that in Figure 5.11

The user PC had just 2 medium risk vulnerabilities which are tabled in Table 5.6 below. The rest were informational vulnerabilities indicated by open ports, this means that they only give information about the target host depending on the service listening on the port.

Plugin	port	Vulnerability	CVSS Score	Exploits	Solution
57608	445/tcp	SMB signing Disabled	5	none	available
59659	3493/tcp	network UPS Tools Plaintext Authentication	5.1	none	available

Table 5.6 Medium Risk Vulnerabilitties on IPv6 user PC

TCP port 445 had a medium risk vulnerability which Nessus called SMB Signing Disabled. This vulnerability could be used for man-in-the-middle attacks against the SMB server. The other medium risk vulnerability, Network UPS Tools Plaintext Authentication, which had a CVSS score of 5.1 may also be used to perform a man-in-the-middle attack.

5.6 IPv6 Network Test Results analysis

From the results highlighted above it is shown that an IPv6 configured network is also susceptible to network attacks. It is also shown that the reconnaissance attacks using Nmap and Nessus scans were successful. It can be predicted from the Nessus reports that an access attack will also be successful in this network. For example, the Network UPS Tools Plaintext Authentication vulnerability detected can be used to execute a man-in-the-middle attack. Further, a DDoS attack can be launched in the network using the web and mail server as was shown in section 5.5.2.1

5.7 Summary

This chapter highlighted the results of Penetration Testing in the IPv4 production network and in the IPv6 island network. The first part sections 5.2 – 5.4 showed the information that was gathered about the IPv4 production network and further the vulnerabilities detected in the network. The vulnerabilities were ranked in terms of how they could impact the network. The ranking of the vulnerabilities was based on the CVSS scoring model. CVSS is a model for measuring and elaborating on the effect and features of IT vulnerabilities. The vulnerabilities discovered in the IPv4 network range from low to high risk vulnerabilities and it was shown that the IPv4 network is susceptible to reconnaissance, access and DoS attacks. The other sections 5.5 – 5.6 of the chapter showed the results obtained in the IPv6 island network Penetration Testing. The information that could be gathered in the IPv6 Island was discussed in Section 5.5.1 and the results of the vulnerability scans were discussed. The IPv6 vulnerabilities were also scaled using the CVSS base scores. The vulnerabilities discovered range from medium to low and no high risk vulnerabilities were discovered. However, from the medium risks identified it was seen that the IPv6 network was also susceptible to reconnaissance, access and DoS attacks.

Chapter Six – Conclusions

This chapter concludes the research done on IPv6 security in the PON network. The chapter illustrates the results and limitations of the research and it also gives possible ideas on further research in the area.

6.1 Summary of the Research

The aim of the research was to investigate the security differences in an IPv4 configured network and an IPv6 configured network. The live PON network was used to test IPv4 network security and an IPv6 island network that emulated the PON network was used to test for IPv6 network security. The research involved finding network attacks that can be used against both types of network environments. The identified network attacks were then implemented to investigate the impact on the networks. It was found that reconnaissance, access and DoS attacks are common to both IPv4 and IPv6 networks. Nmap was used to emulate reconnaissance attacks and the Nessus vulnerability scanner was used to investigate the vulnerabilities of the network or to find out any other information that could be used to further exploit. Following that, Telnet was used to gain access to the various ports identified.

From the tests it could be deduced that both kinds of networks are susceptible to network attacks. One of the main differences between IPv4 and IPv6 network security is that IPv4 network attacks are very well documented compared with IPv6.

6.2 Findings

When this research started the aim was to:

- Conduct a literature study to identify the network attacks that:
 - are considered most threatening to the PON computer network
 - could occur most frequently
 - could interrupt daily operations at the PON

- Design experiments to test the security vulnerabilities of both the current IPv4 network of the PON, as well as the proposed IPv6 computer network. The tests were derived from literature and penetration tests were chosen to test the networks as was highlighted in chapter four.
- Establish the susceptibility of these network environments to various network attacks.

Results showed that many attacks can be used to attack the PON IPv4 network. These attacks are generally grouped into reconnaissance, access and DoS attacks. Both IPv4 and IPv6 networks can be attacked using any of these attack methods. The only difference is how the attacks are carried out as highlighted in section 2.2.5. The section discussed how reconnaissance, access attacks, fragmentation and header manipulation attacks are possible in both IPv4 and IPv6 networks, but the execution of these attacks is different. The researcher used several tools that could execute reconnaissance attacks (Nmap and Nessus Scanner) and vulnerability scans (Nessus Scanner) to find out the kind of information that could be gathered about the networks. In addition the researcher discovered the type of vulnerabilities that are present in both types of networks and the risk level associated with those vulnerabilities. Thus, using Nessus the type of exploits that could be carried out in the networks were shown in sections 5.2.3 and 5.5.2. Therefore, it can be concluded that reconnaissance, access and DoS attacks exploit vulnerabilities in both the IPv6 and IPv4 networks tested. From the results obtained, it was seen that all vulnerabilities associated with finding out information about OSs or services of the network are all low level risk in both IPv4 and IPv6 networks.

6.3 Recommendations for IPv6 Security

It is the goal of the PON to migrate to IPv6 once ITS supports IPv6. In line with this is the need for recommendations for IPv6 security when the institution has finally migrated to using IPv6 in the network. Following are recommendations for IPv6 security based on the tests conducted.

