



**Vaal University of Technology**

**A FRAMEWORK FOR HIGHER ACADEMIC INSTITUTIONS IN THE REPUBLIC OF  
SOUTH AFRICA TO MITIGATE NETWORK SECURITY THREATS AND ATTACKS**

**MATRINTA JOSEPHINE MOHAPI**

**20549911**

**Dissertation submitted in fulfilment of the requirements for the degree of Magister  
Technologiae: Information Technology**

**in the**

**Department of Information and Communications Technology**

**Faculty of Applied and Computer Sciences**

**Vaal University of Technology**

**Vanderbijlpark**

**Supervisor: Prof A Jordaan**

**June 2017**

## **DECLARATION**

I, Matrinta Josephine Mohapi hereby declare that the work submitted here is the product of my own independent research, and that all the sources I have used and quoted have been pointed out and acknowledged by means of complete references. In addition, I declare that the work is submitted for the first time at this university/faculty towards the Masters Technologiae (MTech) degree in the Information Technology department and that it has never been submitted to any other university/faculty for the purpose of obtaining a degree.

.....

Matrinta Josephine Mohapi

June 2017

## **ACKNOWLEDGEMENTS**

First and foremost, I would like to express my sincere gratitude to my supervisor Prof Annelie Jordaan for her guidance, suggestions, constant encouragement and enduring patience she provided me throughout this dissertation. I have learnt much from her and have been fortunate to be supervised by her.

I also would like to thank the following individuals:

- Dr P Conradie, Mrs L Drevin and Prof M Ohanga for their guidance, careful attention and useful comments they had provided in carrying out this work
- I express my heartfelt gratitude to my husband Khasane S Mohapi for his love, support and warm encouragement he has shown during my studies
- My parents, Setho A Mota and Majacob A Mota, for supporting me in every step I took towards my studies and encouraging me

Lastly, I would like to thank the Department of Information and Communication Technology and the Research Department at Vaal University of Technology for the support provided for the success of this work.

## **DEDICATION**

I dedicate this project to my dear parents Majacob A Mota and Setho A Mota, my husband Khasane S Mohapi, my daughter Rethabile A Mohapi, my sister Mamohau C Tepane, and my younger brothers who have been a source of my happiness. They supported and encouraged me throughout the progress of this dissertation. Thank you.

## ABSTRACT

The computer networks of higher academic institutions play a significant role in the academic lives of students and staff in terms of offering them an environment for teaching and learning. These institutions have introduced several educational benefits such as the use of digital libraries, cluster computing, and support for distance learning. As a result, the use of networking technologies has improved the ability of students to acquire knowledge, thereby providing a supportive environment for teaching and learning. However, academic networks are constantly being attacked by viruses, worms, and the intent of malicious users to compromise perceived secured systems. Network security threats and cyber-attacks are significant challenges faced by higher academic institutions that may cause a negative impact on systems and Information and Communications Technology (ICT) resources. For example, the infiltration of viruses and worms into academic networks can destroy or corrupt data and by causing excessive network traffic, massive delays may be experienced. This weakens the ability of the institution to function properly, and results in prolonged downtime and the unavailability of Information Technology (IT) services.

This research determines challenges faced by higher academic institutions, identifies the type of security measures used at higher academic institutions, and how network security could be addressed and improved to protect against network security threats and attacks. Two research approaches were adopted, namely a survey and an experiment. Survey questionnaires were distributed to IT technical staff at higher academic institutions in Gauteng province to determine the challenges they face in terms of securing their networks. It is crucial that network security takes on a prominent role when managing higher academic institutions' networks.

The results of the study reveal several challenges such as budget constraints, inadequate security measures, lack of enforcing network security policies, and lack of penetration testing on systems and the network. The results also reveal that the implementation of security measures can and does address network security threats and attacks. It is therefore extremely important for higher academic institutions to implement proper security measures to help mitigate network security threats and attacks. The framework proposed is based on the results from the research study to help mitigate network security threats and attacks at higher academic institutions.

**Keywords:** Academic networks, cyber-attacks, higher academic institutions, network, network security attacks, network security threats, vulnerabilities

## TABLE OF CONTENTS

<b>DECLARATION.....</b>	<b>i</b>
<b>ACKNOWLEDGEMENTS.....</b>	<b>ii</b>
<b>DEDICATION .....</b>	<b>iii</b>
<b>ABSTRACT .....</b>	<b>iv</b>
<b>LIST OF FIGURES .....</b>	<b>ix</b>
<b>LIST OF TABLES.....</b>	<b>xii</b>
<b>LIST OF ABBREVIATIONS.....</b>	<b>xiii</b>
<b>CHAPTER 1: INTRODUCTION .....</b>	<b>1</b>
1.1 Background.....	2
1.1.1 Confidentiality .....	3
1.1.2 Integrity.....	4
1.1.3 Availability.....	4
1.1.4 Authentication .....	4
1.1.5 Authorisation.....	4
1.1.6 Accountability .....	5
1.2 Rationale and motivation .....	7
1.3 Problem statement .....	8
1.4 Research questions .....	9
1.4.1 Primary research question (PRQ) .....	9
1.4.2 Secondary research questions (SRQs).....	9
1.5 Research objectives .....	9
1.5.1 Primary research objective.....	9
1.5.2 Secondary research objectives .....	9
1.6 Research design and methodology .....	10
1.6.1 Explanatory research .....	11
1.6.2 Experimental design .....	11
1.6.3 Quantitative research.....	12
1.6.4 Research participants .....	12
1.6.5 Data analysis .....	12
1.7 Delimitations .....	13
1.8 Ethical considerations .....	13
1.9 Chapter outline.....	14
<b>CHAPTER 2: LITERATURE REVIEW .....</b>	<b>16</b>
2.1 Introduction .....	16

2.2	Networks in an academic environment.....	17
2.3	Challenges surrounding network security at higher academic institutions .....	18
2.3.1	Vulnerabilities and network threats .....	20
2.3.1.1	Eavesdropping and data modification .....	25
2.3.1.2	Spoofing and session hijacking.....	27
2.3.1.3	Denial of Service (DoS) .....	27
2.3.2	Network security attacks .....	27
2.3.2.1	Denial of Service (DoS) attack.....	28
2.3.2.2	Distributed Denial of Service (DDoS) attack .....	28
2.3.2.3	SYN attack .....	29
2.3.2.4	Phishing attack .....	30
2.3.2.5	Brute-force (password guessing) attack.....	31
2.3.2.6	SQL injection attack.....	31
2.3.3	Network security breaches in academic institutions .....	32
2.4	Network security technologies in academic institutions .....	33
2.4.1	Firewalls .....	33
2.4.1.1	Packet filters.....	34
2.4.1.2	Stateful packet inspection .....	35
2.4.1.3	Proxy server .....	35
2.4.2	Intrusion Detection System (IDS).....	36
2.4.3	Intrusion Prevention System (IPS) .....	38
2.4.4	Network Access Control.....	38
2.4.5	Cryptography .....	38
2.4.6	Virtual Private Network (VPN).....	40
2.4.7	Malware protection software .....	41
2.5	Summary.....	41
<b>CHAPTER 3: RESEARCH METHODOLOGY .....</b>		<b>42</b>
3.1	Introduction .....	43
3.2	Research questions .....	43
3.2.1	Primary research question (PRQ) .....	44
3.2.2	Secondary research questions (SRQs).....	44
3.3	Research objectives.....	44
3.3.1	Primary research objective.....	44
3.3.2	Secondary research objectives .....	44
3.4	Research philosophy.....	45
3.4.1	Ontology .....	45
3.4.1.1	Objectivism.....	45

3.4.1.2	Subjectivism .....	46
3.4.2	Epistemology .....	46
3.4.2.1	Positivism .....	46
3.4.2.2	Realism .....	47
3.4.2.3	Interpretivism .....	47
3.5	Research approach .....	48
3.5.1	Deductive approach .....	48
3.5.2	Inductive approach .....	49
3.6	Research methodology .....	50
3.6.1	Quantitative research .....	50
3.6.2	Qualitative research .....	50
3.6.3	Mixed-methods research methodology .....	52
3.7	Research strategy .....	52
3.7.1	Survey .....	52
3.7.2	Experiment .....	53
3.8	Unit of analysis and unit of observation .....	54
3.9	Data collection .....	54
3.9.1	Questionnaire .....	55
3.9.2	Structured observation .....	56
3.9.3	Sampling .....	57
3.9.4	Sampling techniques .....	57
3.9.4.1	Probability sampling .....	58
3.9.4.2	Non-probability sampling .....	58
3.9.5	Sampling size .....	59
3.10	Research time horizons .....	59
3.11	Data analysis .....	60
3.12	Reliability and validity .....	60
3.13	Research design components .....	61
3.14	Summary .....	62
<b>CHAPTER 4: SURVEY DATA ANALYSIS .....</b>		<b>63</b>
4.1	Introduction .....	63
4.2	Questionnaire analysis .....	63
4.2.1	SECTION A: Demographics analysis .....	63
4.2.2	SECTION B: Network security challenges and security technologies .....	66
4.1.2.1	Secondary research question 1 .....	66
4.1.2.2	Secondary research question 2 .....	77
4.3	Summary .....	80



<b>CHAPTER 5: EXPERIMENTAL DATA ANALYSIS .....</b>	<b>83</b>
5.1 Introduction .....	83
5.2 Experimental setup .....	83
5.2.1 DHCP Starvation attack experiment.....	86
5.2.2 Rogue DHCP Server experiment .....	91
5.2.3 Media Access Control (MAC) Flooding experiment.....	92
5.2.4 Address Resolution Protocol (ARP) Poisoning attack experiment.....	97
5.2 Summary.....	110
 <b>CHAPTER 6: DISCUSSION .....</b>	 <b>113</b>
6.1 Introduction .....	113
6.2 Research questions .....	113
6.3 Discussion and implications of network security .....	113
6.4 Summary.....	120
 <b>CHAPTER 7: RECOMMENDATIONS AND CONCLUSION .....</b>	 <b>122</b>
7.1 Introduction .....	122
7.2 Review of the research study .....	122
7.3 Research Questions.....	123
7.3.1 Secondary Research Question 1 .....	123
7.3.2 Secondary Research Question 2 .....	125
7.3.3 Secondary Research Question 3 .....	125
7.3.4 Secondary Research Question 4 .....	127
7.4 Conclusion .....	131
7.5 Future Work .....	131
 <b>REFERENCES .....</b>	 <b>132</b>
 <b>ANNEXURE A: Informed Letter of Consent for Participant.....</b>	 <b>148</b>
<b>ANNEXURE B: Network Security Questionnaire .....</b>	<b>150</b>

## LIST OF FIGURES

Figure 1.1: A graphical illustration of Chapter 1: Introduction .....	1
Figure 1.2: Types of security breaches affecting higher academic institutions.....	6
Figure 1.3: Number of data breach incidents from 2011 to 2015 .....	6
Figure 1.4: Number of Records exposed after security breach between 2011 and 2015 .....	6
Figure 1.5: 2015 Incidents by threat vector .....	7
Figure 2.1: A graphical illustration of Chapter 2: Literature Review .....	16
Figure 2.2: A Local Area Network (LAN) .....	17
Figure 2.3: A Wide Area Network (WAN) .....	18
Figure 2.4: Eavesdropping attack.....	26
Figure 2.5: A generic representation of Distributed Denial of Service attack .....	29
Figure 2.6: A SYN attack .....	30
Figure 2.7: Basic Firewall setup .....	34
Figure 2.8: Exchanging information between entities using cryptography .....	39
Figure 2.9: VPN connecting two remote sites across the Internet .....	40
Figure 3.1: A graphical illustration of Chapter 3: Research Methodology .....	42
Figure 3.2: Research Onion .....	43
Figure 3.3: Deductive research approach .....	49
Figure 3.4: Inductive approach process .....	50
Figure 3.5: Classic experiment.....	53
Figure 3.6: Types of questionnaire.....	55
Figure 3.7: Relationship between population, sample, and individual cases .....	57
Figure 3.8: Sampling techniques.....	58
Figure 4.1: Type of higher academic institutions .....	64
Figure 4.2: Gender.....	64
Figure 4.3: Age category of participants.....	64
Figure 4.4: Technical IT positions held by participants.....	65
Figure 4.5: Highest qualifications of participants .....	65
Figure 4.6: Systems mostly concerned with at higher academic institutions.....	66
Figure 4.7: Attack vectors and security issues institutions are most concerned with .....	68
Figure 4.8: Network security breaches.....	68
Figure 4.9: Respondents' network security policy awareness .....	70
Figure 4.10: Mandatory user training and education on network security policy .....	72
Figure 4.11: IT budget allocation satisfaction .....	73
Figure 4.12: Staffing level of the IT department.....	74
Figure 4.13: Penetration testing performed .....	75
Figure 4.14: Remedial actions taken on reported security alerts and incidents .....	77

Figure 4.15: Usage of technologies and security controls at higher academic institutions ....	78
Figure 4.16: Level of satisfaction on security technologies.....	79
Figure 5.1: OSI model.....	84
Figure 5.2: Physical network topology for both experimental network and control network ..	85
Figure 5.3: How DHCP works .....	86
Figure 5.4: DHCP Scope and Address pool .....	87
Figure 5.5: Leased client IP addresses .....	87
Figure 5.6: Attacker's computer network configuration .....	88
Figure 5.7: Leased client IP addresses after attacker's computer connected to the network	88
Figure 5.8: Launching DHCP attack.....	88
Figure 5.9: DHCP DISCOVER packet on Yersinia .....	89
Figure 5.10: DHCP DISCOVER on Wireshark .....	90
Figure 5.11: DHCP statistics after attack.....	90
Figure 5.12: Client fails to connect to the network after attack .....	91
Figure 5.13: Client computers assigned APIPA address .....	91
Figure 5.14: Rogue DHCP server IP configuration .....	91
Figure 5.15: Client received fake network configuration after renewing its lease period .....	92
Figure 5.16: MAC address table count before attack.....	93
Figure 5.17: Attacker launching MAC flooding .....	93
Figure 5.18: Fake MAC addresses being sent to the switch.....	94
Figure 5.19: MAC address table count after attack .....	94
Figure 5.20: Fake MAC addresses flooded MAC address table .....	95
Figure 5.21: Analysis of MAC Explorer for MAC flooding .....	96
Figure 5.22: Analysis of MAC Conversation for MAC flooding.....	96
Figure 5.23: The new attacker's IP address obtained from DHCP server.....	97
Figure 5.24: Server's ARP cache before attack.....	97
Figure 5.25: Cisco Catalyst 2096 switch MAC address table and ARP cache before attack.	98
Figure 5.26: Ettercap listening on eth0 interface .....	98
Figure 5.27: List of discovered hosts by Ettercap tool .....	98
Figure 5.28: ARP poisoning status.....	99
Figure 5.29: Captured remote connection from the server to the switch.....	99
Figure 5.30: Spoofed MAC address with attacker's MAC address .....	100
Figure 5.31: Captured credentials over remote connection to switch .....	100
Figure 5.32: Cisco Catalysts switch ARP cache after attack .....	100
Figure 5.33: ARP Poisoning Attack results on Colasoft Capsa 9.1 Enterprise.....	101
Figure 5.34: Initial configuration of the switch .....	103
Figure 5.35: Encrypted console password .....	103
Figure 5.36: Configuring Secure Shell Protocol on the switch .....	104

Figure 5.37: Encrypted password for remote connection to the switch.....	104
Figure 5.38: Creating VLAN 10 and assigning IP address .....	104
Figure 5.39: Port security configuration on FastEthernet 0/1 to FastEthernet 0/5.....	105
Figure 5.40: Configuration on shutting down unused switch ports.....	106
Figure 5.41: Configuration for DHCP snooping and ARP inspection .....	106
Figure 5.42: DHCP snooping and ARP inspection on trusted interface .....	106
Figure 5.43: DHCP snooping and ARP inspection on untrustworthy interfaces.....	107
Figure 5.44: Error message when switch experienced DHCP Starvation attack.....	107
Figure 5.45: Client computer after DHCP Starvation mitigation.....	108
Figure 5.46: Error message when switch experienced MAC Flooding attack .....	108
Figure 5.47: Error message when switch experienced ARP Poisoning Attack .....	108
Figure 5.48: Changing the state of interface FastEthernet 0/5 from shutdown mode .....	108
Figure 5.49: Security violation on interface FastEthernet 0/5 .....	109
Figure 5.50: FastEthernet 0/5 on error disabled mode .....	109
Figure 7.1: Proposed Framework for South African higher academic institutions .....	130

## LIST OF TABLES

Table 2.1: Technological vulnerabilities .....	21
Table 2.2: Configuration vulnerabilities .....	22
Table 2.3: Security policy vulnerabilities.....	23
Table 3.1: Qualitative research versus quantitative research .....	51
Table 3.2: Advantages and disadvantages of questionnaire .....	55
Table 3.3: A summary of research design components and proposed method for each component.....	61
Table 4.1: Summary of findings .....	81
Table 5.1: Summary of findings before and after mitigation.....	111

## LIST OF ABBREVIATIONS

Abbreviation	Full terminology
ADC	Application Defence Centre
ADDS	Active Directory Domain Services
AES	Advanced Encryption Standard
APIPA	Automatic Private IP Addressing
ARP	Address Resolution Protocol
BDE	BitLocker Drive Encryption
BYOD	Bring Your Own Device
CAM	Content Addressable Memory
CPU	Central Processing Unit
DAI	Dynamic Address Resolution Protocol Inspection
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
EFS	Encrypting File System
FTP	File Transfer Protocol
HAI	Higher Academic Institution
HEI	Higher Education Institution
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISP	Internet Service Provider
IT	Information Technology
L2TP	Layer Two Tunnelling Protocol
LAN	Local Area Network
MAC	Media Access Control
NAC	Network Access Control
NBA	Network Behaviour Analysis
NIDS	Network-based Intrusion Detection System
NSM	Network Security Monitor

Abbreviation	Full Terminology
PCA	Principal Component Analysis
PRQ	Primary Research Question
QoS	Quality of Service
SP	Service Provider
SPSS	Statistical Package for the Social Sciences
SQL	Structured Query Language
SRQ	Secondary Research Question
SSH	Secure Shell
SSL/TLS	Secure Sockets Layer/Transport Layer Security
SSTP	Secure Socket Tunnelling Protocol
SVI	Switch Virtual Interface
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UC	University of California
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WWW	World Wide Web

## CHAPTER 1: INTRODUCTION

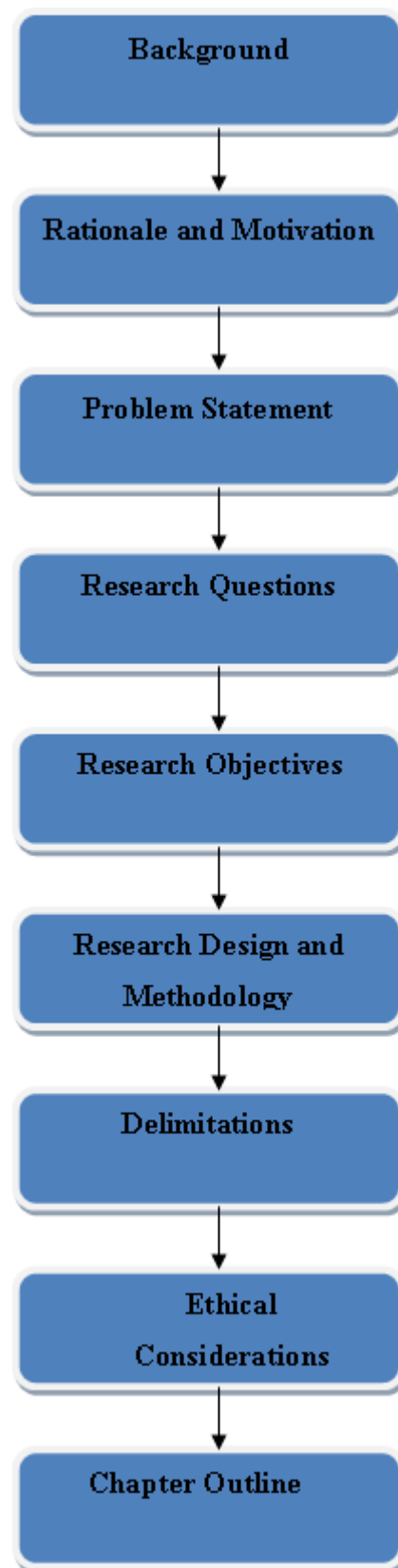


Figure 1.1: A graphical illustration of Chapter 1: Introduction



## 1.1 Background

With network technology growing remarkably fast, network infrastructures are more complicated and it has become more challenging to implement and maintain network security. Most organisations' operational infrastructure use computer and network systems that have numerous capabilities such as storing, processing, and distributing data worldwide. The organisations generally store the information on their networks of which some information can be classified as sensitive and confidential. This information plays a crucial role in running the daily organisations' operations. However, organisations with inadequate network security attract attackers to infiltrate their networks, hence have unauthorised access to organisation's confidential information (Ciampa, 2012). Once the organisation's network is compromised, the organisation may be exposed to security risks such as leakage of confidential records. This act may lead to loss of crucial information and privacy of affected parties hence lead to bad reputation.

The improved integration of computer and network systems allow network users to enjoy the convenience and the benefits of the network. However, this improvement has also brought unique levels of risks that may impact negatively on organisations' operations, especially when using the Internet. The Internet offers computer users the ability to learn and to find valuable and useful sources of information. However, Internet has also made it easy for computer users such as students and staff to access inappropriate content and to use academic networks for non-educational purposes (Wu, 2010; Liu & Zheng, 2011). For example, the introduction of viruses and worms into organisations' networks and usage of organisations' networks for illegal content sharing rendered them open to abuse. Burney & Khan (2010) state that viruses, worms and malicious conduct continue to cause new threats to academic services and assets. Therefore, computer and network security are very important and are key components to enhance security across the network to protect sensitive information; thus, network security should be a necessity for any organisation.

**Computer security** is the process of protecting computer systems from unauthorised users by ensuring data confidentiality, integrity and availability on a computer (Masrom & Ismail, 2008). The main purpose of computer security is to ensure that all information and computer resources on computer systems are secured. Thus, computer security helps to remove any vulnerability on a computer system that can harm or result in data loss when exploited. As a result, security has become one of the main concerns when an organisation connects its private network to the Internet. Despite the business type, network users require different Internet services such as Internet mail, File Transfer Protocol (FTP) and World Wide Web (www). Consequently, the demand of these services is very high. Therefore, network administrators have increasing concerns about the security of their networks as well.

**Network security** can be defined as the protection of information stored, transmitted, shared, and processed over the network from unauthorised users (Yi & Yifei, 2010; Ma et al., 2016). McGee et al. (2004) define network security as a specific field in computer networks constantly evaluating new threats in order to secure network infrastructure. As such, it relies on layers of protection and diversity of components to increase the security of the computer network (Malik, 2003). According to Khobragade et al. (2011), network security ensures privacy, confidentiality, and data integrity by preventing and detecting unauthorised actions performed by network users. In fact, network security is crucial in computer networking as it imposes the policies and procedures developed and to be adopted by organisations—including academic institutions—to protect the information. It also ensures that the projected quality of service (QoS) for the network is not compromised while protecting the data. Therefore, based on a study done by Liu & Zheng (2011), network security ensures data confidentiality, integrity, and availability. As a result, network security has become increasingly a prominent concern that cannot be ignored or else the security and privacy of the organisations will be severely affected by network security threats and attacks.

Thus, the implementation of network security should take into consideration a number of things such as network requirements, tools to be used on the network, and the environment. As a result, a proper implementation of network security could help reduce the possibility of successful attacks by providing timely attack mitigation through intrusion detection systems, intrusion protection systems, and other security measures. This could also help network administrators know how to respond properly to attacks or network incidents. When implementing network security, it is crucial to understand security attributes and objectives in order to provide sufficient protection for network assets. These attributes and objectives include confidentiality, integrity, availability, authentication, authorisation, and accounting.

### **1.1.1 Confidentiality**

Confidentiality can be defined as the protection of information disclosure from unauthorised users (Vachon, 2012; Brooks, 2014; Arachchilage & Love, 2014). Organisations deal with confidential information that is normally processed and stored on computers on the network and communicated among the network users. It is important that confidential information is kept secret, preventing any unauthorised access to it. If this confidential information falls into the reprehensible hands of a hacker due to poor security measures or information being leaked by personnel, this could have negative consequences such as damage to the organisation's reputation, identity theft, and irreparable financial loss.

### **1.1.2 Integrity**

As mentioned by Vachon (2012), Dean (2013) and Brooks (2014), integrity refers to the assurance that information has not been modified without authorisation, hence, it protects against any errors and alteration of data. Within an organisation, there are Information Technology (IT) professionals who are being given the authority to access crucial data; however, they may also be the cause of errors and alteration of data resulting in a malicious threat. Malicious threats happens when authorised or unauthorised personnel misuse their powers to intentionally modify, delete, or corrupt data that is crucial to the smooth operations of the organisation. Attackers from outside the organisation can also intentionally modify the data either stored on the computer system or transmitted across the network.

### **1.1.3 Availability**

Availability is the process of ensuring that the information or network resources are available to authorised users to carry on with their activities in the organisation at any time (Vachon, 2012; Dean, 2013; Brooks, 2014; Safa et al., 2016). As a result, the authorised users are neither denied access to the content of the information nor to the resources. Therefore, this enhances the organisation's productivity and performance.

### **1.1.4 Authentication**

Authentication is the security objective that uniquely identifies a user or device normally using a username and password before being allowed access to network resources (Yu & Tsai, 2011; Regan, 2013; Zacker, 2014). Once the identity of the user or device is verified, the user or device can then access network resources depending on the user or device's authorisation. Authentication can be performed using a variety of methods, such as passwords, smart cards, and biometric factors like fingerprints. However, the most common authentication method in computer networks is the password.

### **1.1.5 Authorisation**

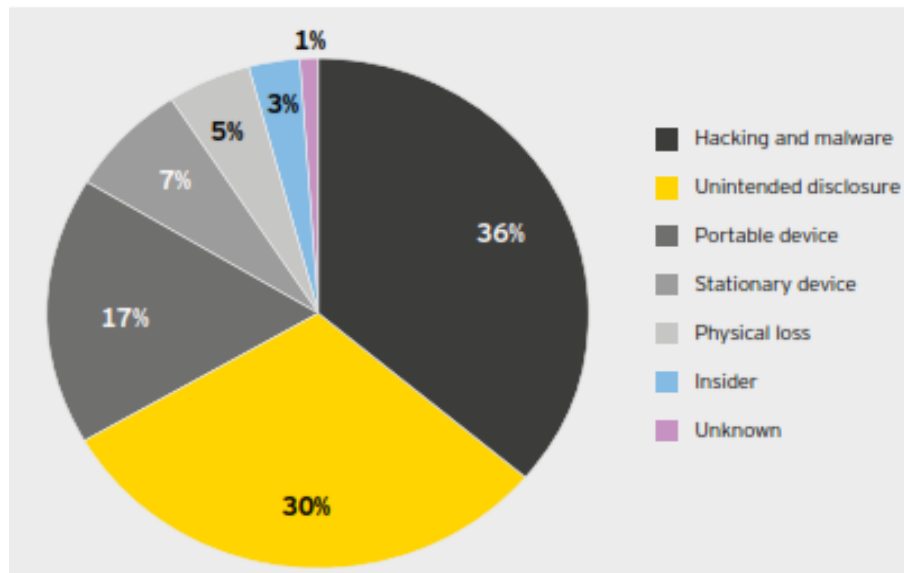
Authorisation is the security objective granting a user or a program access rights and permission to carry out certain actions on a system or computer (Yu & Tsai, 2011; Regan, 2013; Zacker, 2014). This security objective ensures that only authorised users have access to certain resources.

### 1.1.6 Accountability

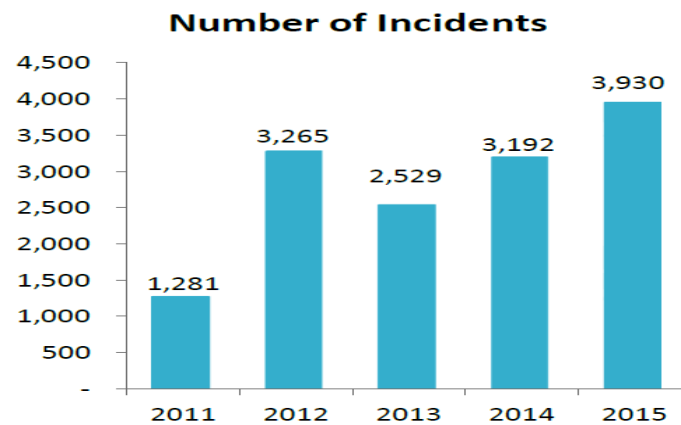
Accountability is the security objective allowing the tracking of an entity's actions on the system back to that particular entity (Yu & Tsai, 2011; Regan, 2013). This actually requires all network users, including network administrators, to be held responsible for their communications and behaviours that affect an organisation's security.

Unlike commercial enterprises, college and university networks are implemented on a complicated network infrastructure, and support confidential information, research outputs and educational functions (Liu & Zheng, 2010). Academic networks are difficult to protect due to the nature of the open computing environment consisting of many users, network devices and applications (Cisco Networking Academy, 2007). As a result, academic network administrators are therefore challenged to ensure that all devices joining the network are secured and ensure a reliable and instinctive user experience (Cisco Networking Academy, 2007; Murphy, 2014) as higher academic institutions do not have sufficient control over the devices used by students and staff on their campuses. Network administrators have to achieve the conflicting goals of maintaining network security while providing an open networking environment (Levine et al., 2003; Luker & Petersen, 2003). In addition, it is difficult for network administrators to effectively identify and mitigate network security threats and attacks and protect limited bandwidth resources from abuse and misuse.

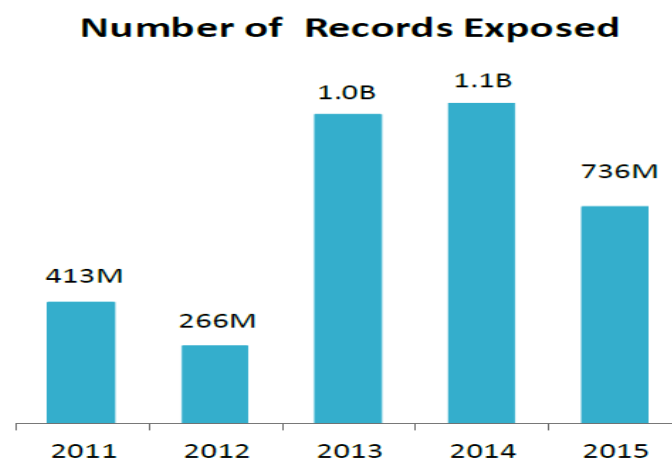
Higher academic institutions are faced with the challenge of network security threats and attacks and are proven vulnerable due to an open environment, leading to loss of confidential information and finances (Jones & Stallings, 2011; Raman et al., 2016). According to Raman et al. (2016), hacking, malware, and unintended disclosure are among the main causes of security breaches at higher academic institutions. Figure 1.2 shows different types of security breaches affecting higher academic institutions. Higher education institutions (HEIs) also experience hacking incidents or network attacks due to research data (intellectual property) that help generate funding from government to contribute to the country's economy (Chabrow, 2015). A security analyst, Tyler Shields (working at Forrester Research), asserts that higher academic institutions are easy targets for network attacks due to their open nature of communication (Roman, 2014). Based on Hearn (2016), about 79% of universities globally have had their reputation damaged due to network security attacks. Figure 1.3 shows the number of incidents worldwide that took place at higher academic institutions over a period of five years from 2011 to 2015. Figure 1.4 shows the number of records exposed over the same period of five years after security breaches.



**Figure 1.2: Types of security breaches affecting higher academic institutions**  
(Source: Raman et al., 2016)

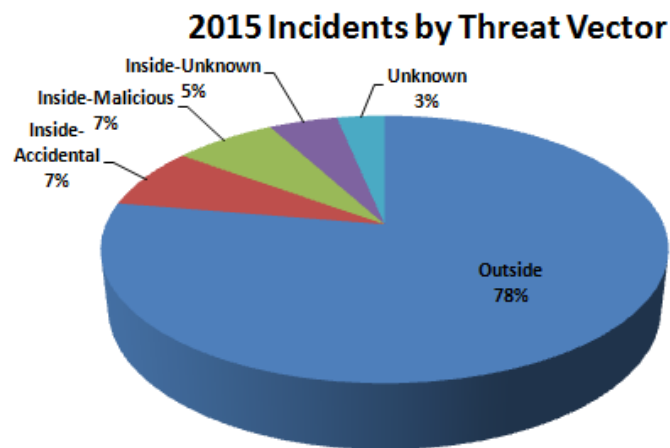


**Figure 1.3: Number of data breach incidents from 2011 to 2015**  
(Source: Risk Based Security, 2016)



**Figure 1.4: Number of Records exposed after security breach between 2011 and 2015**  
(Source: Risk Based Security, 2016)

Based on Figure 1.3, the number of incidents reported increased in 2011 and 2012. In 2013, the number of incidents declined; however, in 2014 the incidents gradually increased again. According to Risk Based Security (2016) in its Data Breach QuickView report, the year 2015 experienced a high number of data breach incidents as compared to other years. In 2015, the number of incidents reported amounted to 3,930, exposing 736 million records as shown in Figures 1.3 and 1.4 respectively. Although there were many incidents in 2015, more than one billion records were exposed in 2013 and 2014. This is worrisome for any type of industry to have such a high number of incidents and records exposed.



**Figure 1.5: 2015 Incidents by threat vector**  
(Source: Risk Based Security, 2016)

According to Risk Based Security (2016), as shown in Figure 1.5, 78% of the incidents reported in 2015 were activities conducted outside the organisation, accounting for 64.6% of hacking incidents and exposing 58.7% of records. Security breaches, regardless of source (internal or external), have a negative impact on any organisation; therefore, network security should be prioritised. The occurrence of network security threats and attacks needs to be addressed urgently in order to improve network security.

The purpose of the study is to uncover ways that can assist in fighting against network security threats and attacks to prevent the misuse/abuse of sensitive information and propose a framework to be implemented at higher academic institutions to improve network security.

## **1.2 Rationale and motivation**

Network security has been of great concern to network managers and information technology (IT) directors because they are responsible for the security of an organisation's information assets. The ever-increasing quantity and complexity of network attacks continue to pose

unforeseen threats to corporate networks, resulting in an increase in the number of successful attacks every year. One such example is network outages caused by viruses and worms. As a result, academic institutions have been suffering from data breaches as well as loss of privacy and productivity degradation that could lead to a negative reputation (Piazza, 2006; Dulanović et al., 2008). The purpose of the study is to find possible ways for mitigating network security threats and attacks at higher academic institutions and protect network resources from security breaches.

The success of this research study could benefit academic institutions as well as non-academic institutions that heavily depend on computer networks, by protecting computer resources, ensuring data integrity, limiting access to authorised users, and maintaining data confidentiality. The study would also help to improve compliance with security policies by making compliance a fundamental requirement for access to the network and minimise vulnerabilities on user machines through periodic evaluation and remediation.

Most importantly, this research study's success could be achieved by implementing various security technologies such as firewalls, intrusion detection and prevention systems (IDPS), encryption, and other security mechanisms to defensively protect information resources. The research study could provide more timely attack mitigation through security intelligence that could recognise threats and recommend action before an entire network is affected.

### **1.3 Problem statement**

The growing dominance of network security threats and attacks has become a concern at higher academic institutions. The academic institutions experience intrusions and attacks, hence suffer financial loss from computer downtime, data integrity and confidentiality breaches (Piazza, 2006). According to McIlwraith (2006), these incidents may be the results caused by inadequate security awareness among the staff members and lack of effectively enforcing security policies. Similarly, colleges and universities such as commercial enterprises face the problem of growing security threats and attacks whereby applications, assets, and information need to be protected (Cisco Networking Academy, 2007). Unlike enterprises, academic environments have unique network requirements for openness, flexibility, and bandwidth resources control that are beyond those of most business networks (Jones & Stallings, 2011). As a result, a network security breach in an academic network can compromise productivity of students, staff, and faculties and tarnish an institution's reputation. Therefore, this study attempts to determine possible ways that can enhance network security at HEIs by combating network security threats and attacks and propose a framework to improve network security at HEIs.

## **1.4 Research questions**

This research study is driven by a primary research question and secondary research questions, indicated below.

### **1.4.1 Primary research question (PRQ)**

**PRQ: What can be done to mitigate network security threats and attacks at higher academic institutions<sup>1</sup> in South Africa?**

### **1.4.2 Secondary research questions (SRQs)**

**SRQ1:** What are the challenges surrounding network security at higher academic institutions?

**SRQ2:** What security technologies are available to protect against network security threats and attacks?

**SRQ3:** How can network security be addressed and improved in order to protect against network security threats and attacks in South Africa?

**SRQ4:** What framework can be proposed for South African higher academic institutions to improve network security?

## **1.5 Research objectives**

The primary and secondary research objectives, derived from the research questions, are as follows:

### **1.5.1 Primary research objective**

- **To establish ways to mitigate network security threats and attacks at higher academic institutions in South Africa**

### **1.5.2 Secondary research objectives**

- To determine the challenges surrounding network security at higher academic institutions

---

<sup>1</sup> Higher academic institutions and higher education institutions (HEIs) are used interchangeably in this study as both refer to post-school academic institutions offering accredited qualifications.



- To identify what security technologies are available to protect against network security threats and attacks
- To determine effective ways to improve network security at higher academic institutions in South Africa to address the network security threats and attacks
- To develop and propose a framework for improving network security in South African higher academic institutions

## **1.6 Research design and methodology**

Research design is defined differently by different authors. According to Grove et al. (2015:245), research design is defined as “a blueprint for conducting a quantitative study that maximizes control over factors that could interfere with the validity of the findings”. Other authors define research design as “the researcher’s overall for answering the research question or testing the research hypothesis” (Polit et al., 2001:167). Therefore, research design can be seen as the master plan shedding light on the research study in order to answer the research questions. In short, research design should clearly specify what kind of data is needed, what methods would be used for data collection and data analysis, and how the research questions are answered.

Research philosophy is associated with ontology and epistemology. This research study adopts an objectivist ontological stance and positivist epistemological stance. A positivist philosophy focuses on discovering the truth and emphasises empirical data through scientific methods (Henning et al., 2004:17). This study thus adopts a deductive approach to studying social phenomena because the researcher wants to be objective. Consequently, this gives importance to research methods focusing on quantitative analysis and specifically for this research study, survey, and experimental research strategies. The survey instrument, primarily a questionnaire, was designed and sent via electronic mail to specialised technical IT security personnel (the IT services sections, not the academic ICT departments) at HEIs in order to identify network security threats and cyber-attacks. The purpose of the survey was to determine what security issues and challenges they experience when securing network systems and what security technologies are being deployed at higher academic institutions.

This research study focuses on HEIs in the Republic of South Africa and seeks to find possible ways to assist HEIs in overcoming network security threats and attacks. The research study is explanatory, experimental, and quantitative.

### 1.6.1 Explanatory research

With explanatory research, the researcher establishes any causal relationship between variables in order to explain effects or factors concerning the research problem (Saunders et al., 2009). In this research study, the researcher determines what causes network threats and attacks and how these pose as network security threats at HEIs.

### 1.6.2 Experimental design

Experimental design was carried out to assess the security threats and attacks on higher academic institutions' networks. Experimental design is the research design whereby experiments are systematically conducted in a natural setting such as the laboratory (Wilson, 2014). This research design is more concerned with determining the causal relationships that exist between the variables, mainly the dependent variable and independent variable(s). According to White & McBurney (2012:120-121), a dependent variable is defined as "a measure of the subject's behaviour that reflects the independent variable's effects," while the independent variable is defined as the variable "that is believed to cause some change in the value of the dependent variable". In this research study, the dependent variable is *network security* and the independent variables are network security *threats* and *attacks* because poor implementation of network security makes a network vulnerable to security threats and attacks.

Experimental design requires intervention or treatment of an independent variable to evaluate the impact it makes on the dependent variable (Saunders et al., 2009). Experimental design involves two groups: experimental group and control group. The experimental group is exposed to intervention or treatment while the control group is not. This is done to assess or measure the changes that occur with the dependent variable before and after the intervention has been incorporated into the independent variable. For this research study, there were two Local Area Networks (LANs) designed, an experimental network and the control network. Both experimental network and control network were configured with minimal security measures and configurations but the experimental network was manipulated to impose threats and attacks on the network. Real-time monitoring tools were used to examine the network traffic in and out of the network. The data captured or collected was analysed for any network intrusions and network attacks to identify the effectiveness of the security protection mechanisms.

### **1.6.3 Quantitative research**

Quantitative research is defined differently by various authors. Aliaga & Gunderson (2002:3) define quantitative research as “explaining phenomena by collecting numerical data that are analysed using mathematically based methods (in particular statistics)”. Hyde (2000:80) defines a quantitative research approach as “research that draws a large and representative sample from the population of interest, measure the behavior, and characteristics of that sample and attempt to construct generalisations regarding the population as a whole”. Bryman & Bell (2011:717) define quantitative research as research that “usually emphasises quantification in the collection and analysis of data”.

Quantitative research can therefore be viewed as research that fundamentally collects numerical data using statistical techniques or mathematical measures in order to provide an explanation of a specific phenomenon. This research methodology is used to measure the problem based on how the numerical data are generated or how data can be changed into useable statistics for the generalisation of the findings from a much bigger sample population (Muijs, 2010). Therefore, quantitative research uses quantifiable data in order to devise facts and discover patterns that exist in a research study/project. The questionnaire questions are designed in a specific manner to enable responses to be mathematically analysed. In summary, a quantitative research methodology is adopted for the researcher to obtain unbiased results independent of personal judgment.

### **1.6.4 Research participants**

The Information Technology (IT) specialised technical security personnel, including IT Manager, IT Director, Security Director, System Engineer, Network Engineer, System Administrator, Security Administrator, Network Administrator, Network Operator, Security Analyst, Security Manager, Compliance Auditor, Compliance Officer and other IT professionals such as Network Technicians, participated in this research study. Mostly these participants hold positions at high ranking levels and as a result, are believed to be competent and equipped with technical knowledge, skills and values relating to systems and network security management. It is therefore assumed that they should be able to provide information that can assist the researcher in understanding the research problem in a wider context and assist towards achieving the research objectives.

### **1.6.5 Data analysis**

The data collected from the experiments and survey questionnaire were analysed to address the following objectives:

- Determine the challenges surrounding network security at HEIs
- Identify what security technologies are available to protect against network security threats and attacks
- Determine effective ways to improve network security at HEIs in South Africa to address network security threats and attacks

The data collected using questionnaires were analysed using statistical analysis techniques utilising a data management software package called *Statistical Package for the Social Sciences (SPSS)*. The data collected from the experiments were analysed using network analysis software packages called *Wireshark Network Analyser* and *Colasoft Capsa 9.1 Enterprise*. The information obtained gives an insight into network security levels at HEIs.

### **1.7 Delimitations**

This study focuses on network security threats and attacks at higher academic institutions in Gauteng province in the Republic of South Africa, mainly to find possible ways to assist in reducing network breaches at HEIs.

### **1.8 Ethical considerations**

Ethics are the moral code concerned with differentiating between good and bad behaviour or values; hence they control the actions and conduct of people or an individual (Blumberg et al., 2014). According to Gay et al. (2015), researchers across all fields have the huge responsibility of carrying out research studies successfully by building a trust relationship with the participants and maintaining professionalism by adhering to ethical standards. To ensure the success of the study and confirming that the proper principles are being followed, the researcher obtained informed consent from the participants before conducting this research study (Annexure A). According to Easterby-Smith et al. (2012), it is essential for the researcher to state the purpose of the study clearly so that the participants can notice the value of the study. The purpose of the study was clearly explained to the participants so that participants could decide whether to take part in the research study or not. This encouraged the participants because they were informed of the benefits of taking part in the research.