Network administrators should be aware of the information that can be obtained through exploitation of the vulnerabilities in the network and to what extent the vulnerabilities can be exploited. The network administrators should conduct Penetration tests periodically or any other security tests that show the kind of security vulnerabilities in the network.

In addition, the administrators should make sure that the threat of attackers is mitigated or addressed. For example, the researcher had detailed information about the network, but easily gathered more

information from PON employees. Therefore, it is recommended that the network administrators should ensure that network users are made aware of potential threats to the network, that they should not divulge any information to unauthorised personnel, as well as the role that they should play in protecting the network.

It is further recommended that the network should be configured in such a way that all services that are not needed should be disabled, network passwords should be changed regularly, services that are in use should be hardened against any known exploits and the authentication of valid users should make sure that right person has been given access .

In addition, as it was found that both IPv4 and IPv6 networks are subject to reconnaissance, access and DoS attacks it is useful to also include all kinds of IPv4 best security practices in the IPv6 network. That is to use IDS, firewalls, access control lists and any other ways and means that were being used in the IPv4 network to make it secure.

6.4 Limitations to the Research

At the time of this research, the Integrated Tertiary System (ITS) does not run on IPv6. ITS is the critical system that is used by the PON for its services. The ITS server is used for student records, by human resources, for inventory and for most operations at the PON. Therefore, it was not possible to test ITS on an IPv6 network. Thus the research was limited to all the services that could run on IPv6 excluding ITS.

On finding the tools to use for penetration testing it was documented that Nessus vulnerability scanner can work in IPv6 networks. For testing the IPv4 network Nessus on Windows 7 was used but, on trying to use the scanner for IPv6 this was not possible, as it only works on UNIX systems. Therefore, the results for the vulnerability scan are limited to Windows for IPv4 and to Linux for IPv6.

In addition the results were only limited to the PON network. Therefore, it cannot be said that the results obtained for the PON network could be generalised for any other network.

6.5 Further Research

From the challenges and limitations of this research, future work on this subject can be recommended.

- Firstly, once the PON acquires an ITS version that supports IPv6 then there is need to retest the network for security to validate the behaviour of the network in a production environment. ITS is a critical system that needs to be tested for the PON because they rely on it for most of their services.
- Secondly, in running the tests it would also be useful to use the same testing environment. In this case the PON production network was used to test for IPv4 and then an island network to test for IPv6. The results might not be the actual evaluation of the differences. Thus, it is important for future work to use the same network setup for both IPv4 and IPv6 network testing.
- It is also important to use the same testing environment. In this research Windows 7 was used to test for IPv4 and the Linux Centos 6 to test for IPv6, as it was not possible to use Windows 7 with Nessus for IPv6. Since it is not yet possible to use Windows 7 to test using Nessus for IPv6 then all the tests for both IPv4 and IPv6 should be tested using the same test bed, which, in this case, is Centos 6.
- It would be useful to use other testing methods and software to find out if the results are still the same or to find out if it is still possible to penetrate the networks.
- Finally, to investigate the difference in network security between IPv4 and IPv6 it would be important to test more than one network setup to make sure that the differences being obtained are significant.

6.6 Conclusion

It was established in section 1.1 that IPv4 was designed without the foresight that the Internet would grow at such a tremendous speed. Amongst other reasons, the fact that IPv4 addresses are no longer enough for all IP users led to the introduction of IPv6. In order for the PON to migrate to IPv6 there was a need to test the security implications of using IPv6 in the network. By conducting a literature study, attacks that could be instigated against networks such as ping sweeps, man-in-the-middle attacks and DoS were identified and Penetration testing was used to find the effects of such attacks in the network. From the Penetration tests that were conducted it was found out that

- Network information could be gathered in both IPv4 and IPv6 networks
- Using Nessus vulnerability scanner, man-in-the-middle and DoS attacks could be carried out in both IPv6 networks

- To compromise IPv4 networks after discovering what to exploit in the networks is much easier than for IPv6. This is because there is, currently, more literature on how to compromise IPv4 networks than there is for IPv6.

This means that in both types of networks there is no difference in security. Thus for the PON to maintain its current security status, the PON should follow the security practices already in place for the IPv4 network and apply them to IPv6.

Chapter Seven – References

Anderson, J. (2001). *An Analysis of Fragmentation attacks*. Retrieved August 13, 2012 from <http://www.ouah.org/fragma.html>

Antunes, J & Neves, N, F. (2011). *Using Behavioral Profiles to Detect Software Flaws in Network Servers*. Retrieved from <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6132948>

Beaver, K. (2010). *Hacking for dummies*, 3rd edition. [Books24x7 version]

Bishop, M. (2003). *Computer Security. Art and Science*. New Jersey. Addison Wesley

Budiarto, R., Ramadass, S, Samsudin, A., Noor, S. (2004). *Development of penetration testing model for increasing network security*. Information and Communication Technologies: From Theory to Applications, 2004. Proceedings. 2004 International Conference on. Doi: 10.1109/ICTTA.2004.1307886

Caicedo, C, E. & Joshi, J,B, D. (2009). *IPv6 Security Challenges*. Retrieved July 22, 2010 from <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4781968>

Choudhary, A, R. (2009). *In-depth Analysis of IPv6 Security Posture*. Retrieved July 22, 2010 from <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5363654>

Convery, S & Miller, D. (2004). *IPv6 and IPv4 Threat Comparison and Best- Practice evaluation (v1.0)*. Retrieved March 12, 2011 from http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf

Cole, E. (2009). *Network security bible*, 2nd edition. [Books24x7 version]

Cunningham, B., Dykstra, T., Fuller, E., Gatford, C., Gold, A., Hoagberg, M, P., Snedaker, S. (2007). *The Best Damn IT Security Management Book Period*. Burlington. Syngress Publishing

Davies, J . (2008). *Understanding IPv6, second edition*. [Books24x7 version] Available from <http://common.books24x7.com/toc.aspx?bookid=24514>.