According to Bryman & Bell (2011), explaining the purpose of the study assures the participants that they would not be subjected to any harm such as emotional stress or embarrassment for taking part in the research study; their dignity would be respected and prioritised. It was clearly stated that participation in the research study is completely voluntary. However, based on McNamara (1994), voluntary participation can sometimes result in a low number of responses leading to response bias. Dillman (2007) recommends

the use of various contacts (communication techniques) to promote high response rates. Easterby-Smith et al. (2012) assert that the survey should be short and made easy to answer in order to increase the chances of obtaining more replies from participants. The researcher should also reassure the participants of their confidentiality and anonymity for participating in the research study in order to gain their trust that could increase the response rate (Easterby-Smith et al., 2012).

To obtain a high response rate, the participants were reminded twice via email to complete the questionnaire. They were also reassured of the confidentiality of their answers and their anonymity should they decide to take part in the study (Annexure A). It was explained to participants that their names, personal information, and responses would remain anonymous unless they give their consent to release the information. This aspect of ethics is crucial as it assures participants that the researcher will protect their privacy regarding the information being provided during the research study. Saunders et al. (2009) confirm the importance of assuring participants of confidentiality and anonymity of the information being provided to remove any doubts or ethical concerns. This, according to Polit et al. (2001) is done to respect human dignity and justice.

## **1.9 Chapter outline**

The outline of this research study is as follows:

### **Chapter 1: Introduction**

In this chapter, a brief introduction of network security in academic networks is provided. The rationale and motivation of the research study are discussed. The problem statement, research questions, research objectives, research design, delimitations, and ethical considerations are described and an outline of the study is given.

### **Chapter 2: Literature Review**

In Chapter 2, an overview of various types of network environments that are implemented at HEIs is provided. The challenges faced by HEIs as well as the different types of security technologies, which may be used at higher academic institutions and relevant literature, are discussed.

### **Chapter 3: Research Methodology**

Chapter 3 provides detailed information on how this research study was carried out. The research philosophy, research approach and research strategy to be implemented in this research study are addressed. The research methods selected for the study are

emphasised. A detailed description of data collection and data analysis techniques are provided.

#### **Chapter 4: Survey Data Analysis**

This chapter entails the analysis and interpretation of the data obtained from the survey questionnaire carried out. Thus, the results obtained in terms of the research objectives are discussed.

#### **Chapter 5: Experimental Data Analysis**

This chapter elaborates on how the experiments were conducted. The outcome of the experiments is provided and the results are discussed.

#### **Chapter 6: Discussion**

This chapter critically examines research findings from both the survey and the experiments conducted and the implications on network security.

#### **Chapter 7: Recommendations and Conclusion**

The final chapter concludes the research study by addressing the research objectives as well as what the study has achieved. This chapter also highlights future research that can be conducted.

## CHAPTER 2: LITERATURE REVIEW

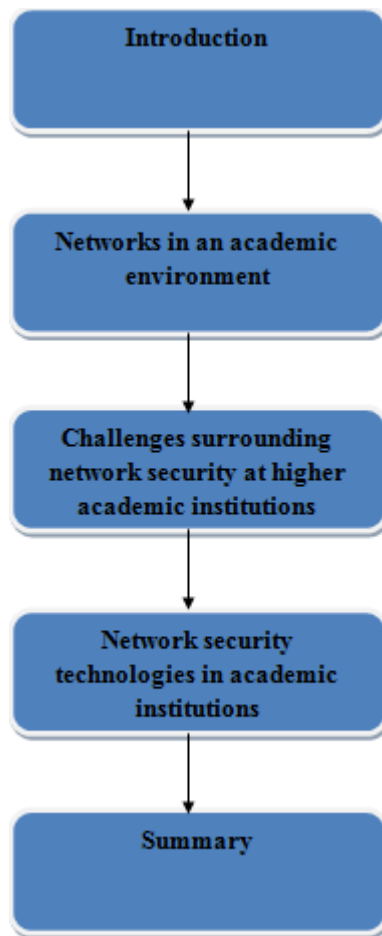


Figure 2.1: A graphical illustration of Chapter 2: Literature Review

### 2.1 Introduction

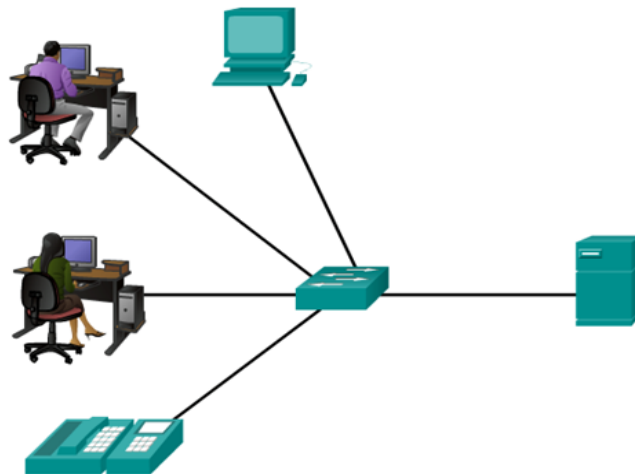
Colleges and universities have introduced many educational benefits through connectivity to academic networks. These include the utilisation of network supported distance learning, cluster computing and digital libraries. It has enhanced students' ability to acquire knowledge, thereby providing a supportive teaching and learning environment. However, HEIs have complex and diverse computer systems that hold crucial information such as financial data and students' academic records, making these systems vulnerable to different kinds of security attacks.

In this chapter, different types of networks commonly deployed in an academic environment are discussed. Also discussed are the network security challenges faced by academic institutions as well as vulnerabilities, network security threats, network security attacks and hacking incidents in HEIs. Lastly, security technologies used in academic institutions are elaborated on.

## 2.2 Networks in an academic environment

A network is a group of computer systems or devices connected together to share information and resources (Cisco Networking Academy, 2014). A network provides easy communication between network users by means of collaboration tools such as instant messaging, voice and video chats. It offers centralised administration that helps reduce the administrative costs that can be incurred when managing the data and devices on the network (Cisco Networking Academy, 2014). A network further assists in reducing data duplication and corruption because data stored on servers can only be accessed by authorised users (Ciampa, 2012).

A network can be distinguished by characteristics such as the area it serves, the media used for connecting network devices and different types of networking devices used (Donahue, 2011; Cisco Networking Academy, 2014). The commonly used network types in an academic environment include Local Area Network (LAN), Wireless Local Area Network (WLAN) and Wide Area Network (WAN). LAN can be defined as the computer network interconnecting end devices within a limited area that run under one administrative control such as a campus, home or school (Dean, 2013; Cisco Networking Academy, 2014). Figure 2.2 shows a generic diagram of a Local Area Network.

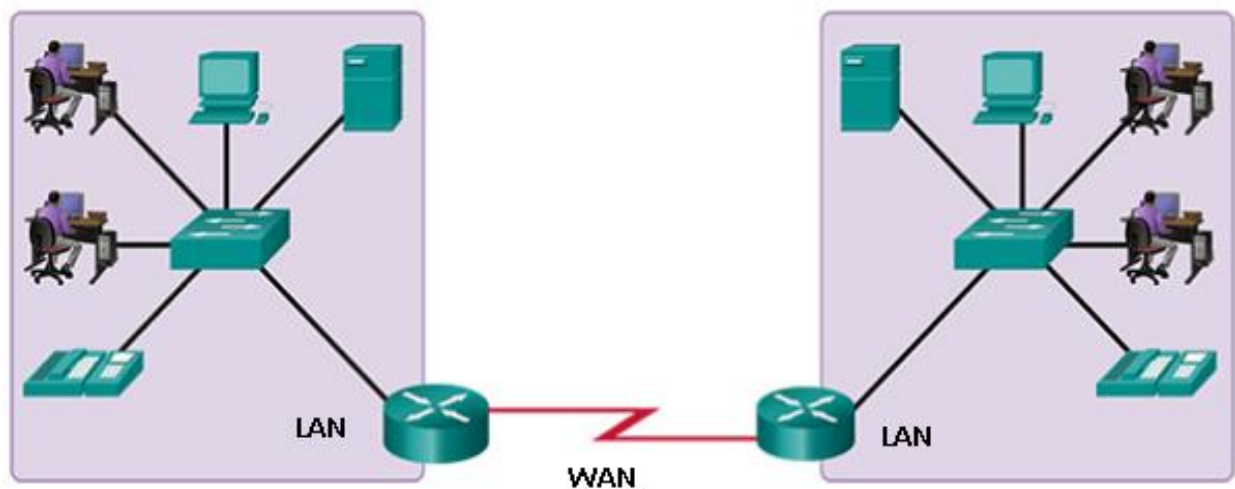


**Figure 2.2: A Local Area Network (LAN)**  
(Source: Cisco Networking Academy, 2013)

In this network, there are three desktop computers, a Voice over IP (VoIP) phone and a server. All of these end devices are connected to a LAN switch using a network cable, in particular, a straight-through cable to communicate with each other. The transmission technologies often used in LANs are Ethernet for twisted pair cabling and wireless connection.



WLAN is a network that connects a group of wireless devices within a certain area to an access point using electromagnetism (Dean, 2013; Gopalakrishnan, 2014). WLAN is well liked because it is easy to install and allows users easy movement or mobility within the coverage area that increases the users' productivity. WAN is a network that connects multiple LANs in locations geographically separated. Wide Area Networks are usually administered by Internet service providers (ISPs) or by service providers (SPs) and offers slower-speed links among Local Area Networks. An Internet is an example of WAN (Dean, 2013). Figure 2.3 shows a generic diagram of a Wide Area Network. In this network, there are two Local Area Networks, each connected to a router to allow network devices within a LAN to communicate with other network devices outside the LAN.



**Figure 2.3: A Wide Area Network (WAN)**  
(Source: Cisco Networking Academy, 2013)

### **2.3 Challenges surrounding network security at higher academic institutions**

With the development and the use of Internet and network technologies ever increasing, academic institutions face many challenges, including vulnerabilities, network security threats and cyber-attacks. These cyber-attacks can originate from different sources such as mobile devices and access channels. Based on a study conducted by Murphy (2014), the cyber-attacks exploit a wide range of potential weaknesses such as social engineering, Bring Your Own Device (BYOD) policies, design flaws and botnet activities. Therefore, network security threats and cyber-attacks are a significant challenge faced by academic institutions, which may cause a negative impact on systems and Information Technology (IT) resources. Rezgui & Marks (2008) state that it is very important to understand challenges and increasing IT security threats and attacks faced by HEIs to avoid potential data loss, bad reputation and financial loss.

According to studies performed by Jones & Stallings (2011) and Singh et al. (2016), colleges and universities are the primary targets of network security threats and cyber-attacks because of the enormous amount of computing power they possess and open access they provide to resources. This open access might result in weak Internet gateway firewalls, minimal configuration of computers and network devices, malware infections, and insufficient monitoring of the network for unauthorised access (Luker & Petersen, 2003; Raman et al., 2016). Thus, providing students and hackers or attackers the opportunity to exploit Information Technology resources makes the systems a target for cyber-crimes. Based on a study by Jackson et al. (2004), the rate of network traffic growth has become ever more difficult to monitor and to isolate threats from normal activities. Therefore, Levine et al. (2003) and Luker & Petersen (2003) believe it is extremely challenging for network administrators at HEIs to provide academic freedom while at the same time attempting to implement strict control measures on the networks. According to Raman et al. (2016), inadequate physical security affects the capability of HEIs to establish the source of network attacks or security incidents that have physical elements. This therefore creates a serious challenge for higher academic institutions.

As stated by Song & Ma (2012), academic institutions have standards and legal responsibility to follow in order to protect data and maintain data confidentiality. Academic institutions must therefore ensure and maintain a secure environment while providing the balance between the open environment and managing security against malware and sensitive data extrusion (Rezgui & Marks, 2008; Marchany, 2014). Thus, balancing academic freedom, which means allowing an open environment and tightening network security, is an extremely challenging task.

Malik (2003) clearly states that network security has become increasingly important to ensure consistent security throughout the entire network. However, according to an Information Security Officer, Joshua Mauk, at the University of Nebraska in his interview with Infosecurity Magazine, academic institutions have decentralised systems that results in applying different security protocols or strategies transversely on the network (Bradbury, 2013). This leads to inconsistent security in the protection of confidential information and intellectual property. Furthermore, it becomes complicated to enforce efficient security practices with decentralised systems (Raman et al., 2016; Singh et al., 2016). Consequently, this essential characteristic of decentralised systems creates a number of challenges such as leadership, technical infrastructure and decision-making. May & Lane (2006) indicate that these decentralised systems often become the target of attacks because they are exposed to vulnerabilities.

Higher academic institutions also face a lack of skilled personnel who possess the required attributes needed in the network security field in order to deploy, maintain, and most importantly, manage the network without creating vulnerabilities with malicious intent in the systems (Marchany, 2014). According to Wu (2010), IT departments are also overwhelmed with budget and resource constraints due to a lack of funding. Funding plays a crucial role in hiring and maintaining qualified IT personnel because of the competitive edge with regard to industry salaries. Furthermore, inadequate funding prevents HEIs from deploying the necessary security technologies to reduce network security threats and attacks (Raman et al., 2016). This has a dire effect on operational efficiency, as the IT departments cannot fully protect the resources of HEIs. As a result, systems might become vulnerable; that can easily be exploited. Once the vulnerabilities in systems have been exploited, the compromised systems can be used to spread malicious code to attack other systems (Wu, 2010).

### **2.3.1 Vulnerabilities and network threats**

Vulnerability is the existence of flaws or weaknesses in a system's design, security controls or implementation that can result in a computer system or network security being compromised (Mendyk-Krajewska & Mazur, 2010; Anderson et al., 2016). The exploitation of vulnerabilities in applications, browsers, operating systems, or misconfiguration of network devices is still common and poses a threat to any organisation. The operating systems and software used by institutions may have design flaws or bugs that could allow an attacker to exploit applications or permit viruses to perform tasks on behalf of the administrator (Wu, 2010). Ryerson University experienced a system error in their student administration system that resulted in the exposure of 588 students' personal information (Ruffolo, 2009). Based on the investigation and analysis group led by Ernst & Young Canada, the software upgrade on the system caused the software glitch that resulted in a privacy breach (Ruffolo, 2009).

Cisco Networking Academy (2013) classifies vulnerabilities into three categories, namely technological, configuration and security policy, all leading to network and other attacks. Technological vulnerabilities include weaknesses that exist on Transmission Control Protocol/Internet Protocol (TCP/IP), operating systems and network equipment as shown in Table 2.1. These vulnerabilities, if overlooked, could create many problems for academic institutions, as the attackers could gain access to institutions' networks and steal confidential information.

**Table 2.1: Technological vulnerabilities**  
(Source: Cisco Networking Academy, 2013)

Network security weaknesses:
<p><b>TCP/IP protocol weakness</b></p> <ul style="list-style-type: none"> <li>• Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Internet Control Message Protocol (ICMP) are inherently insecure.</li> <li>• Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) are related to the inherently insecure structure upon which TCP was designed.</li> </ul> <p><b>Operating system weakness</b></p> <ul style="list-style-type: none"> <li>• Each operating system has security problems that must be addressed.</li> <li>• UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8</li> <li>• They are documented in the Computer Emergency Response Team (CERT) archives at <a href="http://www.cert.org">http://www.cert.org</a>.</li> </ul> <p><b>Network equipment weakness</b></p> <p>Various types of network equipment, such as routers, firewalls, and switches have security weaknesses that must be recognized and protected against. Their weaknesses include password protection, lack of authentication, routing protocols, and firewall holes.</p>

Based on Dzung et al. (2005), attackers use well-known techniques such as password cracking and methods to exploit vulnerabilities in systems to achieve their goals. According to Jingbo & Pingping (2010) and Qader (2016), using weak passwords for authentication purposes poses a security threat as they are easily guessed due to the low entropy they possess. Weak passwords can also be exploited by brute force, hence allowing the attacker to have access to systems or websites. Table 2.2 shows the configuration vulnerabilities as well as how each can be exploited. Network administrators should learn more about configuration vulnerabilities and know how to configure network devices properly in order to protect against such vulnerabilities. The failure to deal with equipment misconfigurations, mainly network devices, can impose threats into an organisation's network. It is therefore essential to use strong cryptic passwords to avoid being easily guessed, and use unique passwords for accounts that have access to confidential data.

In 2002, a student from the University of Delaware was able to hack into a professor's account by guessing the password and successfully changed her grades online (Read, 2002). Because of the incident, the student faced several charges including unauthorised access and misuse of information. Unfortunately, incidents such as this one may undermine the institution's credibility and capability. In January 2005, the hacking in progress was interrupted at George Mason University after the system administrator found inconsistencies with data streaming (Noguchi, 2005). According to Noguchi (2005), the hacker was able to break into one of the computers, trying to hack into a database by guessing the passwords.

**Table 2.2: Configuration vulnerabilities**  
(Source: Cisco Networking Academy, 2013)

Configuration Weakness	How the weakness is exploited
Unsecured user accounts	User account information may be transmitted insecurely across the network, exposing usernames and passwords to snoopers.
System accounts with easily guessed passwords	This common problem is the result of poorly selected and easily guessed user passwords.
Misconfigured Internet services	A common problem is to turn on JavaScript in Web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites. IIS, FTP, and Terminal Services also pose problems.
Unsecured default settings within products	Many products have default settings that enable security holes.
Misconfigured network equipment	Misconfigurations of the equipment itself can cause significant security problems. For example, misconfigured access lists, routing protocols, or SNMP community strings can open up large security holes.

The exploitation of a database is also a common threat since the attacker can use a Structured Query Language (SQL) injection to attack the database. In November 2006, the database of the University of California, Los Angeles, was compromised, exposing confidential information of about 800,000 students and staff (Kawamoto, 2006). The confidential information in the database included home addresses, contact information, social security numbers and dates of birth. According to the acting Chancellor of the University of California, Los Angeles, Norman Abrams, the hacker had been accessing this information for more than a year without being discovered (Kawamoto, 2006). The failure to update or fix operating systems or applications flaws can lead to high recovery costs from a security breach or incident, hence resulting in an unfavourable reputation. It is therefore important for the systems and software to be updated to correct any design flaws and have situational awareness to increase visibility and reduce security risks.

The most crucial aspect in computer network security, and which is often ignored by IT security personnel, is that vulnerability in the system can lead to the network being breached by both internal and external sources (Burney & Khan, 2010). According to Wang & Liu (2011), Haeussinger & Kranz (2013) and Anderson et al. (2016), IT security personnel at HEIs are more focused on protecting the network from external sources and tend to overlook supervision on internal behaviour. This causes students to freely use a variety of network hacking software for experimental purposes to bring harm to the network. Al-Akhras (2006),

asserts that universities experience internal network security breaches because it is easy for staff and students to download hacking software from the Internet and use it to hack the network. Accordingly, this can be attributed to the lack of enforcing security policies within the network. A security policy plays an important role in guiding network administrators to detect, prevent, and know how to respond to security breaches (Von Solms & Von Solms, 2004). Baskerville & Siponen (2002) assert that security policies which will practically guard the confidentiality, integrity, and availability of higher academic institutions' resources, are increasingly needed. Table 2.3 shows security policy vulnerabilities and how these weaknesses are exploited.

**Table 2.3: Security policy vulnerabilities**  
(Source: Cisco Networking Academy, 2013)

Policy Weakness	How the weakness is exploited
Lack of written security policy	An unwritten policy cannot be consistently applied or enforced.
Politics	Political battles and turf wars can make it difficult to implement a consistent security policy.
Lack of authentication continuity	Poorly chosen, easily cracked, or default passwords can allow unauthorized access to the network.
Logical access controls not applied	Inadequate monitoring and auditing allow attacks and unauthorized use to continue, wasting company resources. This could result in legal action or termination against IT technicians, IT management, or even company leadership that allows these unsafe conditions to persist.
Software and hardware installation and changes do not follow policy	Unauthorized changes to the network topology or installation of unapproved applications create security holes.

A security policy is such an important document for an organisation because it states in the form of writing how the organisation intends to safeguard its physical and information assets. However, if the security policy is poorly written and not properly enforced within an organisation, it can create unexpected security threats. In May 2012, the University of Nebraska's most important database, the Nebraska Student Information System which held personal information for 654,000 students, was breached internally (Bradbury, 2013). According to Joshua Mauk, an Information Security Officer at the University of Nebraska, the hacker was able to gain administrative control and accessed student data and financial information (Bradbury, 2013). This can be the result of not enforcing security policies on network users.

Malicious attacks are often carried out by IT security personnel who have system privileges; these attacks therefore pose a threat to any organisation. Experienced IT security personnel may intentionally sabotage the organisation they are working for to steal information by creating backdoors into the systems for accessing information at a later stage. According to Whitman & Mattord (2012), student and staff errors are also found to be among the high-ranking threats to information assets in an organisation. It is therefore deemed essential for IT security personnel to be encouraged to enforce security measures (Pfleeger et al., 2015). Czernowalow (2005) says the occurrence of security breaches can be more costly than establishing a security system. HEIs should therefore put into practice and train network users on policies for improved security results. When users are exposed to policies, this can increase the customs (acceptable practices regarding policies) of the institution policies that in turn increases awareness among the users (Cronan et al., 2006).

Based on studies conducted by Jones & Stallings (2011) and Manshaei et al. (2013), network security has progressively become a concern to different types of organisations due to the high number of various cyber-attacks, i.e. virus or worm propagation, denial of service (DoS) attacks and hacking incidents. It is necessary for academic institutions to protect their information and assets from the same threats affecting general commercial and government networks. HEIs are therefore faced with the need to apply enhanced security measures without compromising their important principles. The infiltration of viruses, worms, and Trojans into academic networks can destroy or corrupt data and by causing excessive network traffic, massive delays may be experienced (Li, 2011). This act may weaken the ability of the institution to function properly and result in prolonged downtime and unavailability of Information Technology services. It can be costly for an organisation to restore IT services to normal and recover data, resulting in an overwhelming task for IT security personnel (Updegrove & Wishon, 2003).

In May 2007, Colorado University Boulder's database was infected by a computer virus that resulted in names and social security numbers for approximately 45,000 students being exposed (PostIndependent, 2007). According to university's security officials, the computer virus penetrated through the vulnerability found in an antivirus program due to security misconfiguration settings (PostIndependent, 2007). In 2009, a network computer containing students' confidential data at Kapiolani Community College suffered a malware infection resulting in an infected computer being accessed and controlled remotely (University of Hawaii's system, 2009). A similar incident occurred at Penn State University in 2013 where computers containing confidential data were infected with malware (Cohen-Abravanel, 2013).

The use of mobile devices or BYOD (Bring Your Own Device) within an organisation allows mobility and flexibility, hence increasing the efficiency and productivity of users (Scarfò,

2012; Morrow, 2012). The faculty and students can perform work-related or study-related tasks from anywhere convenient to them. However, BYOD has brought security concerns and challenges when accessing the institution's network because these devices are not being managed by IT security personnel (Marrow, 2012; Arachchilage & Love, 2014). Raman et al. (2016) assert that IT security personnel have little control over these devices and managing the security controls when connected to HEI networks. According to Eslahi et al. (2012), mobile devices and BYOD become vulnerable to different kinds of malicious attacks that could consume IT resources and cripple the institution's services. Most of these devices do not have malware protection installed; hence, BYOD poses a threat to the network in terms of viruses, worms, or Trojans that could easily infect the network once they are connected to the network.

Furthermore, if a device gets missing or stolen, the data can end up in the wrong hands of an unknown user, resulting in unauthorised access and data loss (AlHarthy & Shawkat, 2013). In fact, the use of mobile devices on an institution's network increases threats to an organisation's data stored on mobile devices. In addition, unknown users in possession of stolen or lost mobile devices could hamper administrative control over the device in terms of monitoring the data or applications. Based on the outcomes of a study by Verizon (2015), published in their Data Breach Investigation Report, incidents on data breaching, which include mobile devices, accounted to 15.3% due to physical theft or loss. In 2005, a laptop at the University of California, Berkeley, was stolen from an unlocked office that resulted in the disclosure of confidential data of more than 98,000 students (Burress, 2005). Therefore, it is necessary for academic institutions to create, revise and enforce user and security policies regarding mobile devices or personal computers within the academic institution's network in an effort to protect data loss or data leakage. The use of encryption techniques to protect sensitive information against data breaches should be encouraged.

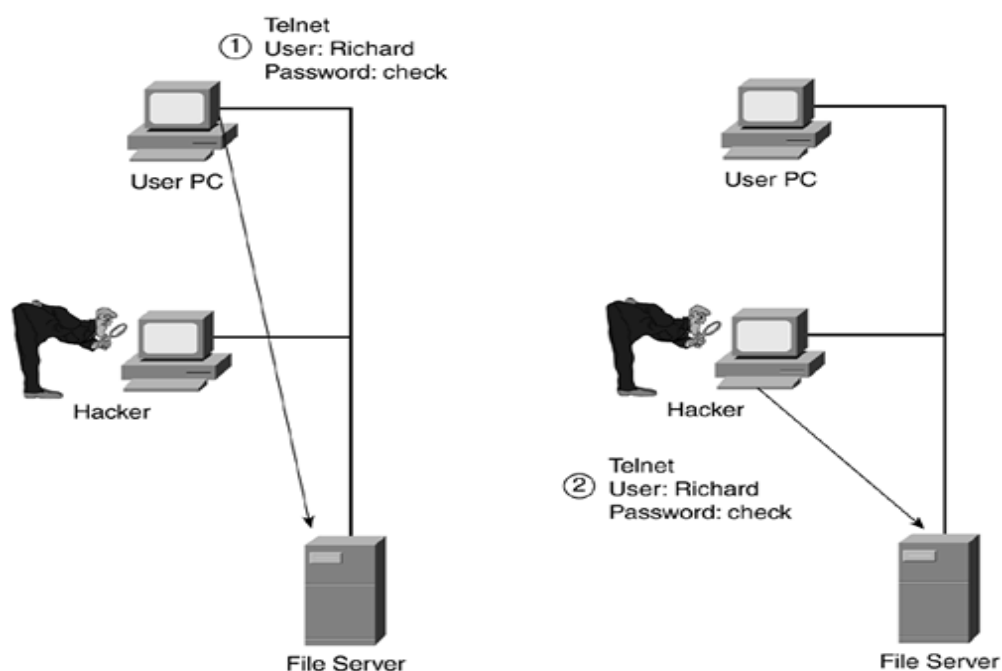
Although wireless networks provide mobility and increase productivity among network users, it poses a set of security challenges and threats to the network. In addition to distinctive problems a wired network and technology devices can create, a lack of security in WLAN can make an institution's network traffic and resources vulnerable to unauthorised access by intruders. Furthermore, a security breach in a wireless network can be an entry point to a number of network attacks. Some of the challenges faced in a wireless network are discussed next.

#### **2.3.1.1 *Eavesdropping and data modification***

WLANs spread the network traffic 'in the air', making it difficult to control who receives these wireless signals. According to a study by Yu et al. (2010), wireless network traffic is mostly in



plaintext format making it easier for an attacker to intercept wireless communication, hence gaining access to confidential data being sent out across the network. Eavesdropping is a process involving examining the packets being transmitted between the source and the destination. Eavesdropping in a wireless local area network is among the biggest security problems as the intruder is able to monitor network traffic. Figure 2.4 shows how the eavesdropping attack works. During the first phase (1), the hacker starts by inspecting the network traffic flowing between the user and the server. Upon inspection, the hacker realises the user has established a Telnet connection, which is a networking protocol that allows a user to establish a remote connection on a remote computer. However, all the communication between the user and server on Telnet protocol is transmitted in plaintext.



**Figure 2.4: Eavesdropping attack**  
(Source: eTutorials.org, 2016)

During phase (2), the hacker is able to obtain the user's credentials and use it on behalf of the user to log on to the server. After the attacker has intercepted data transmitted on a network, the attacker can perform tasks such as modifying the content packets being transmitted on a network, making changes in the way the program functions or performs, and changing the data file value. All these tasks are achieved without the knowledge of both the sender and the receiver. Confidentiality and integrity are compromised because the hacker can now access and modify all files on the server that the user is given permission to. Implementing encryption services based on strong cryptography could assist in the fight against eavesdropping and data modification. Using a virtual private network can also help prevent this type of attack because virtual private networks are equipped with different

encryption algorithms such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) to protect data on the network and systems.

### **2.3.1.2 Spoofing and session hijacking**

The wireless network do not provide authentication for the source address that is mainly the MAC address. As a result, the attacker can easily gain access to data and resources in the network by pretending to be the legitimate user. This can be achieved by spoofing the Media Access Control (MAC) addresses of the devices allowed to access the network and hijack the sessions. If the attacker can successfully hijack the session, the attacker can easily accomplish eavesdropping and disruption. However, implementing authentication and access control mechanisms can help eliminate spoofing.

### **2.3.1.3 Denial of Service (DoS)**

DoS is defined as an attack whereby the intruder sends invalid messages to flood the network in an attempt to make network resources unavailable (Zargar et al., 2013). Since the WLAN uses radio transmission for communication, this network is susceptible to a DoS attack. The use of a powerful transceiver can also generate radio interference that can tamper with communication in a WLAN while using a radio path.

## **2.3.2 Network security attacks**

Networks are vulnerable to different types of attacks and unauthorised monitoring. Network attacks are attempts or intrusions by an attacker to modify or make use of network resources without authorisation. Damages caused by network security attacks can range from data theft and loss of time to disabled or crippled services, loss of data confidentiality, financial loss, and bad reputation. As Fuchsberger (2005) mentioned, cyber-attacks are not implausible incidents occurring to certain exposed networks that are highly publicised; most networks are likely targeted. Hackers are particularly looking for specific types of information such as personal and research data that can be used for identity theft as well as committing criminal activities. In addition, hackers try to compromise network devices and use these to launch attacks while hiding among legitimate applications within a large and under-protected network (Mateski et al., 2012). Therefore, academic networks must be protected and actively monitored for a variety of constantly evolving threats and attacks. If proper security measures or technologies are not implemented, security attacks are likely to take place. The most common network security attacks in academic networks are discussed below.

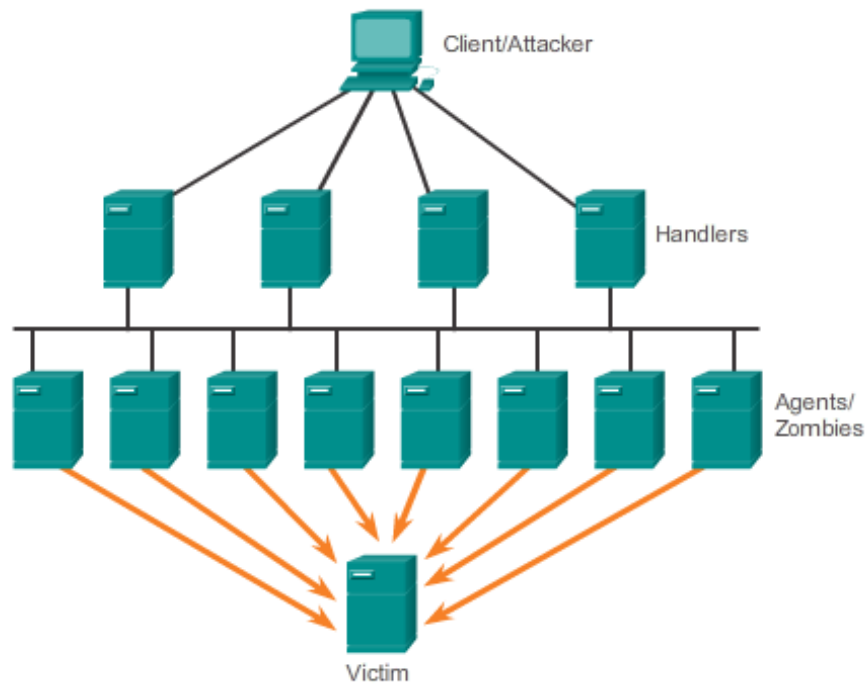
### **2.3.2.1 Denial of Service (DoS) attack**

This is an attack denying legitimate users access to network resources by flooding the server with many requests with the intention to crash the system (Zargar et al., 2013; Hemalatha & Vijithaananthi, 2017; Prabhakar, 2017). The intention of the attacker is to interrupt the services offered to network users or systems and prevent the flow of legitimate network traffic. According to studies by Mirkovic & Reiher (2004) and Ranjan et al. (2006), a DoS attack consumes server resources, network resources and available network bandwidth by sending large number of packets to the network, resulting in slow network performance.

Therefore, a DoS attack imposes as the main threat to network connectivity and network quality of service as it stops communication between network devices (Sharma et al., 2016; Hemalatha & Vijithaananthi, 2017). In April 2006, Ohio University was under a cyber-attack where a database server with more than 300,000 records of alumni, students and staff was hacked, exposing about 137,000 social security numbers belonging to individuals (Sandoval, 2006; Vijayan, 2006). According to the Athens-based University's Chief Information Officer, Bill Sams, the intrusion was discovered by an IT official after realising the compromised server was being used to initiate a DoS attack against an external target (Sandoval, 2006).

### **2.3.2.2 Distributed Denial of Service (DDoS) attack**

A DDoS attack uses multiple infected computers also known as zombies from different geographical locations to launch an attack (Zargar et al., 2013). Figure 2.5 shows a generic representation of a DDoS attack. According to Reid & Lorenz (2008), a DDoS attack follows a specific approach to launch the attack. The attacker initially checks systems for vulnerabilities that can then be exploited to gain access. Once access is granted to several systems (handlers), the attacker installs zombie software that infects agent systems. After the agent systems have been infected, the attacker gains access to these agent systems and runs remote-control attack application to accomplish the DDoS attack on a targeted server. The intention of the DDoS attack is to disrupt the services on the targeted server by crashing the system or resulting in slow response.



**Figure 2.5: A generic representation of Distributed Denial of Service attack**  
(Source: Cisco Networking Academy, 2013)

This attack becomes difficult to trace because zombies are in different locations. Differentiating the legitimate traffic from the attacker's traffic seems impossible, and again, it is not easy to trace the traffic back to its source. Furthermore, a DDoS attack requires qualified network security personnel to discover where the problem originates and then find ways to stop the attack while attempting to manage the network traffic. According to Zargar et al. (2013), a DDoS attack can cause revenue losses for an organisation and result in high costs trying to restore the services to normal.

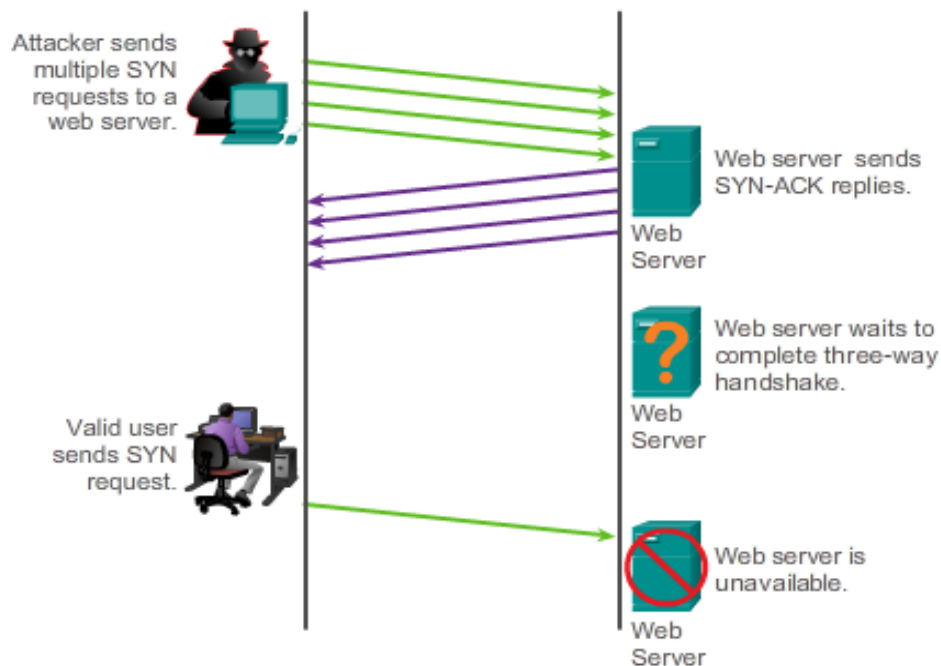
### **2.3.2.3 SYN attack**

A SYN flood is an attack exploiting the Transmission Control Protocol (TCP) flaws by sending a large number of TCP/SYN packets to the targeted server with a forged source IP address (Chao-yang, 2011; Prabhakar, 2017). Figure 2.6 shows the SYN attack where the attacker is sending multiple SYN requests to the server and the server replies but fails to receive the acknowledgement (ACK). This attack does not need the TCP three-way handshake<sup>2</sup> to complete. The server would send a SYN ACK response packet, however it

---

<sup>2</sup> Three-way handshake is a process in a TCP/IP network involving packets' exchange between the client and server before beginning the actual communication. The purpose of sending these packets is to check the availability of the server for any new connections.

would not receive the client's ACK packet because the source IP address is spoofed<sup>3</sup>. As a result, the server will maintain large SYN queues which eventually consume available TCP connection resources and server bandwidth, resulting in legitimate requests from clients being ignored (Liu, 2009; Chao-yang, 2011). This attack makes the location of the attacker's computer difficult to identify and filtering tricky, based on the source IP address.



**Figure 2.6: A SYN attack**  
(Source: Cisco Networking Academy, 2013)

#### **2.3.2.4 Phishing attack**

Phishing is an attack in which the attacker pretends to be a legitimate entity in order to obtain confidential information in an electronic communication (Ramzan, 2010; Khonji et al., 2013; Arachchilage et al., 2016; Aleroud & Zhou, 2017). The electronic communication can claim to be from legitimate entities or users such as the IT administrator, a bank or auction site to tempt unsuspecting victims. The phishing emails may at times have the links that redirect the victim to an infected website with malware. According to Ramzan (2010) and Aleroud & Zhou (2017), the link may also redirect the victim to a login screen of a fake website that looks like a legitimate website in an attempt to obtain the user's credentials (username and password), credit card numbers or security codes. The attacker, after collecting the login credentials, would then use the information on behalf of the victim to carry out the fraud. Khonji et al. (2013) recommend that different spam filters should be used in order to block phishing

<sup>3</sup> A fake source IP address created by an attacker assigned to a computer to disguise as one of the legitimate IP addresses to gain unauthorised access to the network and its resources.

emails, and suggest that improving the security of websites can also assist in combating phishing attacks.

#### **2.3.2.5 Brute-force (password guessing) attack**

Brute-force (password guessing) attack is an attack whereby the attacker attempts to learn the password by guessing the possible combination of the characters of the password until the login is successful. This can also be done using a computer program to guess the password, hence comparing it to the cryptographic hash available. According to Vance (2010), short and simple passwords are easy to guess or crack; therefore, such passwords need to be avoided. In the annual report issued by the Computer Emergency Response Team (CERT) at Carnegie Mellon University, on 16<sup>th</sup> July 1998 an attacker obtained 186,126 encrypted passwords and was able to crack 47,642 passwords before being discovered.

In December 2009, the RockYou.com website was breached and 32 million passwords were leaked on the Internet by the attacker (Cubrilovic, 2009). The attacker took advantage and exploited a database vulnerability to use a Structured Query Language (SQL) injection to steal the passwords. Imperva, an IT security company providing cyber and data security, through its research team at their Application Defence Centre (ADC), performed an analysis and discovered that the passwords were stored in plaintext. In November 2013, GitHub.com had been compromised due to the use of weak passwords, resulting in passwords being reset and personal access tokens being cancelled (Davenport, 2013). Users are therefore recommended to use passwords that include a mixture of letters (uppercase and lowercase characters), special characters (i.e. \*, %, @, #) and numbers, as it is harder to crack or guess. Ristic (2010) suggests that website administrators set account lockout policies to limit the number of attempts an attacker can try guessing the password and block the attacker's IP address.

#### **2.3.2.6 SQL injection attack**

Structured Query Language (SQL) injection is an attack commonly used to attack SQL databases or websites where malicious code is inserted for execution to attack applications (Wei et al., 2006; Desai & Gaikwad, 2016). This attack takes advantage by exploiting vulnerabilities in data-driven applications where user input variables are unexpectedly executed. The databases usually store confidential information; therefore, any damage to these databases can be costly to any organisation affected. As a result, web applications and databases need to be protected against these attacks.

### 2.3.3 Network security breaches in academic institutions

Security breaches or attack incidents occur due to vulnerabilities in software or lack of safeguarding information on the network. With a high number of network security breaches taking place around the world, colleges and universities are faced with a challenge to safeguard confidential information such as research records, financial records, staff and students' data and improve security measures currently in place. Because of colleges and universities' open environment nature they become the target for hackers. According to Piazza (2006), a number of HEIs have experienced data loss or theft, resulting in students' personal information being affected.

- In 2013, Johns Hopkins University was attacked that led to names and email addresses of 848 Biomedical Engineering students being compromised and exposing confidential information of students (Dance, 2014). After the incident, the university's Chief Information Security Officer, Darren Lacey, mentioned the university would prioritise the protection of data depending on its highest level of importance (Dance, 2014)
- In February 2014, the University of Maryland experienced a cyber-attack on its database where records including sensitive information, social security numbers, names, and birth dates of more than 300,000 alumni, students, and staff were exposed to the attackers (Musil, 2014). The representatives of the university stated they were trying to discover the vulnerability of the university's data and how to avoid future attacks. As a result of the breach, the university President, Wallace D. Loh, assured all whose information had been compromised to be provided with free credit monitoring (Musil, 2014)
- In December 2014 and February 2015, the University of California (UC) Berkeley experienced a data breach on two different occasions on one of their web servers containing confidential data of students, alumni, other individuals and students' parents (Gilmore, 2015). According to Gilmore (2015), UC Berkeley officials only became aware of the unauthorised access to their web server on the 14<sup>th</sup> of March 2015 and decided to take it off the network to eliminate any further damage

According to Neil Cosser, the identity and data protection manager at Gemalto for Africa asserts that the number of registered security breaches in the Republic of South Africa seems very low when compared to other countries across the world (Alfreds, 2016). This could be attributed to organisations not yet being aware of the hacking incidents or cyber-attacks in their organisations or they are afraid of disclosing organisational security breaches as it can have a negative impact such as bad reputation. Cosser further states that this can also be due to South African organisations not legally being forced to make such security

breaches public (Alfreds, 2016). As a result, people falsely continue believing that South African organisations are protected against cyber-attacks, which might not be the case.

## **2.4 Network security technologies in academic institutions**

The explosive growth of dependency on computer networks has increased tremendously for organisations, resulting in high security breaches (Tiwari & Jain, 2012). Therefore, higher academic institutions should take advantage of the security measures available in the market to safeguard their networks and reduce the likelihood of security risks. This is because computer networks provide and carry valuable information in digital format across the network. As a result, the network resources need to be protected against these types of attacks in order to maintain data confidentiality, integrity, and availability. However, McIlwraith (2006) asserts that security measures in most academic institutions are often ineffective that can lead to vulnerabilities, threats and attacks into institutions' networks. The attacks can also result in bad reputation, poor or bad academic performance and lack of interest among staff who provide electronic services to other staff and students (Omotayo & Ajayi, 2006). Academic institutions should therefore effectively implement network security measures to reduce network threats and attacks.

However, before purchasing any security measures or implementing network security, academic institutions should know what needs to be protected, protected against what, and how likely security threats are (Paquet, 2013). In fact, according to studies by Cisco Networking Academy (2007) and Paquet (2013), the level of network security should be proportionate to what the institution wants to secure. This can help balance the cost of implementing network security against the value of the assets they are protecting. Any academic institution without strong network security implementation is open to network threats and attacks. The most commonly used network security systems to protect network resources from threats and attacks include Firewalls, Intrusion Detection Systems (IDSs), Intrusion Prevention Systems (IPSs), network access control, cryptography, Virtual Private Networks (VPNs) and malware protection software.

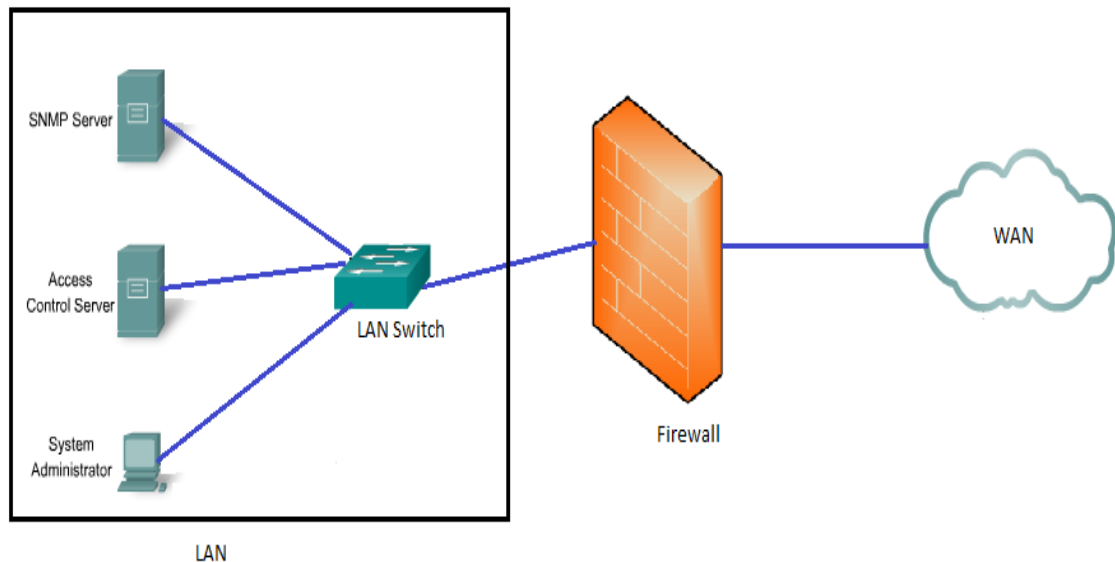
### **2.4.1 Firewalls**

A firewall is a network device usually placed at the perimeter of a network to filter traffic in and out of the network, hence preventing unauthorised access (Yu & Tsai, 2011; Zacker, 2014; Varma et al., 2017). It can be implemented as hardware, software or a combination of both in an effort to block unauthorised traffic. The implementation of a firewall on the network helps protect the internal network from attacks on the outside (Internet) and limit and regulate the access from the Internet to the internal network. A firewall enforces access policies such



as services allowed to be accessed by network users (Prabhakar, 2017; Varma et al., 2017). This can be done by filtering traffic based on protocol, sending or receiving port and Internet Protocol (IP) addresses or packet headers.

Among the distinctive functions of a firewall is the logging ability to generate log messages for any suspicious network traffic detected upon inspecting the packet based on a set of configured rules. These log messages can be valuable to network administrators in determining whether the network has been compromised or not. The configuration of the rules on a firewall should however not reduce the network performance. Therefore, due to its functions, firewalls have become very important in network security. Figure 2.7 shows the basic firewall setup.



**Figure 2.7: Basic Firewall setup**  
(Source: Adapted from Malik, 2003)

Firewalls can be categorised into three basic types, namely:

- i) Packet filters
- ii) Stateful packet inspection
- iii) Proxy server

#### **2.4.1.1 Packet filters**

Packet filters function at the network layer. Packet filters apply sets of rules to packets based on source IP address, destination IP address and port numbers (Cisco Networking Academy, 2014). Packet filters can also filter traffic based on protocols or services such as FTP to determine whether the packets can be forwarded hence be allowed to pass or be dropped. Packet filters are inexpensive and easy to configure and are therefore able to provide

network protection with the least complications. They also tend to be fast and transparent since packet filters do not inspect data in the packet and allow authorised users access with minimal intervention from the firewall. However, packet filters alone are insufficient to prevent an attacker from gaining access on the network as IP addresses can be spoofed (Vachon, 2012).

#### **2.4.1.2 Stateful packet inspection**

Stateful packet inspection firewalls work at the network layer to monitor all network connections and allow known or valid connections to pass through a firewall (Cisco Networking Academy, 2014). Stateful packet inspections use information from data packets and build dynamic state tables to keep track of the connections going through a firewall.

#### **2.4.1.3 Proxy server**

A proxy is a firewall that works at the application layer, usually installed on proxy servers<sup>4</sup> to examine traffic and authorises packets based on a set of rules configured (Malik, 2003). It forces all client applications on workstations protected by the firewall to use a proxy server as a gateway. Proxy server firewalls however, require large processor and memory requirements to support a high number of concurrent users and impose an overhead in heavily loaded networks (Malik, 2003).

Though a firewall is effective to prevent unauthorised access, it may however fail to check potentially harmful content such as worms or Trojans transmitted over the network due to its configuration (Ahmed & Singh, 2012; Varma et al., 2017). As a result, the content of such illegal traffic can therefore pass through a loophole and cause serious damage (Varma et al., 2017). Greenwald et al. (1996) stated that although a firewall can block unwanted traffic or unauthorised access, it is impossible to achieve complete protection in an academic environment. This is because students, staff and constituents need to access data off or away from the campus on the institutions' computers. Since not all computers accessing the network either within or outside the institutions' networks can be trusted, this poses a security threat if proper security measures are not in place. Based on several studies by Jackson et al. (2004), Liu & Zheng (2011) and Wattanapongsakorn et al. (2012), firewalls alone are not sufficient to protect the network from attacks that originate within the firewall, but if used with other mechanisms, the overall security can effectively be increased.

---

<sup>4</sup> Proxy server is a server acting as an intermediary between the clients and other servers by validating the incoming clients' requests and forwards them to other servers.

## **2.4.2 Intrusion Detection System (IDS)**

Intrusion detection system has been widely studied in recent years to overcome network security threats and attacks. An intrusion detection system (IDS) is a security system that attempts to detect malicious activities that may compromise confidentiality, integrity, and availability of a computer or network (Sharma & Singhrova, 2011; Meeta, 2011; Desai & Gaikwad, 2016). With today's computing environment driven by technology and the Internet, it has become nearly impossible to keep up with vulnerabilities and potential threats in systems. IDSs have therefore become imperative in computer network systems because it is able to help detect intrusions and alert the IT security personnel (Spitzner, 2003; Chen et al., 2017). This helps system and network administrators to eliminate threats and attacks or damage caused by intrusions as IDSs can collect crucial information or evidence on malicious network traffic in order to identify the intruder and the source of attacks (Yu & Tsai, 2011). As stated by Malik (2003), detecting intrusions is simply not enough. It is of the utmost importance to trace the intrusions and deal with the attacker effectively to reduce the likelihood of potential attacks.

Intrusion detection systems can be categorised into host-based intrusion detection systems (HIDSs) and network-based intrusion detection systems (NIDSs) (Almakrami, 2016; Gupta et al., 2016). HIDSs collect information about activities on a specific system to identify anomalous behaviour and unauthorised access (Almakrami, 2016; Wang & Jones, 2017). In an HIDS, agents or sensors are installed on each system believed to be at risk to threats and attacks to monitor the operating system and record data to log files. The data collected by the HIDS can be helpful in preventing future attacks by establishing the origin of potential network attacks. HIDSs are considered necessary, as they are capable of keeping track of individual users' activities, making it easier to detect intrusion attempts before causing damage to the system. However, HIDSs are criticised for several reasons. HIDSs can only monitor the systems in which the agents are installed and if the system is compromised, the attacker can disable the HIDS, leaving the system vulnerable (Sharma & Singhrova, 2011). In addition to that, HIDSs increase administrative workloads in large networks due to different operating systems and configurations required, thus making it difficult to maintain (Sarkar & Brindha, 2014).

NIDSs monitor network traffic by inspecting the packets on a network segment to identify unauthorised and anomalous behaviour (Almakrami, 2016; Desai & Gaikwad, 2016; Javaid et al., 2016; Gupta et al., 2016). The sensors installed on a segment can only examine the packet headers travelling across that network segment for attacks or intrusions. Therefore, any abnormal behaviour or intrusion sensed alerts the administrator. Examples of NIDSs include Bro Network Security Monitor ([www.bro.org](http://www.bro.org)) and Snort ([www.snort.org](http://www.snort.org)). NIDSs

provide real time detection, respond quickly to network attacks, and are extremely cost effective (Almakrami, 2016). However, NIDSs are not efficient on high-speed networks as each packet passing on a segment has to be examined; hence, scalability becomes an issue (Gupta et al., 2016).

Intrusion detection Systems can be categorised into two detection techniques namely misuse detection (also known as signature detection) and anomaly detection (Aiming & Li, 2012; Abdulhammed et al., 2016; Hadri et al., 2016). Misuse detection recognises an intrusion based on known attack characteristics or predefined descriptions of intrusions (Kumar & Sangwan, 2012; Pfleeger et al., 2015; Abdulhammed et al., 2016). Events matching the attack characteristics or known techniques are understood to be possible signs of intrusions into the network or system. For this reason, misuse detection is capable of detecting well-known attacks since it uses a rule-based system (Aiming & Li, 2012; Hadri et al., 2016). The detection decision is made based on knowledge of the model intrusive processes and trace of intrusions the detector finds in the observed system (Meeta, 2011). Although misuse detection is believed to be highly accurate, Yu & Tsai (2011:21) assert that it cannot however “detect any new intrusion without a pattern or signature”. As a result, a database with attack signatures and an expert system are usually used to identify and detect intrusions based on a predefined knowledge base (Yu & Tsai, 2011). The system would not detect intrusions unless the conditions in the signature database are met and correspond with the detect module. Thus, the signature database needs to be updated continuously.

Anomaly detection identifies an intrusion by calculating a deviation from normal system behaviour based on the assumption that an activity is abnormal and is most likely to be an intrusion (Pfleeger et al., 2015; Ahmed et al., 2016). Therefore, to identify the intrusions, anomaly detection does not need prior knowledge or information of security flaws. However, according to Yu & Tsai (2011) and Van et al. (2017), anomaly detection may cause a high number of false alarms because normal behaviour varies widely and obtaining complete descriptions of normal behaviour is often difficult. Zhengbing et al. (2005) assert that detailed system event records are needed for anomaly detection as a way to distinguish normal behaviour patterns.

Wang & Battiti (2006) propose a novel method based on Principal Component Analysis (PCA) for intrusion identification. For anomaly detection, intrusions are detected based on normal behaviour while for intrusion identification, an individual type of attack or a new attack is identified based on ‘abnormal’ behaviour, i.e. an attack. Network administrators have to investigate and identify which type of attack the abnormal behaviour belongs to and manually add the identified attack into the database containing associated types of attacks. According to Gascon et al. (2011), although deploying intrusion detection systems on computer

systems or networks may help fight against intrusions and attacks, this deployment however results in network administrators being overconfident regarding the level of protection. Overconfidence plays a critical role in network intrusions due to fallacies that lead to administrators believing the network is more secure than it really is. Delays in releasing new detection rules can result in the chances of missing a successful attack because the security is viewed as being strong based on the network intrusion detection systems installed.

### **2.4.3 Intrusion Prevention System (IPS)**

An Intrusion Prevention System (IPS) is a security system that attempts to detect intrusions and has the capabilities to block malicious activities on the network or system (Meeta, 2011; Wang & Jones, 2017). It monitors the network traffic for any intrusions and system activities, as well as blocks activities, considered as intrusions or threats. IPSs can be classified into host-based intrusion prevention systems (HIPSs), network-based intrusion prevention systems (NIPSs), network behaviour analysis (NBA), and wireless intrusion prevention systems (WIPSs). HIPSs monitor and analyse the activities on the (single) host where it is installed and block any suspicious activities. NIPSs analyse the protocol activities by monitoring the network for malicious traffic. According to Dulanović et al. (2008) and Wang & Jones, 2017, NIPSs have the capability to block both internal and external attacks. NBA identifies threats by examining network traffic for the violation of policies and unusual traffic flow generated. WIPSs analyse protocols on wireless networks by monitoring these networks for malicious traffic.

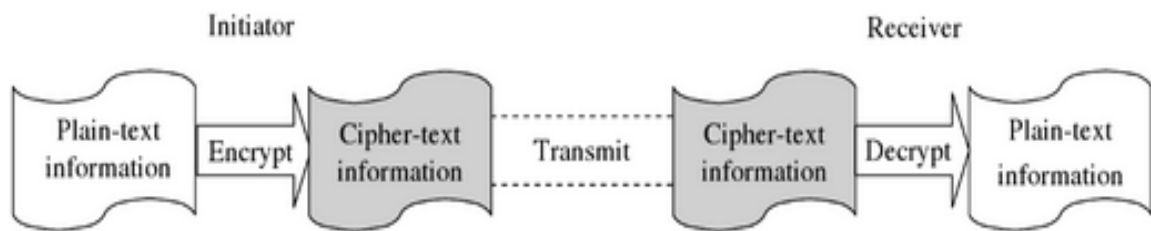
### **2.4.4 Network Access Control**

Network Access Control (NAC) is an approach that determines secure access to a network by a device or user by checking the identification and system security (Amiri et al., 2012). It ensures system efficiency and network management ability against any unauthorised access, as it can force the devices connecting to the network to comply with the security policy. As a result, any device not meeting the security policy requirements will be denied access. NAC solutions help protect organisations against network security threats and attacks. NAC furthermore helps to enforce policies for devices' compliance with the security requirements of an organisation.

### **2.4.5 Cryptography**

Cryptography is a technique that involves encrypting and decrypting data. This technique is often used to protect sensitive contents such as communication, files, and passwords.

Encryption is the process of converting the plaintext into ciphertext<sup>5</sup> by scrambling the contents of a file, allowing only authorised users to read it (Vachon, 2012; Regan, 2013). When data or information on the file has been encrypted, authorised users must use the password or secret key (decryption key) to decrypt the file. This process enhances data security by providing protection against unauthorised access. Figure 2.8 shows the process involved when exchanging information over the communication channel between two entities. The plaintext information is encrypted by the initiator into ciphertext. The ciphertext is transmitted over the communication channel to the receiver who then decrypts it into plaintext in order to read its content.



**Figure 2.8: Exchanging information between entities using cryptography**

(Source: Yu & Tsai, 2011:23)

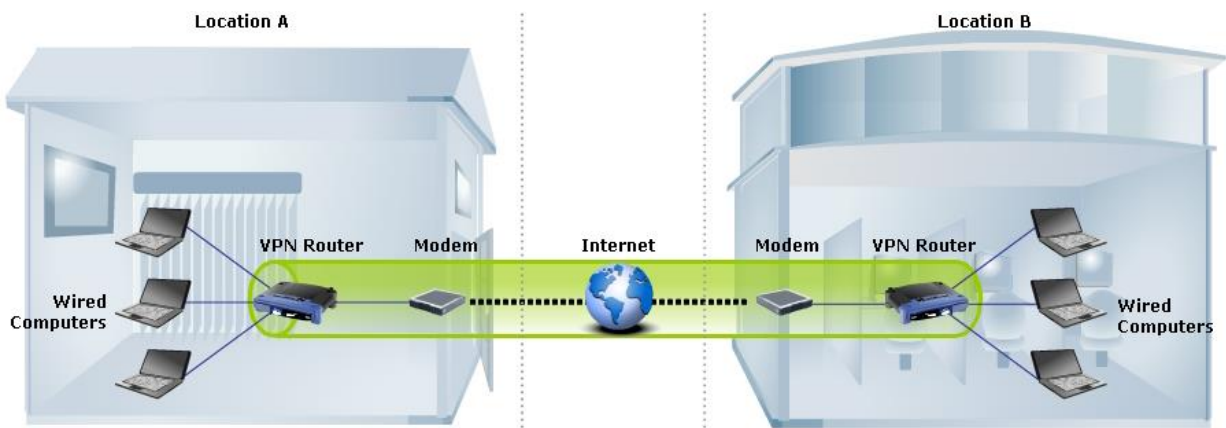
Encryption can be used to protect data stored on computers and storage devices, processed and transmitted across networks. The latest versions of Windows offer encryption technologies to protect files or folders on computers and protect entire volumes by using Encrypting File System (EFS) and BitLocker Drive Encryption (BDE) respectively. However, according to Regan (2013), the EFS encryption technology does not encrypt data that are transmitted across a network and recommends the use of Internet Protocol Security (IPsec) or Secure Sockets Layer/Transport Layer Security (SSL/TLS). If the storage device or the computer storing the encrypted data is stolen, any confidential data on that device cannot be exposed without using the correct decryption key (Regan, 2013). Furthermore, Yu et al. (2010) state that when data transmitted across a network is encrypted, it can help protect against eavesdropping and reduce the likelihood of data being intercepted by unauthorised users. Although encryption preserves the confidentiality of data, it takes time to process the encrypted file, thus consuming Central Processing Unit (CPU) power (Palmer, 2009; Prabhakar, 2017). This is the reason why the process of encryption results in a slower speed rate and subsequently increases communication delays when sending the data over the network, especially when stronger encryption is used.

---

<sup>5</sup> Encrypted text

#### 2.4.6 Virtual Private Network (VPN)

VPN is the technology that expands a private network across a public network (Regan, 2013). It ensures a secure way of transporting traffic across a public network such as the Internet (Palmer, 2009; Prabhakar, 2017). VPN makes use of encryption, authentication, and tunnelling protocols to protect the user's data privacy. As a result, it enables authorised users to connect securely and remotely to their organisation's intranet and access data away from the office or site. Figure 2.9 shows a VPN connecting two remote sites, Location A and Location B, across the Internet. For communication purposes, a link called VPN connection is created over the Internet. The VPN connection uses tunnelling protocols such as Secure Socket Tunnelling Protocol (SSTP) and Layer Two Tunnelling Protocol (L2TP) for encapsulating and encrypting private data as it is being sent across public network. This VPN connection ensures that data are not intercepted, and hence, maintains data confidentiality.



**Figure 2.9: VPN connecting two remote sites across the Internet**  
(Linksys, 2016)

Users can still be able to access network resources, and send and receive data just as with any other network device connected directly to a private network (Microsoft TechNet, 2003). This, according to Mason (2002), enables remote users to benefit from the security, management policies, and functionality of a private network because of the point-to-point connection that exists between the VPN client and the organisation's VPN server. To connect private networks and retaining secure communications, a site-to-site VPN connection (router-to-router connection) is used as depicted in Figure 2.9. The packets from one VPN router are forwarded across a VPN connection to another VPN router.

#### **2.4.7 Malware protection software**

Attackers use different methods or malicious software such as viruses, worms, Trojans, spyware and adware (Zhao et al., 2010) to gain access into systems without user consent. Malicious software is used to steal, alter, or destroy the data on a targeted system using the system's vulnerabilities. According to Huang et al. (2010), malware attacks on the network have become a serious issue as it causes a loss of crucial information. Therefore, academic institutions should protect information and provide means for risk management processes in case of a data breach. Malware protection such as anti-virus software, anti-spyware, and anti-adware are required to be installed on servers and workstations to eliminate virus spread and data destruction. As a result, these also require the malware protection software database updates to be updated regularly in order to maintain efficiency.

### **2.5 Summary**

This chapter discussed the common types of networks deployed in HEIs. The challenges faced by HEIs and how these can be addressed were highlighted. Security technology measures implemented at higher academic institutions' networks were discussed. A detailed discussion was provided on using each security technology, how each security technology can help enhance network security, and how to protect against network security threats and attacks.

The next chapter discusses in detail the research methodology, thus how the entire research study is to be carried out.



## CHAPTER 3: RESEARCH METHODOLOGY

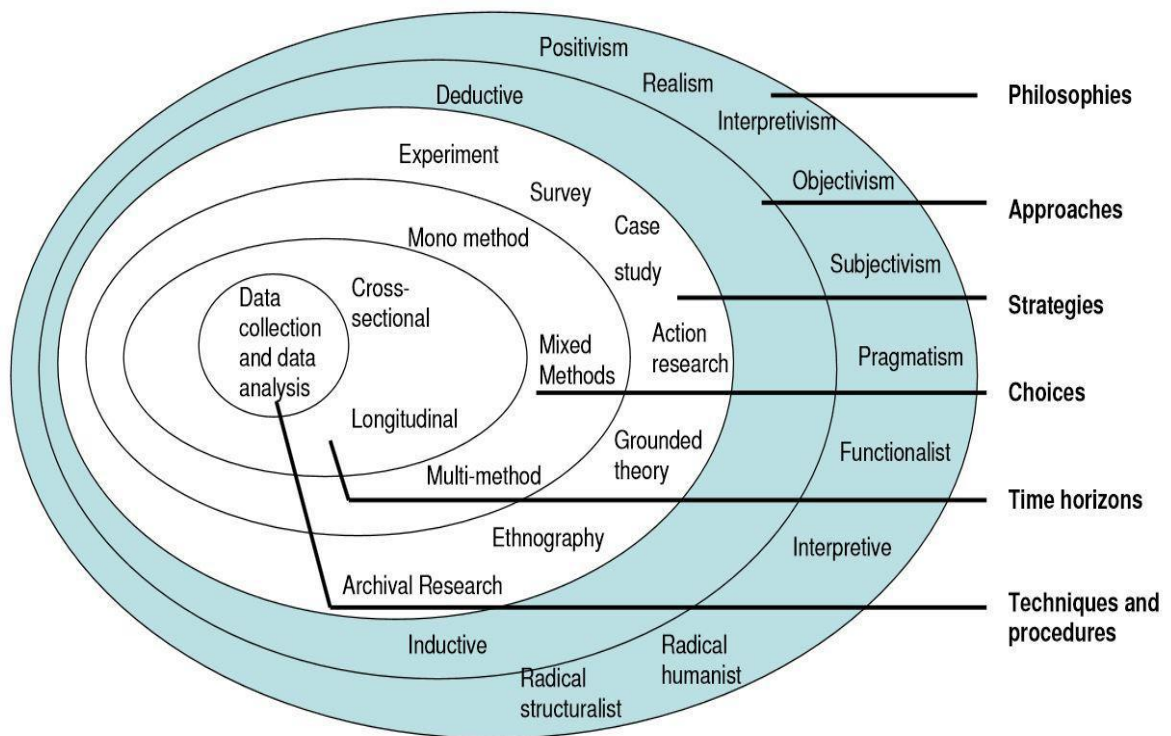


Figure 3.1: A graphical illustration of Chapter 3: Research Methodology

### 3.1 Introduction

For this research study, the researcher attempts to answer the research questions to find a solution to the problem. Both the research questions and research objectives are repeated in sections 3.2 and 3.3 respectively for the reader's convenience. This research methodology chapter is concerned with discussing the research philosophy chosen for the study and how it relates to other research philosophies. The research approach, research strategy and research design adopted for the study, are discussed. The method used for data collection and data analysis, are elaborated on.

The research philosophy, research approach, research strategy, research choice, research time horizon and research techniques and procedures as shown in Figure 3.2 are the main foci of the chapter and are discussed in the next sections.



**Figure 3.2: Research Onion**  
(Source: Saunders et al. 2009)

### 3.2 Research questions

Both the primary and secondary research questions are expressed and discussed in the next sub-sections.

### **3.2.1 Primary research question (PRQ)**

The primary research question is indicated as follows:

**PRQ: What can be done to mitigate network security threats and attacks at higher academic institutions in South Africa?**

### **3.2.2 Secondary research questions (SRQs)**

The secondary research questions are indicated as follows:

**SRQ1:** What are the challenges surrounding network security at higher academic institutions?

**SRQ2:** What security technologies are available to protect against network security threats and attacks?

**SRQ3:** How can network security be addressed and improved in order to protect against network security threats and attacks in South Africa?

**SRQ4:** What framework can be proposed for South African higher academic institutions to improve network security?

## **3.3 Research objectives**

### **3.3.1 Primary research objective**

- To establish ways to mitigate network security threats and attacks at higher academic institutions in South Africa

### **3.3.2 Secondary research objectives**

- To determine the challenges surrounding network security at higher academic institutions
- To identify what security technologies are available to protect against network security threats and attacks
- To determine effective ways to improve network security at higher academic institutions in South Africa to address the network security threats and attacks
- To develop and propose a framework for improving network security in South African higher academic institutions

### **3.4 Research philosophy**

Research philosophy is the belief whereby the researcher develops the knowledge and attempts to understand the research background related to the research topic and its nature (Saunders et al., 2009). According to Easterby-Smith et al. (2012), the researcher needs to understand philosophical research issues and the importance thereof in order to have a better understanding of different research methods and deliver high-quality results from research activities conducted. Based on Easterby-Smith et al. (2012), this would help with research design clarification; hence, the acquired knowledge on research philosophy by the researcher would be useful regarding which design is deemed most feasible and appropriate to be used in the study. Easterby-Smith et al. (2012) further assert that this understanding of philosophical research issues enables the researcher to gather more information to answer the research questions and assist the researcher with creativity and examining the research method.

Saunders et al. (2009) assert that the research philosophy decided on by the researcher has essential assumptions on how the world is perceived. These assumptions highlight the research strategy and methods to be used by the researcher as part of the process. According to Wilson (2014), it is important for the researcher to understand the research philosophy as this would help the researcher in becoming more involved and thinking of the role being played by the researcher during the research study. A research philosophy has two major branches, namely ontology and epistemology.

#### **3.4.1 Ontology**

Ontology, according to Easterby-Smith et al. (2012:344), is defined as the “views about the nature of reality and existence”. Ontology can be explained as a belief that reveals the understanding of an individual about what makes a fact (Blaikie, 2007). Ontology is linked to a central question on social entities and how these can be perceived—either objective or subjective. As a result, there are two imperative aspects of ontology, namely objectivism and subjectivism.

##### **3.4.1.1 Objectivism**

According to Saunders et al. (2009:110), objectivism “portrays the position that social entities exist in reality external to social actors concerned with their existence”. Bryman & Bell (2011:21) state that, “objectivism is an ontological position that asserts that social phenomena and their meanings have an existence that is independent of social actors”. This

indicates that whatever happens every day with people, it is being challenged by social phenomena as external facts that are beyond people's influence or reach.

#### **3.4.1.2 Subjectivism**

Subjectivism can be defined as “ontological position which asserts that social phenomena and their meanings are continually being accomplished by social actors” (Bryman & Bell, 2011:22). Saunders et al. (2009:110) define subjectivism as “social phenomena created from perceptions and consequent actions of those social actors concerned with their existence”. This simply means that social phenomena are created during social interaction and they are constantly being revised.

This research study adopts an objectivist ontological position because the researcher does not want personal opinions and feelings to affect the measurement of reality.

#### **3.4.2 Epistemology**

Epistemology, according to Easterby-Smith et al. (2012:341) is defined as “the views about the most appropriate ways of enquiring into the nature of the world”. Epistemology is more concerned with what knowledge is considered to be, and should be passed as acceptable in a discipline (Bryman & Bell, 2011). The epistemological positions, positivism, realism and interpretivism are discussed in the next sub-sections.

##### **3.4.2.1 Positivism**

According to Saunders et al. (2009) and Veal (2011), positivism is the framework of research whereby the researcher's view is concerned with emphasising empirical data and using scientific methods. The results of the research would therefore be comparable to those employed by natural scientists (Remenyi et al., 1998). Hence, a positivist philosophical approach is concerned with the researcher observing and performing experiments in order to collect numerical data (Easterby-Smith et al., 2012). Since positivists believe in empiricism, the idea of observation and measurement are at the core of their scientific endeavour. Based on Trochim & Donnelly (2006), the scientific method approach is the experiment that is an attempt to distinguish between natural laws through direct manipulation and observation. Positivism exists in science and assumes that science quantitatively measures independent facts about reality (Healy & Perry, 2000). In other words, the data and its analysis are value-free and data do not change because they are being observed.

### **3.4.2.2 Realism**

According to Bryman & Bell (2011:718), realism is “an epistemological position that acknowledges a reality independent of the senses that are accessible to the researcher’s tools and theoretical speculations”. Realism puts more emphasis on reality and the beliefs surrounding the researcher’s environment. This research philosophy is distinguished mainly by direct realism and critical realism. Direct realism asserts that what an individual experiences through using different senses, represents the world truthfully (Saunders et al., 2009). As a result, reality in this philosophical position can only be understood when proper methods are being utilised by the researcher. Therefore, realism claims the researcher needs to understand social structures that have caused the phenomena in order to have a better understanding of social world events and occurrences. Critical realism on the other hand, asserts that, “the study of the social world should be concerned with identification of the structures that generate that world” (Bryman & Bell, 2011:713). According to Sekaran & Bougie (2010), critical realism therefore asserts that individuals are more concerned with what they experience in certain situations.

### **3.4.2.3 Interpretivism**

Interpretivism is defined by Bryman & Bell (2011:715) as “an epistemological position that requires the social scientist to grasp the subjective meaning of social action”. This implies that the researcher needs to have a better understanding and differentiate the role being played by the humans as social actors. Based on Saunders et al. (2009), this therefore stresses the variation that exists when a research study is not conducted on objects such as networking devices and laptops but carried out among people. According to Easterby-Smith et al. (2012), in order for the researcher to give the research problem enough validation, it is imperative to understand interpretivist research philosophy beliefs and values. Therefore, the researcher’s focal point is to draw attention to the real facts and figures based on the research problem at hand.

The epistemological position of this research study is positivism because the researcher believes the phenomenon needs to be studied making use of facts and observations to acquire authentic knowledge. By adopting a positivist stance, the researcher’s views and beliefs will not influence the value of judgments and therefore unbiased and reliable research results will be delivered (Tashakkori & Teddlie, 1998). The finished product of the research will be similar to the one of a natural scientist (Remenyi et al., 1998:32).

### **3.5 Research approach**

When designing the research study it is important for the researcher to know which research approach would be best appropriate to use. The researcher must therefore have a good understanding of research approaches in order to increase the efficiency of the research study. This will also help making a sound choice to support the research approach being adopted. A research approach can be deductive or inductive. The sub-sections below explore these two approaches.

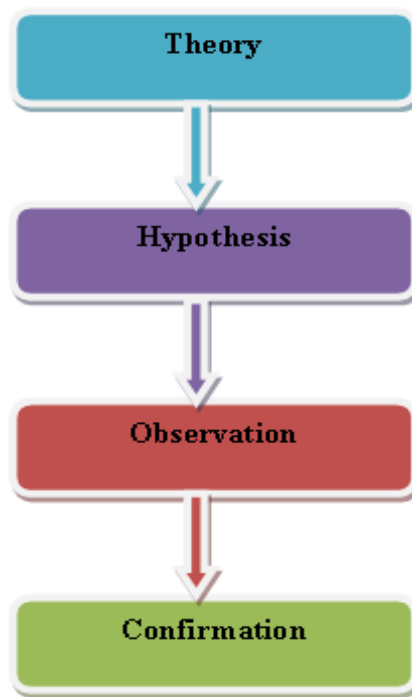
#### **3.5.1 Deductive approach**

With a deductive research approach the researcher establishes a hypothesis making use of a known theory. As described by Beiske (2007), Gill & Johnson (2010) and Wilson (2014), a deductive research approach is based on the idea of developing a hypothesis using existing theory and formulating a research strategy that can be used to test the hypothesis. This research approach therefore follows deductive reasoning. According to Lichtman (2013:19), “deductive reasoning works from the general to the specific”. This is mainly to confirm or validate the theory used in the research study based on the research objectives. Thus, a deductive approach at times is referred to as a ‘top-down’ approach because it mainly follows the logic path more closely.

Based on Beiske (2007), a deductive approach looks at a well-known theory and tests the validity of the theory in a given situation. The researcher collects a diversity of data by reading the available literature in order to validate or eliminate the hypothesis while trying to resolve the problem (Blaikie, 2007; Gill & Johnson, 2010). However, if the results are not satisfactory, further testing is undertaken and the theory can be modified. Figure 3.3 shows the process being followed when the deductive approach is being used in a research study.

This research approach, according to Crowther & Lancaster (2008), is associated with a positivist philosophy and uses general ideas to achieve a specific outcome. Robson & McCartan (2015) identify the stages to be followed when the researcher uses the deductive research approach as follows:

- i) Deduce a hypothesis from the theory
- ii) Formulate the hypothesis in operational terms
- iii) Test operational hypothesis
- iv) Examine specific outcomes of the enquiry, thus giving the confirmation or rejection of the theory
- v) Modify the theory if the findings are not satisfactory



**Figure 3.3: Deductive research approach**  
(Source: Adapted from Beiske, 2007)

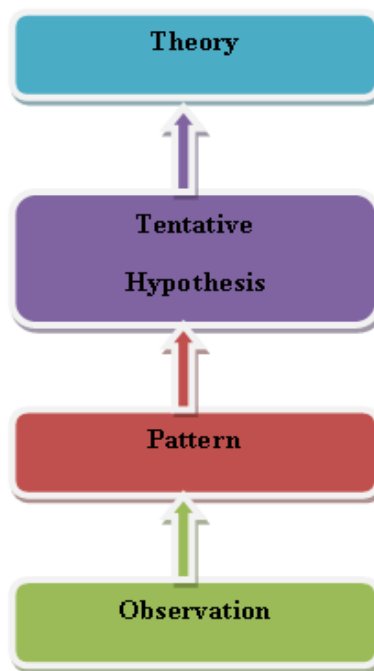
### 3.5.2 Inductive approach

An inductive research approach is where the researcher is engaged in a preliminary search for patterns from observations and formulates the theory through a hypothesis (Goddard & Melville, 2004; Bernard, 2011). Neuman (2011) and Burney & Mahmood (2006) confirm that an inductive approach involves a more comprehensive observation of the world and it works towards theoretical generalisations and ideas as shown in Figure 3.4. As a result, this approach is different from a deductive approach because theory is not applied at the beginning when the researcher starts working on the research study; therefore, the theory may develop based on the outcome of the research. Furthermore, hypotheses do not exist at the beginning of the research that results in the researcher not being sure about the nature or type of the research findings until the entire study is completed (Lancaster, 2005). Therefore, the researcher has the ability to change the direction of the research study after commencing.

According to Saunders et al. (2009), a deductive approach requires the researcher to be independent of what is being studied and apply control measures to ensure data validity.

This research study adopts a deductive research approach because the researcher focuses on reaching a specific outcome using a general idea. As a result, a hypothesis is to be built according to the connections found between variables.





**Figure 3.4: Inductive approach process**  
(Source: Adapted from Beiske, 2007)

### **3.6 Research methodology**

Research methodology can be classified into three groups, namely quantitative, qualitative and mixed-method research.

#### **3.6.1 Quantitative research**

Quantitative research is an objective and systematic empirical process used for determining the results by observing the phenomena through mathematical and statistical techniques (Creswell, 2014; Grove et al., 2015). Quantitative research entails three components namely data collection, analysis and interpretation. According to Hittleman & Simon (2005), quantitative research uses several methods such as surveys, questionnaires, and experiments to collect numerical data and perform statistical analysis. In order to resolve the research problem, statistical analysis is mainly applied because the data are mostly in mathematical and statistical format. The researcher analyses the numerical data to yield the results that are believed to be unbiased and generalisable. As a result, quantitative research aims to test relations, and observe cause and effect associations between variables by using mathematical models or theories concerning the phenomena (Grove et al., 2015).

#### **3.6.2 Qualitative research**

Qualitative research is a subjective and systematic process mainly used for describing life's incidents and attaching meaning to such experiences (Munhall, 2012). This research

methodology, based on Creswell (2014), works closely with images and texts, and puts emphasis on words and pictures so that observation can take place. According to Grove et al. (2015:20), qualitative research attempts to understand “the unique, dynamic and holistic nature of humans” and is concerned with theory development to describe human experiences and situations. It aims to achieve insight by discovering the depth and difficulty underlying in phenomena. This is done by involving participants to answer broadly asked questions in order to collect word data (from open-ended questions).

Qualitative research involves in-depth interviews, focus groups, and participant observation for data collection and analysis. This research methodology places emphasis mainly on an inductive approach for the relationship that exists between the theory and the research problem that forms the base of generating theories. As a result, it emphasises and focuses on how individuals are able to interpret and understand the social world. Table 3.1 shows a comparison between the two research approaches.

**Table 3.1: Qualitative research versus quantitative research**  
(Source: Adapted from Johnson & Christensen, 2014; Lichtman, 2013)

“Criteria	Qualitative Research	Quantitative Research
<b>Purpose</b>	To understand and interpret social interactions	To test hypotheses, look at the cause and effect and make predictions
<b>Group studied</b>	Smaller and not randomly selected	Larger and randomly selected
<b>Variables</b>	Study of the whole, not variables	Specific variable studied
<b>Type of data collected</b>	Words, images, or objects	Numbers and statistics
<b>Form of data collected</b>	Qualitative data such as open-ended responses, interviews, participant observations, field notes and reflections	Quantitative data based on precise measurements using structured and validated data-collection instruments
<b>Type of data analysis</b>	Identify patterns, features and themes	Identify statistical relationships
<b>Objectivity and Subjectivity</b>	Subjectivity is expected	Objectivity is critical
<b>Role of researcher</b>	Researchers and their biases may be known to participants in the study and participant characteristics may be known to the researcher	Researchers and their biases are not known to participants in the study and participant characteristics are deliberately hidden from the researcher
<b>Results</b>	Particular or specialised findings that are less generalisable	Generalisable findings that can be applied to other populations
<b>Scientific method</b>	Exploratory or bottom-up: the researcher generates a new hypothesis and theory from the data collected	Confirmatory or top-down: the researcher tests the hypothesis and theory with the data
<b>Nature of observation</b>	Study behaviour in a natural environment	Study behaviour under controlled conditions; isolate causal effects

“Criteria	Qualitative Research	Quantitative Research
<b>Nature of reality</b>	Multiple realities; subjective	Single reality; objective
<b>Final report</b>	Narrative report with contextual description and direct quotations from research participants	Statistical report with correlations, comparisons of means, and statistical significance of findings

### 3.6.3 Mixed-methods research methodology

Mixed-methods research “combines the qualitative and quantitative approaches into the research methodology of a single study or multi-phased study” (Tashakkori & Teddlie, 1998:17-18). This research methodology is often used when both qualitative and quantitative research methodologies are combined to provide valuable results. According to Bryman & Bell (2011), the results obtained when both research methodologies are combined are therefore cross-checked against each other. Webb et al. (1966) asserts that the adaption of a mixed-methods research methodology gives confidence in the research findings obtained; hence, confidence can be enhanced by using different ways for measuring the concept. According to Frankel & Devers (2000) and Bryman & Bell (2011), quantitative research is aligned with a deductive approach because the hypothesis is developed first and then tested to either confirm or reject the theory. As a result, this research methodology follows natural scientific model standards, particularly positivism (Bryman & Bell, 2011).

This research study adopts quantitative research as the researcher wants to be objective; thus, the researcher’s personal opinions and feelings will not affect measurement of reality.

## 3.7 Research strategy

Based on Saunders et al. (2009), a research strategy is a plan generally helping the researcher to answer the research questions in order to achieve the research objectives using a systematic approach. The research strategy assists the researcher in gathering significant information and data most relevant to the research problem. It is therefore important to select a research strategy that addresses the research questions properly and achieves the research objectives. There is a variety of research strategies to choose from as shown in Figure 3.2. The chosen strategies for this study are discussed in the next sub-sections.

### 3.7.1 Survey

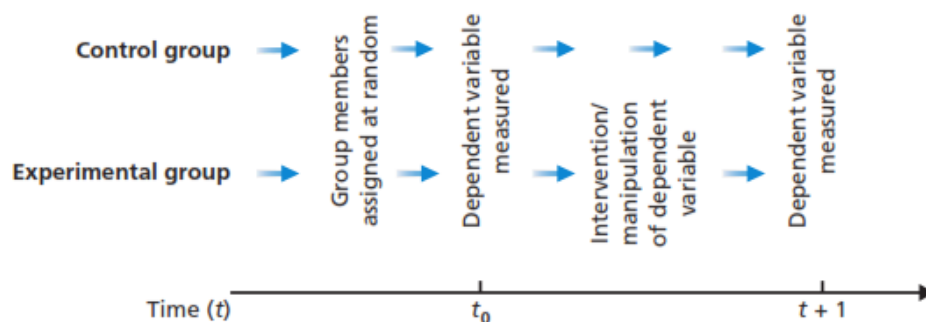
The survey is a cost-effective research strategy enabling the researcher to gather a large volume of data from a chosen population of interest and involves data collection techniques such as a questionnaire, among others (Saunders et al., 2009). This research strategy is

planned in such a way that it provides suggestions of how things are at a particular time of importance for the research study. A survey is generally regarded to be authoritative since it is easy to explain, compare, and understand.

Saunders et al. (2009) assert that a survey strategy enables the researcher to gather quantitative data that allow the use of descriptive and inferential statistics for data analysis. Furthermore, the data collected using this research strategy can help the researcher clarify relationships that exist between the variables, giving the researcher control over the entire research process. The survey strategy allows the researcher to create the findings represented by the sample of the population cost-effectively and can adopt quantitative and/or qualitative measures. However, based on Saunders et al. (2009), a number of researchers complain about this strategy, as the progress is dependent on information obtained from others.

### 3.7.2 Experiment

Saunders et al. (2009:142) define experiment as “a form of research that owes much to the natural sciences”. According to Hakim (2000), experiments are often conducted to discover causal links; thus, determining whether an independent variable can cause any changes to the dependent variable. Experiments can be as simple as involving two variables to find an existing relationship or be more complex in terms of the size and the significance of more independent variables. In a classic experiment as shown in Figure 3.5, there are two groups established, namely the experimental group and the control group.



**Figure 3.5: Classic experiment**  
(Source: Saunders et al. 2009:142)

These two groups become the starting point of experimental manipulation in respect of the independent variable. The experimental group is exposed to a planned manipulation or treatment while there is no such manipulation or treatment done to the control group (Saunders et al., 2009; Wilson, 2014). To ensure that pre-test and post-test analysis can be

carried out, the dependent variable is measured before and after experimental manipulation. Any variation between these two groups is caused by treatment of the independent variable. As a result, this builds the researcher's confidence that he/she did not interfere with the outcome of the experiment (Bryman & Bell, 2011).

The survey and experiment strategies are adopted for this research study, mainly because the researcher would like to:

- Determine the challenges surrounding network security at higher academic institutions
- Identify security technologies that are available to protect against network security threats and attacks
- Study the causal links to determine whether proper implementation of security technologies in academic networks can address network security threats and attacks
- Based on the findings, propose a framework to be implemented at South African higher academic institutions to enhance network security

### **3.8 Unit of analysis and unit of observation**

Unit of analysis is defined as the major single entity being investigated in the research study (Welman et al., 2007). Unit of analysis can be anything that is being studied such as individuals, objects, and groups. For this research study, the units of analysis are network security threats and attacks. The unit of observation is defined as the subject under investigation from which information is collected (Richey & Klein, 2014). For this research study, there are two units of observation; one for each research strategy adopted. For the questionnaire, the units of observation are the IT technical staff at higher academic institutions and for the experiment the units of observation are the two LANs in the computer laboratory.

### **3.9 Data collection**

Both primary and secondary data are collected in the research study. Primary data are collected by the researcher when conducting the research study for a specific purpose through a variety of data collection tools such as questionnaires, interviews and observation (Bryman & Bell, 2011). Secondary data have previously been published; the researcher collects and obtains this data from other sources such as documents, Internet, scientific journals and books (Bryman & Bell, 2011). In order to understand and address the research questions, the secondary data are critically assessed before being included in the study. This research study adopts the questionnaire as the survey strategy and structured observation as the experimental strategy.