Deal, R. (2008). *CCNA Cisco Certified Network Associate Study Guide (Exam 640-802)*, 4th edition. Osbourne. McGram-Hill. Retrieved April 12, 2011 from Books24x7

Duan, B., Zhang, Y., Gu, D. (2008). *An Easy-to-deploy Penetration testing Platform*. Young Computer Scientists, 2008. ICYCS 2008. Doi: 10.1109/ICYCS.2008.335

Gregg, M. (2008). *Build your own security lab: a field guide for network testing*. [Books24x7 version]

Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G. & Williams, T. (2011). *Gray hat hacking: the ethical hacker's handbook*, third edition. [Books24x7 version]

Hogg, S. & Vyncke, E. (2009). *IPv6 Security*. Indianapolis. Cisco Press

Hogg, S & Vyncke, E. (2009). *IPv6 security: information assurance for the next-generation internet protocol*. [Books24x7 version]

Hwang, J, S & Park S. (2010). Korea Republic of. In S Akhtar, M, A Hassan, P Arinto. *Digital Review of Asia Pacific 2009 -2010* (pp 234 -240). Retrieved August 2, 2012 from http://www.digital-review.org/uploads/files/pdf/2009-2010/chap-26_korea_republic.pdf

Kaspersky Security Bulletin. (2008) retrieved May 14, 2012 from http://www.securelist.com/en/analysis/204792052/Kaspersky_Security_Bulletin_Statistics_2008

Kaspersky Security Bulletin. (2009) retrieved May 14, 2012 from http://www.securelist.com/en/analysis/204792101/Kaspersky_Security_Bulletin_2009_Statistics_2009

Kaspersky Security Bulletin. (2010) retrieved May 14, 2012 from http://www.securelist.com/en/analysis/204792162/Kaspersky_Security_Bulletin_2010_Statistics_2010

Kaspersky Security Bulletin. (2011) retrieved May 14, 2012 from http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011

Kim, J., Cho, H., Mun, G. & Seo, J. (2007). *Experiments and Countermeasures of Security Vulnerabilities on Next Generation Network*. [PDF document]. Retrieved March 2, 2011 from <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4426304>

Kost, S & Kanter, J. (2007). *Oracle Database Listener Security Guide*. [White Paper]. Retrieved from http://www.integrigy.com/security-resources/whitepapers/Integrigy_Oracle_Listener_TNS_Security.pdf

Lammle, T. (2011). *Ccna cisco certified network associate study guide*, seventh edition (exam 640-802). [Books24x7 version]

Lyon, G, F. (2009). *Nmap Network Scanning*. Retrieved May 26, 2011 from <http://nmap.org/book/>

McClure, S., Scambray, J & Kurtz, G. (2009). *Hacking exposed 6: network security secrets and solutions*. [Books24x7 version]

Mell, p., Scarfone, K. & Romanosky, S. (2007). *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*. Retrieved September 18, 2012 from <http://www.first.org/cvss/cvss-guide.pdf>

Metasploit. (2012). Retrieved May 27, 2012 from <http://www.metasploit.com/>

Montoro, M. (2011). *Cain and Abel*. Retrieved May 31, 2012 from <http://www.oxid.it/cain.html>

NIST Special Publication 800-42, 2003. Retrieved May 28, 2012 from <http://www.iwar.org.uk/comsec/resources/netsec-testing/sp800-42.pdf>

Norman, G. (2011). *NetStumbler*. Retrieved June 1, 2011 from <http://netstumbler.findmysoft.com/review/>

O'leary, Z. (2010). *Doing Your Research Project*. New Dehli. SAGE Publications

Orebaugh, A. (2007). *Wireshark & ethereal network protocol analyzer toolkit, jay beale's open source security series*. [Books24x7 version]

Orebaugh, A & Pinkard, B. (2008). *Nmap in the enterprise: your guide to network scanning*. [Books24x7 version]

Paquet, C. (2009). *Implementing Cisco IOS Network Security (IINS): (CCNA Security exam 640-553) (Authorized Self-Study Guide)*. Cisco Press. Retrieved August 2, 2011 from Books24x7

Pilihanto, A. (2012). *A Complete Guide on IPv6 Attack and Defense*. Retrieved June 29, 2012 from http://www.sans.org/reading_room/whitepapers/detection/complete-guide-ipv6-attack-defense_33904

Polytechnic of Namibia. (N. D). *Acceptable ICT use Policy*. Retrieved June 1, 2011 from http://mail.polytechnic.edu.na:8080/institutepolicies/docs/2009/acceptable_use_policy_1_5.pdf