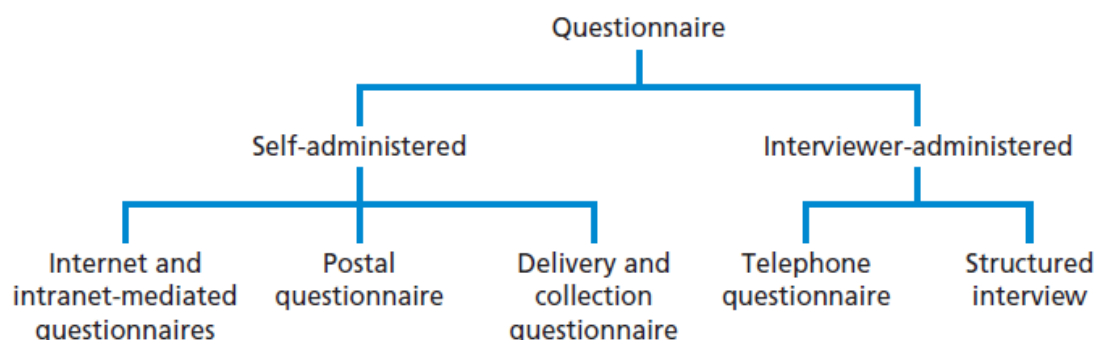
### 3.9.1 Questionnaire

The questionnaire is a commonly used method among researchers for collecting data to obtain a wide range of data required for a study. Wilson (2014:163) defines questionnaire as “a method of data collection that comprises a set of questions designed to generate data suitable for achieving the objectives of a research project”. A questionnaire, like any other data collection method, has its own advantages and disadvantages as shown in Table 3.2.

**Table 3.2: Advantages and disadvantages of questionnaire**  
(Source: Adapted from Bryman and Bell, 2011)

Advantages of questionnaire	Disadvantages of questionnaire
<ul style="list-style-type: none"><li>• Cost effective</li></ul>	<ul style="list-style-type: none"><li>• Low response rate</li></ul>
<ul style="list-style-type: none"><li>• Quicker to administer</li></ul>	<ul style="list-style-type: none"><li>• Respondents cannot probe due to absence of interviewer</li></ul>
<ul style="list-style-type: none"><li>• Biases eliminated due to absence of interviewer</li></ul>	<ul style="list-style-type: none"><li>• Difficulty of asking many questions</li></ul>
<ul style="list-style-type: none"><li>• No interviewer variability</li></ul>	<ul style="list-style-type: none"><li>• Incomplete entries are discarded</li></ul>
<ul style="list-style-type: none"><li>• Convenience for respondents</li></ul>	<ul style="list-style-type: none"><li>• Difficulty of asking sensitive questions</li></ul>
<ul style="list-style-type: none"><li>• Wide geographical coverage</li></ul>	<ul style="list-style-type: none"><li>• Difficulty to collect additional data</li></ul>
<ul style="list-style-type: none"><li>• Anonymity of respondents is ensured</li></ul>	<ul style="list-style-type: none"><li>• Questions can easily be misinterpreted</li></ul>

Questionnaire can be classified into two categories, namely self-administered and interviewer-administered questionnaire. Self-administered questionnaires are completed by the respondents without any help from the researcher or interviewer and are often administered using different media such as Internet, post or hand delivery (Saunders et al., 2009). With interviewer-administered questionnaires, the researcher or interviewer is present and records the answers given by the respondent. Figure 3.6 shows different types of questionnaires.



**Figure 3.6: Types of questionnaire**  
(Source: Saunders et al. 2009:363)

- The Internet and Internet-mediated questionnaires are managed electronically using the Internet, thus, the respondent completes the questionnaire online
- Postal questionnaires require the researcher to send the questionnaire to the respondents' addresses to be completed and returned to the researcher's address upon completion (Wilson, 2014). Wilson (2014) asserts that postal questionnaires are mostly targeted because they are inexpensive to administer and the respondents are free and open to answer the questions in the absence of the researcher or the interviewer
- For delivery and collection questionnaires the researcher or interviewer delivers it personally to the respondent and collects it again upon completion
- Telephone questionnaire data are collected by telephone—a fairly quick and inexpensive method used when respondents are geographically dispersed (Wilson, 2014). Wilson (2014) asserts that this method, however, can be time-consuming and expensive, as the right respondent has to be contacted. Also, the complex questions can be more difficult to explain over the phone (Wilson, 2014)
- Structured interviews can be expensive because the researcher or an interviewer must be present when each respondent answers the questions (Easterby-Smith et al., 2012)

This research study adopts the self-administered questionnaire as survey strategy to enable the respondents to complete the questionnaires in the comfort of their homes and without invading their privacy. The purpose for adopting this research method is to discover the challenges surrounding network security at higher academic institutions and identify available security technologies that can be used to protect against network security threats and attacks. The information obtained from the questionnaire enables the researcher to examine and explain the causal relationships between the variables, thus, whether implementing proper security technologies in higher academic institutions can help mitigate network security threats and attacks.

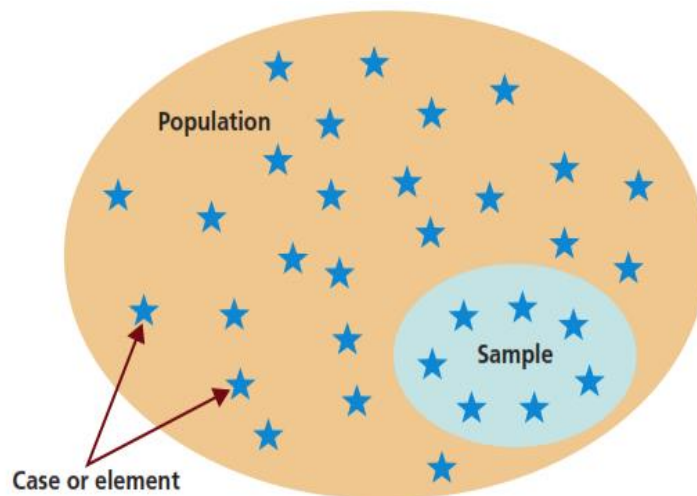
### **3.9.2 Structured observation**

Bryman & Bell (2011:719), define structured observation as “a technique in which the researcher employs explicitly formulated rules for the observation and recording of behaviour”. For the experimental strategy of this research, quasi-experiments conducted in a structured environment (computer laboratory) in which the Local Area Networks are set up to observe the threats and attacks in the networks, are adopted. The subjects are conveniently selected or assigned to the experimental and control groups, and assessed through observation. As this part of the study involves quantitative research, standard procedures have to be followed to deliver quantitative data. Thus, the researcher observes the behaviour

of the networks when security threats and attacks are imposed on the networks. The observations take place in the computer laboratory during the same week the networks are implemented specifically for this study. Two network analysis software packages, *Wireshark Network Analyser* and *Colasoft Capsa 9.1 Enterprise* have been selected to record and collect observational data for analysis purposes.

### 3.9.3 Sampling

According to Saunders et al. (2009), it is important for the researcher to consider whether to conduct sampling, i.e. draw a sample from the total population. Easterby-Smith et al. (2012:222) define population as “the whole set of entities that decisions relate to; while the term sample refers to a subset of those entities from which evidence is gathered”. Due to the inability to access the entire population as well as time and budget constraints, sampling is conducted. In this research study, the population is identified as all higher academic institutions (Universities, Universities of Technology, both private and public colleges) in the Republic of South Africa, and the sample is higher academic institutions in Gauteng province. Figure 3.7 shows the relationship between population, sample, and individual cases.



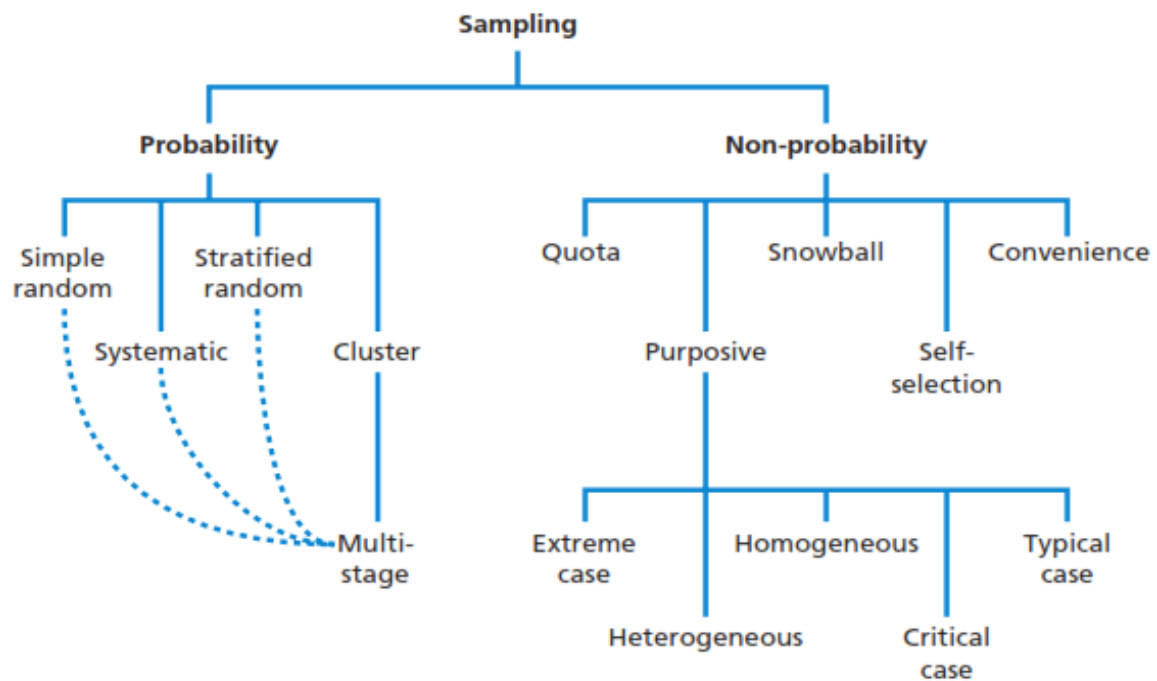
**Figure 3.7: Relationship between population, sample, and individual cases**  
(Source: Saunders et al. 2009:211)

### 3.9.4 Sampling techniques

Sampling techniques can be classified into two types as shown in Figure 3.8, namely:

- i. Probability sampling
- ii. Non-probability sampling





**Figure 3.8: Sampling techniques**  
(Source: Saunders et al. 2009:213)

#### 3.9.4.1 Probability sampling

Probability sampling is a technique where the chance of each entity of the population being selected in the sample, is known (Easterby-Smith et al., 2012; Bryman & Bell, 2011).

#### 3.9.4.2 Non-probability sampling

Non-probability sampling is a technique where the chance of each entity of the population being selected in the sample, is not known (Easterby-Smith et al., 2012).

This research study adopts convenience sampling for its experimental strategy and purposive sampling for its survey strategy.

- **Convenience sampling:** Convenience sampling is defined as “a form of non-probability sampling design where entities are included in a sample on the basis of their ease of access” (Easterby-Smith et al., 2012:340). Convenience sampling is relatively inexpensive to collect data when compared to other sampling techniques. This sampling technique is adopted because it is convenient for the researcher to conduct experiments at the institution where she is enrolled for her studies. Therefore, the samples are conveniently selected based on availability
- **Purposive sampling:** Purposive sampling is a non-probability sampling technique in which the entities are deliberately included in a sample to provide crucial information that

cannot be obtained when using probability sampling techniques (Maxwell, 2013). In this research study, purposive sampling is adopted because the researcher wants to find network security challenges faced by higher academic institutions and determine which available security technologies can be used to protect against network security threats and attacks. Hence, this is a critical factor important to the research study because only IT technical staff at higher academic institutions can provide such required information, enhancing the credibility of the research results. The information provided using this sampling technique "...may be more valuable than those that could be obtained in a random sample" (White & McBurney, 2012:230)

### **3.9.5 Sampling size**

The two Local Area Networks for the experimental strategy were conveniently selected based on their availability at the institution where the researcher is studying. For the questionnaire, 60 participants were purposively selected from various higher academic institutions in Gauteng province. The participants were selected because of the technical and networking knowledge they possess in network security; hence, the researcher believes they are capable of providing in-depth information that could provide optimal insight into the research problem.

### **3.10 Research time horizons**

The time horizon is the timeframe associated with the research study in terms of how long the research lasts for gathering the data (Wilson, 2014). The two time horizons are cross-sectional and longitudinal. A cross-sectional study is conducted over a short period of time such as a few days, weeks or months to gather data, while a longitudinal study is carried out over a long period of time such as several years (Saunders et al., 2009; Wilson, 2014). Each of these time horizons has limitations. Due to time constraints, a cross-sectional study becomes difficult to be carried out on studies requiring comparisons of studies that adopt different timeframes. As a result, not all research topics are appropriate for cross-sectional studies.

In a longitudinal study, the researcher observes any variations and development over a long period of time. Therefore, there is a high possibility that a research participant (or participants) may withdraw from the research study before completion (Wilson, 2014). The participants' withdrawal may negatively affect the research findings.

This research study adopts a cross-sectional time horizon due to limited time for collecting data and meeting the submission deadline.

### **3.11 Data analysis**

Raw data collected for a research study using different data collection methods is useless unless the data are analysed and interpreted correctly and effectively so that it can convey useful and meaningful information that can assist the researcher in answering the research questions and achieve the research objectives (Saunders et al., 2009). Quantitative data can be analysed using a variety of quantitative analysis techniques such as frequency distribution, descriptive statistics, statistical testing, and linear regressions. These data analysis techniques can be used to obtain a clear picture of the data, help describe the values observed, and test relationships between the variables.

In this research study, the statistical software package *SPSS* is used to analyse data obtained from the questionnaire. For experiments, the network analysis software packages called *Wireshark Network Analyser* and *Colasoft Capsa 9.1 Enterprise* are deemed best to analyse network traffic for network threats and attacks to determine what transpires on the network. These packages present the network traffic in a readable format for data analysis purposes.

### **3.12 Reliability and validity**

Reliability and validity are two important concepts to be considered in research to ensure the trustworthiness and credibility of the research study. Saunders et al. (2009:156-157) define reliability as “the extent to which your data collection techniques or analysis procedures will yield consistent findings”, while validity “is concerned with whether the findings are really about what they appear to be about”. Therefore, reliability is concerned with the repeatability and replicability of the research study. This means other researchers will be able to apply the same method used when conducting research in order to replicate and reproduce similar results. Reliability therefore ensures that the research findings are consistent when the study is replicated. In order to increase the reliability of this research study, data triangulation is also adopted. The two data collection methods applied in this research study are questionnaires and structured observation.

The detailed questionnaire as indicated in Annexure B enables other researchers to replicate this study, hence generating comparable results. The questionnaire has been reviewed by the researcher’s supervisor holding a PhD qualification and two IT technical staff where the researcher enrolled for her studies to ensure that the questions in the measuring instrument adequately address the research questions. It is important to allow the participants sufficient time to complete the questionnaire to avoid participant error and to ensure that they respond freely without being under pressure. The participants also need to be assured of anonymity

for the information provided through the questionnaire, and that the results will be summarised, making it difficult to identify the respondents or participants (Annexure A).

To ensure the validity of the experiments selected for this study, a control group is introduced. The introduction and existence of this group ensures that the same treatment is experienced by both the experimental group and the control group. The presence of the control group also assures the researcher that the variation measured between these groups is attributed to the intervention of an independent variable. As the subjects are conveniently selected according to their availability, random selection is not used. However, the same treatment in counterbalanced order for both experimental group and control group in the laboratory settings applies. The results from both the experimental group and the control are then compared and the difference encountered in behaviour attributed to the variation of the independent variable in these two groups.

### 3.13 Research design components

Table 3.3 shows a summary of the research design components adopted for this research study as well as the proposed method for each component.

**Table 3.3: A summary of research design components and proposed method for each component**

Research design components	Proposed method
Research philosophy	Positivism
Research approach	Deductive
Research methodology	Quantitative
Research strategy	(i) Survey (ii) Experiment
Population	All higher academic institutions in Gauteng (Universities, University of Technologies, Private and Public colleges), selected with convenience sampling from all higher academic institutions in South Africa
Data collection	(i) Survey: Questionnaire (closed-question) (ii) Wireshark Network Analyser and Colasoft Capsa 9.1 Enterprise
Sample technique	(i) Purposive sampling (ii) Convenience sampling
Sample and sample size	(i) 60 technical staff at higher academic institutions in Gauteng (ii) Two Local Area Networks(LANs) in a computer laboratory at higher academic institutions in Gauteng
Unit of analysis	Network security threats and attacks

Unit of observation	(i) The IT technical staff at higher academic institutions (participants) (ii) The two LANs in the computer laboratory
Data Analysis	(i) SPSS (ii) Wireshark Network Analyser and Colasoft Capsa 9.1 Enterprise

### 3.14 Summary

The purpose of this chapter was to provide detailed information on how the research study was carried out. The adopted research philosophy, research approach, research methodology, research strategy, data collection methods, research time horizon and data analysis were discussed. The reliability and validity of the data were elaborated on to address the trustworthiness of the research study.

The study adopts an objectivist ontological stance, as the researcher does not want personal opinions or feelings to have an impact on the measurement of reality. A positivist epistemological stance is adopted as scientific method to carry out experiments when collecting numerical data and achieve comparable results. The research study also adopts the deductive research approach and quantitative research, as these are deemed appropriate for the study. The two research strategies selected are survey and experiment to answer the research questions and achieve research objectives.

The unit of analysis has been identified as network security threats and attacks. The units of observation for the questionnaire are 60 IT technical staff at higher academic institutions, selected purposively. For the experiment, the units of observation are the two LANs in the computer laboratory, selected conveniently. The data are collected using two data collection methods, namely questionnaire as survey strategy and structured observation for experiments. Data analysis from the questionnaire is conducted and analysed using the *SPSS software package* while the data collected by means of experiments are analysed using *Wireshark Network Analyser* and *Colasoft Capsa 9.1 Enterprise*. The reliability and validity of the research study and how to achieve this, were discussed.

The next chapter provides the data analysis conducted for the survey strategy.

## CHAPTER 4: SURVEY DATA ANALYSIS

### 4.1 Introduction

The previous chapter elaborated on the research design and methodology of this research study. In this chapter, the analysis and interpretation of the data obtained from the survey questionnaire are discussed. The data collected from the questionnaire were analysed using the SPSS software package. The chapter further contains the results obtained to answer the research questions of the study. The self-administered questionnaires were distributed to various institutions in Gauteng province in order to answer the following secondary research questions (SRQs):

**SRQ1:** What are the challenges surrounding network security at higher academic institutions?

**SRQ2:** What security technologies are available to protect against network security threats and attacks?

### 4.2 Questionnaire analysis

The questionnaire was divided into two sections:

- Section A: Demographic data
- Section B: Network security challenges and security technologies (Annexure B)

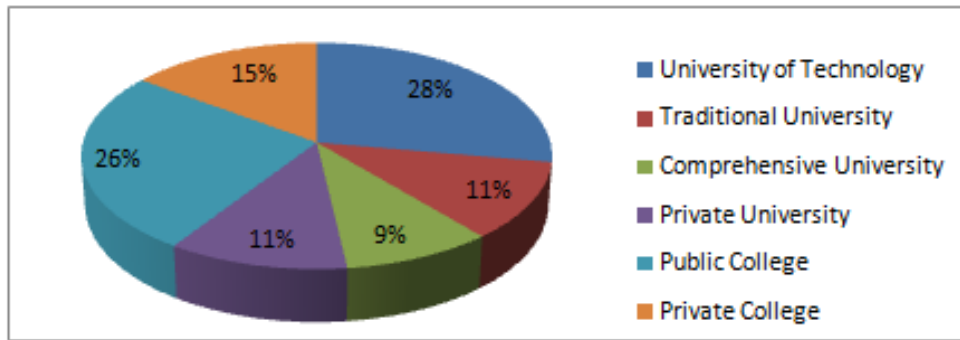
Sixty (60) questionnaires were sent out to participants (section 1.6.4) in Gauteng province, and fifty four (54) questionnaires were returned, giving a total response rate of 90%.

#### 4.2.1 SECTION A: Demographics analysis

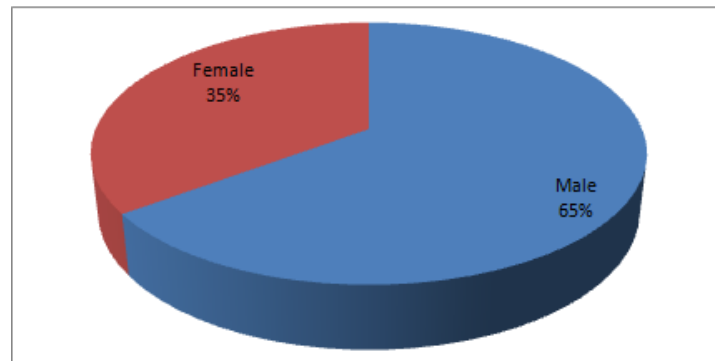
The questionnaires were distributed to 25 higher academic institutions in Gauteng province. These include two universities of technology, three traditional universities, two comprehensive universities, five private universities, seven public colleges, and six private colleges (Figure 4.1).

Figure 4.2 shows the representative population of 35 (65%) male and 19 (35%) female participants in this research study.

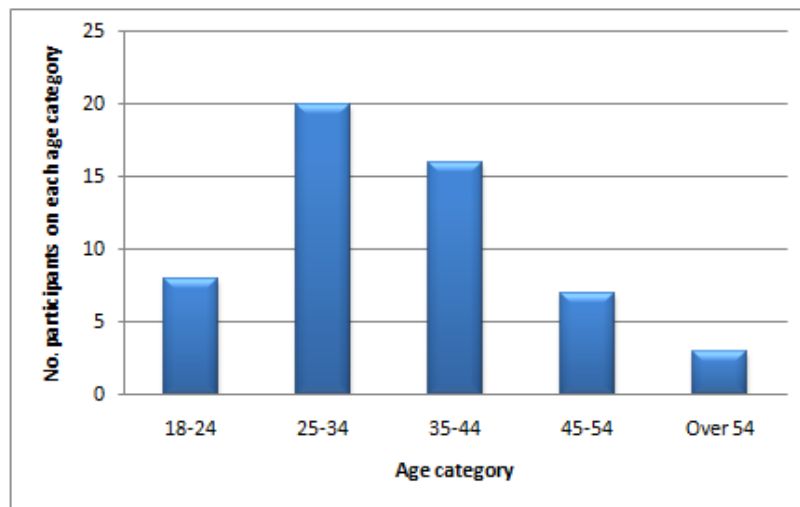
Those who showed interest and participated were mostly aged from 25 to 44 years, constituting 67% in the age category (Figure 4.3).



**Figure 4.1: Type of higher academic institutions**

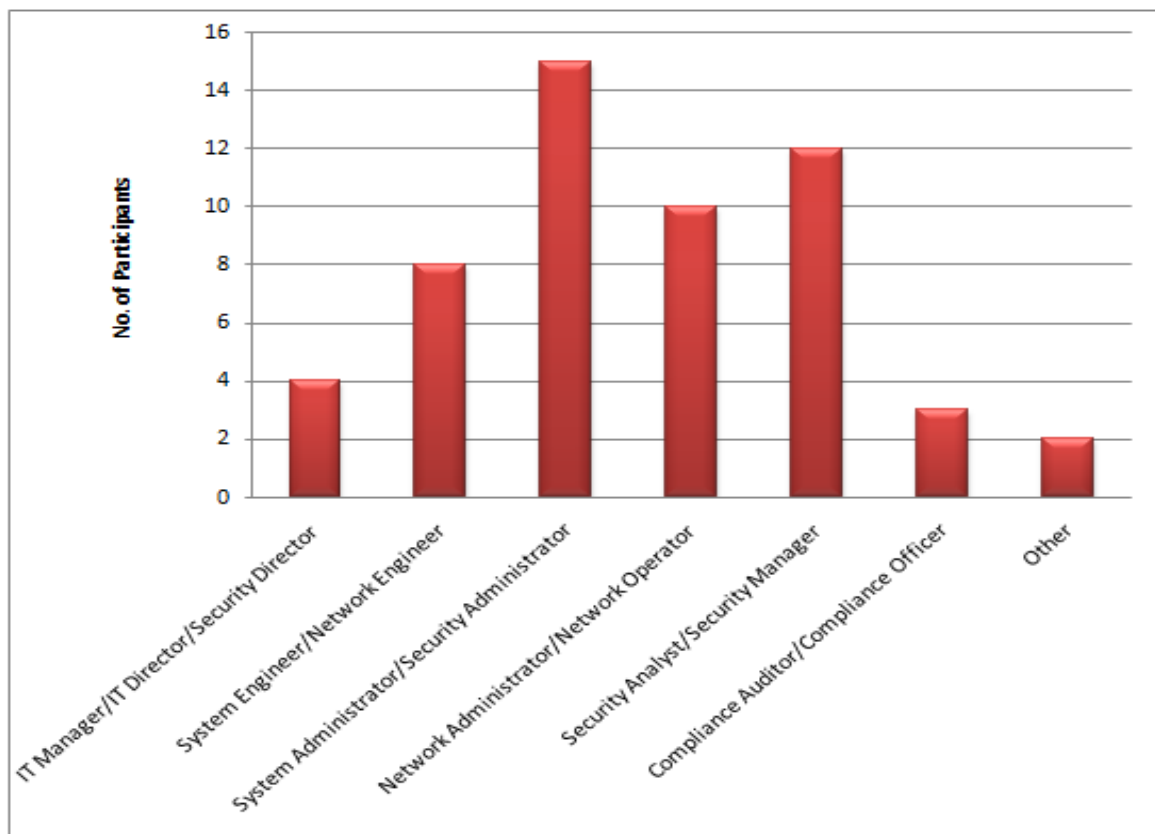


**Figure 4.2: Gender**



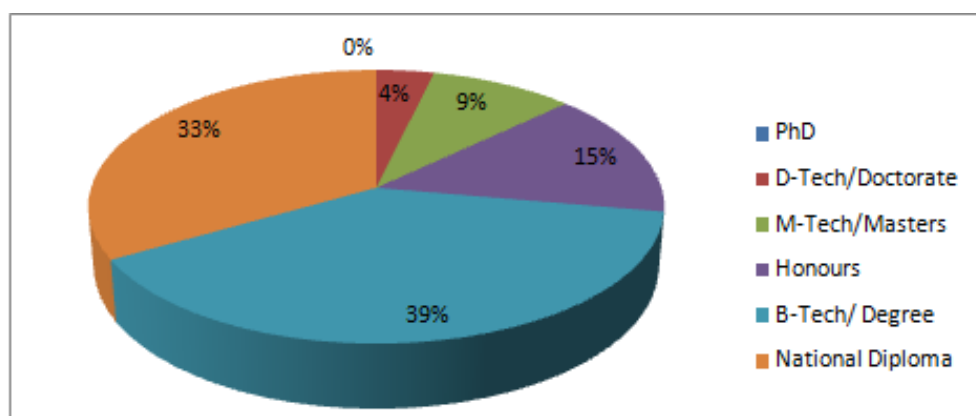
**Figure 4.3: Age category of participants**

The participants were personnel with technical knowledge in computers and networks. Participants primarily holding System Administrator or Security Administrator positions contributed 28%, followed by 22% working as Security Analyst or Security Manager, 18% were Network Administrators or Network Operators, and 15% were System Engineers or Network Engineers. Other IT positions such as Computer Technician, Network Technician, Developers, Compliance Auditor, or Compliance Officers made up 10%. IT Managers, IT Directors and Security Directors contributed 7% (Figure 4.4).



**Figure 4.4: Technical IT positions held by participants**

The majority of the participants (39%) indicated as their highest qualification a degree/BTech, followed by National Diploma (33%). It is surprising to notice that only 13% of participants hold postgraduate qualifications such as MTech/Masters and DTech/PhD, with 15% having an Honours qualification (Figure 4.5). At the time of the research conducted, 28% of participants were working for universities of technology, followed by 26% of participants working for public colleges. Twenty two percent (22%) of participants were working for private universities and traditional universities, 15% of participants for private colleges, leaving 9% of participants working for comprehensive universities.



**Figure 4.5: Highest qualifications of participants**



**Finding A:** The male participants showed interest in taking part in the survey

**Finding B:** Most participants were aged between 25 and 44 years at the time of the research study

**Finding C:** Respondents represented a good mixture of IT technical security positions being held at higher academic institutions

**Finding D:** Postgraduate qualifications are lacking among the IT technical staff at higher academic institutions

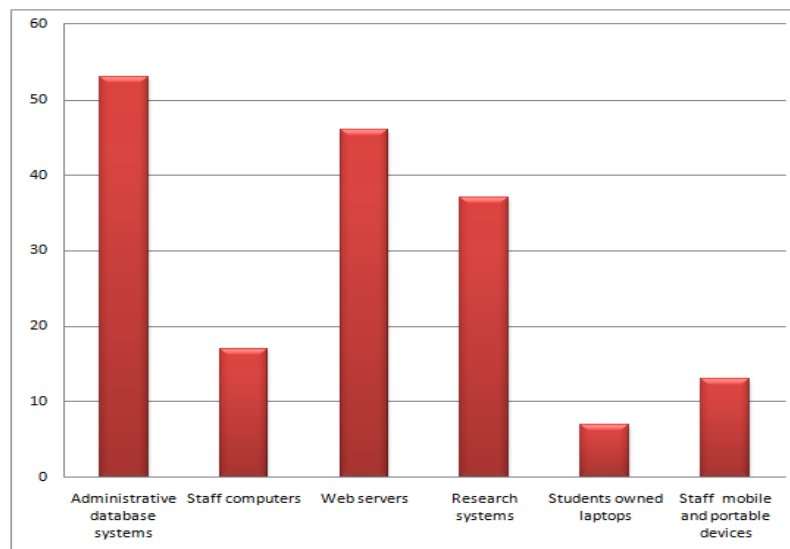
**Finding E:** IT technical personnel from different types of institutions took part in the research study

## 4.2.2 SECTION B: Network security challenges and security technologies

### 4.1.2.1 Secondary research question 1

**SRQ1:** What are the challenges surrounding network security at higher academic institutions?

**Questionnaire Question 1:** *From a risk perspective, which systems are you most concerned with? (Choose all that apply)*



**Figure 4.6: Systems mostly concerned with at higher academic institutions**

Figure 4.6 shows the systems mostly concerned with at higher academic institutions in South Africa. Thirty one percent (31%) of respondents are mostly concerned with administrative database systems that hold financial records as well as staff and students records, while

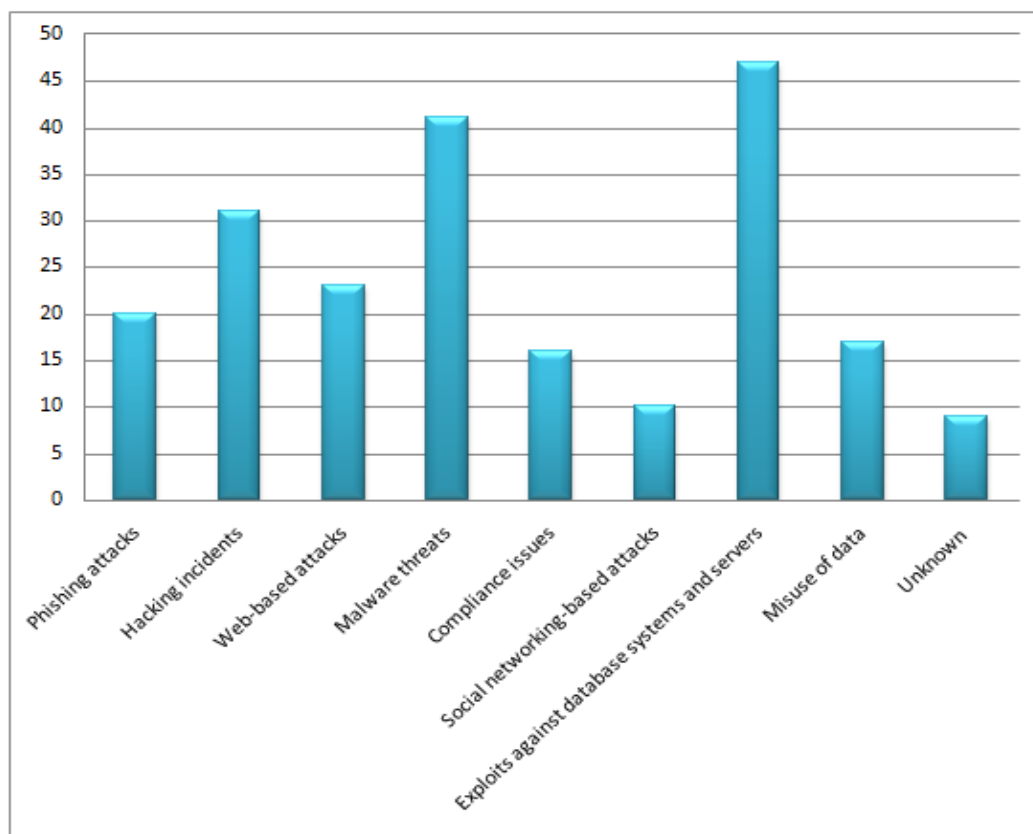
27% are concerned with web servers. Twenty one percent (21%) of respondents are concerned with research systems, 10% with staff computers, and 7% with staff mobile and portable devices, while 4% of participants are less concerned with student-owned laptops.

The highest systems of concern are administrative database systems, followed by web servers and research systems. It makes complete sense because administrative database systems handle the most crucial information (including financial records, staff and students records) about HEIs. The exposure of such data due to compromised systems put institutions at risk. Web servers are of concern because they are more likely to be attacked, which can cause a severe disruption on the network and inconvenience users by delaying web services such as emails or resulting in slow or unavailable web pages. Research systems are of concern because they store intellectual property for which institutions may receive research funding based on their research outputs. It is not surprising that student-owned laptops are of less concern. Students mostly deal with their own personal data and their laptops do not handle sensitive data, which can affect the institution in case of a data breach.

**Finding 1:** Participants are aware of the risks that could be imposed should the systems be compromised. As a result, the respondents showed greater concern with administrative database systems than student-owned laptops on their academic networks. This, therefore, reflects what kinds of systems need more protection.

**Questionnaire Question 2:** *Which attack vectors and security issues is your organisation most concerned with to protect against? (Choose all that apply)*

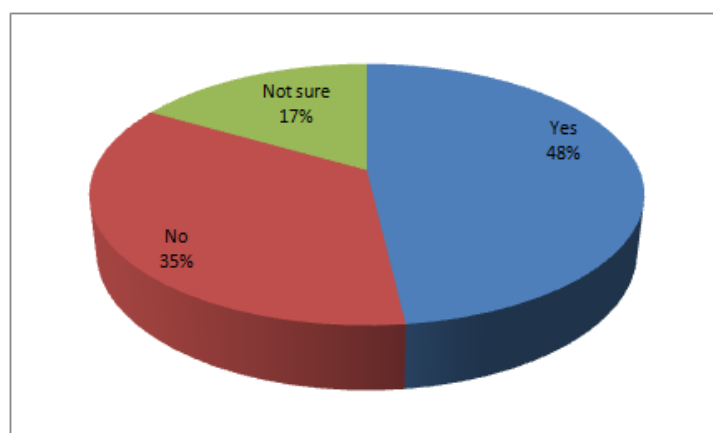
Based on the results shown in Figure 4.7, the majority of the respondents are concerned with exploits against database systems and servers, followed by malware attacks, hacking incidents and phishing attacks. The top five attack vectors and security issues participants are most concerned with are associated with the capability of the institutions to patch their systems. Misuse of data, compliance issues, and social networking-based attacks could be addressed through network security policy enforcement and user training and education. Addressing these issues is crucial in ensuring that all network users comply with the security policy implemented by an institution.



**Figure 4.7: Attack vectors and security issues institutions are most concerned with**

**Finding 2:** Due to sensitive data stored on databases and servers, attacks and security issues against these systems are among the highest concerns to protect against as it could easily be exploited. The second highest attack vectors and security issues identified are malware threats followed by hacking incidents.

**Questionnaire Question 3:** *Has your institution's network been internally or externally compromised in the past two years?*



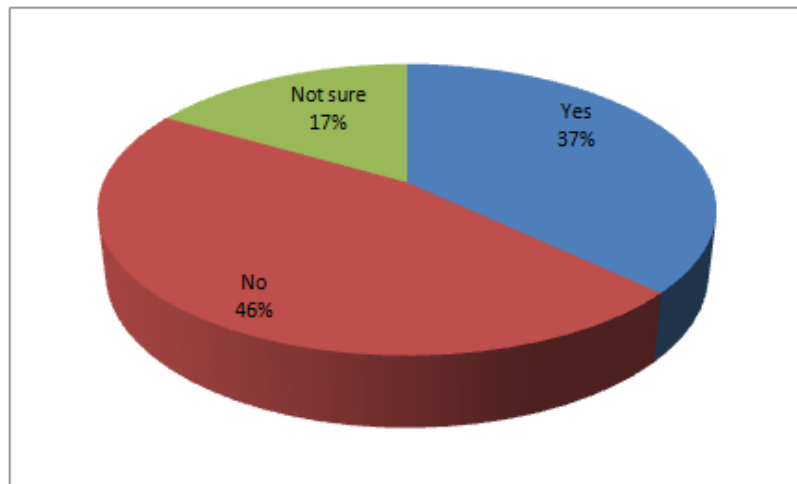
**Figure 4.8: Network security breaches**

As shown in Figure 4.8, 48% of participants reported that their institution's network had been compromised in the last two years; 35% indicated they had not experienced network security breaches, while 17% said they were not sure. The results are worrying because the majority of respondents have indicated network security breaches during the period specified. Network security breaches can have negative consequences such as interruption of institutions' processes, bad reputation, loss of data, and financial loss. Network security breaches within an institution could occur due to a number of reasons such as: a) when the institution does not enforce its network security policy; b) lack of programmes such as patch management and threat management programmes; c) misuse of rights by personnel; d) deploying systems that are inadequately secured; and e) insufficient security maintenance.

Lack of programmes such as patch and threat management programmes could make systems and networks more vulnerable to network security threats and attacks. This poses a threat due to a delay in applying patches regularly on the systems or in time before damage could happen. Another threat is the use of outdated anti-malware file definitions because any anti-malware programme installed would not be effective to detect the latest malicious activities without regular updates. Implementing patch and threat programmes is very important in protecting systems against different attacks and security issues. The implementation of these programmes could help the institutions reduce network threats and attacks associated with attackers exploiting flaws on systems. Furthermore, deployment of systems that are inadequately secured and insufficient security maintenance jeopardise network security, as the network is vulnerable to threats and attacks. Lack of enforcing network security policy could lead to personnel being irresponsible in terms of activities they perform on the network that could make it vulnerable to threats and attacks.

**Finding 3:** Institutions have experienced network security breaches in the past two years

**Questionnaire Question 4:** *Does your institution have a well-designed and written network security policy?*



**Figure 4.9: Respondents' network security policy awareness**

Figure 4.9 shows a summary of the respondents' awareness of network security policy. The majority of the respondents (46%) indicated they do not have a network security policy, 37% said they actually do have a policy, while 17% said they are not sure whether such a document exists or not. This leaves 63% of participants with risks that may be imposed due to the lack of network security policy. A network security policy is such an imperative document in an institution because it clearly communicates the institution's vision and commitment regarding the security on their network. It is worrisome to learn that most respondents do not have a well-designed and written network security policy at their institutions. This means such institutions might not have a solid foundation in terms of acceptable behaviours, standards and procedures regarding the use of their institution's resources as well as no firm guidelines on processes taking place on their networks. As a result, it is likely challenging to achieve institutional network security goals, and this might impose threats and attacks on the network. Some respondents indicated that they are not sure of a network security policy presence that reflects the lack of responsibility by the institution to make users aware of such policy upon appointing them.

**Finding 4:** There is a lack of a well-designed and written network security policy at most institutions.

**Questionnaire Question 5:** *Does your institution enforce network security policy to all network users?*

To ensure that network users comply with network security policy, this policy must be enforced. However, 54% of participants do not enforce network security policy, 31% said they do enforce network security policy, while 15% of participants were not sure whether network security policy is enforced to all users. Network security policy should not only exist

on paper without substantial benefits; it must also be adhered to in order to meet its expectations initially set out. If network security policy is not enforced, waste of time and resources invested in designing the policy may occur. Top management should therefore support the implementation and enforcement of network security policy to ensure that every user adheres to the rules stipulated and know the consequences of violating the policy.

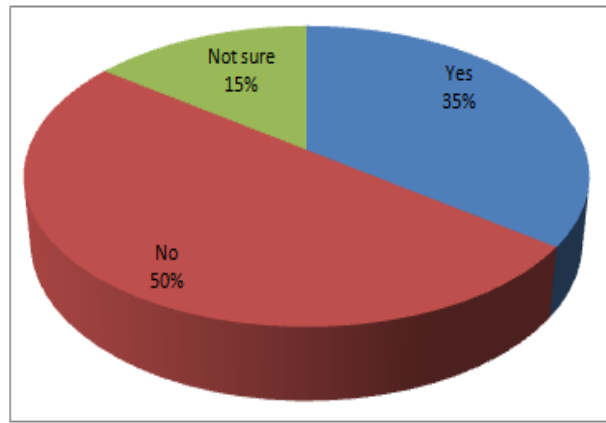
**Finding 5:** There is inadequate network security policy enforcement to all network users at most institutions

**Questionnaire Question 6:** *Is the network security policy at your institution periodically being reviewed and updated to include security controls and standards that can help combat the latest network security threats and attacks?*

Based on the responses, 59% of the participants reported that network security policy is not regularly being reviewed and updated; 28% reported that they do review and update their network security policy regularly while 13% of participants said they were not sure. Looking at the results, one would wonder whether responsible personnel at different institutions are aware of the importance of constantly reviewing and updating network security policy. This enhances the functionality of network security policy and provides the necessary protection against network security threats or any other security issues as well as ensuring that new network security threats are being addressed properly. Without constantly reviewing and updating the policy it becomes dysfunctional and ineffective, failing to address new threats and security issues (such as compliance, latest technologies and changes, and failures occurring on the system) that may hamper network security.

**Finding 6:** There is a lack of network security policy reviews and updates on a regular basis at most institutions.

**Questionnaire Question 7:** *Does your institution offer mandatory training and education on network security policy to users?*

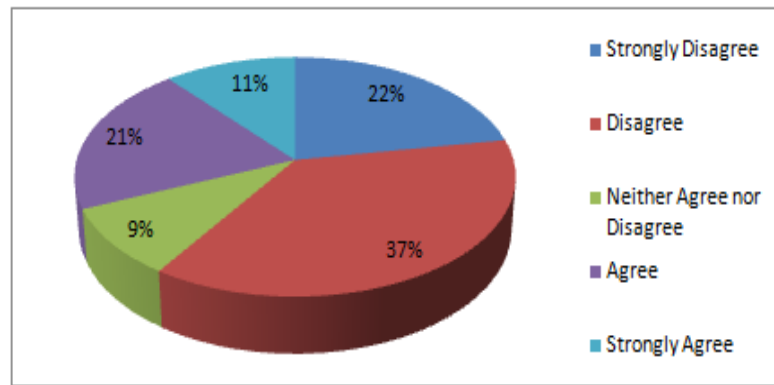


**Figure 4.10: Mandatory user training and education on network security policy**

Training and educating network users help to address network security issues. However, the results indicate that 50% of the participants are not offered mandatory training and education on network security policy, 35% of participants do receive such training and education, while 15% of participants said they are not sure whether this type of training and education is provided. The lack of exposure to training and education for network users would likely hinder addressing network security threats and attacks due to lack of users' knowledge. This would further make it difficult for technical users to find mechanisms that could be used to address any security issues. Due to inadequate training and education, users would not comply with the institution's network security policy because some users might not know the existence of such a document. The manner in which resources are secured requires users to be taught and this needs to be done regularly through training to make users aware of the latest mechanisms for securing resources related to their institution's network security as well as knowing the importance of network security. It would further help users to understand how to benefit from network security with their daily tasks performed via the network. A lack of training on how to do things differently could hamper network security as users would not be able to know how to improve the institution's operations and protect assets and information. Figure 4.10 shows the respondents' knowledge on the implementation of mandatory user training and education on network security policy at their institutions.