Rogers, R. (2008). *Nessus network auditing*, second edition. [Books24x7 version]

Radhakrishnan, R., Jamil, M., Mehfuz, S., Moinuddin. (2007). *Security Issues in IPv6*. [PDF document]. Retrieved March 2, 2011 from <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4438359>

RFC 791. (1981). *Internet Protocol*

RFC 1858. (1989). *Security Considerations for IP Fragment Filtering*

RFC 2460. (1999). *Internet Protocol, Version 6 (IPv6) Specification*

RFC 4861. (2007). *Neighbor Discovery for IP version 6 (IPv6)*

Rowe, B. & Gallaher, M. (2006). *Could IPv6 Improve Network Security? And, If So, at What Cost?*. Retrieved September 24, 2009 from <http://is-journal.org/V02I02/2ISJLP231-Rowe%20and%20Gallaher.pdf> possible

Sanders, C. (2011). *Practical packet analysis: using wireshark to solve real-world network problems*, second edition. [Books24x7 version]

Scambray, J, Liu, V & Sima, C. (2011). *Hacking exposed web applications: web application security secrets and solutions*, third edition. [Books24x7 version]

Seagren, E. (2007). *Secure your network for free: using nmap, wireshark, snort, nessus, and mrtg*. [Books24x7 version]

Sectools.org, (2006). *Top 100 Network Security tools*. Retrieved April 28, 2011 from <http://sectools.org/>

Tenable Network Security. (2011). *Nessus Product Overview*. Retrieved April 28, 2011 from <http://www.tenable.com/products/nessus/nessus-product-overview>

Whitman, M, E. & Mattord, H, J. (2005). *Principles of Information Security*. Canada. Thomson course technology.

Wang, S., Xu, D & Yan, S. (2010). *Analysis and Application of Wireshark in TCP/IP Protocol Teaching*. Retrieved May 28, 2012 from <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5496372>

Whitaker, A & Newman, D. (2006). *Penetration testing and Network Defense*. Indianapolis. Cisco Press

Wiles, J. & Reyes, A. (2007). *The best damn cybercrime and digital forensics book period*. [Books24x7 version]

Witte, G., Cook, M., Kerr, M & Shaffer, S. (2012). *Security automation essentials: streamlined enterprise security management & monitoring with scap*. [Books24x7 version]

Zagar, D. & Grygic, k. (2009). *IPv6 Security Threats and Possible Solutions*. Retrieved July 22, 2010 from <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4259826>

Zhao-wen, L. (2007). *Possible Attacks based on IPv6 Features and Its Detection*. Retrieved August 6, 2010 from http://www.apan.net/meetings/xian2007/publication/031_lin.pdf

Appendix A : IPv6 Test Island Routers and Switch Configurations

Inside router configuration	Outside router configuration	Switch configuration
<pre> sh run Building configuration... Current configuration : 1409 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname inside ! boot-start-marker boot-end-marker ! no aaa new-model ! ip cef ! ip auth-proxy max-nodata-conns 3 ip admission max-nodata-conns 3 ! ipv6 unicast-routing ! voice-card 0 no dspfarm ! interface Loopback0 ip address 2.2.2.2 255.0.0.0 ! interface FastEthernet0/0 ip address 10.1.2.1 255.255.255.0 duplex auto speed auto ipv6 address FEC0:1::1/64 ipv6 enable ipv6 ospf 1 area 0 ! </pre>	<pre> sh run Building configuration... Current configuration : 2447 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname outside ! boot-start-marker boot-end-marker ! no aaa new-model ! ip cef ! ip auth-proxy max-nodata-conns 3 ip admission max-nodata-conns 3 ! ipv6 unicast-routing ! voice-card 0 no dspfarm ! interface Loopback0 ip address 1.1.1.1 255.0.0.0 ! interface Loopback1 no ip address ipv6 address 2001:DB8:11::1/64 ! interface FastEthernet0/0 no ip address duplex auto speed auto ipv6 address FEC0:1::2/64 ipv6 enable </pre>	<pre> sh run Building configuration... Current configuration : 3368 bytes ! version 12.2 no service pad service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname Switch ! boot-start-marker boot-end-marker ! no aaa new-model system mtu routing 1500 ip subnet-zero ! spanning-tree mode pvst spanning-tree extend system-id ! vlan internal allocation policy ascending ! interface FastEthernet0/1 switchport mode trunk ! interface FastEthernet0/2 ! interface FastEthernet0/3 ! interface FastEthernet0/4 ! interface FastEthernet0/5 ! interface FastEthernet0/6 ! interface FastEthernet0/7 </pre>

<pre> interface FastEthernet0/1 ip address 10.1.1.1 255.255.255.0 duplex auto speed auto ! interface FastEthernet0/1.10 encapsulation dot1Q 10 ipv6 address FEC0:2::1/64 ipv6 enable ipv6 ospf 1 area 0 ! interface FastEthernet0/1.20 encapsulation dot1Q 20 ipv6 address FEC0:3::1/64 ipv6 enable ipv6 ospf 1 area 0 ! interface Serial0/0/0 no ip address shutdown no fair-queue clock rate 125000 ! interface Serial0/0/1 no ip address shutdown clock rate 125000 ! interface Serial0/2/0 no ip address shutdown clock rate 125000 ! interface Serial0/2/1 no ip address shutdown clock rate 125000 ! ip forward-protocol nd ! ip http server no ip http secure-server ! ipv6 router ospf 1 log-adjacency-changes ! control-plane ! </pre>	<pre> ipv6 traffic-filter outside_inbound out ipv6 ospf 1 area 0 ! interface FastEthernet0/1 no ip address shutdown duplex auto speed auto ! interface Serial0/0/0 no ip address shutdown clock rate 2000000 ! interface Serial0/0/1 no ip address shutdown clock rate 2000000 ! ip forward-protocol nd ! ip http server no ip http secure-server ! ipv6 router ospf 1 log-adjacency-changes ! ipv6 access-list outside_inbound permit icmp FE80::/10 any nd- na permit icmp FE80::/10 any nd-ns sequence 40 permit tcp any host FEC0:2::2 range 1024 65535 permit udp any host FEC0:2::2 range 1024 65535 permit icmp any FEC0:1::/64 1 3 permit icmp any FEC0:2::/64 1 3 permit icmp any FEC0:3::/64 1 3 permit icmp any FEC0:1::/64 packet-too-big permit icmp any FEC0:2::/64 packet-too-big permit icmp any FEC0:3::/64 packet-too-big permit icmp any FEC0:3::/64 parameter-problem permit icmp any FEC0:2::/64 parameter-problem </pre>	<pre> ! interface FastEthernet0/8 ! interface FastEthernet0/9 ! interface FastEthernet0/10 ! interface FastEthernet0/11 switchport access vlan 10 switchport mode access ! interface FastEthernet0/12 switchport access vlan 10 switchport mode access ! interface FastEthernet0/13 switchport access vlan 10 switchport mode access ! interface FastEthernet0/14 switchport access vlan 10 switchport mode access ! interface FastEthernet0/15 ! interface FastEthernet0/16 ! interface FastEthernet0/17 ! interface FastEthernet0/18 ! interface FastEthernet0/19 ! interface FastEthernet0/20 ! interface FastEthernet0/21 switchport access vlan 20 switchport mode access ! interface FastEthernet0/22 switchport access vlan 20 switchport mode access ! interface FastEthernet0/23 switchport access vlan 20 switchport mode access ! interface FastEthernet0/24 switchport access vlan 20 </pre>
---	--	--

<pre> line con 0 line aux 0 line vty 0 4 login ! scheduler allocate 20000 1000 ! end </pre>	<pre> permit icmp any FEC0:1::/64 parameter-problem permit icmp any FEC0:1::/64 echo-reply permit icmp any FEC0:2::/64 echo-reply permit icmp any FEC0:3::/64 echo-reply deny ipv6 any any ! ipv6 access-list inside_outbound permit icmp FE80::/10 any nd- na permit icmp FE80::/10 any nd-ns permit icmp FEC0:1::/64 any 1 3 permit icmp FEC0:2::/64 any 1 3 permit icmp FEC0:3::/64 any 1 3 permit icmp FEC0:1::/64 any packet-too-big permit icmp FEC0:2::/64 any packet-too-big permit icmp FEC0:3::/64 any packet-too-big permit icmp FEC0:1::/64 any parameter-problem permit icmp FEC0:2::/64 any parameter-problem permit icmp FEC0:3::/64 any parameter-problem permit icmp FEC0:1::/64 any echo-reply permit icmp FEC0:2::/64 any echo-reply permit icmp FEC0:3::/64 any echo-reply deny ipv6 any any log ! control-plane ! line con 0 line aux 0 line vty 0 4 login ! scheduler allocate 20000 1000 ! end </pre>	<pre> switchport mode access ! interface GigabitEthernet0/1 ! interface GigabitEthernet0/2 ! interface Vlan1 no ip address no ip route-cache shutdown ! ip http server ip http secure-server ! control-plane ! line con 0 line vty 0 4 login line vty 5 15 login ! End </pre>
---	--	---

Appendix B: Penetration Test Agreement

This document is an agreement between the Polytechnic of Namibia Bureau of Computer Services hereafter referred to as PON and Mercy Bere

With regard to the Security Penetration Test, the PON hereby acknowledges and agrees:

1. That Mercy Bere will perform a Security Penetration Test that will attempt to identify security vulnerabilities in PON network from the 31st January 2012 to 29 February 2012
2. That the PON has the legal right to subject the designated network to the aforementioned Security Penetration Test and that if it is not the owner of the computer system it has obtained such right from the legal owner of the system.
3. Not to hold Mercy Bere liable for any indirect, punitive, special, incidental, or consequential damage (including but not limited to loss of business, revenue, use, data or other economic advantage) however it arises, whether for breach or in tort, even if Mercy Bere has been previously advised of the possibility of such damage.
4. That it has the sole responsibility for adequate protection and backup of data and/or equipment used in connection with this Security Penetration Test and will not make a claim against Mercy Bere for lost data, re-run time, inaccurate output, work delays resulting from the Security Penetration Test.
5. That Mercy Bere will not divulge any information about the PON network she received as a result of this Security Penetration Test. All results are confidential and will be treated as such.
6. It will respond in a normal fashion when it detects the Security Penetration Test in its firewall logs, alert systems, etc. as it would do in case of a real security penetration; in order not to distort the results of the test. However, the PON agrees not to notify legal or public authorities of this penetration.
7. The test results will be provided to the PON Bureau of Computer Services as a written report.