**Finding 7:** There is insufficient mandatory training and education on network security for network users

**Questionnaire Question 8:** *Are you satisfied with the budget allocated to the IT department in your institution for improving network security?*



**Figure 4.11: IT budget allocation satisfaction**

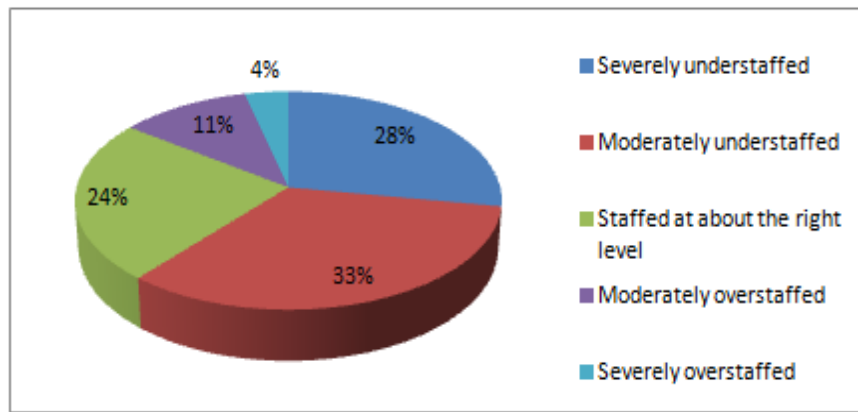
According to the results shown in Figure 4.11, 37% of participants indicated their dissatisfaction with the IT budget allocation, followed by 22% who indicated that they were very dissatisfied, leaving a total of 32% of participants who indicated they were satisfied/very satisfied, and 9% neither agreed nor disagreed with the question. Budget allocation to the IT department of an institution plays an important role in ensuring that the institution's network and resources are properly secured. However, insufficient budget allocation could create security issues affecting negatively on the capability of the institution to maintain its network security. Because of a lack of funds, the institution's IT department may fail to purchase industrial hardware and software that require continuing expenses related to licensing and maintenance. This would therefore force the institution to revert to open source products that in return may impose network security threats.

**Finding 8:** The majority of participants are not satisfied with the allocation of the IT budget

**Questionnaire Question 9:** *How would you describe IT technical staffing at your institution?*

In Figure 4.12, respondents' results on IT technical staffing are indicated. Thirty three percent (33%) of the respondents indicated they are moderately understaffed, 28% indicated they are severely understaffed, 24% opined that staffing is at about the right level, 11% of respondents opted for moderately overstaffed, and 4% of respondents believe the IT department is severely overstaffed.





**Figure 4.12: Staffing level of the IT department**

Understaffing could be attributed to the competitive edge on salary offers between higher academic institutions and the private sector (industries). The private sector offers high remuneration levels, hence they are able to attract and retain highly qualified candidates suitable for the job. Because of budget constraints at higher academic institutions, institutions might lose qualified and competent personnel.

**Finding 9:** The IT departments at higher academic institutions are short-staffed

**Questionnaire Question 10:** *Do you think your institution needs to hire more IT technical staff?*

Based on the responses, 41% of respondents agree that their institutions should hire more IT technical staff, followed by 26% of respondents who strongly agree. Twenty two percent (22%) of respondents constitute those who disagree/strongly disagree, leaving 11% of respondents who could neither agree nor disagree. A good balance of IT technical staff at higher academic institutions is very important when it comes to the planning and management of network security. The results indicate a high percentage of respondents who want their institutions to increase their IT technical staff. Staffing in small environments might not be of concern, as individual personnel could be responsible for various roles within the IT department. However, staffing issues in large and complex environments such as higher academic institutions raise many concerns, as there is a need for many qualified and competent personnel to handle different responsibilities and play different roles. The need for skilled and competent personnel would help in the proper implementation of security technologies, managing and maintaining network security.

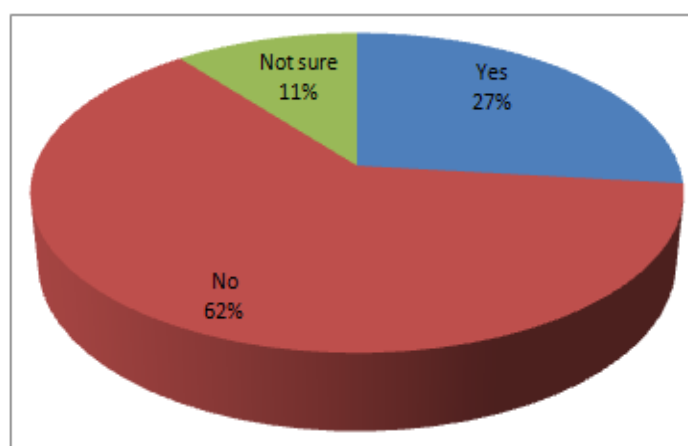
**Finding 10:** There is a need at higher academic institutions to increase IT technical staff

**Questionnaire Question 11:** *Does the IT department at your institution perform vulnerability assessment on the systems and network?*

Based on the results, 46% of respondents reported that they do perform vulnerability assessment on the systems and network, 39% indicated that they do not perform vulnerability assessments, while 15% were not sure. It is interesting to find that the majority of the participants do indeed perform vulnerability assessments. This assessment is very important as the systems and network are being tested to identify the presence of weaknesses and any possible exposure and threats they might have to the institution's resources. Performing this assessment would help an institution eliminate network security threats and attacks whereby an attacker may take advantage of exploiting vulnerabilities against the institution's systems and network. Vulnerability assessment could also assist in evaluating the effectiveness of implemented security controls. The lack of performing vulnerability assessment might make the systems and network susceptible to network security threats and attacks hence put them at risk. The lack of performing this assessment might be due to ignorance or the fact that IT personnel might not be aware of the existence of vulnerabilities on their systems that could easily be exploited.

**Finding 11:** Majority of participants are aware of the importance of performing vulnerability assessments

**Questionnaire Question 12:** *Does the IT department at your institution perform penetration testing to exploit vulnerabilities against the systems and network?*



**Figure 4.13: Penetration testing performed**

The results in Figure 4.13 show that most respondents (62%) reported they do not perform penetration testing to exploit vulnerabilities against the systems, 27% indicated that they do perform penetration testing, while 11% of respondents were not sure. The results are

significant as a high percentage of respondents indicated that penetration testing is not conducted. Penetration testing is as essential as vulnerability assessment because effort is made to exploit identified vulnerabilities on the systems and network by bypassing security controls in order to gain access. This test could help the institution check whether it has the capability to defend itself against network security threats and attacks, hence determine whether unauthorised users could gain access to the institution's network and resources. As a result, this test is imperative to determine the effectiveness of implemented security controls and enable the IT department within the institution to make the necessary adjustments to implemented security controls to eliminate existing vulnerabilities. Penetration testing could also assist in enhancing the systems and network functionality and ensure that security controls are adequate for protecting the network and its resources.

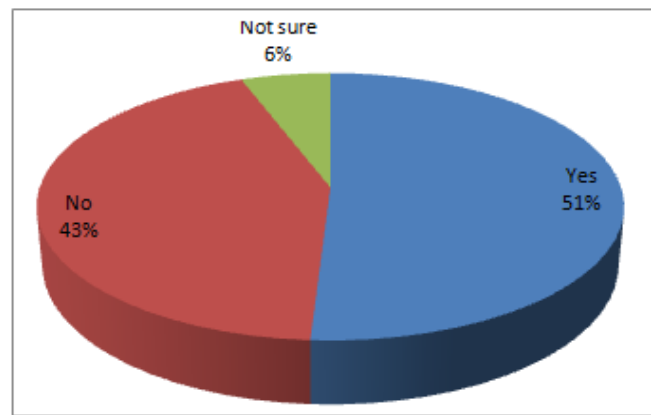
**Finding 12:** The lack of penetration testing on the systems and network is substantial

**Questionnaire Question 13:** *How often does the IT department perform vulnerability assessment or penetration testing to eliminate vulnerabilities, threats, and attacks?*

Periodic testing or assessment of systems and networks for security threats and attacks provide tangible results. Participants indicated that either vulnerability assessment or penetration testing is conducted on a yearly basis, followed by half-yearly and a monthly basis. Vulnerability assessment should be performed frequently, i.e. on a weekly or monthly basis, in order to find any flaws in systems and applications to avoid security attacks that can exploit these vulnerabilities. Waiting until the end of each year to perform vulnerability assessment could expose the institution to network security threats and attacks as the IT personnel might not be aware of the existence of such vulnerabilities, hence fail to mitigate them. Furthermore, waiting for a long period before performing vulnerability assessment could impede IT personnel to evaluate their systems effectively. Penetration testing, if conducted on an annual basis, could still enable the IT personnel to evaluate their security controls. However, to achieve the institution's security objectives and obtain valuable results, both the vulnerability assessment and network security tests are to be conducted frequently and also after major changes have been done to the institution's network environment.

**Finding 13:** Vulnerability assessment or penetration testing are performed only after a long period of time such as on a yearly basis

**Questionnaire Question 14:** *Does the IT department at your institution investigate and take remedial actions for reported security alerts and incidents?*



**Figure 4.14: Remedial actions taken on reported security alerts and incidents**

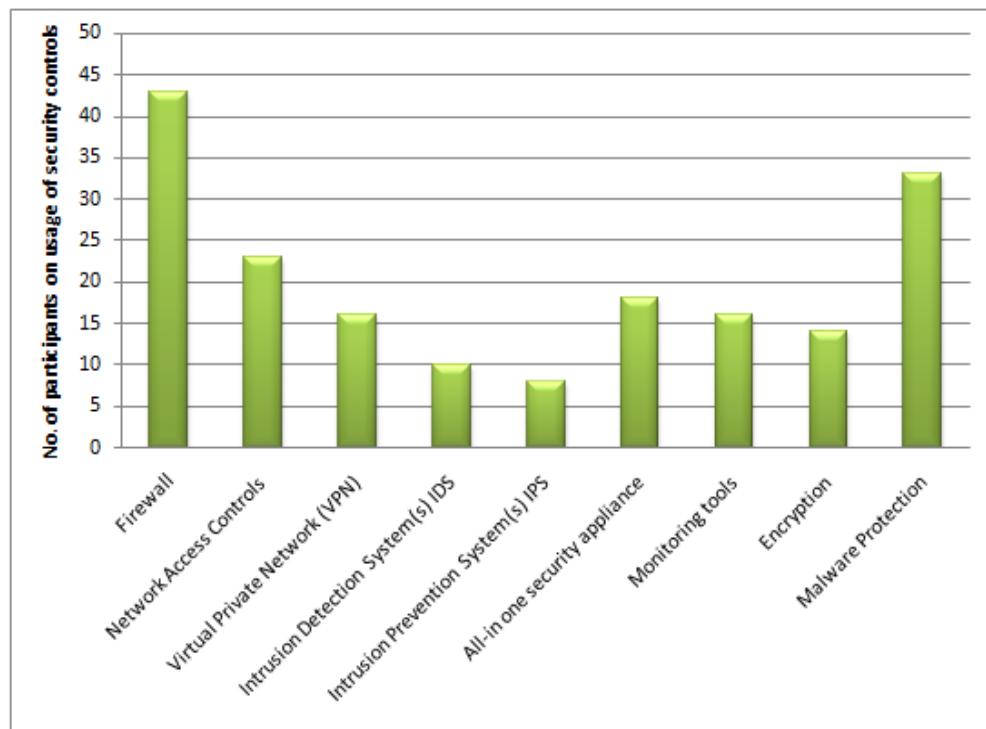
Based on the results in Figure 4.14, 51% of the respondents indicated that the staff in the IT department in their institution investigate and take remedial actions for reported security alerts and incidents, 43% do not investigate and take remedial actions, while 6% of the respondents were not sure. Security alerts and incidents could be caused by actions such as outsiders attempting to attack the institution's valuable systems, users not following the network security policy within the institution, improper use of the systems, and the existence of vulnerability on systems. A slight difference exists between those investigating and taking remedial actions and those who do not. This becomes a concern because reported security alerts and incidents should be taken very seriously in order to mitigate consequences as well as preventing such security incidents from happening again. When there are no actions taken, offenders would carry on with their suspicious activities knowing that nothing would happen to them because of their misconduct. Institutions need to conduct detailed investigations and take proper actions upon reported security alerts and incidents threatening the confidentiality, integrity, and availability of the institution's network resources.

**Finding 14:** Although the majority of respondents indicated that the staff in the IT department investigate and take remedial actions for reported security alerts and incidents, the percentage of those who do not take responsibility, is still high

#### **4.1.2.2 Secondary research question 2**

**SRQ2:** What security technologies are available to protect against network security threats and attacks?

**Questionnaire Question 15:** Which of the following technologies, security measures, or controls are used by your institution? (Choose all that apply)



**Figure 4.15: Usage of technologies and security controls at higher academic institutions**

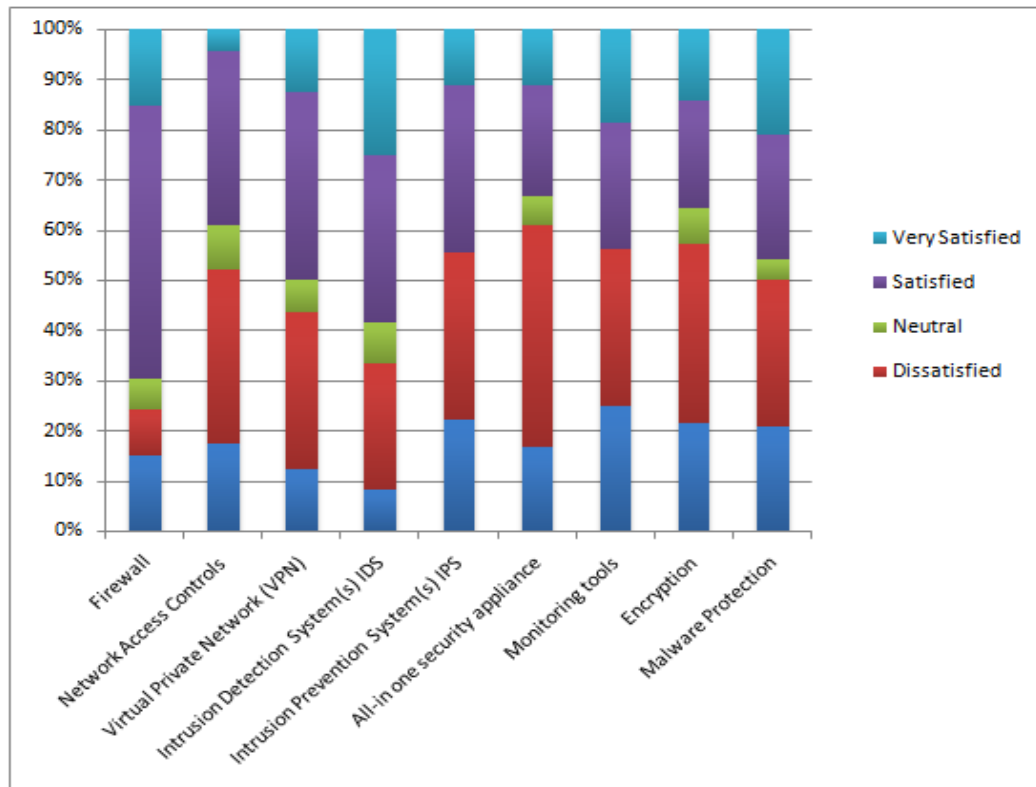
The results in Figure 4.15 indicate that the majority of participants rely mainly on firewalls, followed by malware protection, network access controls, and all-in-one security appliances. It is not surprising that most respondents indicated the use of firewalls because it is a traditional technology protecting internal networks from outsiders. Because of the security threats that malware pose to systems, malware protection seemed to be the second most used security control. Not all malicious traffic can be blocked by a firewall, hence the need for malware protection. It is however significant to find that intrusion detection systems, intrusion prevention systems, and encryption and monitoring tools are the least used by institutions. Monitoring tools could assist in ensuring that any technical design flaws, improper configuration, implantation code, and unsafe services in systems are detected and solved before any major damage is experienced. These security controls should be among the highest used security controls to ensure protection of institution's network resources (Paquet, 2013). The limited use of some of these technologies and security controls could be due to high purchase costs as well as deploying them in large environments such as higher academic institutions' networks. However, this challenge could lead to exposure of academic networks to hackers and cyber criminals.

**Finding 15:** Firewalls, malware protection, and network access controls are the top three most used security technologies

**Finding 16:** The inadequate use of intrusion detection systems, intrusion prevention systems and encryption technologies has been detected

**Questionnaire question 16:** Please indicate your level of satisfaction on the intended operation of security technologies implemented at your institution.

Figure 4.16 shows the participants' level of satisfaction on security technologies used in higher academic institutions.



**Figure 4.16: Level of satisfaction on security technologies**

The majority of participants who indicated that their institutions use different security technologies were satisfied with the security technologies they use. The top three security technologies participants are satisfied with are firewall, Intrusion Detection System and Virtual Private Network. Based on their level of satisfaction of firewalls, the majority of participants indicated that they are generally satisfied with the product. Although malware protection is one of the top three security technologies being used, most participants were not happy with the product. The few participants who indicated the use of IDSs in their institutions seem to be pleased with this technology.

The use of different security technologies could assist in mitigating network security threats and attacks. The configuration of each security technology and applying patches on these security technologies could also have an impact on the satisfaction levels of network users. Therefore, IT personnel should ensure proper configuration and apply patches periodically to achieve optimal performance and the desired satisfaction.

**Finding 17:** Firewall technology received the highest satisfaction rate among participants and all-in one security appliance received the lowest satisfaction rate

**Finding 18:** The configuration of each security technology have an impact on the satisfaction levels of users

**Finding 19:** The vulnerabilities of each security technology affect the satisfaction levels of users

### **4.3 Summary**

This chapter presented the results and discussion on the data obtained from the survey conducted at higher academic institutions in Gauteng province. The objective was to determine the challenges surrounding network security at HEIs and to identify which security technologies are available to protect HEI networks against security threats and attacks. The results revealed a number of challenges faced by higher academic institutions, including insufficient budget allocation to IT departments to address network security, inadequate IT technical staff to handle technical issues, and the lack of network security policy as well as its enforcement. Firewalls, malware protection, and network access controls are among the security technologies most used by higher academic institutions. IDS/IPS, encryption and monitoring tools are the least security technologies used.

Table 4.1 shows a summary of the findings after the data collected by means of questionnaire have been analysed to answer two research questions, SRQ1 and SRQ2.

**Table 4.1: Summary of findings**

Research Questions	Findings
<b>SRQ1: What are the challenges surrounding network security at higher academic institutions?</b>	<b>Finding 1:</b> Participants are aware of the risks that could be imposed should the systems be compromised. As a result, the respondents showed greater concern with administrative database systems than student-owned laptops on their academic networks. This, therefore, reflects what kinds of systems need more protection
	<b>Finding 2:</b> Due to sensitive data stored on databases and servers, attacks and security issues against these systems are among the highest concerns to protect against as it could easily be exploited. The second highest attack vectors and security issues identified are malware threats followed by hacking incidents
	<b>Finding 3:</b> Institutions have experienced network security breaches in the past two years
	<b>Finding 4:</b> There is a lack of a well-designed and written network security policy at most institutions.
	<b>Finding 5:</b> There is inadequate network security policy enforcement to all network users at most institutions
	<b>Finding 6:</b> There is a lack of network security policy reviews and updates on a regular basis at most institutions
	<b>Finding 7:</b> There is insufficient mandatory training and education on network security for network users
	<b>Finding 8:</b> The majority of participants are not satisfied with the allocation of the IT budget
	<b>Finding 9:</b> The IT departments at higher academic institutions are short-staffed
	<b>Finding 10:</b> There is a need at higher academic institutions to increase IT technical staff
	<b>Finding 11:</b> Majority of participants are aware of the importance of performing vulnerability assessments
	<b>Finding 12:</b> The lack of penetration testing on the systems and network is substantial
	<b>Finding 13:</b> Vulnerability assessment or penetration testing are performed only after a long period of time such as on a yearly basis
	<b>Finding 14:</b> Although the majority of respondents indicated that the staff in the IT department investigate and take remedial actions for reported security alerts and incidents, the percentage of those who do not take responsibility is still high
<b>SRQ2: What security technologies are available to protect against network security threats and attacks?</b>	<b>Finding 15:</b> Firewalls, malware protection and network access controls are the top three most used security technologies
	<b>Finding 16:</b> The inadequate use of intrusion detection systems, intrusion prevention systems and encryption technologies has been detected



Research Questions	Findings
	<b>Finding 17:</b> Firewall technology received the highest satisfaction rate among participants and all-in-one security appliance received the lowest satisfaction rate
	<b>Finding 18:</b> The configuration of each security technology have an impact on the satisfaction levels of users
	<b>Finding 19:</b> The vulnerabilities on each security technology affect the satisfaction levels of users

## CHAPTER 5: EXPERIMENTAL DATA ANALYSIS

### 5.1 Introduction

This research study made use of two research strategies, namely survey and experiment, as mentioned in Chapter 3, to provide answers to the research questions. The previous chapter discussed the results obtained from survey questionnaire. Network security challenges may be addressed on a non-technical and technical level. A non-technical level, however, involves mostly the creation and designing of network security policies, as well as reviewing and updating networking security policies. Addressing network security challenges on a technical level involves the implementation of network security measures. This chapter addresses network security challenges identified in the survey questionnaire and literature review that could be addressed on a technical level. This chapter furthermore focuses on how networks could be protected against such security challenges, hence improving network security. This chapter answers the following research question:

**SRQ3: How can network security be addressed and improved in order to protect against network security threats and attacks in South Africa?**

### 5.2 Experimental setup

Due to the sensitivity of network security, the experiments were set up and conducted in a laboratory to avoid violating the university's policies and disrupting its network operations. The two private networks, one being the control network and the other being the experimental network, were set up and configured in a laboratory to emulate various network challenges. The experimental network was manipulated to find the implications of network security threats and attacks on network security before and after implementing security measures. Since the experiments were not performed on the university's network, the threats and attacks imposed on these experiments could not disrupt the campus network.

The survey findings in Table 4.1 reveal that most institutions' networks had been breached internally or externally within the past two years. In addition, it was also found from literature that one of the challenges faced by institutions was that their networks were mostly attacked internally (Al-Akhras, 2006). These security breaches, if external, mean the attacks come from the 'outside world', hence, the configuration of the firewall or technology used to protect the network might have been exploited. However, if attacks are internal, it means their origin is within the network and therefore affects Layer 2 (Data Link layer) of the Open Systems Interconnection (OSI) model (Figure 5.1). The OSI model is the reference model ensuring interoperability among network devices by offering a standardised way for network devices to

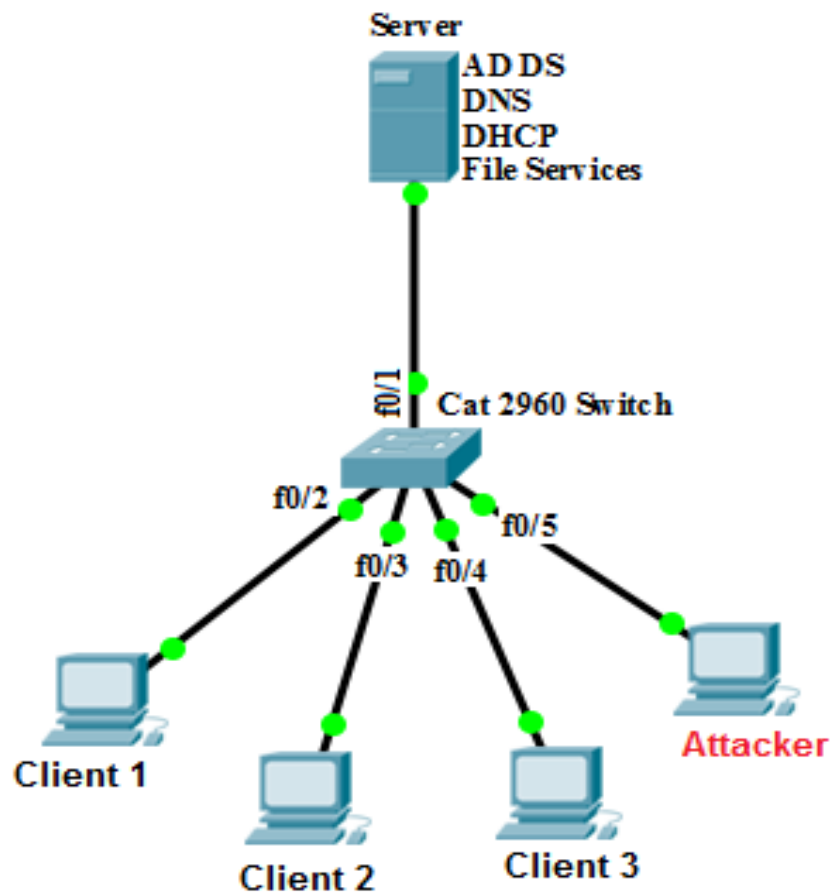
communicate (Cisco Networking Academy, 2014). This model segregates network communication functions into seven specific layers as shown in Figure 5.1. Each layer is partly responsible for processing data to be sent across the network. The Data Link layer in particular is responsible for checking errors in the data being transmitted to ensure validity. Therefore, internal penetration testing experiments were conducted to address network security on Layer 2 of the internal private network to assume the attacker's identity or the identity of the malicious insider. Network security threats and attacks such as the DHCP Starvation attack (section 5.2.1), Rogue DHCP Server attack (section 5.2.2), MAC Flooding (section 5.2.3), ARP Poisoning attack (section 5.2.4), and unauthorised access were exploited.



**Figure 5.1: OSI model**  
(Source: Cisco Networking Academy, 2014)

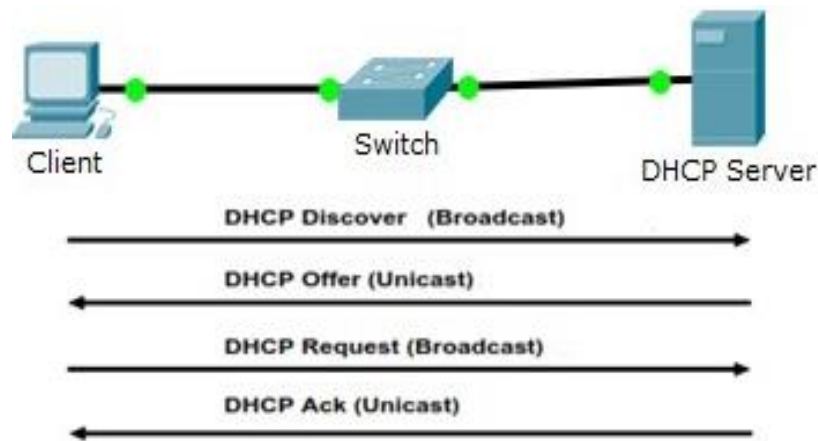
The experimental setup in the laboratory as shown in Figure 5.2 had four personal computers and a server connected to a Cisco Catalyst 2960 series switch running the 12.2 Cisco IOS software version. The Windows Server 2012 R2 operating system was installed on the server and the following services were deployed: Active Directory Domain Services (AD DS), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and File services. These services were deployed to allow centralised access to resources, easy

management of objects, resolution of computer names, domain names and Internet Protocol (IP) addresses, and offering dynamic assignment of IP addresses to client computers.



**Figure 5.2: Physical network topology for both experimental network and control network**

The IT personnel from different institutions also showed their concern (via the survey) on attacks against database systems and servers (Table 4.1). These systems and servers run different services such as DHCP, DNS and file services that may be vulnerable to a number of security attacks. Dynamic Host Configuration Protocol (DHCP) is the protocol that assigns IP addresses automatically to hosts as they connect to the network (Cisco Networking Academy, 2014). However, the IP addresses are temporarily assigned for a certain period and are returned to the server pool once the lease period expires. The use of DHCP in a large network environment could be effective, as it reduces administrative workload for manual configuration on each host on the network with proper network settings. Figure 5.3 shows how DHCP works when a host joins the network.



**Figure 5.3: How DHCP works**  
(Source: Adapted from Zacker, 2014)

When a host joins the network, it broadcasts DHCPDISCOVER on the network in order to identify any available DHCP server. When the server receives the broadcast, it replies by sending DHCPOFFER that contains TCP/IP settings configured on the server. Due to the possibility of multiple DHCP servers on the network, the host might receive multiple offers. Upon accepting the TCP/IP settings offered, the host broadcasts DHCPREQUEST to notify the server of the acceptance or rejection of the offer. Depending on the availability or validity of the offered addresses, the server sends out DHCPACK to the host to complete acknowledgment of the process. However, according to Duangphasuk et al. (2011), DHCP is vulnerable to security attacks such as DHCP Starvation and DHCP Spoofing (Rogue DHCP Server attack).

### 5.2.1 DHCP Starvation attack experiment

The attacker targets the DHCP server by sending a large number of fake DHCP requests (DHCPDISCOVER) in order to use all available IP addresses in the address pool (Duangphasuk et al., 2011). The DHCP server issues addresses upon each request, until all available IP addresses are exhausted. Any request from legitimate clients after exhausting all the IP addresses, would result in a Denial of Service attack as the server could not assign any IP addresses, hence deny such clients access to network resources (Mukhtar et al., 2012).

In this experiment, the legitimate DHCP server was configured with a Class C IP address accommodating 30 hosts on the network. Figure 5.4 shows the DHCP scope (192.168.10.0/27) with the address pool ranging from 192.168.10.1 to 192.168.10.30 and exclusion IP addresses ranging from 192.168.10.1 to 192.168.10.5. These were the IP addresses used in the experiments. Excluded IP addresses are those that cannot be distributed by the DHCP server to client computers. These addresses can however be

manually assigned to network devices such as servers, routers, switches and printers. The purpose of excluding some of the IP addresses in this experiment was to ensure that the server and network switch have static IP addresses assigned (an IP address that does not change) to ensure constant network connectivity.

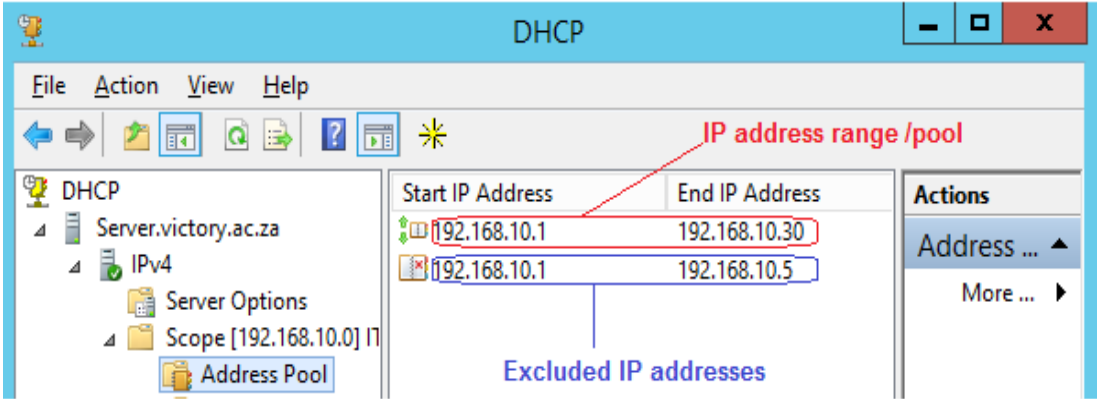


Figure 5.4: DHCP Scope and Address pool

Once the DHCP server was configured, three client computers were connected to the network to receive network configuration settings. Figure 5.5 shows addresses that had been leased out to these connected computers on the network.

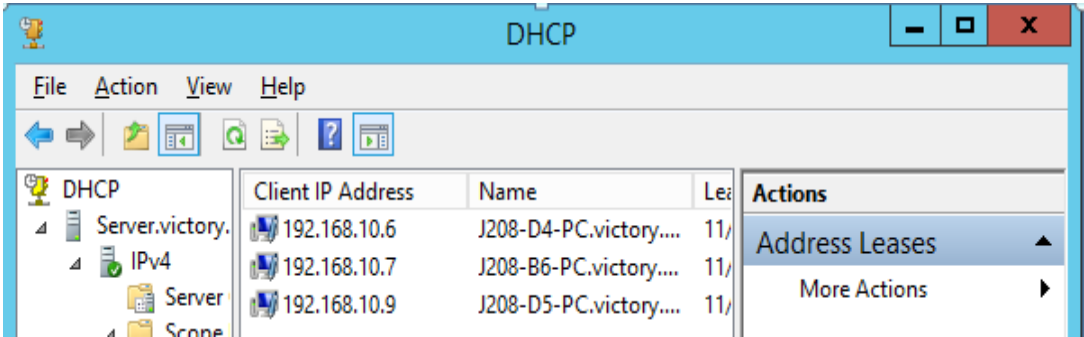


Figure 5.5: Leased client IP addresses

The attacker's computer was attached to the switch to receive network configuration settings from the DHCP server as shown in Figure 5.6. The attacker's computer was automatically assigned IP address 192.168.10.8 and subnet mask 255.255.255.224. Making use of unmanaged switch ports or leaving unused switch ports open, poses a security threat on the network as the attacker or malicious user could connect their devices, hence, gaining unauthorised access to the network and its resources.

```

root@Rethabile:~# ifconfig
eth0: Link encap:Ethernet HWaddr b8:ac:6f:2d:b2:70
      inet addr:192.168.10.8 Bcast:192.168.10.31 Mask:255.255.255.224
      inet6 addr: fe80::baac:6fff:fe2d:b270/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:230 errors:0 dropped:0 overruns:0 frame:0
      TX packets:32536 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:29653 (28.9 KiB) TX bytes:6680136 (6.3 MiB)
      Interrupt:21 Memory:fe6e0000-fe700000

```

Figure 5.6: Attacker's computer network configuration

Looking at the DHCP server, the attacker's computer appeared among the client computers issued with IP address 192.168.10.8 as can be seen in Figure 5.7.

Client IP Address	Name	Lease	Actions
192.168.10.6	J208-D4-PC.victory....	11/	Address Leases More Actions
192.168.10.7	J208-B6-PC.victory....	11/	
192.168.10.8	Rethabile.victory.ac...	11/	
192.168.10.9	J208-D5-PC.victory....	11/	

Figure 5.7: Leased client IP addresses after attacker's computer connected to the network

The attacker's computer ran Kali Linux (a Debian-based operating system with a variety of hacking tools). The Yersinia tool was used to launch the DHCP Starvation Attack to target the legitimate DHCP Server by sending DISCOVER packets as shown in Figure 5.8. The purpose of sending these packets was to flood the target server with many requests to exhaust all IP addresses available and render the server non-responsive to clients joining the network or renewing their lease period.

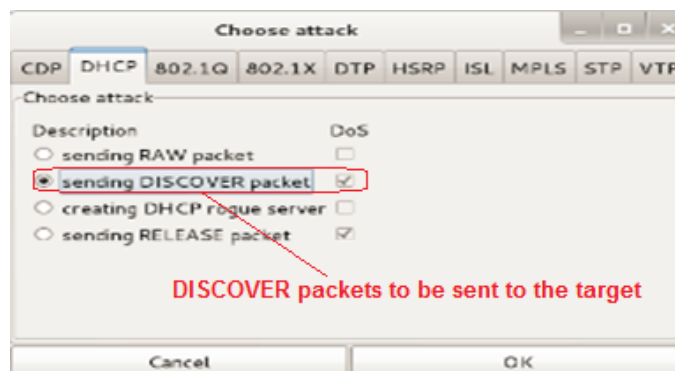


Figure 5.8: Launching DHCP attack

Figure 5.9 shows the number of DISCOVER packets that had been sent out to the target server. These packets flooded the server and used all the available IP addresses from the address pool. Based on the results shown in Figure 5.9, 828026 DISCOVER packets were sent from the attacker’s computer using the DHCP protocol to flood the target computer. These packets were more than the addresses available on the address pool after connecting only four computers.

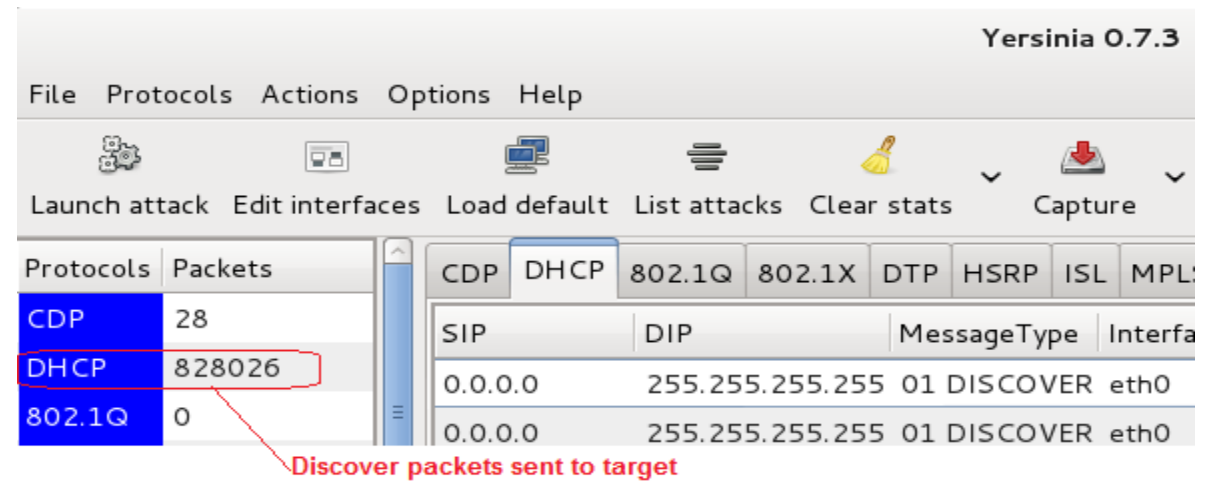


Figure 5.9: DHCP DISCOVER packet on Yersinia

The results from the Wireshark<sup>6</sup> network analyser show the DISCOVER packets were sent from an unknown source with source IP address set to 0.0.0.0, as shown in Figure 5.10. The packets from unknown sources were broadcasted as the destination IP address is 255.255.255.255. This means the attacker does not know the IP address of the DHCP server, hence sent the packets to all the devices on the network, but only the DHCP server would reply to the DISCOVER packets because it uses the DHCP protocol.

<sup>6</sup> Wireshark is a free software network protocol analyser that allows the IT professionals to administer the network communications in order to determine performance problems, find security breaches and analyse the behaviour of the applications (Chappell, 2012).



No.	Time	Source	Destination	Protocol	Length	Info
302	130.268809	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
303	130.268809	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
304	130.268810	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
305	130.268811	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
306	130.268811	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
307	130.268812	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
308	130.268812	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
309	130.268814	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
310	130.268814	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
311	130.269178	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
312	130.269179	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
313	130.269180	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
314	130.269180	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
315	130.269181	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
316	130.269181	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
317	130.269182	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
318	130.269183	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
319	130.269529	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
320	130.269530	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
321	130.269530	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
322	130.269531	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869
323	130.269531	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0x643c9869

Figure 5.10: DHCP DISCOVER on Wireshark

After the attack, all the available IP addresses on DHCP server were exhausted. Figure 5.11 shows DHCP statistics after the attack. There are no available IP addresses left to use for lease renewal or assigned to any client joining the network.

Description	Details
Start Time	11/7/2016 11:17:58 AM
Up Time	1 Hours, 39 Minutes, 11 Seconds
Discovers	821502
Offers	31
Delayed Offers	0
Requests	23
Acks	55
Nacks	0
Declines	0
Releases	1
Total Scopes	1
Scopes with delay configured	0
Total Addresses	25
In Use	25 (100%)
Available	0 (0%)

Figure 5.11: DHCP statistics after attack

Any computer that attempted to join the network or renew IP addresses after all the IP addresses have been leased, failed to connect to the network as shown in Figure 5.12. The DHCP server failed to respond to issuing the IP address. This therefore resulted in a Denial of Service Attack that denies legitimate users access to network resources (Zargar et al., 2013).

```
C:\Users\J208-D4>ipconfig /renew

Windows IP Configuration

An error occurred while renewing interface Local Area Connection : unable to con-
tact your DHCP server. Request has timed out.
```

Figure 5.12: Client fails to connect to the network after attack

Since the DHCP server failed to issue a valid IP address, the client used Automatic Private IP Addressing (APIPA) address 169.254.41.242 and subnet mask 255.255.0.0 as shown in Figure 5.13. APIPA is a failover mechanism used with windows-based operating systems to assign IP addresses automatically to clients in cases where the DHCP server was unreachable (Zacker, 2014).

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . : 
Link-local IPv6 Address . . . . . : fe80::40cc:e0e3:968e:29f2%11
Autoconfiguration IPv4 Address. . : 169.254.41.242
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
```

Figure 5.13: Client computers assigned APIPA address

### 5.2.2 Rogue DHCP Server experiment

A Rogue DHCP Server attack happens when a fake DHCP server is introduced on the network by the attacker. The intention is to assign client computers on that network with a fake IP configuration (Duangphasuk et al., 2011). For this experiment, the rogue DHCP server was configured to use IP addresses more or less similar to the legitimate network addresses at quick glance to obfuscate administrator from seeing the fake IP configuration. The DHCP server was configured as shown in Figure 5.14 on Kali Linux.

```
msf auxiliary(dhcp) > set DHCPEND 192.168.100.30
DHCPEND => 192.168.100.30
msf auxiliary(dhcp) > set DHCPSTART 192.168.100.1
DHCPSTART => 192.168.100.1
msf auxiliary(dhcp) > set dnserver 192.168.100.3
dnserver => 192.168.100.3
msf auxiliary(dhcp) > set srver 192.168.100.3
srver => 192.168.100.3
msf auxiliary(dhcp) > set netmask 255.255.255.224
netmask => 255.255.255.224
msf auxiliary(dhcp) > set router 192.168.100.1
router => 192.168.100.1
```

Figure 5.14: Rogue DHCP server IP configuration

The rogue DHCP server was configured with address pool 192.168.100.1 to 192.168.100.30 and with subnet mask 255.255.255.224. At quick glance, these IP addresses look legitimate to an administrator, possibly preventing the administrator from recognising an intruder on the network. After the DHCP server was flooded by DISCOVER packets, the rogue DHCP server was initiated to issue fake IP addresses to any new clients joining the network or renewing their lease period. Once the client renewed the IP address, the rogue DHCP server issued the IP configuration as can be seen on Figure 5.15. This was because the legitimate server had been flooded with fake DISCOVER packets and had exhausted all IP addresses.

```

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : fabian.ac.za
    Description . . . . . : Intel(R) 82567LM-3 Gigabit Network Connection
    Physical Address. . . . . : B8-AC-6F-2E-7A-33
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::40cc:e0e3:968e:29f2%11(Preferred)
    IPv4 Address. . . . . : 192.168.100.6(Preferred)
    Subnet Mask . . . . . : 255.255.255.224
    Lease Obtained. . . . . : Thursday, November 03, 2016 11:25:09 PM
    Lease Expires . . . . . : Thursday, November 03, 2016 11:55:09 PM
    Default Gateway . . . . . : 192.168.100.1
    DHCP Server . . . . . : 192.168.100.3
    DHCPv6 IAID . . . . . : 246983791
    DHCPv6 Client DUID. . . . . : 00-01-00-01-1C-68-24-49-B8-AC-6F-2E-7A-33

    DNS Servers . . . . . : 192.168.100.3
    NetBIOS over Tcpip. . . . . : Enabled

```

Figure 5.15: Client received fake network configuration after renewing its lease period

### 5.2.3 Media Access Control (MAC) Flooding experiment

During this attack—also referred to as the Content Addressable Memory (CAM) Table Overflow attack—the attacker sends multiple Ethernet frames to flood the switch with fake MAC addresses in order to consume memory (Ostapenko et al., 2013). This attack forces the switch to enter fail-open mode when its MAC address table is flooded. As a result, the switch does not save any MAC addresses; hence, it sends the frames to all devices connected on the network just like a hub. The attacker then uses network-sniffing tools to capture sensitive data such as usernames and passwords.

The switch as a Layer 2 device normally uses the MAC addresses for communication purposes within the LAN. When a device wants to send the message to another device on the network, it forwards its frame to the switch. The switch would check in its MAC address table whether it contains the MAC address of the destination device and then forward the frame. However, if there is no MAC address of the destination device, the switch broadcasts the frame to all the devices connected on the network. Only the device with that specific MAC address replies, and the switch saves it in its MAC address table for future reference.

The MAC address table can store a certain number of MAC addresses depending on the model of each switch.

In this experiment, the computer running on Kali Linux was used as the attacker's computer, connected on port 5 (FastEthernet 0/5) of the switch. Before carrying out the attack, the number of MAC addresses learned<sup>7</sup> by the Cisco switch used in the experiment was displayed as shown in Figure 5.16. As it can be seen, this switch in its MAC address table can accommodate 8047 MAC addresses, of which 5 of them are currently in use.

```
Switch#show mac address-table count
Mac Entries for Vlan 1:
-----
Dynamic Address Count   : 5
Static Address Count    : 0
Total Mac Addresses     : 5

Total Mac Address Space Available: 8042
```

Figure 5.16: MAC address table count before attack

The attacker used the Macof<sup>8</sup> toolset to launch the attack by executing the command shown in Figure 5.17 to flood the switch with fake MAC addresses. This command launched the attack on the eth0 interface, which is an Ethernet adapter on the Kali Linux computer (attacker's computer).

```
root@Rethabile: ~
File Edit View Search Terminal Help
root@Rethabile:~# macof -i eth0
```

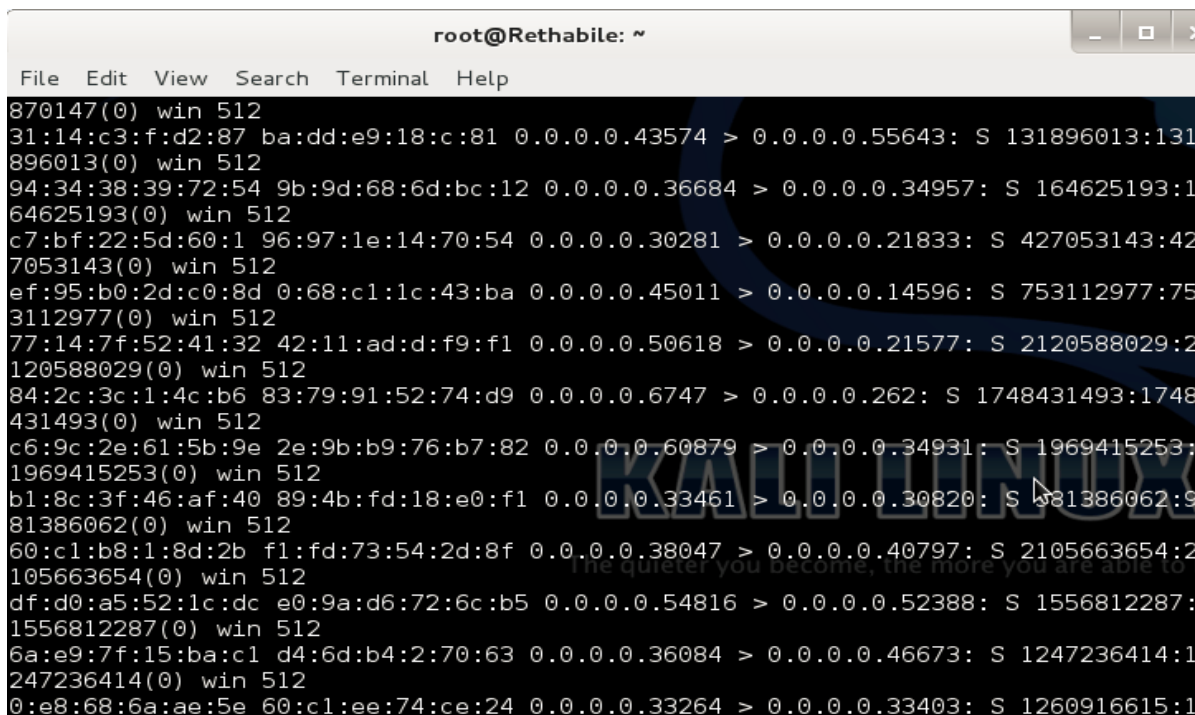
Figure 5.17: Attacker launching MAC flooding

---

<sup>7</sup>All communications between computers in the LAN pass through a switch. A switch checks the destination MAC address in the frame (data) to determine which computer the frame should be forwarded to. Once the switch has the destination MAC address, it uses its own MAC address table (database of all the computers with their MAC addresses that had previously communicated on the network) to find the computer to which the frame should be forward. If the MAC address is not found in the MAC address table, it broadcasts the message to all computers on the network in order to get the destination MAC address and save that MAC address in its table for future reference. All the MAC addresses in the MAC address table have been '**learned**' by the switch when computers communicate on the network.

<sup>8</sup>Macof toolset is an efficient tool that facilities sniffing on a LAN by sending a random number of fake MAC addresses to flood the switch so that it acts like a hub (Dimitrios, 2011).

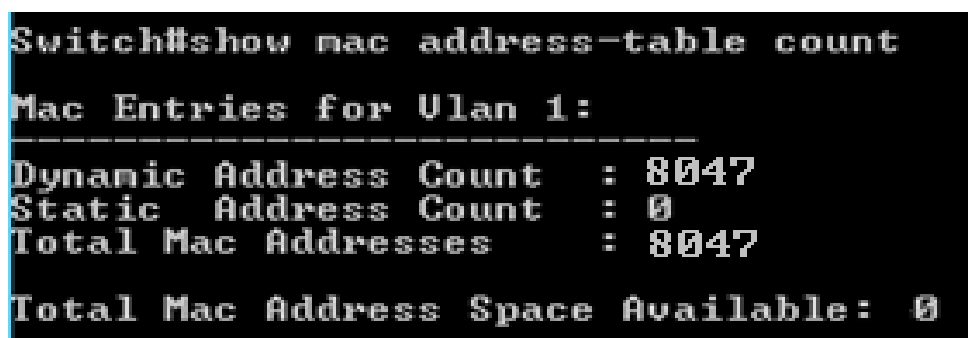
After issuing the command in Figure 5.17, the attack began sending the fake MAC addresses as shown in Figure 5.18.



```
root@Rethabile: ~
File Edit View Search Terminal Help
870147(0) win 512
31:14:c3:f:d2:87 ba:dd:e9:18:c:81 0.0.0.0.43574 > 0.0.0.0.55643: S 131896013:131
896013(0) win 512
94:34:38:39:72:54 9b:9d:68:6d:bc:12 0.0.0.0.36684 > 0.0.0.0.34957: S 164625193:1
64625193(0) win 512
c7:bf:22:5d:60:1 96:97:1e:14:70:54 0.0.0.0.30281 > 0.0.0.0.21833: S 427053143:42
7053143(0) win 512
ef:95:b0:2d:c0:8d 0:68:c1:1c:43:ba 0.0.0.0.45011 > 0.0.0.0.14596: S 753112977:75
3112977(0) win 512
77:14:7f:52:41:32 42:11:ad:d:f9:f1 0.0.0.0.50618 > 0.0.0.0.21577: S 2120588029:2
120588029(0) win 512
84:2c:3c:1:4c:b6 83:79:91:52:74:d9 0.0.0.0.6747 > 0.0.0.0.262: S 1748431493:1748
431493(0) win 512
c6:9c:2e:61:5b:9e 2e:9b:b9:76:b7:82 0.0.0.0.60879 > 0.0.0.0.34931: S 1969415253:
1969415253(0) win 512
b1:8c:3f:46:af:40 89:4b:fd:18:e0:f1 0.0.0.0.33461 > 0.0.0.0.30820: S 81386062:9
81386062(0) win 512
60:c1:b8:1:8d:2b f1:fd:73:54:2d:8f 0.0.0.0.38047 > 0.0.0.0.40797: S 2105663654:2
105663654(0) win 512
df:d0:a5:52:1c:dc e0:9a:d6:72:6c:b5 0.0.0.0.54816 > 0.0.0.0.52388: S 1556812287:
1556812287(0) win 512
6a:e9:7f:15:ba:c1 d4:6d:b4:2:70:63 0.0.0.0.36084 > 0.0.0.0.46673: S 1247236414:1
247236414(0) win 512
0:e8:68:6a:ae:5e 60:c1:ee:74:ce:24 0.0.0.0.33264 > 0.0.0.0.33403: S 1260916615:1
```

Figure 5.18: Fake MAC addresses being sent to the switch

Figure 5.19 shows the MAC address table after the attack. Based on the results, all the MAC address spaces were filled up with fake random MAC addresses.



```
Switch#show mac address-table count
Mac Entries for Ulan 1:
-----
Dynamic Address Count      : 8047
Static Address Count       : 0
Total Mac Addresses        : 8047
Total Mac Address Space Available: 0
```

Figure 5.19: MAC address table count after attack

Figure 5.20 shows the fake MAC addresses in the MAC address table. The switch could not save any new MAC addresses; hence, it started broadcasting MAC addresses to all connected ports. All these fake random MAC addresses originated from FastEthernet 0/5.



```
Switch#show mac address-table dynamic
```

Mac Address Table

---

Vlan	Mac Address	Type	Ports
1	0000.b42c.1840	DYNAMIC	Fa0/5
1	0005.b114.79b7	DYNAMIC	Fa0/5
1	0010.c00a.6df9	DYNAMIC	Fa0/5
1	0012.da78.4a47	DYNAMIC	Fa0/5
1	0012.f105.8f09	DYNAMIC	Fa0/5
1	0014.557a.aa00	DYNAMIC	Fa0/5
1	0017.3641.4365	DYNAMIC	Fa0/5
1	0018.6a63.ec98	DYNAMIC	Fa0/5
1	001f.5934.368c	DYNAMIC	Fa0/5
1	0027.3559.109b	DYNAMIC	Fa0/5
1	0027.7406.fb21	DYNAMIC	Fa0/5
1	0027.dd77.9d60	DYNAMIC	Fa0/5
1	0029.9464.ffc6	DYNAMIC	Fa0/5
1	002d.926f.29e8	DYNAMIC	Fa0/5
1	0030.c07c.ffa4	DYNAMIC	Fa0/5
1	0033.d034.a38d	DYNAMIC	Fa0/5
1	0036.7366.dd5c	DYNAMIC	Fa0/5
1	0036.e30a.b74d	DYNAMIC	Fa0/5
1	003d.281c.9158	DYNAMIC	Fa0/5
1	003f.1b25.7813	DYNAMIC	Fa0/5
1	0044.3002.b910	DYNAMIC	Fa0/5
1	004f.fb39.0a0e	DYNAMIC	Fa0/5
1	0055.427a.9a3c	DYNAMIC	Fa0/5
1	0059.6279.0247	DYNAMIC	Fa0/5
1	0061.6e27.af7a	DYNAMIC	Fa0/5
1	0068.d41b.6be9	DYNAMIC	Fa0/5
1	0069.c918.1a3e	DYNAMIC	Fa0/5
1	006d.df29.25d7	DYNAMIC	Fa0/5
1	0079.3230.920e	DYNAMIC	Fa0/5
1	007b.421f.89a6	DYNAMIC	Fa0/5
1	007f.9d25.2ba5	DYNAMIC	Fa0/5
1	007f.dc6b.cf5c	DYNAMIC	Fa0/5

Figure 5.20: Fake MAC addresses flooded MAC address table

The Colasoft Capsa 9.1 Enterprise Demo was used as network analyser to analyse the network traffic for any attacks. Figure 5.21 shows the results of MAC flooding. Based on the results, there were 9556 MAC addresses available on the network. The total number of MAC addresses was too high considering this network segment could only accommodate 30 computers. This abnormality meant there was an attack on the network.

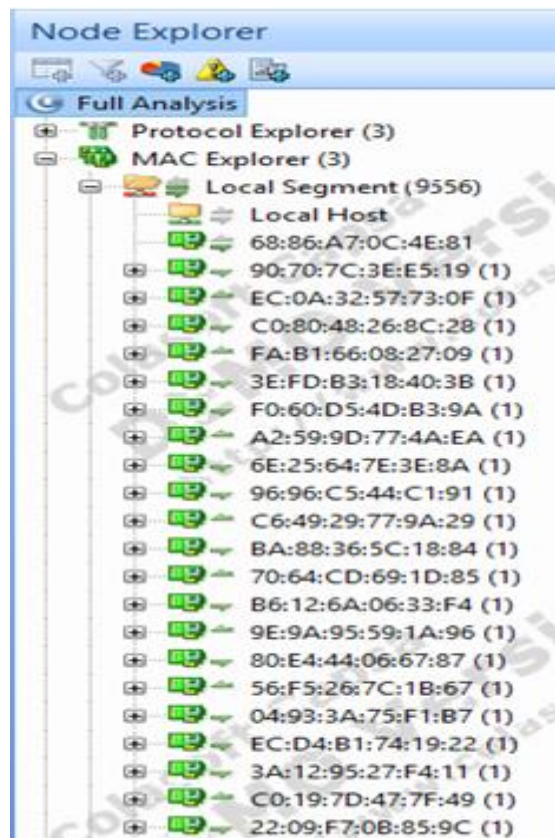


Figure 5.21: Analysis of MAC Explorer for MAC flooding

To analyse the results further, Figure 5.22 shows the MAC Conversation tab. In this tab, it can also be seen that each node communicating was sending only one packet of 64 bytes. This therefore confirms the presence of the attack because the communicating nodes cannot all send the same number of packets of the same size.


Summary Diagnosis Protocol MAC Endpoint MAC Conversation X Matrix Packet Log Report							
Filter: All Exactly Match							
Node 1 ->	<- Node 2	Duration	Bytes	Bytes ->	<- Bytes	Packets	
42:61:B9:3A:6E:4A	8C:B5:92:76:42:19	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
5C:54:F3:4E:E4:26	41:99:F2:68:6A:84	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
62:36:C4:47:7D:9B	82:3F:DB:23:D3:5A	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
A6:07:5A:0C:86:D7	90:B2:8A:7F:D4:AA	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
EC:00:85:14:67:EC	3F:16:6E:46:3B:BB	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
B2:85:3E:16:B9:62	21:CD:9D:4F:24:9E	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
C0:B5:5C:07:94:A2	7F:F1:E7:73:66:D1	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
9C:20:FB:42:C0:4F	C8:80:70:18:C1:09	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
9E:14:CA:69:35:77	08:B6:09:45:90:54	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
FC:8E:77:4A:DB:6C	9F:EE:04:67:A3:03	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
C2:3F:E5:1E:40:68	E3:C6:14:30:9E:A8	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
E0:6F:76:55:A8:87	EB:A3:3E:02:64:5C	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
E2:A6:69:4B:8E:8C	6C:C8:3A:68:B3:D7	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
A8:44:58:29:66:71	79:6F:0C:6B:15:69	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
90:4A:E4:53:4D:55	D3:44:41:17:05:23	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	
CC:AA:0F:2D:8C:2E	D5:F6:1B:73:61:32	00:00:00.000000	64.00 B	64.00 B	0.00 B	1	

Figure 5.22: Analysis of MAC Conversation for MAC flooding

### 5.2.4 Address Resolution Protocol (ARP) Poisoning attack experiment

This is an attack where the victim's ARP cache is 'poisoned' with the attacker's MAC address in order to steal information sent by the victim on the network (Nam et al., 2010). After the ARP cache is poisoned, the attacker can sniff the traffic sent from the victim's computer and steal any sensitive information. The attacker can also inject data to send to the victim that will result in an attack known as Man-In-The-Middle.

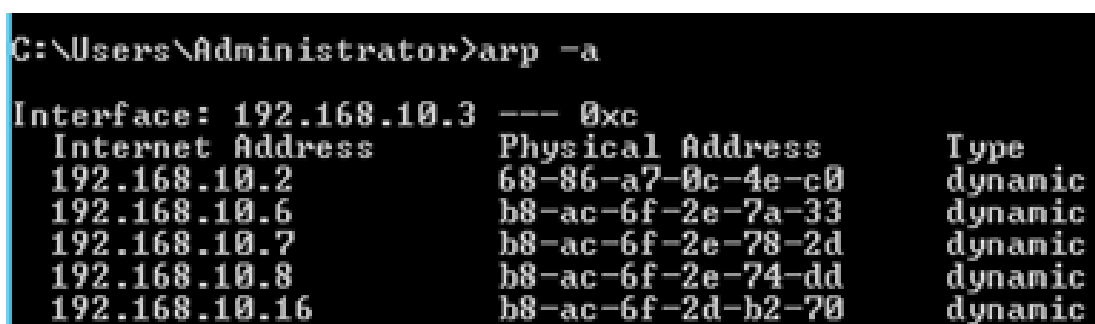
In this experiment, the setup was the same as shown in Figure 5.2. During the ARP Poisoning attack, the attacker's computer had obtained a different IP address from the DHCP server as shown in Figure 5.23.



```
root@Rethabile:~# ifconfig
eth0      Link encap:Ethernet  HWaddr b8:ac:6f:2d:b2:70
          inet addr:192.168.10.16  Bcast:192.168.10.31  Mask:255.255.255.224
          inet6 addr: fe80::baac:6fff:fe2d:b270/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:40  errors:0  dropped:0  overruns:0  frame:0
          TX packets:37  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3797 (3.7 KiB)  TX bytes:6100 (5.9 KiB)
          Interrupt:21 Memory:fe6e0000-fe700000
```

Figure 5.23: The new attacker's IP address obtained from DHCP server

Before conducting the experiment, the ARP cache for the Server and the Cisco Catalyst 2096 switch were checked as shown in Figure 5.24 and Figure 5.25.



```
C:\Users\Administrator>arp -a

Interface: 192.168.10.3 --- 0xc
Internet Address      Physical Address      Type
192.168.10.2          68-86-a7-0c-4e-c0     dynamic
192.168.10.6          b8-ac-6f-2e-7a-33     dynamic
192.168.10.7          b8-ac-6f-2e-78-2d     dynamic
192.168.10.8          b8-ac-6f-2e-74-dd     dynamic
192.168.10.16         b8-ac-6f-2d-b2-70     dynamic
```

Figure 5.24: Server's ARP cache before attack



Switch#show mac address-table dynamic

Mac Address Table

Vlan	Mac Address	Type	Ports
1	b8ac.6f2d.b270	DYNAMIC	Fa0/5
1	b8ac.6f2e.74dd	DYNAMIC	Fa0/3
1	b8ac.6f2e.782d	DYNAMIC	Fa0/4
1	b8ac.6f2e.7a33	DYNAMIC	Fa0/2
1	b8ac.6f2e.7b99	DYNAMIC	Fa0/1

Total Mac Addresses for this criterion: 5

Switch#show arp

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.10.2	-	6886.a70c.4ec0	ARPA	Vlan1
Internet	192.168.10.3	0	b8ac.6f2e.7b99	ARPA	Vlan1
Internet	192.168.10.6	0	b8ac.6f2e.7a33	ARPA	Vlan1
Internet	192.168.10.7	0	b8ac.6f2e.782d	ARPA	Vlan1
Internet	192.168.10.16	10	b8ac.6f2d.b270	ARPA	Vlan1

Attacker's computer

Server's computer

Attacker's computer

Figure 5.25: Cisco Catalyst 2096 switch MAC address table and ARP cache before attack

On the attacker's computer, a network sniffer tool called Ettercap was set up to launch the ARP Poisoning attack. The Ettercap was configured to promiscuous mode in order to listen to the traffic sent to its interface (eth0) by the victims as shown in Figure 5.26.

Listening on:  
eth0 -> B8:AC:6F:2D:B2:70  
192.168.10.16/255.255.255.224  
fe80::baac:6fff:fe2d:b270/64

Figure 5.26: Ettercap listening on eth0 interface

The attacker scanned the hosts on the network and five hosts were discovered as shown in Figure 5.27. The victim's computer (server) was added as the targeted host. Before starting the attack, ARP Poisoning was selected from the list of attacks and was configured to sniff remote connections.

Start Targets Hosts View Mitm Filters Logging Plugins ?

Host List Connections

IP Address	MAC Address	Description
192.168.10.2	68:86:A7:0C:4E:C0	
192.168.10.3	B8:AC:6F:2E:7B:99	
192.168.10.6	B8:AC:6F:2E:7A:33	
192.168.10.7	B8:AC:6F:2E:78:2D	
192.168.10.8	B8:AC:6F:2E:74:DD	

Figure 5.27: List of discovered hosts by Ettercap tool

Once the ARP attack was initiated, the **chk-poison 1.1** plug-in was started to check the status of the poisoning. Figure 5.28 shows the status of the poisoning. The poisoning was successful, meaning the attacker was able to sniff the traffic on its interface.

```
Activating chk_poison plugin...
chk_poison: Checking poisoning status...
chk_poison: Poisoning process successful!
```

Figure 5.28: ARP poisoning status

The activity on the server was captured by the attacker when the remote connection using Telnet was established from the server to the Cisco Catalyst 2960 switch. Figure 5.29 shows the connection made to the switch on IP address 192.168.10.2 using port 23 that is the port used by the Telnet protocol.

Start Targets Hosts View Mitm Filters Logging Plugins ?								
Host List		Connections						
Host	Port	-	Host	Port	Proto	State	Bytes	
192.168.10.16	33628	-	192.168.10.3	53	U	idle	41	
192.168.10.16	56631	-	192.168.10.3	53	U	idle	27	
192.168.10.16	48410	-	192.168.10.3	53	U	idle	27	
192.168.10.3	65121	-	192.168.10.2	23	T	idle	50	
192.168.10.16	41032	-	192.168.10.3	53	U	idle	86	
192.168.10.16	53618	-	192.168.10.3	53	U	idle	86	
192.168.10.16	52082	-	192.168.10.3	53	U	idle	41	

Figure 5.29: Captured remote connection from the server to the switch

Looking at the connection details as shown in Figure 5.30, the destination MAC address is spoofed, as it does not correspond with the destination IP address of 192.168.10.2 of the switch as previously shown in Figure 5.25. The spoofed MAC address belonged to the attacker computer, meaning that any traffic sent from the server was being sent to the attacker's computer that captured sensitive data (username and password) as shown in Figure 5.31. The username captured was "admin" and the password was "Admin@J208". The joined view was used for better viewing. The attacker could read the captured authentication data as it was in plaintext. The Telnet protocol had been used to establish a remote connection. This protocol however lacks encryption that therefore means any connection established using this non-cryptographic network protocol could easily be intercepted during data transmission.

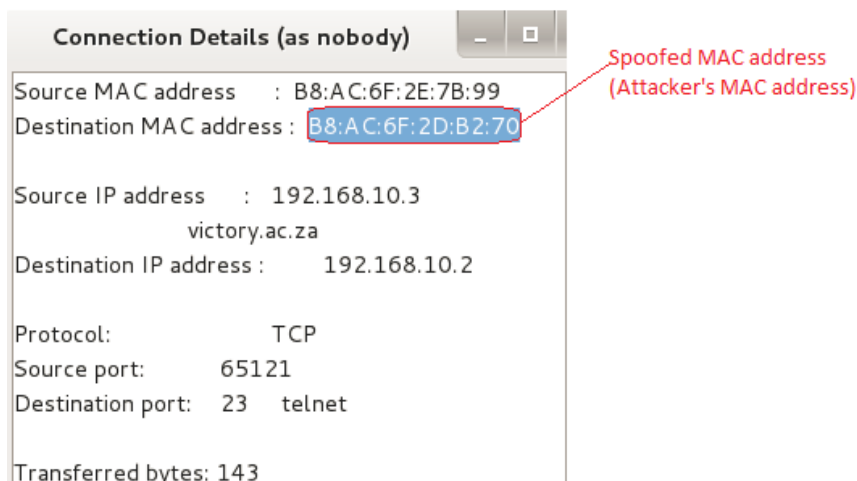


Figure 5.30: Spoofed MAC address with attacker's MAC address

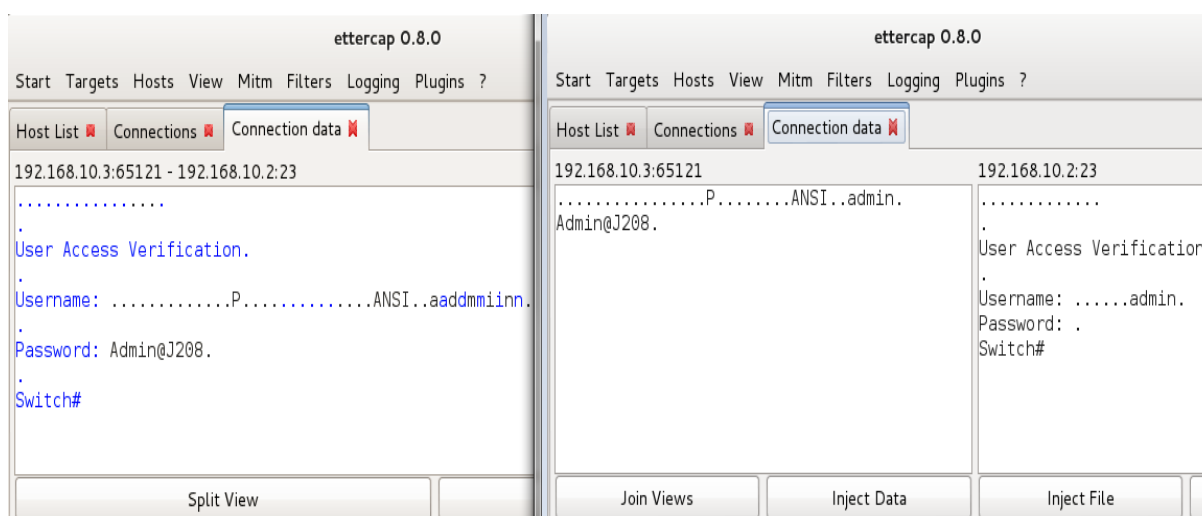


Figure 5.31: Captured credentials over remote connection to switch

Figure 5.32 shows the switch's ARP cache after the attack. The server's MAC address has been replaced by the attacker's MAC address. As a result, any communication to and from the server would be directed to the attacker's computer to listen in on the conversation between communicating devices, and stealing information.

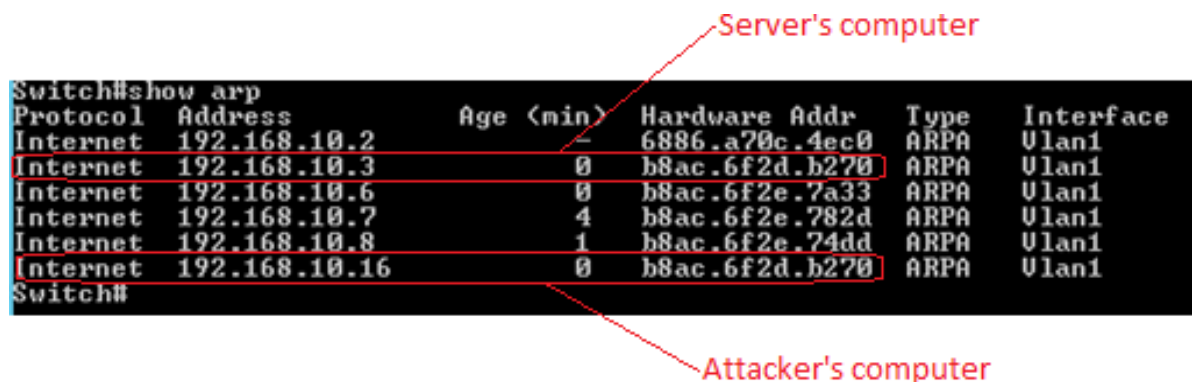


Figure 5.32: Cisco Catalysts switch ARP cache after attack

The ARP attack tab shows the host initiating the attack to verify the presence of security threats on the network. Based on the results, the attacker's MAC address was mapped with two IP addresses, 192.168.10.16 and 192.168.10.3. The 192.168.10.3 IP address belonged to the server (the victim). This confirmed the poisoned ARP cache of the switch as shown in Figure 5.32. Figure 5.33 shows the detection of the ARP Poisoning attack on Colasoft Capsa 9.1 Enterprise.

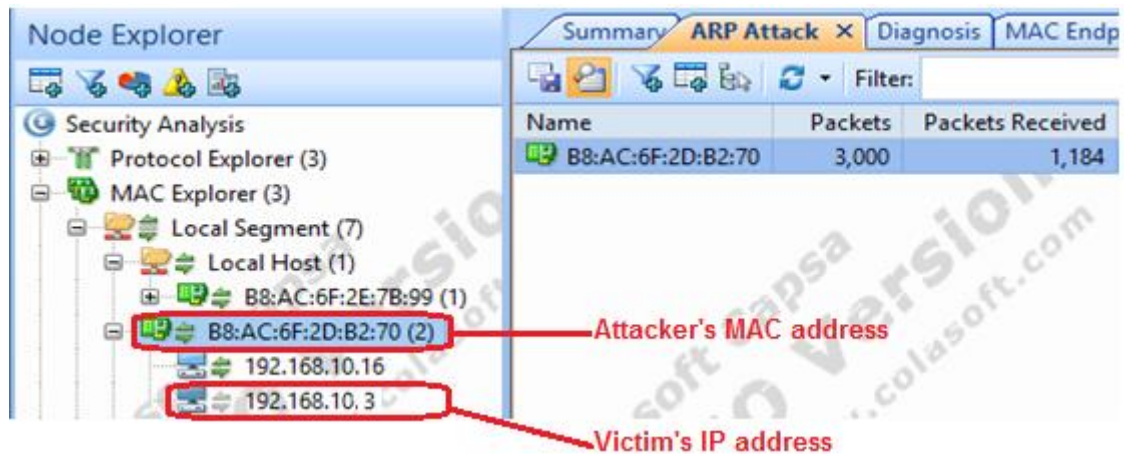


Figure 5.33: ARP Poisoning Attack results on Colasoft Capsa 9.1 Enterprise

- Finding A1:** A lack of network security enforcement was identified during the experiment that correlated with literature stating that this lack exists in general
- Finding A2:** Unmanaged switches and open switch ports posed a security threat as the malicious user or attacker was able to connect his device to the network and gained unauthorised access
- Finding A3:** Due to unauthorised access, the attacker caused excessive traffic targeted at the server that caused downtime and subsequently denied legitimate clients network access
- Finding A4:** Inadequate monitoring of networks to detect and prevent suspicious traffic
- Finding A5:** There is a lack of proper configuration on network devices for integrated security mechanisms
- Finding A6:** A rogue device could easily be connected to the network, issuing false network configurations
- Finding A7:** A malicious user or attacker could redirect the outgoing traffic from the victim's computer and intercept it

**Finding A8:** A malicious user or attacker could easily sniff network packets while the network switch was under the attack and acted as a hub

**Finding A9:** An unlimited number of devices could establish a connection from a single network switch port

**Finding A10:** The use of insecure network protocols lacking encryption allowed the authentication of data such as username and plaintext passwords to be captured in transit across the network

**Finding A11:** The use of default settings on network devices in general poses a security threat

### **5.2.5 DHCP Starvation, MAC Flooding attack, Rogue DHCP Server attack and ARP Poisoning attack mitigation**

In order to mitigate the DHCP Starvation and MAC Flooding attack, the port security was configured on connected switch ports as a security measure for controlling unauthorised access. This assisted in improving network security, addressing network security threats and attacks by ensuring that a certain number of devices can connect to the network switch without violating the network security policy. Should any violations be detected, the switch would take action depending on the configured parameters.

To mitigate the Rogue DHCP Server attack, DHCP snooping was configured on the switch as a security measure. This allowed the DHCP messages from untrustworthy hosts or sources to be authenticated before they could be passed on to the trusted DHCP server, hence, allowed filtering of invalid messages. In so doing, this feature assisted in improving network security by preventing the Rogue DHCP Server Attack.

To mitigate the ARP Poisoning attack, Dynamic Address Resolution Protocol Inspection (DAI) was configured as a security measure. This enabled the switch to confirm the validity of ARP requests and responses before updating its ARP cache. This further ensured that any invalid ARP packets were dropped if they do not match the binding table.

The switch was configured with parameters to change the name of the switch, and to secure access to the switch through the console port and when managing the switch remotely. Figure 5.34 shows the switch's initial configuration. These commands changed the default name of the switch to Victory-SW and secured the console port by assigning password

**Admin@J208** to log in to the switch in user EXEC mode. This is the mode with limited capabilities because it allows the user to view the basic operations of devices.

The commands were also issued to enable the need for a password (**Admin@T208**) to enter privileged EXEC mode and to encrypt all the passwords. Encrypting the passwords on network devices ensured that the passwords were not stored in a plaintext format that the intruder could easily steal. The banner message was also configured on the switch to warn intruders that unauthorised access was prohibited. This is crucial in cases where legal action is taken against the intruder, confirming that a warning was issued, but ignored.

```
Switch(config)#hostname Victory-SW
Victory-SW(config)#line console 0
Victory-SW(config-line)#password Admin@J208
Victory-SW(config-line)#login
Victory-SW(config-line)#exit
Victory-SW(config)#enable password cisco
Victory-SW(config)#enable secret Admin@T208
Victory-SW(config)#service password-encryption
Victory-SW(config)#banner motd #Unauthorised Access Prohibited!!#
```

Figure 5.34: Initial configuration of the switch

Figure 5.35 shows the encrypted password for accessing the switch through the console port. When analysing the password, the attacker could not make sense of the cryptographic password.

```
line con 0
password 7 03255F060F0101661C5941
login
```

Figure 5.35: Encrypted console password

To ensure secure remote management of the switch, the Secure Shell (SSH) protocol was configured as shown in Figure 5.36. This was to ensure that the communication to the switch was not in plaintext, hence secured. The account policy was implemented to allow the user three unsuccessful attempts before timeout.

```

Victory-SW(config)#ip domain-name victory.ac.za
Victory-SW(config)#crypto key generate rsa
The name for the keys will be: Victory-SW.victory.ac.za
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
    a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar  1 01:12:30.113: %SSH-5-ENABLED: SSH 1.99 has been enabled
Victory-SW(config)#username ITServices privilege 15 secret Admin@R007
Victory-SW(config)#line vty 0 15
Victory-SW(config-line)#transport input ssh
Victory-SW(config-line)#login local
Victory-SW(config-line)#exit
Victory-SW(config)#ip ssh version 2
Victory-SW(config)#ip ssh time-out 60
Victory-SW(config)#ip ssh authentication-retries 3
Victory-SW(config)#

```

Figure 5.36: Configuring Secure Shell Protocol on the switch

Figure 5.37 shows the encrypted password for logging remotely to the switch. This ensured that any remote connection established was secured by using a cryptographic network protocol such as SSH instead of Telnet, as the communication is encrypted.

```

!
username ITServices secret 5 $1$PnKB$jql.CTA/gKIIENzI85mr0/
!

```

Figure 5.37: Encrypted password for remote connection to the switch

The use of device-certain default settings was avoided as it could make the network vulnerable to attacks by exploiting the default settings on the switch. As a result, the new Virtual Local Area Network (VLAN) on the switch was created and configured as shown in Figure 5.38 to avoid using the default switch virtual interface (SVI) VLAN 1 on the Cisco switch.

```

Victory-SW(config)#vlan 10
Victory-SW(config-vlan)#name IT
Victory-SW(config-vlan)#exit
Victory-SW(config)#int vlan 10
Victory-SW(config-if)#ip address 192.168.10.2 255.255.255.224
Victory-SW(config-if)#no shutdown

```

Figure 5.38: Creating VLAN 10 and assigning IP address



VLAN is a mechanism that enables the network administrator to manage the switch remotely over the network when using IPv4 (Cisco Networking Academy, 2013). The VLAN 10 was configured with static IP address 192.168.10.2 and subnet mask 255.255.255.224. This IP address configured was one of the excluded IP addresses that could not be distributed by the DHCP server as mentioned in section 5.2.1.

Once the VLAN was created and assigned the IP address, port security was configured to currently used ports as shown in Figure 5.39. These configuration commands allowed FastEthernet 0/1 to FastEthernet 0/5 access to VLAN 10 created and turned port security on. These configurations further allowed each switch port to learn up to 3 MAC addresses to communicate on that particular port and to shut down the switch port access to VLAN 10 should any violation occur. This therefore means that if the MAC addresses on a particular port exceeded three MAC addresses, the switch port would be disabled. This allowed the use of three different computers to connect on a single port. The MAC addresses would automatically be learned and stored in the MAC address table. Based on these configurations, the learned MAC addresses would be removed from the MAC address table after 15 minutes of inactivity on the switch port.

```
Victory-SW(config)#int range f0/1-5
Victory-SW(config-if-range)#switchport mode access
Victory-SW(config-if-range)#switchport access vlan 10
Victory-SW(config-if-range)#switchport port-security
Victory-SW(config-if-range)#switchport port-security max 3
Victory-SW(config-if-range)#switchport port-security violation shutdown
Victory-SW(config-if-range)#switchport port-security mac-address sticky
Victory-SW(config-if-range)#switchport port-security aging time 15
Victory-SW(config-if-range)#switchport port-security aging type inactivity
Victory-SW(config-if-range)#
```

**Figure 5.39: Port security configuration on FastEthernet 0/1 to FastEthernet 0/5**

Any unused switch ports were disabled to prevent unauthorised access to network resources. Figure 5.40 shows the configuration when shutting down unused switch ports.

As can be seen, interfaces FastEthernet 0/6 to FastEthernet 0/24 and interfaces GigabitEthernet 0/1 to GigabitEthernet 0/2 were administratively down. FastEthernet 0/5, used by the attacker, was not shut down for demonstration purposes of the experiment.



```

Victory-SW(config)#int range f0/6-24
Victory-SW(config-if-range)#shutdown
Victory-SW(config-if-range)#
*Mar 1 01:34:45.362: %LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
*Mar 1 01:34:45.378: %LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
*Mar 1 01:34:45.404: %LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
*Mar 1 01:34:45.420: %LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
*Mar 1 01:34:45.446: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
*Mar 1 01:34:45.462: %LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down
*Mar 1 01:34:45.479: %LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down
*Mar 1 01:34:45.504: %LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
*Mar 1 01:34:45.521: %LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
*Mar 1 01:34:45.555: %LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
*Mar 1 01:34:45.571: %LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
*Mar 1 01:34:45.597: %LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
*Mar 1 01:34:45.613: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
*Mar 1 01:34:45.638: %LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
*Mar 1 01:34:45.655: %LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
*Mar 1 01:34:45.680: %LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
*Mar 1 01:34:45.697: %LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
*Mar 1 01:34:45.722: %LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
*Mar 1 01:34:45.739: %LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
Victory-SW(config)#int range g0/1-2
Victory-SW(config-if-range)#shutdown
Victory-SW(config-if-range)#
*Mar 1 01:35:52.521: %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
*Mar 1 01:35:52.546: %LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
Victory-SW(config-if-range)#

```

Figure 5.40: Configuration on shutting down unused switch ports

Figure 5.41 shows the configuration of DHCP snooping and ARP inspection on the global mode of the switch. These configurations enabled the DHCP snooping and ARP inspection on VLAN 10 to allow up to 1024 entries in the log file in 15 seconds intervals.

```

Victory-SW(config)#ip dhcp snooping vlan 10
Victory-SW(config)#no ip dhcp snooping information option
Victory-SW(config)#ip dhcp snooping
Victory-SW(config)#ip arp inspection vlan 10
Victory-SW(config)#ip arp inspection log-buffer entries 1024
Victory-SW(config)#ip arp inspection log-buffer logs 1024 interval 15
Victory-SW(config)#

```

Figure 5.41: Configuration for DHCP snooping and ARP inspection

Figure 5.42 shows the configuration of DHCP snooping and ARP inspection on the trusted interface. Interface FastEthernet 0/1 was configured to be the trusted port to issue IP addresses from the legitimate DHCP server to client computers. This means only the DHCP server connected on this port could issue IP addresses to client computers. Any other DHCP server that tried to issue IP addresses from a different switch port would be ignored.

```

Victory-SW(config)#int f0/1
Victory-SW(config-if)#ip dhcp snooping trust
Victory-SW(config-if)#ip arp inspection trust
Victory-SW(config-if)#

```

Figure 5.42: DHCP snooping and ARP inspection on trusted interface

Figure 5.43 shows the configuration of DHCP snooping and ARP inspection on untrustworthy interfaces. The untrustworthy interfaces were from FastEthernet 0/2 to FastEthernet 0/5. These commands ensured that any IP addresses or ARP packets coming from these interfaces could not be trusted; hence, their messages had to be verified to ensure validity.

```
Victory-SW(config)#int range f0/2-5
Victory-SW(config-if-range)#no ip dhcp snooping trust
Victory-SW(config-if-range)#ip dhcp snooping limit rate 12
Victory-SW(config-if-range)#no ip arp inspection trust
Victory-SW(config-if-range)#ip arp inspection limit rate 15
Victory-SW(config-if-range)#exit
Victory-SW(config)#
```

**Figure 5.43: DHCP snooping and ARP inspection on untrustworthy interfaces**

The DHCP Starvation Attack was launched to attack the DHCP server on network. The same procedure was followed as mentioned in section 5.2.1. As the FastEthernet 0/5 started the attack, DHCP snooping detected the security violation; as many as 10 DHCP packets were sent to the target within a short period of time from FastEthernet 0/5. As a result, the FastEthernet 0/5 entered error disabled mode and shutdown as shown in Figure 5.44. This meant the attacker was unable to connect to the network unless the network administrator could enable the FastEthernet 0/5 on the switch.

```
Victory-SW#
*Mar 1 01:56:31.359: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/5, putting Fa0/5 in err-disable state
*Mar 1 01:56:31.376: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address d41a.bb38.a9a3 on port FastEthernet0/5.
*Mar 1 01:56:31.392: %DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE WARNING: DHCP Snooping received 10 DHCP packets on interface Fa0/5
*Mar 1 01:56:31.392: %DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The interface Fa0/5 is receiving more than the threshold set
*Mar 1 01:56:32.374: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
*Mar 1 01:56:33.380: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to down
```

**Figure 5.44: Error message when switch experienced DHCP Starvation attack**

The rogue DHCP server was introduced on the network but the client was able to receive an IP address from the trusted DHCP server.

Figure 5.45 shows the results of a client computer after the Rogue DHCP Server attack.

```

Windows IP Configuration

Host Name . . . . . : J208-D4-PC
Primary Dns Suffix . . . . . : victory.ac.za
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : victory.ac.za

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : victory.ac.za
    Description . . . . . : Intel(R) 82567LM-3 Gigabit Network Connection
    Physical Address. . . . . : B8-AC-6F-2E-7A-33
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::40cc:e0e3:968e:29f2%11(Preferred)
    IPv4 Address. . . . . : 192.168.10.6(Preferred)
    Subnet Mask . . . . . : 255.255.255.224
    Lease Obtained. . . . . : Saturday, November 12, 2016 9:04:35 PM
    Lease Expires . . . . . : Saturday, November 12, 2016 10:19:49 PM
    Default Gateway . . . . . : 192.168.10.1
    DHCP Server . . . . . : 192.168.10.3
    DHCPv6 IAID . . . . . : 246983791
    DHCPv6 Client DUID. . . . . : 00-01-00-01-1C-68-24-49-B8-AC-6F-2E-7A-33

    DNS Servers . . . . . : 192.168.10.3
    NetBIOS over Tcpip. . . . . : Enabled

```

Figure 5.45: Client computer after DHCP Starvation mitigation

Figure 5.46 and Figure 5.47 show error messages when the security violation occurred for the MAC Flooding and ARP Poisoning attacks.

```

Victory-SW#
*Mar 1 02:09:03.817: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/5, putting Fa0/5 in err-disable state
*Mar 1 02:09:03.825: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 926c.707f.f664 on port FastEthernet0/5.
*Mar 1 02:09:04.824: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
*Mar 1 02:09:05.822: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to down
Victory-SW#

```

Figure 5.46: Error message when switch experienced MAC Flooding attack

```

Victory-SW#
*Mar 1 02:26:55.621: %SW_DAI-4-PACKET_RATE_EXCEEDED: 32 packets received in 436 milliseconds on Fa0/5.
*Mar 1 02:26:55.621: %PM-4-ERR_DISABLE: arp-inspection error detected on Fa0/5, putting Fa0/5 in err-disable state
*Mar 1 02:26:56.628: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
*Mar 1 02:26:57.634: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to down
Victory-SW#

```

Figure 5.47: Error message when switch experienced ARP Poisoning Attack

To repeat each attack after mitigation techniques were implemented, the FastEthernet 0/5 was re-enabled after the switch entered error disabled mode. The **shutdown** and **no shutdown** commands were executed as shown in Figure 5.48.