The PON agrees that Mercy Bere will perform the Security Penetration Test on the following IP address(es) and that the test components will include Gathering Publicly available Information, Network Scanning, System Profiling, Service Profiling, vulnerability Identification, Vulnerability Validation/Exploitation, Privilege Escalation

under the aforementioned conditions:

.....
.....

Mercy Bere will inform the PON of the Security Penetration Test originating IP address.

Signed for and on behalf of PON,

Name

Mercy Bere

.....

Date

Date

.....

Signature

.....

Signature

.....

.....

Appendix C: Acceptable ICT Use Policy

1.0 Overview

The Polytechnic of Namibia's (PON) intentions for publishing an Acceptable ICT Use Policy are not to impose restrictions that are contrary to the PON's established culture of openness, trust, integrity and technological advancement. PON is committed to protecting its employees, students, partners and Council from illegal or damaging actions by individuals or groups, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, ITS system access and FTP, are the property of PON. These systems are to be used for business purposes in serving the interests of PON, and of our clients and customers in the course of normal operations. Human Resources rules and regulations can be consulted for further details.

Effective security as well as optimum use of ICT equipment are a team effort involving the participation and support of every PON user and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at PON. These rules are in place to protect the Council of PON. Inappropriate use exposes PON to risks including virus attacks, compromise of network systems and services, disclosure of confidential information and legal issues.

3.0 Scope

This policy applies to employees, students, contractors, consultants, official guests and visitors, contract and part-time workers, and all other workers at PON, including all personnel affiliated with third parties. They are all categorised as users. This policy applies to equipment that is owned, leased or in use in PON's premises.

4.0 Policy

4.1 General Use and Ownership

1. While PON's network administration desires to provide privacy, users should be aware that the data they create on the corporate systems remains the property of PON, but the following exceptions apply: External consultancies, Open source software development, data downloaded from the internet, data that is not the Intellectual property of PON and data stored on equipment that does not belong to PON. Because of the need to protect PON's network, management cannot guarantee the confidentiality of information stored on any device belonging to PON, although PON will not routinely intercept or monitor electronic communications.
2. Users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such guidelines, users should be guided by section / sector policies on personal use, and if there is any uncertainty, users should consult their supervisor, manager, lecturer or lab technician, whoever is applicable.
3. PON recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see PON Information Sensitivity Policy. For guidelines on encrypting emails and documents, contact the Bureau of Computer Services (BCS).

4. For security and network maintenance purposes, individuals who are authorised to do so by the Director: BCS may monitor equipment, systems and network traffic at any time, per PON's ICT Audit Policy.
5. PON reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
6. Personal use: Users may use electronic communications resources for incidental personal purposes provided that such use does not:
 - 6.1 directly or indirectly interfere with the University operations
 - 6.2 interfere with the user's conditions of employment or other obligations to the university
 - 6.3 affect the performance of the user
 - 6.4 burden the university with additional costs
 - 6.5 violate any of either the laws of the Republic of Namibia, international law or university policy.
7. Students and guests may bring computer equipment on campus, but may not plug them into the physical network (network sockets) nor may they attempt to connect to the wireless network without the written authorisation of the Director: BCS or the Manager: Networks of BCS. Any attempt to connect to either network without authorisation shall be interpreted as a hacking attempt and dealt with accordingly

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by the institution's confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: Institution's corporate strategies, strategic planning, trade secrets, customer lists, student records, payroll, personal and research data. Users should take all necessary steps to prevent unauthorised access to this information.
2. Keep all passwords secure and do not share accounts. Authorised users are responsible for the security of their passwords and accounts. System level passwords should be changed on a quarterly basis, while user level passwords should be changed at least every six months. Deviation from such policies shall have to be approved by the Director: BCS.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when hosts will be left unattended.
4. Use encryption of information in compliance with PON's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with laptop security tips that are available from the Manager: PC Support of BCS.
6. Postings by employees or students from a PON email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of PON, unless posting is in the course of business duties. Courtesy should be observed in all communications (Netiquette, available at <http://en.wikipedia.org/wiki/Netiquette> or at <http://tools.ietf.org/html/rfc1855>).
7. All Microsoft based hosts used by users that are connected to the PON internal network, whether the hosts are owned by the user or PON, have to be continually executing BCS approved virus-scanning software with a current virus database as well as anti-spyware. Hosts running Linux or other robust operating systems (excluding all Microsoft products) are less sensitive to viruses and trojans and as such are simply encouraged to run virus protection at all times. Palms and cell phones are in general not expected to be running anti-virus or spyware

protection. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. Users should report all real or perceived virus or other systems warnings or malfunctions to BCS officials as soon as possible in order to prevent the spread of malicious software.

8. It is the responsibility of users to backup data located on their hard drives or other storage devices, using either CD's, DVD's, memory sticks, or any other method recommended or advised by BCS upon request. No hard drive shall be sent outside the institution for data recovery, since it is assumed that users perform backups on a regular basis. The only exception to this rule shall be at the discretion of the Director: BCS.

4.3. Unacceptable Use

The following activities are, in general, prohibited, but BCS officials and staff of the School of IT may be exempted at the discretion of the Director: BCS from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may need to disable the network access of a host if that host is disrupting production services, while IT students may be required to perform network penetration attacks as part of their practicals).

Under no circumstances with the exception defined above is a user of PON authorised to engage in any activity that is illegal under local or international law while utilising PON-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by PON.
2. Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which PON or the end user does not have an active license.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. BCS or the appropriate line management should be consulted prior to the export of any material that is in question.
4. Playing computer games on PON equipment, but games deemed educational by academic staff and games loaded as part of operating system installation are tolerated.
5. Reckless behaviour: Wasting of PON employees time, human or physical resources such as, but not limited to: Printing several times the same item in the belief that re-printing may solve printer or print server issues, printing recklessly, not taking into consideration any systems warnings or messages that may lead to costly data updates and / or repairs by either internal resources or third parties, reckless use of support BCS staff owing to incompetence, repeat of similar mistakes.

PON may either deduct the salary of staff member/s or impose a fee on student(s), or start legal or any other action against external users, whoever is accountable for such action to recover direct costs, provided

5.1.1 the user has been found guilty of such actions as a result of disciplinary proceedings, or

5.1.2 the user has, notwithstanding initiation of disciplinary action, admitted his or her responsibility for such action, and agreed in writing to such deduction.

5.1.3 it is feasible and financially reasonable to pursue action against external users.

5.1.4

6. Revealing one's account password to others or allowing use of one's account by others. This includes family and other household members when work is being done at home.
7. Introduction -*mala fides*- of damaging or malicious programs into the network or server(s) (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
8. Using a PON computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment regulations.
9. Making fraudulent offers of products, items, or services originating from any PON account.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless the Director: BCS is notified and has approved such scanning in writing.
12. Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty or assignment.
13. Circumventing user authentication or security of any host, network or account.
14. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Email and Communications Activities

1. Sending unsolicited email messages, including but not restricted to the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam and/or unsolicited emails). Official announcements sent to all staff do not fall in this category. No user may unsubscribe or attempt to unsubscribe from the Rectorate announcements list.
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorised use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters" or any "pyramid" schemes of any type.
6. Use of unsolicited email originating from within PON's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by PON or connected via ON's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment in the case of employees or expulsion in the case of students. Disciplinary action may be initiated by the direct supervisor / HOD / section / sector Head of the employee and/or by the Director: Bureau of Computer Services.

6.0 Terms and Definitions

Chain letter

A typical **chain letter** consists of a message that attempts to induce the recipient to make a number of copies of an attached letter and then pass them on to one or more new recipients, usually ten.

Pyramid schemes

Fraudulent investment operations that involve paying abnormally high returns ("**profits**") to investors out of the money paid in by subsequent investors, rather than from net revenues generated by any real business.

Spam

Unauthorised and/or unsolicited electronic mass mailings.

Trojan horse

Computer program that installs malicious software while under the guise of doing something else.

7.0 Revision History

1.2 - 15 May 2007

Sent to deans and senior management, integrated comments received from Dr. Stefan Schulz. Presented at Senate on 15 June 2007.

1.3 -- 15 June 2007

Senate requested the documents to be discussed in a CTL session. Integrated comments from Senate.

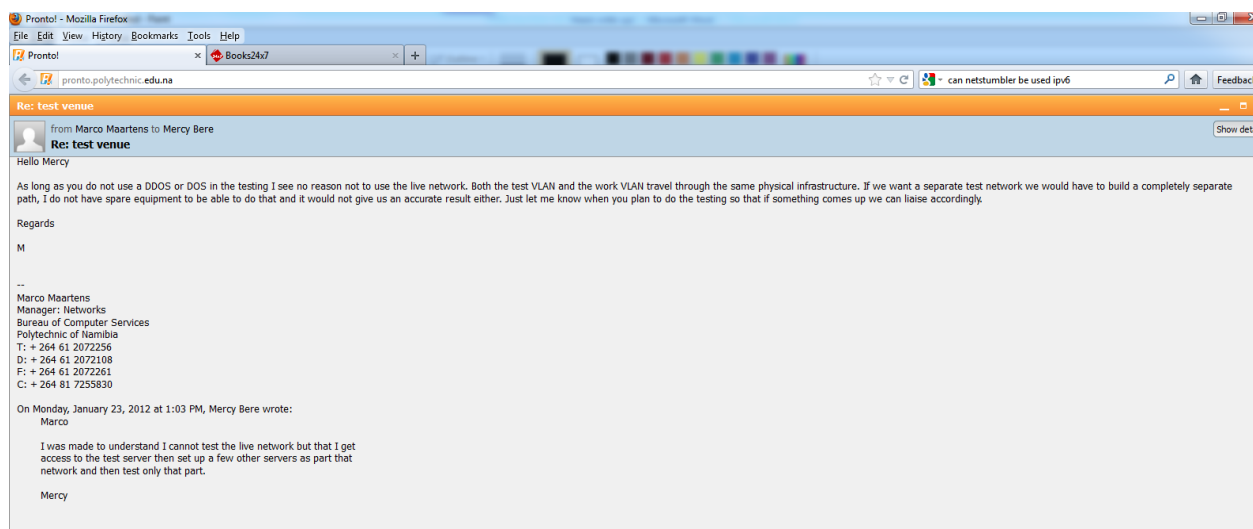
1.4 - 08 August 2007

Following CTL presentation on 01 August 2007, integrated comments received from: Prof Angela Clarke, Mr. van Wyk du Plessis, Mr. Calvin Mouton, Mr. Peter Gallert, Dr. Christian Rich.