```

Victory-SW(config)#int f0/5
Victory-SW(config-if)#shutdown
Victory-SW(config-if)#no shutdown
*Mar 1 02:02:43.494: %LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
Victory-SW(config-if)#
*Mar 1 02:02:47.965: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to up
*Mar 1 02:02:48.972: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
Victory-SW(config-if)#exit

```

Figure 5.48: Changing the state of interface FastEthernet 0/5 from shutdown mode

Figure 5.49 shows the security violation where the attacker's computer was connected. Based on the results, the FastEthernet 0/5 port was configured to learn three MAC addresses, of which the port was shut down when the number on the same port exceeded three. Figure 5.49 shows a security violation that occurred; every time the security violation occurred, the switch was disabled. Figure 5.50 shows the FastEthernet 0/5 in its error-disabled mode by the indication of the orange colour on the switch port.

```
Victory-SW#show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	3	1	0	Shutdown
Fa0/2	3	1	0	Shutdown
Fa0/3	3	1	0	Shutdown
Fa0/4	3	1	0	Shutdown
Fa0/5	3	3	1	Shutdown

Attacker's computer

Figure 5.49: Security violation on interface FastEthernet 0/5

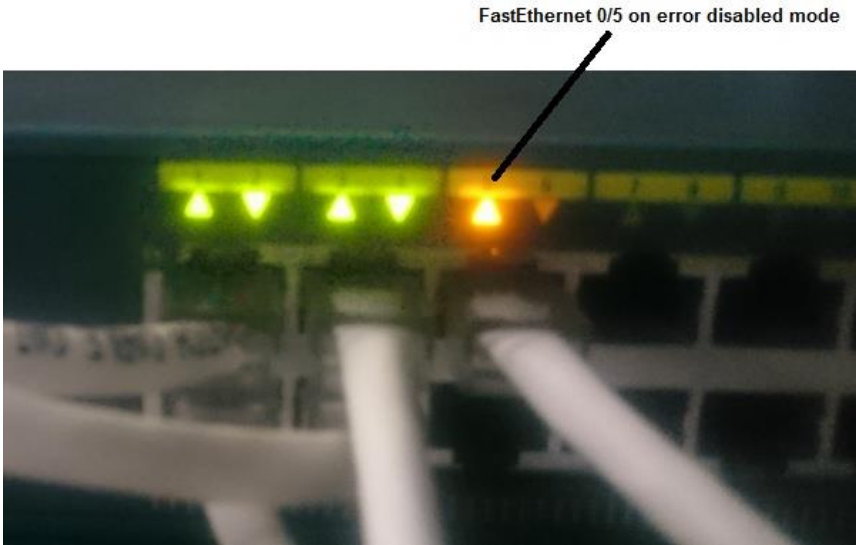


Figure 5.50: FastEthernet 0/5 on error disabled mode

- Finding A12:** Enforcing network security on the network enhanced the security
- Finding A13:** Using managed switches and shutting down unused switch ports mitigated network security threats and attacks
- Finding A14:** Unauthorised access was controlled on the network; hence, excessive traffic experienced to the server was mitigated. Thus, downtime caused by the attackers was eliminated to allow network access by legitimate clients

- Finding A15:** The use of monitoring tools such as Wireshark network analyser and Colasoft Capsa 9.1 Enterprise detected suspicious traffic
- Finding A16:** Proper configuration on network devices for integrated security mechanisms enhanced network security by detecting and preventing suspicious traffic
- Finding A17:** Rogue devices were denied access to the network to issue false network configurations
- Finding A18:** The number of devices connecting to a single network switch port was controlled that reduced the security risks
- Finding A19:** Cryptographic network protocols were used to improve network security by ensuring that the communication was encrypted
- Finding A20:** The use of default settings on network devices was eliminated that improved network security

## 5.2 Summary

This chapter addressed the security issues on Layer 2—the Data Link layer—in order to improve network security. The experiments were conducted on two Local Area Networks: one being the control network and the other being the experimental network. The experimental network was manipulated to find the implications of network security threats and attacks on network security before and after implementing security measures.

A detailed discussion on how the experiments were carried out, and the results we elaborated on. Internal penetration testing was performed to address attacks on Layer 2; the attacks included DHCP Starvation, Rogue DHCP server, MAC flooding, and ARP poisoning. Security measures were implemented to help mitigate these threats and attacks on the network to improve network security. *Wireshark* and *Colasoft Capsa 9.1 Enterprise* network analysers were used to analyse network traffic for different attacks.

Table 5.1 below shows the summary of findings before and after mitigation.

**Table 5.1: Summary of findings before and after mitigation**

<b>Research Question:</b> <b>SRQ3: How can network security be addressed and improved in order to protect against network security threats and attacks in South Africa?</b>	
<b>FINDINGS BEFORE MITIGATION</b>	<b>FINDINGS AFTER MITIGATION</b>
<b>Finding A1:</b> A lack of network security enforcement was identified during the experiment that correlated with literature stating that this lack exists in general	<b>Finding A12:</b> Enforcing network security on the network enhanced the security
<b>Finding A2:</b> Unmanaged switches and the open switch ports posed a security threat as the malicious user or attacker was able to connect his device to the network and gained unauthorised access	<b>Finding A13:</b> Using managed switches and shutting down unused switch ports mitigated network security threats and attacks
<b>Finding A3:</b> Due to unauthorised access, the attacker caused excessive traffic targeted at the server that caused downtime and subsequently denied legitimate clients network access	<b>Finding A13:</b> Using managed switches and shutting down unused switch ports mitigated network security threats and attacks  <b>Finding A14:</b> Unauthorised access was controlled on the network; hence, excessive traffic experienced to the server was mitigated. Thus, downtime caused by the attackers was eliminated to allow network access by legitimate clients
<b>Finding A4:</b> Inadequate monitoring of network to detect and prevent suspicious traffic	<b>Finding A15:</b> The use of monitoring tools such as Wireshark network analyser and Colasoft Capsa 9.1 Enterprise detected suspicious traffic.  <b>Finding A16:</b> Proper configuration on network devices for integrated security mechanisms enhanced network security by detecting and preventing suspicious traffic
<b>Finding A5:</b> There is a lack of proper configuration on network devices for integrated security mechanisms	<b>Finding A16:</b> Proper configuration on network devices for integrated security mechanisms enhanced network security by detecting and preventing suspicious traffic
<b>Finding A6:</b> Rogue device could easily be connected to the network and start issuing false network configurations	<b>Finding A13:</b> Using managed switches and shutting down unused switch ports mitigated network security threats and attacks  <b>Finding A17:</b> Rogue devices were denied access to the network to issue false network configurations
<b>Finding A7:</b> Malicious user or attacker could redirect the outgoing traffic from the victim's computer and intercept it	<b>Finding A16:</b> Proper configuration on network devices for integrated security mechanisms enhanced network security by detecting and preventing suspicious traffic
<b>Finding A8:</b> Malicious user or attacker could easily sniff network packets when network switch is under attack and acting like a hub	<b>Finding A16:</b> Proper configuration on network devices for integrated security mechanisms enhanced network security by detecting and preventing suspicious traffic

**Research Question:**

**SRQ3: How can network security be addressed and improved in order to protect against network security threats and attacks in South Africa?**

**FINDINGS BEFORE MITIGATION**

**Finding A9:** Unlimited number of devices could establish connection from a single network switch port

**Finding A10:** The use of insecure network protocols that lack encryption allowed authentication data such as username and plaintext passwords to be captured in transit across the network

**Finding A11:** The use of default settings on network devices poses a security threat

**FINDINGS AFTER MITIGATION**

**Finding A18:** Number of devices connecting to a single network switch port was controlled hence reduced the security risks

**Finding A19:** The cryptographic network protocols were used to improve network security by ensuring that the communication was encrypted

**Finding A20:** The use of default settings on network devices was eliminated hence improved network security

## **CHAPTER 6: DISCUSSION**

### **6.1 Introduction**

Chapter 4 presented research findings to determine challenges faced by higher academic institutions concerning network security. The chapter also presented findings on security technologies available for protecting against network security threats and attacks at these institutions. Chapter 5 presented findings on how network security can be addressed and improved on a technical level in order to protect against network security threats and attacks at HEIs in South Africa. Chapter 6 critically examines research findings from both the survey and the experiment conducted (summarised in Table 4.1 and Table 5.1) and the implications on network security.

### **6.2 Research questions**

For the reader's convenience, the primary and secondary research questions are again stated:

**PRQ:** What can be done to mitigate network security threats and attacks at higher academic institutions in South Africa?

**SRQ1:** What are the challenges surrounding network security at higher academic institutions?

**SRQ2:** What security technologies are available to protect against network security threats and attacks?

**SRQ3:** How can network security be addressed and improved in order to protect against network security threats and attacks in South Africa?

**SRQ4:** What framework can be proposed for South African higher academic institutions to improve network security?

### **6.3 Discussion and implications of network security**

In order to answer the research questions, a questionnaire was designed and distributed to IT technical staff at 25 higher academic institutions in Gauteng province, South Africa. The selected HEIs consisted of UoTs, traditional universities, comprehensive universities, private universities, public colleges, and private colleges. SRQ1 and SRQ2 were addressed by data collected and analysed from the questionnaire that determined the challenges HEIs are facing when securing their networks and identifying the available security technologies they



use. Rezgui & Marks (2008) assert that the knowledge and understanding of security challenges faced by HEIs could help these institutions to mitigate network security threats and attacks, hence avoiding bad reputation as well as financial and data loss. However, there are limited research studies done in this field to address challenges faced by HEIs concerning network security and how to improve this type of security. The challenges identified in SRQ1 and SRQ2 that could be attended to on a technical level, were addressed in SRQ3. The two Local Area Networks (experimental and control networks) were set up in a computer laboratory at the HEI where the researcher is employed. These networks were isolated from the institution's network to avoid any interruptions that could be caused by the experimental and control networks.

For the questionnaire phase of the research, it was revealed that 46% of the participants reported a lack of well-designed and written network security policies. This is disturbing as organisations such as HEIs without network security policies would continue failing to achieve their network security goals and would therefore be subjected to network security threats and attacks. The objective for a security policy is to know how to address the security risks by implementing security measures to assist in mitigating network security threats and attacks. As a result, institutions without network security policies lack network security feasibility as IT security personnel may not know when security breaches or violations are taking place and whether data have been compromised. This might result in HEIs incurring high costs for restoring their network services and their securing network resources, as confirmed by Rezgui & Marks (2008). Johnson (2006) asserts that a security policy provides a good foundation within an organisation to secure resources. Johnson (2006) further argues that organisations without well-designed and written network security policies have no assurance on the level of protection of their networks and resources.

According to Herath & Rao (2009), Ifinedo (2012) and Gundu & Flowerday (2013), a network security policy guides network users (end-users and IT technical personnel), thus establishing behaviours and acceptable procedures to be followed for accessing network resources that in turn regulate network activities. Knapp & Ferrante (2012) state that a network security policy is crucial as it sets directives and expected behaviours of network users when using an organisation's systems and handling data. Therefore, HEIs that implemented network security policies would likely benefit from improved network security as network resources would be protected against security threats and attacks (Baskerville & Siponen, 2002). A network security policy defines and approves consequences against security violations, hence minimises security risks. Defining expectations of user behaviour on the network and stipulating the consequences when failing to adhere to these rules would enhance network security.

Herath & Rao (2009) argue that the implementation of a network security policy to protect assets and ensure network security within an organisation does not necessarily guarantee user compliance and adherence to the policy. The network security policy needs to be enforced to ensure that users follow proper procedures when accessing network resources (Bulgurcu et al., 2010; Pfleeger et al., 2015). The research findings revealed that 54% of the participants from the various HEIs do not enforce network security policies. The lack of enforcing network security policy increases network security threats and attacks as users are not likely to follow their institution's guidelines to protect the network and access the systems and network resources that could impact negatively on HEIs should they be affected and reports be publicised. Knapp & Ferrante (2012) assert that the impact network security threats and attacks have on network security should compel organisations to tighten and enforce their security policies. The authors also state that network security threats and attacks could weaken the operations and system performance of organisations.

According to Bulgurcu et al. (2010) and Barton et al. (2016), top management needs to provide adequate support to the IT department to ensure network security policy compliance across the network. This would ensure that strict measures are employed, which forces users to follow rules set out and to meet the institution's behavioural expectations, thus improving network security. Support from top management impacts directly on network security policy compliance to ensure that institutions meet their expected network security goals. This supports the findings of Knapp et al. (2006), Da Veiga & Martins (2015) and Pham et al. (2017). Insufficient support from top management is reflected in the efficiency of the network security of an institution. Top management support is crucial to the effectiveness of network security policy functions, and especially in terms of funding allocation to IT department.

Insufficient funds allocated to the budget for IT security development affects network security, as the institution might not be able to purchase the latest security technologies, appoint more IT technical personnel, and offer mandatory training and education (Wu, 2010). The findings of this study revealed that the majority of participants are not pleased with the IT budget allocation. An inadequate IT department budget restricts IT technical personnel to address the security needs of the institution adequately and effectively. It affects the purchase of required security technology products due to high costs, hence hampering proper network security implementation to reduce network security threats and attacks. This is supported by Raman et al. (2016). However, Bunter (2011) and Knapp & Ferrante (2012) argue that buying the latest security technologies might not be effective if the institution does not have trained and qualified personnel who can utilise the full potential and capabilities of existing security technologies in order to mitigate network security threats and attacks.

Therefore, training and educating IT technical personnel is imperative for improving network security. Raman et al. (2016) assert that HEIs need to evaluate the costs incurred due to network security breaches versus the cost of buying security technologies. The authors argue that this evaluation could help top management realise the importance of network security, hence offering their support as it is not easy to accomplish and sustain a satisfactory level of network security at HEIs without any costs.

An insufficient budget does affect the proper implementation of network security and appointment of qualified personnel, especially when HEIs offer lower salaries compared to salary offers in industry (Marchany, 2014). This insufficiency leads to understaffed IT technical personnel, as skilled candidates are likely to opt for better salary offers. As a result, inadequate IT staff may lead to increased workloads and many responsibilities assigned to personnel that may not fall within their field of expertise. Understaffing at HEIs may lead to insufficient training of IT technical personnel due to time constraints (Marchany, 2014). The author also states that excessive workloads put more strain on personnel to finish the work while at the same time they are required to meet performance expectations, thus limiting the capabilities of personnel to serve the institution that subsequently affects the institution's network security. This corroborates the studies by David (2011), D'Arcy et al. (2014) and Tsai (2015) who indicate that overworked IT technical personnel often overlook technology issues affecting network security that include controlling unauthorised access to network devices, monitoring network traffic, and misconfiguring network devices.

The use of unmanaged network switches, open switch ports, insecure protocols, and default settings affect network security. Using unmanaged switches and having open ports on the network enable malicious users or attackers to gain unauthorised access to the network and connect their devices on open ports of unmanaged network devices. Furthermore, insecure protocols lead to network traffic being intercepted by an attacker and stolen confidential information being transmitted. Working with network devices using default settings also poses a security threat as the attacker could easily gain unauthorised access to these devices. However, utilising managed switches, shutting down unused ports of network devices, and using secure protocols and built-in security mechanisms help mitigate network security threats and attacks as confirmed by the experiments conducted.

Apart from the enforcement of network security policy, this policy also needs to be reviewed and updated frequently. According to Knapp & Ferrante (2012) and Alotaibi et al. (2016), security policies should be updated and aligned with changes across the network or infrastructure. This ensures that IT technical personnel on all levels within HEIs are properly guided, and that they apply security policy updates consistently. The maintenance of network security policies also ensures relevance to the latest security concerns and activities, thus

assisting IT technical personnel to anticipate and prevent any potential security risks in future. It ensures that vulnerabilities on the networks are properly addressed, which improves network security.

The research findings also revealed that 50% of the participants are not offered training and education concerning network security policy. This lack of training and education for network users hampers network security at HEIs as IT technical personnel may not have the necessary expertise to secure networks and resources by taking proper actions. As a result, HEIs might be negatively affected, as their networks would be subjected to network security threats and attacks, exposing these institutions to security risks (Willison & Siponen, 2009; Sarkar, 2010). Johnson (2006), Alotaibi et al. (2016), Safa et al. (2016) and Warkentin et al. (2016) argue that adequate training and education could aid in reducing network security risks to manageable levels and therefore improve network security. Gundu & Flowerday (2013), Ong & Chong (2014) and Tsohou et al. (2015) also state that training and educating network users could raise awareness and promote acceptable security behaviour at HEIs. Once security personnel understand the impact of their behaviour on their institution's network security, they are more likely to change and adopt good behaviours. Adequate training and education programmes ensure that network users are aware of the importance of network security and the impact non-compliance has on the institution's network security (Cox, 2012; Da Veiga & Martins, 2015; Warkentin et al., 2016; Pham et al., 2017). Therefore, the training of IT technical personnel needs to be a continuous process to ensure that these professionals improve their abilities to protect networks and resources and follow the guidelines and procedures written for their institutions.

Having a network security policy directly affects the implementation of security technologies, as these technologies are often seen as hindering the daily operations of HEIs. Although security technologies are crucial for protecting the network against security threats and attacks, their implementation within an institution as specified by the network security policy could be perceived as conflicting with the interest of the users. According to Greitzer et al. (2014), some network users may be concerned that the implementation of security technologies would limit the use of the network and operations performed, and therefore inhibit their academic freedom. However, Johnson (2006) argues that if users are trained and educated, this could change their negative attitude and perception of a network security to a better understanding of why such policies are needed. This change in attitude could help improve network security concerning the way assets and data are protected, thereby ensuring an effective and safe working environment. According to Bulgurcu et al. (2010) and Ifinedo (2012), network users who are trained and educated are more likely to have good

behavioural intentions and comply with their organisation's guidelines and procedures, reducing security risks that may be imposed by non-compliant users.

The increasing rate of network security breaches at HEIs globally has made network security a serious concern for most institutions, as network administrators have to deal with these security breaches. Despite knowing that any network is vulnerable to attacks regardless of its nature, it seems that HEIs tend to ignore this fact. Forty-eight percent (48%) of the participants reported that their institutions' networks have experienced security breaches in the past two years. Jones & Stallings (2011), Roman (2014), and Raman et al. (2016) assert that HEIs have become the target of network security threats and attacks because of their open environmental nature. This means that as these institutions provide open access to resources, they also need to provide a good balance to implement mechanisms that secure both their environment and their resources (Rezgui & Marks, 2008; Marchany, 2014). Nurse et al. (2014) assert that the emphasis to protect networks against security threats and attacks is placed more on external threats hence ignoring internal threats that pose a greater concern to the security of institutions. This is corroborated by Wang & Liu (2011), Haeussinger & Kranz (2013) and Anderson et al. (2016) who state that user management within institutions are often overlooked that results in HEIs failing to provide restricted access and leading to network security breaches. This confirms the critical nature of network security that needs to be addressed urgently by institutions to avoid data loss, financial loss, and bad reputation. According to Hearn (2016), 79% of higher academic institutions have a bad reputation because of security breaches on their networks.

Due to negative publicity and the subsequent widespread negative impact this may have, many institutions still do not report network security breaches to law enforcement. South African law does not force organisations to publicly report security breaches (Cosser, as stated by Alfreds, 2016), thereby allowing institutions to withhold security breach reports in order to avoid public embarrassment and bad reputation. However, this leads to institutions applying temporary solutions when addressing security breaches that negatively affect network security. HEIs therefore need to develop a sound and effective security policy by creating a strong security infrastructure that is applicable to achieving their security objectives. This would obligate IT technical personnel to understand the security threats and attacks faced by HEIs and plan for proper security architecture that is vital because it enhances the importance of security technologies by providing the required protection. Well-designed, written, and enforced network security policies could also protect assets and resources efficiently against internal and external security threats and attacks, while at the same time keeping the primary focus on network security. However, to achieve this goal,

institutions' top management needs to provide the necessary support to ensure that network security threats and attacks are properly mitigated.

Network security can also be achieved through the implementation of various security technologies. This corroborates the studies by Jackson et al. (2004), Liu & Zheng (2011), and Wattanapongsakorn et al. (2012) who state that different security technologies can help improve network security by protecting network assets and preventing unauthorised access to the network. However, Safa et al. (2016) assert that the implementation of different technologies alone cannot provide assurance that the environment is secured; the human aspect concerning the network security should be considered as well. Therefore, IT technical personnel need to understand how to utilise these security technologies effectively in order to improve network security while at the same time considering the institution's network security policy, thereby ensuring that security technologies are implemented in accordance with the network security policy.

The study revealed that the majority of participants mostly use firewalls, malware protection, and network access controls at their HEIs. According to Yu & Tsai (2011) and Zacker (2014), these security measures, especially firewalls, are able to protect the network at the perimeter from unauthorised access. However, Ahmed & Singh (2012) assert that the misconfiguration of network devices and security technologies may lead to malicious traffic passing through the network's perimeter without being noticed, causing damage to the network. According to Marchany (2014), the lack of qualified IT technical personnel also affects the proper configuration of security technologies and systems on the network, posing a serious concern to the network security of HEIs. The misconfiguration of network devices due to a lack of knowledge or negligence from IT technical personnel makes devices and networks susceptible to threats and attacks. IT professional expertise could thus enhance network security because of the knowledge these personnel have acquired in the IT field. To reduce network security threats and attacks, HEIs need to protect their assets effectively against security risks by implementing appropriate security technologies, and maintaining and updating their security (Onwubiko & Lenaghan, 2007). This will ensure that vulnerabilities in systems and network devices are not exploited by malicious attackers who want to gain access to the network and resources.

The findings from this study revealed that the majority of participants do perform vulnerability assessments at their institutions. It is evident that institutions are aware of the impact security threats and attacks could have on their networks. No security measure is considered as being completely effective; there are always factors hampering security, including the correct configuration of the network and devices, and limited funds. As a result, institutions should take responsibility and find innovative ways to mitigate security risks.

The findings from this study also revealed the lack of penetration testing on the networks of the HEIs that were included in the research. The frequency of performing vulnerability assessment and penetration testing is crucial as it affects the network security. The study found that vulnerability assessment and penetration testing are not frequently performed. According to Lai & Hsia (2007), vulnerabilities on network devices and systems are repeatedly increasing, making it difficult to patch and manage all the vulnerabilities in time before further exploitation occurs. The exploitation of these vulnerabilities on network devices and systems by an attacker could result in data loss; this means the frequency of performing vulnerability assessment and applying patches in time could reduce the chances of vulnerabilities exploitation and security risks. Performing penetration testing could assist HEIs in evaluating their own network security to determine the extent to which the attacker can access their network and what damage can be caused. This testing would therefore help IT technical personnel to increase security on the network before an attack, hence reducing any vulnerabilities and threats.

Although the damage caused by security breaches may differ, vulnerability management is imperative to control security threats and attacks. Adequate and skilled personnel as well as top management support play a crucial role in preventing the exploitation of vulnerabilities and improving network security. Lai & Hsia (2007) argue that performing vulnerability assessment requires patience as it is an exhausting and time-consuming process, but preventing vulnerabilities' exploitation reduces the damages that could occur and the financial costs the institutions might incur. Although monitoring of the network for suspicious traffic is a huge responsibility, it is essential in reducing network security risks as it helps IT technical personnel in gaining a better understanding of network activities that leads to improved network security. The implementation of intrusion detection systems could help institutions monitor their networks and alert network administrators to take remedial protective action in cases of security breaches or suspicious activities (Sharma & Singhrova, 2011). Intrusion prevention systems, on the other hand, could detect and stop such activities from taking place, hence improving network security (Meeta, 2011). However, Gascon et al. (2011) argue that the implementation of these systems result in unnecessary overconfidence of network administrators.

#### **6.4 Summary**

In this chapter the research findings from both the survey and experiment, employed as the research strategies utilised in this study, were critically analysed. The implications of the challenges faced by higher academic institutions on network security when securing their networks were also discussed.

The next and final chapter provides the recommendations and conclusion of the research study.



## **CHAPTER 7: RECOMMENDATIONS AND CONCLUSION**

### **7.1 Introduction**

This chapter provides the findings drawn on establishing ways to mitigate network security threats and attacks at higher academic institutions in South Africa. This research study's focal point was addressing network security threats and attacks, thus improving network security. As a result, a survey was conducted at HEIs in Gauteng province in South Africa to determine network security challenges faced by these institutions and identify the kind of network security technologies being used. The experiments were conducted to address technical challenges at Layer 2 of the OSI model that could be addressed practically. The implications of network security threats and attacks were drawn before and after applying mitigation techniques. This chapter addresses the research questions of the study. A framework to improve network security in South African HEIs is proposed based on the findings of the research study.

### **7.2 Review of the research study**

Chapter 1 provided a short introduction of network security for academic networks. The rationale and motivation of the research study were discussed, and the problem statement, research questions, and research objectives were elaborated on. The research design, delimitations, and ethical considerations of the research study were explained. Lastly, the outline of the research study was provided.

In Chapter 2, the network environment implemented at higher academic institutions was sketched. The challenges faced by HEIs were pointed out, and the different kinds of security technologies applicable for use at HEIs were discussed.

Chapter 3 provided detailed information on how this research study was carried out. The research philosophy, research approach, and research strategy that were implemented in this research study, were addressed. The research methods selected for the study were emphasised, and a detailed description of data collection as well as how the collected data were analysed, was provided.

Chapter 4 entailed the analysis and interpretation of the data obtained from the survey questionnaire conducted. The results obtained were discussed in terms of the research objectives of the study.

Chapter 5 described how the security threat experiments were conducted on a dedicated network at a selected HEI in Gauteng, and the outcomes of the experiments were provided.

Chapter 6 provided a discussion on the findings derived from the survey results as indicated in Chapter 4 and the experiment outcomes as indicated in Chapter 5.

### **7.3 Research Questions**

This study was conducted to find possible ways for mitigating network security threats and attacks at HEIs. For guidance in completing this research study, both primary research question (PRQ) and secondary research questions (SRQ) have been presented as follows:

Primary research question (PRQ):

**PRQ:** What can be done to mitigate network security threats and attacks at higher academic institutions in South Africa?

Secondary research questions (SRQ):

**SRQ1:** What are the challenges surrounding network security at higher academic institutions?

**SRQ2:** What security technologies are available to protect against network security threats and attacks?

**SRQ3:** How can network security be addressed and improved in order to protect against network security threats and attacks in South Africa?

**SRQ4:** What framework can be proposed for South African higher academic institutions to improve network security?

The following outcomes are provided for each secondary research question in order to answer the primary research question.

#### **7.3.1 Secondary Research Question 1**

**SRQ1: What are the challenges surrounding network security at higher academic institutions?**

Higher academic institutions are faced with several network security challenges impacting negatively on their network security. The following findings regarding network security challenges at HEIs in South Africa were drawn from the survey analysis:

- The lack of a well-designed and written network security policy poses a threat to network security at HEIs, as these institutions might not have properly established

how network users should behave when accessing network resources, and how to secure such resources. Some institutions do not have a network security policy as this valuable document is perceived as an obstacle to progress because it often clashes with user activities on the network

- The lack of enforcing a network security policy on network users poses another serious problem that cannot be ignored. A network security policy should be enforced in order to be effective and valuable. However, this enforcement should happen with assistance from top management as the leaders of an institution play a critical role in the success of network security enforcement. The lack of enforcing a network security policy could result in network security breaches that have the ability to destroy the reputation of the institution
- Insufficient reviews and updates of the network security policy on a regular basis could lead to a dysfunctional and ineffective network security policy, affecting the institution's network security and causing a vulnerable network as systems might not be patched and updated periodically
- When a network security policy is not adequately enforced and support from top management is lacking, the personnel could misuse their rights knowing there would not be any consequences against such unethical acts
- Attacks and security issues against servers and database systems were among the highest concerns to protect against as these could easily be exploited. The second highest attack vectors and security issues identified were malware threats, followed by hacking incidents
- Insufficient mandatory training and education for network users poses a threat because the users' activities might unknowingly endanger network security
- IT budget allocation plays a significant part in ensuring that network security is addressed and improved. Insufficient IT budget allocations can seriously affect the use and implementation of security technologies at institutions
- Lower salary offers at HEIs lead to reduced staffing levels. This results in a shortage of qualified personnel able to help improve network security
- There is a call for HEIs to increase IT technical staff in order to address network security effectively and efficiently
- Vulnerability assessment should be conducted on a regular basis to discover vulnerabilities on systems and network devices

- There seems to be a lack of penetration testing on HEIs' systems and networks. This testing should be conducted to determine the degree of damage should the network be breached
- Vulnerability assessment or penetration testing was only performed after a long period of time, such as on an annual basis that might not be effective
- A high percentage of participants indicated that they do not investigate network threats or take remedial actions that shows a lack of responsibility by IT personnel

### **7.3.2 Secondary Research Question 2**

#### **SRQ2: What security technologies are available to protect against network security threats and attacks?**

Participants showed that firewalls, malware protection, and network access controls are the top three security technologies used at HEIs in South Africa. However, security technologies such as intrusion detection systems, intrusion prevention systems, and encryption are insufficiently utilised. The lack of an IT budget probably contributes to limited usage of security technologies at HEIs. Of all the security technologies used, respondents were the most satisfied with the firewall.

### **7.3.3 Secondary Research Question 3**

#### **SRQ3: How can network security be addressed and improved in order to protect against network security threats and attacks in South Africa?**

In order to adequately address and improve network security threats and attacks, both at non-technical level and technical level, the following are the recommendations that should be implemented:

- Higher academic institutions should have a well-designed and written network security policy. This document can help improve network security, as users will have formalised and structured guidelines, procedures, and principles to follow; leading to a reduced likelihood of network security threats and attacks within HEIs
- A network security policy should be enforced adequately to be effective and to ensure that all network users adhere to the policy. The top management of the institution should be actively involved in this process, assisting in addressing violation issues by implementing consequences for users (staff and students) who disrupt these established rules and regulations in terms of networks. Enforcing a network security policy will also promote the proper use and configuration of network devices, thereby

eliminating security threats posed by the use of unmanaged switches, misconfiguration of devices, and open switch ports

- Institutions should ensure that every employee is aware of the network security policy and that each new staff member receives a copy. The institutions should also make institutional policies easily available to staff in order to reduce suspicious actions committed by users who might not be aware of the danger their actions might pose
- Institutions should regularly review and update their network security policy to improve its functionality and ensure that it provides the required protection against network security threats and attacks
- Institutions should ensure the effective implementation of management programmes such as patch and threat management to combat network security threats and attacks by ensuring that patches and program updates are applied regularly. This will reduce the security threats on systems that could jeopardise network security
- Institutions should offer appropriate training and educational programmes for network users in order to educate them on the importance of network security. When users are aware of the network security policy and what role it plays in their daily working activities, they would probably behave differently, not intentionally violating the policy by misusing their rights. This could help improve network security and change the way in which network security policies are perceived - as being an obstacle to development
- Institutions should consider increasing the budget allocated to the IT department for improving network security. This will ensure that institutions have the ability to purchase security technologies that help protect against network security threats and attacks
- HEIs should consider revising the salary packages offered to applicants in order to attract and attain higher qualified personnel, specifically the IT technical staff, to increase the expertise level. Skilled personnel have the ability to ensure that the proper security technologies are adequately configured and deployed to improve network security. The increase in IT technical staff at HEIs could ensure that maintenance on the network is sufficiently conducted
- Institutions should adequately protect the systems holding confidential information in order to avoid security breaches. Thus, institutions should patch and update their systems periodically to reduce vulnerabilities that can be exploited
- Institutions should utilise integrated security mechanisms on network devices to help protect against network security threats and attacks

- Institutions should adequately monitor their networks to detect and prevent suspicious traffic. Therefore, monitoring tools, intrusion detection systems, and intrusion prevention systems should be used to ensure that suspicious activities and traffic are detected and prevented before any damage can occur on the network. This helps preserving the confidentiality, integrity, and availability of network resources
- Institutions should consider making use of cryptographic network protocols to ensure that communication across the network is secured and to reduce the likelihood of authentication data being stolen during data transmission
- The institutions should avoid using the default settings on network devices as it poses a security threat on the network. Default settings could be exploited by the attacker and impact negatively on network security
- Institutions should conduct vulnerability assessment to discover vulnerabilities on the systems before being exploited; remedial actions should also be taken to solve such security threats. This would eliminate the security threats posed by the existence of vulnerabilities and the likelihood of the systems and networks being attacked. This assessment should at least be conducted on a monthly basis to avoid institutions' networks being vulnerable to attacks
- Institutions should adequately perform penetration testing on systems and networks to ensure that vulnerabilities identified are resolved before endangering systems and networks. This test should at least be conducted on a bi-annual basis
- Institutions should sufficiently respond and investigate all reported security alerts and incidents for better improvement of network security

#### **7.3.4 Secondary Research Question 4**

**SRQ4: What framework can be proposed for South African higher academic institutions to improve network security?**

This research study has determined a number of challenges facing HEIs when it comes to securing their networks and network resources. The researcher therefore proposes the framework as shown in Figure 6.1 to mitigate network security threats and attacks. The proposed framework comprises five phases: Phase 1: Identification, Phase 2: Planning, Phase 3: Protection, Phase 4: Response, and Phase 5: Penetration Testing. These phases are discussed in detail below.

### **a) Phase 1: Identification**

This phase identifies the network security threats and attacks problem. Based on the problem, each institution should conduct a risk vulnerability assessment in order to identify security risks imposed by these threats and attacks. This assessment enables institutions to define security requirements and effectively plan how to address network security threats and attacks, thus improving network security.

### **b) Phase 2: Planning**

This is the phase where institutions plan on how to address network security threats and attacks against their networks, thus, designing and structuring the network security policy. This document forms the foundation for institutions to achieve their network security goals. Once the security policy has been designed and structured, it should be enforced in order to derive the benefits it provides. For its success and effectiveness, top management should be committed and supportive by enforcing disciplinary actions against security policy violation caused by personnel. Any misconduct by personnel should be dealt with to reduce the likelihood of personnel repeatedly carrying out the same acts. This would ensure that network users comply with network security policy. As part of the planning phase, institutions should ensure that continuous monitoring and auditing are carried out. This process ensures that all network activities such as network usage, configuration of network devices, and methods of authentication are monitored to detect any misconduct by personnel or unauthorised users. The process also reduces the likelihood of applying different configurations of systems across the network.

### **c) Phase 3: Protection**

This phase is responsible for ensuring the protection of the network and its resources. Institutions should know how to control access to the network and its resources in order to ensure restricted access, hence limit unauthorised access. This would further ensure that user access rights are controlled and removed when necessary. This phase also covers the physical security of the network to ensure that IT or network equipment are secured against theft and damage that may disrupt the network operability and hamper the security. The entry to the premises holding the network equipment needs to be protected to avoid unauthorised access. Different types of security technology protection such as firewalls, encryption, intrusion detection systems, intrusion prevention systems, and malware protection should be used across the network to enhance network security. To warrant the effectiveness of the security technologies implemented, security maintenance needs to be

conducted regularly. For institutions to achieve a high level of protection, they need funding or allocate extra budgets for network security.

**d) Phase 4: Response**

This phase is responsible for ensuring that mitigation techniques are applied, and that the security policy is updated and reviewed after encountering security breaches. This phase also ensures that network users are trained and educated on network security to equip both end users and technical users with necessary information they need to know. The end user knowledge would ensure that users comply with the security policy. The staff expertise would ensure that systems and network devices are properly configured and appropriate security technologies are implemented within the institutions. This would also ensure that personnel know and understand how to manage security incidents, when to apply patches, and how to manage security threats.

**e) Phase 5: Penetration Testing**

This is the phase where the institutions test how secure their networks are against network security threats and attacks. This test reveals the degree of damage that might be caused should the network be compromised internally or externally. Both the internal and external penetrating tests exploit vulnerabilities of the network and the kind of damage that could be caused.



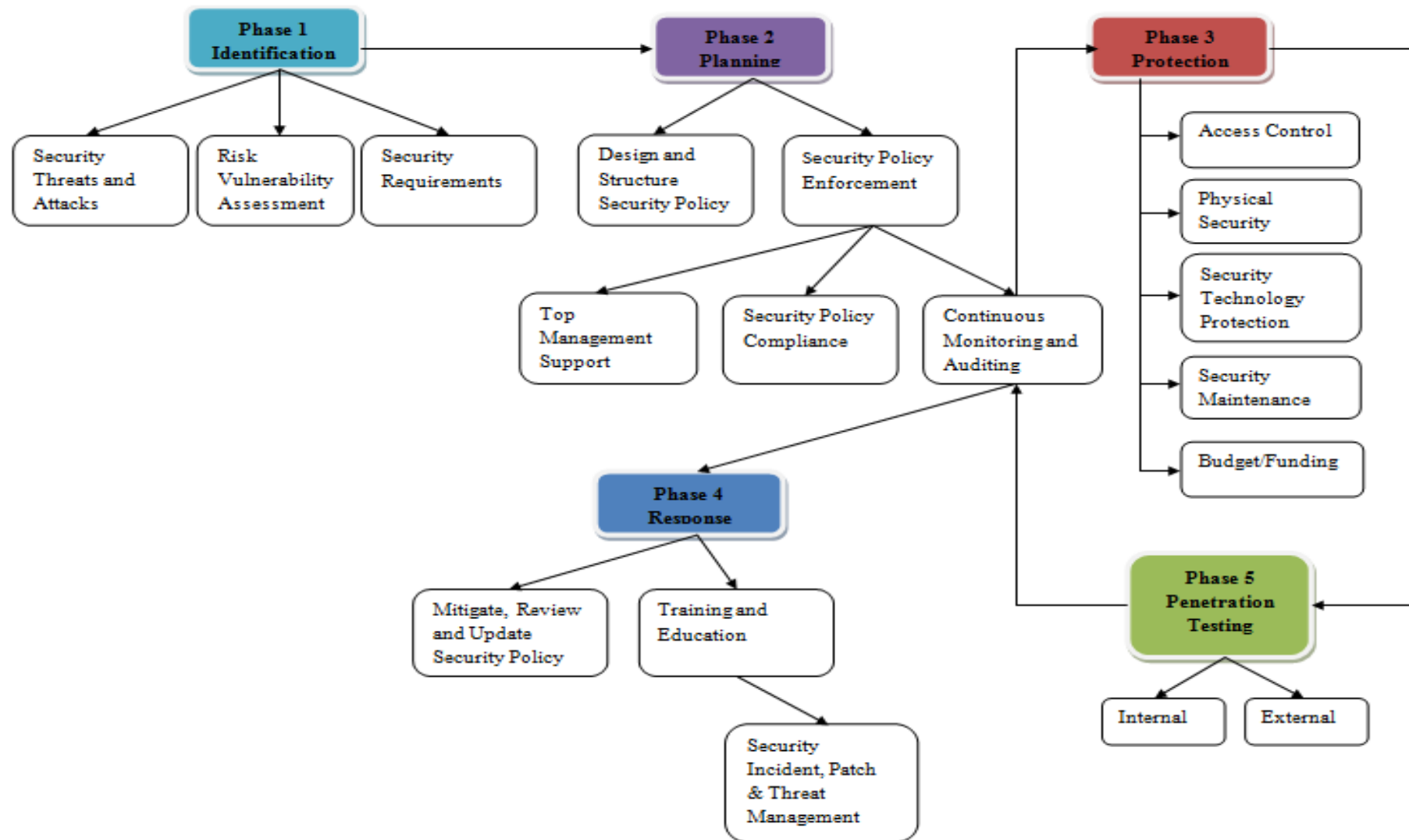


Figure 7.1: Proposed Framework for South African higher academic institutions

## **7.4 Conclusion**

This research study was conducted to establish ways to help mitigate network security threats and attacks at higher academic institutions in South Africa. To achieve the main objective, the research questions were presented (sections 1.4.1 and 1.4.2). This study was conducted at higher academic institutions in Gauteng province to determine the challenges faced and the type of security technologies that are used and implemented. This study found several challenges facing higher academic institutions regarding the protection of the networks and resources. Among the challenges, insufficient budget allocation to IT department, inadequate staffing, lack of penetration testing, inadequate use of cryptographic network protocols, and lack of network security policy and its enforcement were determined. The study conducted internal penetration testing at Layer 2 of the OSI model to deal with challenges that could be addressed practically. The findings showed that inadequate network security policy negatively impacts the network security as unauthorised network users could easily gain access to the network. Mitigation techniques were applied, which showed improvement of network security, as the unauthorised access was successfully restricted. Based on the research findings, a framework was proposed for mitigating network security threats and attacks at HEIs in South Africa.

## **7.5 Future work**

Due to time constraints, on a technical level, this research study's focal point was internal penetration testing on Layer 2 of the OSI model. For future work, intensive penetration testing, which covers both internal and external testing on other OSI model layers, is proposed. This future work could assist network administrators in obtaining more information on how to control and reduce vulnerabilities on the systems that could be exploited to gain greater access on the network. Further research can also be conducted in a different province in South Africa to determine the level of network security at HEIs in a different province. Due to the high cost of network devices and systems, and the potential impact penetration testing may have, in future, all experiments could be conducted on virtual networks to reduce any impact the attacks may cause on systems.

## REFERENCES

- ABDULHAMMED, R., FAEZIPOUR, M. & ELLEITHY, K. M. (2016). Network intrusion detection using hardware techniques: a review. *Proceedings. 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. p. 1-7.
- AHMED, M., MAHMOOD, A. N. & HU, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*. 60. p. 19-31.
- AHMED, T. & SINGH, J. (2012). Efficient firewall designing using ant colony optimization and hierarchical distribution. *UACEE International Journal of Advances in Computer Networks and its Security*. 2(1). p. 53-57.
- AIMING, Q. & LI, S. (2012). Method on rule extracting in misuse intrusion detection based on rough set genetic algorithm. *Proceedings. 2012 7<sup>th</sup> International Conference on Computing and Convergence Technology (ICCCT)*. p. 731-734.
- AL-AKHRAS, M. A. (2006). Wireless network security implementation in universities. *2<sup>nd</sup> Information and Communication Technologies ICTTA '06*. 2. p. 3192-3197.
- ALEROUD, A. & ZHOU, L. (2017). Phishing environments, techniques, and countermeasures: a survey. *Computers & Security*. 68. p. 160-196.
- ALFREDS, D. (2016). *SA fails to make data breaches public-expert*. [Online] Available from: <http://www.fin24.com/Tech/Cyber-Security/sa-fails-to-make-data-breaches-public-expert-20160226> [Accessed: 30/03/2016]
- ALHARTHY, K. & SHAWKAT, W. (2013). Implementing network security control solutions in BYOD environment. *Proceedings. IEEE International Conference on Control Systems, computing and Engineering (ICCSCE)*. p. 7-13.
- ALIAGA, M. & GUNDERSON, B. (2002). *Interactive statistics*. 3<sup>rd</sup> ed. Upper Saddle River, New Jersey: Pearson Prentice Hall.
- ALMAKRAMI, H. (2016). Intrusion detection system for smart meters. *Proceedings. 2016 Saudi Arabia Smart Grid (SASG)*. p. 1-8.
- ALOTAIBI, M., FURNELL, S. & CLARKE, N. (2016). Information security policies: a review of challenges and influencing factors. *Proceedings. 2016 11<sup>th</sup> International Conference for Internet Technology and Secured Transactions (ICITST)*. p. 352-358.
- AMIRI, E., AFSHAR, E., NAJI, H. R. & ARDEKANI, M. M. (2012). Survey on network access control technology in MANETs. *Proceedings. 2012 International Conference on Innovation, Management, and Technology Research (ICIMTR2012)*. p. 367-372.