1.5 – 29 August 2007

Added instance of student and guest equipment brought on campus and their relation to network security.

Appendix D: DoS Email



Appendix E: Typical Nessus Scan Results

The screenshot shows the Nessus web interface in a Mozilla Firefox browser window. The address bar shows 'localhost:8834'. The interface has a navigation bar with 'Reports', 'Scans', 'Policies', and 'Users'. The 'Reports' section is active, showing a report for 'pronto.'. On the left, there is a 'Report Info' sidebar with details: Name: pronto., Last Update: May 30, 2012 9:02, Status: Completed. Below this are buttons for 'Download Report', 'Show Filters', and 'Reset Filters', followed by an 'Active Filters' section. The main area displays a table of scan results for the host 'pronto.polytechnic.edu.na'. The table has columns for Host, Total, High, Medium, Low, and Open Port. The data row shows 96 total issues, 2 high, 3 medium, 78 low, and 13 open ports. The interface also includes a 'Feedback' link in the top right and a system tray at the bottom showing the time as 1:22 PM on 5/29/2012.

Host	Total	High	Medium	Low	Open Port
pronto.polytechnic.edu.na	96	2	3	78	13

Appendix F: Typical Nessus Scan Report

Nessus Report

Report

21/Sep/2012:13:24:37 GMT

HomeFeed: Commercial use of the report is prohibited

Any time Nessus is used in a commercial environment you MUST maintain an active subscription to the ProfessionalFeed in order to be compliant with our license agreement.<http://www.nessus.org/products/nessus-professionalfeed>

Table Of Contents

Vulnerabilities By Host

fec0:2::2

Vulnerabilities By Host

[-] Collapse All

[+] Expand All

fec0:2::2

Scan Information

Start time: Fri Sep 21 13:10:23 2012

End time: Fri Sep 21 13:24:37 2012

Host Information

DNS Name: fec0:2::2

IP: fec0::2

Results Summary

Critical	High	Medium	Low	Info
0	0	1	0	3

Results Details

0/tcp

12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]

Synopsis

It was possible to resolve the name of the remote host.

Description

Nessus was able to resolve the FQDN of the remote host.

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2004/02/11, Modification date: 2011/07/14

Ports

tcp/0

fec0::2 resolves as fec0:2::2.

46215 - Inconsistent Hostname and IP Address

[-/+]

Synopsis

The remote host's hostname is not consistent with DNS information.

Description

The name of this machine either does not resolve or resolves to a different IP address.

This may come from a badly configured reverse DNS or from a host file in use on the Nessus scanning host.

As a result, URLs in plugin output may not be directly usable in a web browser and some web tests may be incomplete.

Solution

Fix the reverse DNS or host file.

Risk Factor

None

Plugin Information:

Publication date: 2010/05/03, Modification date: 2011/10/06

Ports

tcp/0

The host name 'fec0:2::2' resolves to fec0:2::2, not to fec0::2

19506 - Nessus Scan Information

[-/+]

Synopsis

Information about the Nessus scan.

Description

This script displays, for each tested host, information about the scan itself :

- The version of the plugin set
- The type of plugin feed (HomeFeed or ProfessionalFeed)
- The version of the Nessus Engine
- The port scanner(s) used
- The port range scanned
- Whether credentialed or third-party patch management checks are possible
- The date of the scan
- The duration of the scan
- The number of hosts scanned in parallel
- The number of checks done in parallel

Solution

n/a

Risk Factor

None

Plugin Information:

Publication date: 2005/08/26, Modification date: 2012/04/18

Ports

tcp/0

Information about this scan :

Nessus version : 5.0.1

Plugin feed version : 201206262038

Type of plugin feed : HomeFeed (Non-commercial use only)

ERROR: Your plugin feed has not been updated since 2012/6/26

Performing a scan with an older plugin set will yield out of date results and produce an incomplete audit. Please run `nessus-update-plugins` to get the newest vulnerability checks from Nessus.org.

Scanner IP : fec0:3::5

WARNING : no port scanner was enabled during the scan. This may

lead to incomplete results

Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
CGI scanning : disabled
Web application tests : disabled
Max hosts : 80
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2012/9/21 13:10
Scan duration : 850 sec

3493/tcp

59659 - Network UPS Tools Plaintext Authentication

[-/+]

Synopsis

The UPS monitoring tool on the remote host does not support encrypted authentication.

Description

The remote Network UPS Tools instance does not support exchanging credentials through an encrypted channel. An unauthenticated, remote attacker may be able to perform a man-in-the-middle attack, intercept credentials, and alter the settings on the UPS that the server manages.

See Also

<http://www.networkupstools.org/docs/developer-guide.chunked/ar01s09.html>

<http://www.networkupstools.org/docs/user-manual.chunked/ar01s09.html>

Solution

Enable StartTLS support on the server using the 'CERTFILE' directive.

Risk Factor

Medium

CVSS Base Score

5.1 (CVSS2#AV:N/AC:H/Au:N/C:P/I:P/A:P)

Plugin Information:

Publication date: 2012/06/22, Modification date: 2012/06/23

Ports

[tcp/3493](#)