- ANDERSON, B. B., VANCE, A., KIRWAN, C. B., EARGLE, D. & JENKINS, J. L. (2016). How users perceive and respond to security messages: a neuroIS research agenda and empirical study. *European Journal of Information Systems*. 25(4). p. 364-390.
- ARACHCHILAGE, N. A. G. & LOVE, S. (2014). Security awareness of computer users: a phishing threat avoidance perspective. *Computers in Human Behaviour*. 38. p. 304-312.
- ARACHCHILAGE, N. A. G., LOVE, S. & BEZNOSOV, K. (2016). Phishing threat avoidance behaviour: an empirical investigation. *Computers in Human Behavior*. 60. p. 185-197.
- BARTON, K. A., TEJAY, G., LANE, M. & TERRELL, S. (2016). Information system security commitment: a study of external influences on senior management. *Computers & Security*. 59. p. 9-25.
- BASKERVILLE, R. & SIPONEN, M. (2002). An information security meta-policy for emergent organisations. *Logistics Information Management*. 15(5). p. 337-346.
- BEISKE, B. (2007). *Research methods: Uses and limitations of questionnaires, interviews, and case studies*. GRIN Verlag.
- BERNARD, H. R. (2011). *Research methods in anthropology: qualitative and quantitative approaches*. 5<sup>th</sup> ed. London: AltaMira Press.
- BLAIKIE, N. (2007). *Approaches to social enquiry*. 2<sup>nd</sup> ed. Cambridge: Polity Press.
- BLUMBERG, B., COOPER, D. R. & SCHINDLER, P. S. (2014). *Business research methods*. Boston: McGraw-Hill.
- BRADBURY, D. (2013). *Higher learning: Information security on campus*. [Online] Available from: <https://www.infosecurity-magazine.com/magazine-features/higher-learning-information-security-on-campus/> [Accessed: 18/11/2015]
- BRO. (2017). *Bro FAQ*. [Online] Available from: <https://www.bro.org/documentation/faq.html#what-is-bro> [Accessed: 03/11/2017].
- BROOKS, R. R. (2014). *Introduction to computer and network security: navigating shades of gray*. Boca Raton: CRC Press.
- BRYMAN, A. & BELL, E. (2011). *Business research methods*. 3<sup>rd</sup> ed. New York: Oxford University Press.
- BULGURCU, B., CAVUSOGLU, H. & BENBASAT, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*. 34(3). p. 523-548.

- BUNTER, B. (2011). *Training and education: an essential ingredient of small business security strategy*. [Online] Available from: <http://www.brighthub.com/computing/smb-security/articles/2152.aspx> [Accessed: 26/04/2016]
- BURNEY, S. M. A. & KHAN, M. S. A. (2010). Network usage security policies for academic institutions. *International Journal of Computer Application*. 7(14). p. 6-11.
- BURNEY, S. M. A. & MAHMOOD, N. (2006). A brief history of mathematical logic and applications of logic in CS/IT. *Karachi University Journal of Science*. 34(1). p. 61-75.
- BURRESS, C. (2005). *Cal issues alert about stolen laptop computer*. [Online] Available from: <http://www.sfgate.com/bayarea/article/BERKELEY-Cal-issues-alert-about-stolen-laptop-2719570.php> [Accessed: 13/08/2015]
- CHABROW, E. (2015). *China blamed for Penn State Breach- Hackers remained undetected for more than two years*. [Online] Available from: <http://www.databreachtoday.com/china-blamed-for-penn-state-breach-a-8230> [Accessed: 16/07/2015]
- CHAO-YANG, Z. (2011). DoS attack analysis and study of new measures to prevent. *Proceedings*. 2011 International Conference on Intelligence Science and Information Engineering. p. 426-429.
- CHAPPELL, L. (2012). *Wireshark network analysis: The official Wireshark certified network analyst study guide*. 2<sup>nd</sup> ed. Reno, Nevada: Chappell University.
- CHEN, Z., YEO, C. K., LEE, B. S. & LAU, C. T. (2017). Detection of network anomalies using Improved-MSPCA with sketches. *Computers & Security*. 65. p. 314-328.
- CIAMPA, M. (2012). *Security+ guide to network security fundamentals*. 4<sup>th</sup> ed. Boston: Cengage Learning.
- CISCO NETWORKING ACADEMY. (2007). *Protecting and optimizing higher education networks: Cisco campus secure*. San Jose: Cisco Systems.
- CISCO NETWORKING ACADEMY. (2013). *Introduction to networks: Companion guide*. Indianapolis: Cisco Press.
- CISCO NETWORKING ACADEMY. (2014). *IT essentials: PC hardware and software companion guide*. 5<sup>th</sup> ed. Indianapolis: Cisco Press.
- COHEN-ABRAVANEL, D. (2013). *Penn State computer with confidential student data infected with malware*. [Online] Available from: <http://www.seculert.com/blog/2013/08/penn-state-malware.html> [Accessed: 13/08/2015]

- COMPUTER EMERGENCY RESPONSE TEAM (CERT). (1998). *1998 Annual Report*.  
[Online] Available from: [http://www.cert.org/historical/annual\\_rpts/cert\\_rpt\\_98.cfm](http://www.cert.org/historical/annual_rpts/cert_rpt_98.cfm)  
[Accessed: 12/08/2015]
- COX, J. (2012). Information systems user security: a structures model of the knowing-doing gap. *Computers in Human Behaviour*. 28(5). p. 1849-1858.
- CRESWELL, J. W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches*. 4<sup>th</sup> ed. Thousand Oaks, California: Sage.
- CRONAN, T. P., FOLTZ, B. & JONES, T. W. (2006). Piracy, computer crime and IS misuse at the university. *Communications of the ACM*. 49(6). p. 84-90.
- CROWTHER, D. & LANCASTER, G. (2008). *Research methods: a concise introduction to research in management and business consultancy*. 2<sup>nd</sup> ed. London: Butterworth-Heinemann.
- CUBRILOVIC, N. (2009). *RockYou Hack: from bad to worse*. [Online] Available from: <http://techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/> [Accessed: 20/08/2015]
- CZERNOWALOW, M. (2005). *Lack of policy causes IT risks*. [Online] Available from: <http://www.itweb.co.za> [Accessed: 15/04/2012]
- D'ARCY, J., HERATH, T. & SHOSS, M. K. (2014). Understanding employee responses to stressful information security requirements: a coping perspective. *Journal of Management Information Systems*. 31(2). p. 285-318.
- DANCE, S. (2014). *Hacking incidents prompt universities to rethink balance between openness, security*. [Online] Available from: [http://articles.baltimoresun.com/2014-03-15/news/bs-md-higher-ed-hacking-20140315\\_1\\_personal-data-social-security-universities](http://articles.baltimoresun.com/2014-03-15/news/bs-md-higher-ed-hacking-20140315_1_personal-data-social-security-universities) [Accessed: 21/08/2015]
- DA VEIGA, A. & MARTINS, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*. 49. p. 162-176.
- DAVENPORT, S. (2013). *Weak passwords brute forced*. [Online] Available from: <https://github.com/blog/1698-weak-passwords-brute-forced> [Accessed: 20/08/2015]
- DAVID, K. (2011). *Human behaviour: a critical security threat*. [Online] Available from: <http://www.brighthub.com/computing/smb-security/articles/18561.aspx> [Accessed: 23/11/2016]
- DEAN, T. (2013). *Network+ guide to networks*. 6<sup>th</sup> ed. Boston: Cengage Learning.

- DESAI, A. S. & GAIKWAD, D. P. (2016). Real time hybrid intrusion detection system using signature matching algorithm and fuzzy-GA. *Proceedings. 2016 IEEE International Conference on Advances in Electronic, Communications and Computer Technology (ICAECCT)*. p. 291-294.
- DILLMAN, D. A. (2007). *Mail and Internet surveys: The tailored design method*. 2nd ed. Hoboken, New Jersey: John Wiley & Sons.
- DIMITRIOS, T. (2011). *Flood network with random MAC addresses with macof tool*. [Online] Available from: <https://tournasdimitrios1.wordpress.com/2011/03/04/flood-network-with-random-mac-addresses-with-macof-tool/> [Accessed: 21/08/2016]
- DONAHUE, G. A. (2011). *Network warrior*. 2<sup>nd</sup> ed. Sebastopol, California: O'Reilly Media.
- DUANGPHASUK, S., KUNGPISDAN, S. & HANKLA, S. (2011). Design and implementation of improved security protocols for DHCP using digital certificates. *Proceedings. 2011 7<sup>th</sup> IEEE International Conference on Networks (ICON)*. p. 287-292.
- DULANOVIĆ, N., HINIĆ, D. & SIMIĆ, D. (2008). An intrusion prevention system as a proactive security mechanism in network infrastructure. *Yugoslav Journal of Operations Research*. 18(1). p. 109-122.
- DZUNG, D., NAEDELE, M., VON HOFF, T. P. & CREVATIN, M. (2005). Security for Industrial Communication Systems. *Proceedings of the IEEE*. 93(6). p. 1152-1177.
- EASTERBY-SMITH, M., THORPE, R. & JACKSON, P. (2012). *Management research*. 4<sup>th</sup> ed. London: Sage.
- ESLAHI, M., SALLEH, R. & ANUAR, N. B. (2012). MoBots: a new generation of bitnets on mobile devices and networks. *Proceedings. 2012 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE)*. p. 262-266.
- E-TUTORIALS.ORG. (2016). *Categories of threat*. [Online] Available from: <http://etutorials.org/Networking/Router+firewall+security/Part+I+Security+Overview+and+Firewalls/Chapter+1.+Security+Threats/Categories+of+Threats/>. [Accessed: 28/03/2016]
- FRANKEL, R. M. & DEVERS, K. J. (2000). Study design in quantitative research: developing questions and assessing resource needs. *Education for Health*. 13(2). p. 251-261.
- FUCHSBERGER, A. (2005). Intrusion detection systems and intrusion prevention systems. *Information Security Technical Report*. 10(3). p. 134-139.
- GASCON, H., ORFILA, A. & BLASCO, J. (2011). Analysis of update delays in signature-based network intrusion detection systems. *Computers & Security*. 30(8). p. 613-624.

- GAY, L. R., MILLS, G. E. & AIRASIAN, P. W. (2015). *Educational research: competencies for analysis and applications*. Upper Saddle River, New Jersey: Prentice Hall.
- GILL, J. & JOHNSON, P. (2010). *Research methods for managers*. 4<sup>th</sup> ed. London: Sage.
- GILMORE, J. (2015). *Campus announces data breach*. [Online] Available from: <http://news.berkeley.edu/2015/04/30/campus-announces-data-breach/> [Accessed: 23/03/2016]
- GODDARD, W. & MELVILLE, S. (2004). *Research methodology: an introduction*. 2<sup>nd</sup> ed. Lansdowne: Juta.
- GOPALAKRISHNAN, S. (2014). A survey of wireless network security. *International Journal of Computer Science and Mobile Computing*. 3(1). p. 53-68.
- GREENWALD, M., SINGHAL, S. K., STONE, J. R. & CHERITON, D. R. (1996). Designing an academic firewall: policy, practice, and experience with SURF. *Proceedings. The Symposium on Network and Distributed System Security*. p. 79-92.
- GREITZER, F. L., STROZER, J., COHEN, S., BERGEY, J., COWLEY, J., MOORE, A. & MUNDIE, D. (2014). Unintentional insider threat: contributing factors, observables, and mitigation strategies. *Proceedings. 2014 47<sup>th</sup> Hawaii International Conference on System Sciences*. p. 2025-2034.
- GROVE, S. K., GRAY, J. R. & BURNS, N. (2015). *Understanding nursing research: building an evidence-based practice*. 6<sup>th</sup> ed. St. Louis, Missouri: Elsevier Saunders.
- GUNDU, T. & FLOWERDAY, S. V. (2013). Ignorance to awareness: towards an information security awareness process. *SAIEE Africa Research Journal*. 104(2). p. 69-79.
- GUPTA, D., SINGHAL, S., MALIK, S. & SINGH, A. (2016). Network intrusion detection system using various data mining techniques. *Proceedings. 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS)*. p. 1-6.
- HADRI, A., CHOUGDALI, K. & TOUAHNI, R. (2016). Intrusion detection system using PCA and fuzzy PCA techniques. *Proceedings. International Conference on Advanced Communication Systems and Information Security (ACOSIS)*. p. 1-7.
- HAEUSSINGER, F. & KRANZ, J. (2013). Information security awareness: its antecedents and mediating effects on security compliant Behavior. *Proceedings. 34<sup>th</sup> International Conference on Information Systems, Security and Privacy of Information and IS*. p. 1-16.
- HAKIM, C. (2000). *Research design: Successful designs for social and economic research*. 2<sup>nd</sup> ed. London: Routledge.



- HEALY, M. & PERRY, C. (2000). Comprehensive criteria to judge validity and reliability of qualitative research within the realism paradigm. *Qualitative Market Research-An International Journal*. 3(3). p. 118-126.
- HEARN, T. (2016). *University challenge cyber-attacks in higher education*. [Online] Available from: <http://www.comtact.co.uk/wp-content/uploads/2016/04/University-Challenge-Cyber-Attacks-in-Higher-Education-April-2016.pdf> [Accessed: 23/09/2016]
- HEMALATHA, P. & VIGITHAANANTHI, J. (2017). An effective performance for denial of service attacks (DOS) detection. *Proceedings*. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud). p. 229-233.
- HENNING, E., VAN RENSBURG, W. & SMIT, B. (2004). *Finding your way with qualitative research*. Pretoria: Van Schaik.
- HERATH, T. & RAO, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support System*. 47(2). p. 154-165.
- HITTLEMAN, D. R. & SIMON, A. J. (2005). *Interpreting educational research: an introduction for consumers of research*. 4<sup>th</sup> ed. Upper Saddle River, New Jersey: Prentice Hall.
- HUANG, H. D., CHUANG, T. Y., TSAI, Y. L & LEE, C. S. (2010). Ontology-based intelligent system for malware behavioural analysis. *Proceedings*. 2010 IEEE International Conference on Fuzzy systems (FUZZ). p. 1-6.
- HYDE, K. F. (2000). Recognising deductive process in qualitative research. *Qualitative Market Research: An International Journal*. 3(2). p. 82-89.
- IFINEDO, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computers & Security*. 31(1). p. 83-95.
- JACKSON, T. R., LEVINE, J. G., GRIZZARD, J. B. & OWEN, H. L. (2004). An investigation of a compromised host on a honeynet being used to increase the security of a large enterprise network. *Proceedings*. The 2004 IEEE Workshop on Information Assurance and Security. p. 9-14.
- JAVAID, A., NIYAZ, Q., SUN, W. & ALARM, M. (2016). A deep learning approach for network intrusion detection system. *Proceedings*. 9<sup>th</sup> EAI International Conference on Bio-inspired Information and Communications Technologies. p. 21-26.
- JINGBO, Y. & PINGPING, S. (2010). A secure strong password authentication protocol. *Proceedings*. 2010 2<sup>nd</sup> International Conference on Software Technology and Engineering (ICSTE). 2. p. 355-357.

- JOHNSON, E. C. (2006). Security awareness: switch to better programme. *Network Security*. 2006(2). p. 15-18.
- JOHNSON, R. B. & CHRISTENSEN, L. (2014). *Educational research: quantitative, qualitative, and mixed approaches*. 5<sup>th</sup> ed. Thousand Oaks, California: Sage.
- JONES, R. & STALLINGS, T. J. (2011.) Challenges to network security on college campuses. *Consortium for Computing Sciences in College*. 27(2). p. 37- 42.
- KAWAMOTO, D. (2006). *UCLA break-in data on 800,000 at risk*. [Online] Available from: <http://www.cnet.com/news/ucla-break-in-puts-data-on-800000-at-risk/> [Accessed: 15/08/2015]
- KHOBRADE, S.S., SARDARE, P., KUMBHARE, B., DONGRE, P. & JHA, D. (2011). Cryptography and Network Security. *International Journal of Advances in Computer Networks and its Security*. 1(1). p. 177-180.
- KHONJI, M., IRAQI, Y. & JONES, A. (2013). Phishing detection: a literature survey. *IEEE Communications Survey & Tutorials*. 15(4). p. 2091-2121.
- KNAPP, K. J. & FERRANTE, C. J. (2012). Policy awareness, enforcement and maintenance: critical to information security effectiveness in organizations. *Journal of Management Policy and Practice*. 13(5). p. 66-80.
- KNAPP, K., MARSHALL, T., RAINER, R. & FORD, F. (2006). Information security: management's effect on culture and policy. *Information Management and Computer Security*. 14(1). p. 24-36.
- KUMAR, V. & SANGWANE, O. P. (2012). Signature based intrusion detection system using SNORT. *International Journal of Computer Applications & Information Technology*. 1(3). p. 35-41.
- LAI, Y. P. & HSIA, P. L. (2007). Using the vulnerability information of computer systems to improve the network security. *Computer Communications*. 30(9). p. 2032-2047.
- LANCASTER, G. (2005). *Research methods in management: a concise introduction to research in management and business consultancy*. Oxford: Butterworth-Heinemann.
- LEVINE, J., LABELLA, R., OWEN, H., CONTIS, D. & CULVER, B. (2003). The use of honeynets to detect exploited systems across large enterprise networks. *Proceedings. The 2003 IEEE Workshop on Information Assurance and Security*. p. 92-99.
- LI, F. (2011). The research on information safety problem of digital campus network. *Proceedings. 2011 2<sup>nd</sup> International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC)*. p. 828-831.

- LICHTMAN, M. (2013). *Qualitative research in education: a user's guide*. 3<sup>rd</sup> ed. Thousand Oaks, California: Sage.
- LINKSYS. (2016). *Setting up a VPN Tunnel on two (2) routers*. [Online] Available from: <http://www.linksys.com/us/support-article?articleNum=132865> [Accessed: 22/03/2016]
- LIU, H. & ZHENG, L. (2010). Application and research on active protection for campus network based on multi-cores UTM. *Proceedings*. 2010 International Conference on Multimedia Information Networking and Security (MINES). p. 589-592.
- LIU, H. & ZHENG, L. (2011). Application and analysis on real-time protection for educational network based on new UTM technologies. *Applied Mechanics and Materials*. 40. p. 570-576.
- LIU, W. (2009). Research on DoS attack and detection programming. *Proceedings*. 2009 Third International Symposium on Intelligent Information Technology Application. p. 207-210.
- LUKER, M. A. & PETERSEN, R. J. (2003). *Computer and network security in higher education*. San Francisco: Jossey-Bass.
- MA, J., MA, T., LI, H., LI, X. & YANG, J. (2016). Research on security management of computer network system. *Proceedings*. 2<sup>nd</sup> International Conference on Advances in Mechanical Engineering and Industrial Informatics (AMEII 2016). p. 292-295.
- MALIK, S. (2003). *Network security principles and practices (CCIE Professional Development)*. Indianapolis: Cisco Press.
- MANSHAEI, M. H., ZHU, Q., ALPCAN, T., BACSAR, T. & HUBAUX, J. P. (2013). Game theory meets network security and privacy. *ACM Computing Survey (CSUR)*. 45(3). p. 25.
- MASON, A. G. (2002). *Cisco secure virtual private network*. Indianapolis: Cisco Press.
- MARCHANY, R. (2014). *Higher education: open and secure*. [Online] Available from: <http://www.sans.org/reading-room/whitepapers/analyst/higher-education-open-secure-35240> [Accessed: 23/02/2015]
- MASROM, M. & ISMAIL, Z. (2008). Computer security and computer ethics awareness: a component of management information system. *Proceedings*. 2008 International Symposium on information Technology (ITSim 2008). 3. p. 1-7.
- MATESKI, M., TREVINO, C.M., VEITCH, C.K., MICHALSKI, J., HARRIS, J.M., MARUOKA, S. & FRYE, J. (2012). *Cyber Threat Metrics*. Sandia Report. Albuquerque: Sandia National Laboratories.

- MAXWELL, J. A. (2013). *Qualitative research design: an interactive approach*. 3<sup>rd</sup> ed. London: Sage.
- MAY, L. & LANE, T. (2006). A model for improving e-security in Australian universities. *Journal of Theoretical and Applied Electronic Commerce Research*. 1(2). p. 90-96.
- MCGEE, A. R., VASIREDDY, R. S., XIE, C., PICKLESIMER, D. D., CHANDRASHEKHAR, U. & RICHMAN, S. H. (2004). A framework for ensuring network security. *Bell Labs Technical Journal*. 8(4). p. 7-27.
- MCILWRAITH, A. (2006). *Information security and employee behaviour: how to reduce risk through employee, training, and awareness*. England: Gower Publishing Limited.
- MCMAMARA, J. F. (1994). *Surveys and experiments in education research*. Lancaster, Pennsylvania: Technomic.
- MEETA, P. J. D. (2011). Intrusion detection and prevention system. *International journal of Advances in Computer Networks and its Security*. 1(1). p. 264-268.
- MENDYK-KRAJEWSKA, T. & MAZUR, Z. (2010). Problem of network security threats. *Proceedings*. 2010 3<sup>rd</sup> Conference on Human System Interactions (HSI). p. 436-443.
- MICROSOFT TECHNET. (2003). *What is VPN?* [Online] Available from: [https://technet.microsoft.com/en-us/library/cc739294\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc739294(v=ws.10).aspx) [Accessed: 06/11/2015]
- MIRKOVIC, J. & REIHER, P. (2004). A taxonomy of DDoS attack and DDoS defence mechanisms. *ACM SIGCOMM Computer Communications Review*. 34(2). p. 39-53.
- MORROW, B. (2012). BYOD security challenges: control and protect your most sensitive data. *Network Security*. 2012(12). p. 5-8.
- MUIJS, D. (2010). *Doing quantitative research in education with SPSS*. 2<sup>nd</sup> ed. London: Sage.
- MUKHTAR, H., SALAH, K. & IRAQI, Y. (2012). Mitigation of DHCP starvation attack. *Computers & Electrical Engineering*. 38(5). p. 1115-1128.
- MUNHALL, P. L. (2012). *Nursing research: a qualitative perspective*. 5<sup>th</sup> ed. Sudbury, Massachusetts: Jones & Bartlett Learning.
- MURPHY, R. (2014). *Usability and network security in higher education*. [Online] Available from: <http://www.educause.edu/blogs/vvogel/usability-and-network-security-higher-education> [Accessed: 07/03/2015]

- MUSIL, S. (2014). *Data breach at University of Maryland exposes 300K records*. [Online] Available from: <http://www.cnet.com/news/data-breach-at-university-of-maryland-exposes-300k-records/>. [Accessed: 02/09/2015]
- NAM, S. Y., KIM, D. & KIM, J. (2010). Enhanced ARP: preventing ARP poisoning-based man-in-the-middle attacks. *IEEE communications letters*. 14(2). p. 187-189.
- NEUMAN, W. L. (2011). *Social research methods: Qualitative and quantitative approaches*. 7<sup>th</sup> ed. Boston: Allyn and Bacon.
- NOGUCHI, Y. (2005). *George mason official investigate hacking incident*. [Online] Available from: <http://www.washingtonpost.com/wp-dyn/articles/A5188-2005Jan12.html?referrer=email> [Accessed: 12/08/2015]
- NURSE, J. R. C., BUCKLEY, O., LEGG, P. A., GOLDSMITH, M., CREESE, S., WRIGHT, G. R. T. & WHITTY, M. (2014). Understanding insider threat: a framework for characterising attacks. *Proceedings. 2014 IEEE Security and Privacy Workshops (SPW)*. p. 214-228.
- OMOTAYO, B. O. & AJAYI. N. A. (2006). An appraisal of security measures in Hezekiah Oluwasanmi Library. *Nigerian Libraries*. 39. p. 65-78.
- ONG, L. & CHONG, C. (2014). Information security awareness: an application of psychological factors – a study in Malaysia. *Proceedings. International Conference on Computer, Communications and Information Technology (CCIT 2014)*. p. 98-101.
- ONWUBIKO, C. & LENAGHAN, A. P. (2007). Managing security threats and vulnerabilities for small to medium enterprises. *Proceedings. 2007 IEEE Intelligence and Security Informatics*. p. 244-249.
- OSTAPENKO, A. G., KULIKOV, S. S., TOLSTYKH, N. N., PASTERNAK, Y. G. & POPOVA, L. G. (2013). Denial of service in components of Information Telecommunication Systems through the Example of “Network storm” attacks. *World Applied Sciences Journal*. 25(3). p. 404-409.
- PALMER, M. (2009). *Hands-on Microsoft windows server 2008*. Boston: Cengage Learning.
- PAQUET, C. (2013). *Implementing Cisco IOS network security (IINS): Foundation learning guide*. 2<sup>nd</sup> ed. Indianapolis, Indiana: Cisco Press.
- PFLEEGER, C. F., PFLEEGER, S. L. & MARGULIES, J. (2015). *Security in computing*. 5<sup>th</sup> ed. Upper Saddle River: Prentice Hall.
- PHAM, H. C., PHAM, D. D., BRENNAN, L. & RICHARDSON, J. (2017). Information security and people: a conundrum for compliance. *Australasian Journal of Information Systems*. 21. p. 1-16.

- PIAZZA, P. (2006). Security goes to school. *Security Management*. 50(12). p. 46-51.
- POLIT, D. F., BECK, C. T. & HUNGLER, B. P. (2001). *Essentials of nursing research: methods, appraisal and utilization*. 5<sup>th</sup> ed. Philadelphia: Lippincott.
- POSTINDEPENDENT. (2007). *CU computer hacked, 45k student names, S.S. numbers exposed*. [Online] Available from: <http://www.postindependent.com/article/20070523/FRONTPAGE/70523002> [Accessed: 16/08/2015]
- PRABHAKAR, S. (2017). Network security in digitalisation: attacks and defence. *International Journal of Research in Computer Applications and Robotics*. 5(5). p. 46-52.
- QADER, N. N. (2016). Boosting authentication security by building strong password and individualising easy to remember techniques. *Journal of University of Human Development*. 2(3). p. 520-527.
- RAMAN, A., KABIR, F., HEJAZI, S. & AGGARWAL, K. (2016). Cybersecurity in higher education: the changing threat landscape. *Performance*. 8(3). p. 46-53.
- RAMZAN, Z. (2010). *Phishing attacks and countermeasures*. In Stravroulakis, P. & Stamp, M. (eds). *Handbook of information and communication security*. New York: Springer.
- RANJAN, S., SWAMINATHAN, R., UYSAL, M. & KNIGHTLY, E. (2006). DDoS-resilient scheduling to counter application layer attacks under imperfect detection. *Proceedings. 25<sup>th</sup> IEEE International Conference on Computer Communications (INFOCOM 2006)*. p. 1-13.
- READ, B. (2002). *Delaware student allegedly changed her grades online*. [Online] Available from: <https://chronicle.com/article/Delaware-Student-Allegedly/19846> [Accessed: 15/08/2015]
- REGAN, P. (2013). *Administering Windows server 2012*. Hoboken: John Wiley & Sons.
- REID, A. & LORENZ, J. (2008). *Networking for home and small business: CCNA discovery learning guide*. Indianapolis: Cisco Press.
- REMENYI, D., WILLIAMS, B., MONEY, A. & SWARTZ, E. (1998). *Doing research in business and management: an introduction to process and method*. London: Sage.
- REZGUI, Y. & MARKS, A. (2008). Information security awareness in higher education: an exploratory study. *Computers & Security*. 27(7). p. 241-253.
- RICHEY, R. C. & KLEIN, J. D. (2014). *Design and development research*. In Spector, J.M., Merrill, M. D., Elen, J. & Bishop, M. J. (eds). *Handbook of research on educational communications and technology*. New York: Springer.

- RISK BASED SECURITY. (2016). *2015 Data breach quickview*. [Online] Available from: <https://www.riskbasedsecurity.com/2015-data-breach-quickview/> [Accessed: 31/03/2016]
- RISTIC, I. (2010). *Modsecurity handbook*. London: Feisty Duck.
- ROBSON, C. & MCCARTAN, K. (2015). *Real world research*. 4<sup>th</sup> ed. Oxford: Wiley.
- ROMAN, J. (2014). *Add Butler University to breach list-Latest incident highlights breach vulnerabilities in academia*. [Online] Available from: <http://www.databreachtoday.com/add-butler-university-to-breach-list-a-7007> [Accessed: 31/03/2015]
- RUFFOLO, R. (2009). *Ryerson privacy breach highlights immature IT, analyst says*. [Online] Available from: <http://www.itworldcanada.com/article/ryerson-privacy-breach-highlights-immature-it-analyst-says/11040> [Accessed: 26/01/2016]
- SAFA, N. S., VON SOLMS, R. & FURNELL, S. (2016). Information security policy compliance model in organisations. *Computers & Security*. 56. p. 70-82.
- SANDOVAL, G. (2006). *University server in hackers' hands for a year*. [Online] Available from: <http://www.cnet.com/news/university-server-in-hackers-hands-for-a-year/>. [Accessed: 09/08/2015]
- SARKAR, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report*. 15(3). p. 112-133.
- SARKAR, S. & BRINDHA, M. (2014). High performance network security using NIDS approach. *International Journal of Information Technology and Computer Science (IJITCS)*. 6(7). p. 47-55.
- SAUNDERS, M., LEWIS, P. & THORNHILL, A. (2009). *Research methods for business students*. 5<sup>th</sup> ed. Harlow: Pearson Education.
- SCARFÒ, A. (2012). New security perspectives around BYOD. *Proceedings. 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA)*. p. 446-451.
- SEKARAN, U. & BOUGIE, R. (2010). *Research methods for business: a skill building approach*. 5<sup>th</sup> ed. West Sussex: John Wiley & Sons.
- SHARMA, A. & SINGHROVA, A. (2011). A host based intrusion detection system for DDoS attack in WLAN. *Proceedings. 2011 2<sup>nd</sup> International Conference on Computer and Communication Technology (ICCCT)*. p. 433-438.

- SHARMA, S., GUPTA, A. & AGRAWAL, S. (2016). An intrusion detection system for detecting denial-of-service attack in cloud using artificial bee colony. *Proceedings. International Congress on Information and Communication Technology*. p. 137-145.
- SINGH, U. K., JOSHI, C. & GAUD, N. (2016). Measurement of security dangers in university network. *International Journal of Computer Applications*. 155(1). p. 6-10.
- SNORT. *Snort FAQ*. [Online] Available from: [https:// www.snort.org/faq/what-is-snort](https://www.snort.org/faq/what-is-snort) [Accessed: 22/06/2015].
- SONG, D. & MA, F. (2012). Strategy and implementation of campus network security. *Proceedings. 2012 International Conference on Systems and Informatics (ICSAI)*. p. 1017-1019.
- SPITZNER, L. (2003). *Honeypots: Tracking hackers*. New York: Addison-Wesley.
- TASHAKKORI, A. & TEDDLIE, C. (1998). *Mixed methodology: combining qualitative and quantitative approaches*. London: Sage.
- TIWARI, R. & JAIN, A. (2012). Improving network security and design using honeypots. *Proceedings. The CUBE International Information Technology Conference 2012*. p. 847-852.
- TSAI, P. (2015). *Is your IT department overworked and understaffed?* [Online] Available from: <http://www.itproportal.com/2015/12/12/is-your-it-department-overworked-understaffed/> [Accessed: 15/11/2016]
- TSOHOU, A., KARYDA, M. & KOKOLAKIS, S. (2015). Analysing the role of cognitive and cultural biases in the internationalisation of information security policies: recommendations for information security awareness programs. *Computers & Security*. 52. p. 128-141.
- TROCHIM, W. M. & DONNELLY, J. P. (2006). *The Research methods knowledge base*. 3<sup>rd</sup> ed. Cincinnati: Atomic Dog.
- UNIVERSITY OF HAWAI'I SYSTEM. (2009). *Kapiolani Community College students warned of Internet security breach*. [Online] Available from: <http://www.hawaii.edu/news/article.php?ald=2848> [Accessed: 02/09/2015]
- UPDEGROVE, D. & WISHON, G. (2003). Foreword. In Luker, M. A. & Petersen, R. J. (eds). *Computer and Network Security in Higher Education*. San Francisco: Jossey-Bass.
- VACHON, B. (2012). *CCNA security portable command guide*. Indianapolis: Cisco Press.
- VAN, N. T., THINH, T. N. & SACH, L. T. (2017). An anomaly-based network intrusion detection system using Deep learning. *Proceedings. 2017 International Conference on Systems Science and Engineering (ICSSE)*. p. 210-214.



- VANCE, A. (2010). *If your password is 123456, Just make it HackMe*. [Online] Available from: [http://www.nytimes.com/2010/01/21/technology/21password.html?\\_r=0](http://www.nytimes.com/2010/01/21/technology/21password.html?_r=0) [Accessed: 20/08/2015]
- VARMA, P. R. K., KUMARI, V. V. & KUMAR, S. S. (2017). Packet filter firewall rule anomalies and mitigation techniques: a technical review. *Networking and Communication Engineering*. 9(4). p. 101-108.
- VEAL, A. J. (2011). *Research methods for leisure and tourism: Practical guide*. 4<sup>th</sup> ed. Harlow: Prentice Hall.
- VERIZON. (2015). *2015 Data breach investigation report*. [Online] Available from: <http://www.verizonenterprise.com/DBIR/2015/> [Accessed: 22/09/2015]
- VIJAYAN, J. (2006). *Ohio University reports two separate security breaches*. [Online] Available from: <http://www.computerworld.com/article/2555130/security0/ohio-university-reports-two-separate-security-breaches.html> [Accessed: 17/08/2015]
- VON SOLMS, R. & VON SOLMS, B. (2004). From policies to culture. *Computer & Security*. 23(4). p. 275-279.
- WANG, L. & JONES, R. (2017). Big data analytics for network intrusion detection: a survey. *International Journal of Networks and Communications*. 7(1). p. 24-31.
- WANG, W. & BATTITI, R. (2006). Identifying Intrusions in Computer Networks with Principal Component Analysis. *Proceedings*. First International Conference on Availability, Reliability, and Security. p. 8.
- WANG, J. & LIU, X. (2011). Computer network security of university and preventive strategy. *Proceedings*. 2011 IEEE 3<sup>rd</sup> International Conference on Communication Software and Networks (ICCSN). p. 143-145.
- WARKENTIN, M., JOHNSTON, A. C., WALDEN, E. & STRAUB, D. W. (2016). Neural correlates of protection motivation for secure IT behaviours: an fMRI examination. *Journal of the Association for Information Systems*. 17(3). p. 194-215.
- WATTANAPONGSAKORN, N., SKRAKAEW, S. & CHARNSRIPINYO, C. (2012). A practical network-based intrusion detection and prevention system. *Proceedings*. 2012 IEEE 11<sup>th</sup> International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). p. 209-214.
- WEBB, E. J., CAMPBELL, D. T., SCHWARTZ, R. D. & SECHREST, L. (1966). *Unobtrusive measure: nonreactive measures in the social sciences*. Chicago: Rand McNally.
- WEI, K., MUTHUPRASANNA, M. & KOTHARI, S. (2006). Preventing SQL injection attacks in stored procedures. *Proceedings*. Australian Software Engineering Conference. p. 8-15.

- WELMAN, C., KRUGER, F. & MITCHELL, B. (2007). *Research methodology*. 3<sup>rd</sup> ed. Cape Town: Oxford University: Press Southern Africa.
- WHITE, T. L. & MCBURNEY, D. H. (2012). *Research methods*. 9<sup>th</sup> ed. Belmont, California: Thomson Wadsworth.
- WHITMAN, M. E. & MATTORD, H. J. (2012). *Principles of information security*. 4<sup>th</sup> ed. Boston, Massachusetts: Cengage Learning.
- WILLISON, R. & SIPONEN, M. (2009). Overcoming the insider: reducing employee computer crime through situational crime prevention. *Communications of the ACM*. 52(9). p. 133-137.
- WILSON, J. (2014). *Essentials of business research: a guide to doing your research study*. 2<sup>nd</sup> ed. London: Sage.
- WU, C. (2010). The problems in campus network information security and its solutions. 2<sup>nd</sup> *International Conference on Industrial and Information Systems*. 1. p. 261-264.
- YI, H. & YIFEI, Z. (2010). Research of campus network security system based on intrusion detection. *2010 International Conference on Computer Design and Applications (ICCD 2010)*. 4. p. 618-621.
- YU, Y., WANG, Q. & JIANG, Y. (2010). Research on security of the WLAN campus network. *2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies (EDT)*. 2. p. 175-178.
- YU, Z. & TSAI, J. J. P. (2011). *Intrusion detection: A machine learning approach*. London: Imperial College Press.
- ZACKER, C. (2014). *Installing and configuring Windows Server 2012 R2 Exam 70-410*. Hoboken: John Wiley & Sons.
- ZARGAR, S. T., JOSHI, J. & TIPPER, D. (2013). A survey of defence mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials*. 15(4). p. 2046-2069.
- ZHAO, H., XU, M., ZHENG, N., YAO, J. & HO, J. (2010). Malicious executables classification based on behavioural factor analysis. *Proceedings. International Conference on e-Education, e-Business, e-Management and e-Learning*. p. 502-506.
- ZHENGBING, H., SHIROCHIN, V. P. & JUN, S. (2005) An intelligent lightweight intrusion detection system (IDS). *Proceedings. 2005 IEEE Region 10 TENCN*. p. 1-7.

## ANNEXURE A: Informed Letter of Consent for Participant



**Vaal University of Technology**

**FACULTY OF APPLIED AND COMPUTER SCIENCES**

**INFORMATION AND COMMUNICATIONS TECHNOLOGY DEPARTMENT**

### **Informed Letter of Consent for Research Participant**

**Title of the research study:** A framework for higher academic institutions in the Republic of South Africa to mitigate network security threats and attacks

**Name of researcher:** Matrinta Josephine Mohapi

**Contact details:** Email: mmotajosie@gmail.com Phone: 082 434 9994

**Name of supervisor:** Prof Annelie Jordaan

**Contact details:** Email: annjor@yebo.co.za Phone: 082 084 0385

**Purpose of the study:** To determine possible ways that can enhance and increase network security in academic institutions by combating network security threats and attacks.

**Participation:** The participation will primarily involve Information Technology (IT) specialised or technical security personnel at higher academic institutions in Gauteng.

**Confidentiality and Anonymity:** The information you will provide for this survey will be kept confidential, anonymous and only be used for the purpose of this research study. The data collected will be stored on a computer that is password-protected to restrict access. It is important to note that no participant can be identified as the data collected will be summarised.

**Voluntary participation:** Participation in this research study is completely voluntary. Should you choose to participate, you are kindly requested to sign the consent form. If at any stage you decide to withdraw your participation to this study, you are free to do so without any negative consequences.

**Consent of participant:** I fully understand and acknowledge the information provided above and that I can freely withdraw my participation at any time. Therefore, I agree to voluntarily participate in this study.

If there are any questions concerning the study, you may contact the researcher or the supervisor for clarity. For any concerns relating to ethical conduct which may result from participating in this study, you may freely contact Research Administrator, **Musonda Kaniki** at 016 950 9004 or musondak@vut.ac.za.

---

Participant's signature/Print Name

---

Date

---

Researcher's signature/Print Name

---

Date

## ANNEXURE B: Network Security Questionnaire

### Network Security Questionnaire at Higher Academic Institutions

Thank you for taking this Network Security Questionnaire. This questionnaire will help the researcher better understand challenges that you are experiencing in your institution and help to identify the network security threats and attacks. This questionnaire should take you no more than 30 minutes to complete and your responses will remain anonymous. Questions related to this questionnaire can be addressed to Ms MJ Mohapi at [mmotajosie@gmail.com](mailto:mmotajosie@gmail.com). Thank you for your participation.

#### SECTION A – DEMOGRAPHIC DATA (*please mark with X to indicate your answer*)

1. **Gender:** Male ☐ Female ☐
2. **Age:** 18-24 ☐ 25-34 ☐ 35-44 ☐ 45-54 ☐ Over 54 ☐
3. **Position:**
- |   |                          |
|---|--------------------------|
| IT Manager / IT Director/Security Director    | <input type="checkbox"/> |
| System Engineer / Network Engineer            | <input type="checkbox"/> |
| System Administrator / Security Administrator | <input type="checkbox"/> |
| Network Administrator/ Network Operator       | <input type="checkbox"/> |
| Security Analyst/ Security Manager            | <input type="checkbox"/> |
| Compliance Auditor/ Compliance Officer        | <input type="checkbox"/> |
| Other: ( <i>Please specify</i> ) _____        |                          |

4. Please indicate your highest qualifications:	
PhD	<input type="checkbox"/>
DTech/Doctorate	<input type="checkbox"/>
MTech/Masters	<input type="checkbox"/>
Honours	<input type="checkbox"/>
BTech/Degree	<input type="checkbox"/>
National Diploma	<input type="checkbox"/>
Other: ( <i>Please specify</i> )	<input type="checkbox"/>

5. What type of higher academic institution do you work for?	
University of Technology	<input type="checkbox"/>
Traditional University	<input type="checkbox"/>
Comprehensive University	<input type="checkbox"/>
Private University	<input type="checkbox"/>
Public College	<input type="checkbox"/>
Private College	<input type="checkbox"/>

## SECTION B: NETWORK SECURITY CHALLENGES AND SECURITY TECHNOLOGIES

1. From a risk perspective, which systems are you most concerned with? <i>(Choose all that apply)</i>	Administrative database systems	
	Staff computers	
	Web servers	
	Research systems	
	Students owned computers	
	Staff and Students mobile devices	
Other: Specify		

2. Which attack vectors and security issues is your organisation most concerned with to protect against? <i>(Choose all that apply)</i>	Phishing attacks	
	Hacking incidents	
	Web-based attacks	
	Malware threats	
	Compliance issues	
	Social networking-based attacks	
	Exploits against database systems and servers	
	Misuse of data	
	Unknown	
Other: Specify		

3. Has your institution's network been internally or externally compromised within the past two years?	Yes	
	No	
	Not sure	

4. Does your institution have a well-designed and written network security policy?	Yes	
	No	
	Not sure	

5. Does your institution enforce network security policy to all network users?	Yes	
	No	
	Not sure	

6. Is the network security policy at your institution periodically being reviewed and updated to include security controls and standards that can help combat the latest network security threats and attacks?	Yes	
	No	
	Not sure	

7. Does your institution offer mandatory training and education on network security policy to users?	Yes	
	No	
	Not sure	

8. Are you satisfied with the budget allocated to the IT department in your institution for improving network security?	Very Dissatisfied (1)	
	Dissatisfied (2)	
	Neutral (3)	
	Satisfied (4)	
	Very Satisfied (5)	

9. How would you describe IT technical staffing at your institution?	Severely understaffed	
	Moderately understaffed	
	Staffed at about the right level	
	Moderately overstaffed	
	Severely overstaffed	

10. Do you think your institution needs to hire more IT technical staff?	Strongly Disagree (1)	
	Disagree (2)	
	Neither Agree nor Disagree (3)	
	Agree (4)	
	Strongly Agree (5)	

11. Does the IT department at your institution perform vulnerability assessment on the systems and network?	Yes	
	No	
	Not sure	

12. Does the IT department at your institution perform penetration testing to exploit vulnerabilities against the systems and network?	Yes	
	No	
	Not sure	

13. How often does the IT department perform vulnerability assessment or penetration testing to eliminate vulnerabilities, threats, and attacks?	Weekly	
	Monthly	
	Quarterly	
	Half-yearly	
	Yearly	
	Not at all or Not sure	

14. Does the IT department at your institution investigate and take remedial actions for reported security alerts and incidents?	Yes	
	No	
	Not sure	

15. Which of the following technologies, security measures, or controls are used by your institution? (Choose all that apply)	Firewalls	
	Network Access Controls	
	Virtual Private Network (VPN)	
	Intrusion Detection System(s) (IDS)	
	Intrusion Prevention System(s) (IPS)	
	All-in one security appliance	
	Monitoring tools	
	Encryption	
Malware Protection		
Other: Specify		

16. Please indicate your level of satisfaction on the intended operation of security technologies implemented at your institution:					
Rating					
	Very Dissatisfied (1)	Dissatisfied (2)	Neutral (3)	Satisfied (4)	Very Satisfied (5)
Firewalls					
Network Access Controls					
Virtual Private Network (VPN)					
Intrusion Detection System(s) (IDS)					
Intrusion Prevention System(s) (IPS)					
All-in-one security appliance					
Monitoring tools					
Encryption					
Malware Protection					