PENETRATION TESTING AND VULNERABILITY ASSESSMENT ON THE NAMIBIAN INTER-BANKING SYSTEM: NAMSWITCH

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE (INFORMATION TECHNOLOGY)

OF

THE UNIVERSITY OF NAMIBIA

BY

SION S. NGHOSHI
200627813

APRIL 2023

SUPERVISOR: PROF. WILLIAM SVERDLIK (School of Computing, University of Namibia)

ABSTRACT

Information Technology (IT) has become crucial to the operation of modern businesses. Financial service firms rely on IT to deliver services to their customers. In the Namibian context, the Bank of Namibia and the Payment Association of Namibia have discontinued the use of cheques as a payment method and provided Electronic Fund Transfers, cards, and electronic money as alternative payment methods. This means that the Namibian Payment System (NPS) now solely relies on IT in order to deliver services to its customers. The Namibian inter-banking system, known as Namswitch, is classified as an Information Service Provider to the NPS, enabling inter-communication between Namibian financial institutions. Often, the target of cyberattacks are financial institutions and hackers with malicious intents are continually attempting to infiltrate their IT systems. As such, the financial services industry has unique information security requirements, and banks in particular conduct more stringent due diligence and due care in order to ensure the confidentiality, integrity and availability of their services. In order to address these security challenges, this study sought to explore ways to proactively strengthen and enhance the cybersecurity of the Namswitch system by evaluating the system's security posture by proposing remedial actions, and further proposing a framework to automate and perform routine penetration tests in order to prevent future cyberattacks. The findings revealed the presence of vulnerabilities on the Namswitch system, some of which posed a high severity rating according to the CVSS risk rating. An example was the presence of default credentials on some internal systems and the use of low to medium strength ciphers on the external systems. A malicious user can leverage these vulnerabilities to perform attacks such as man-in-the-middle attacks. In an effort to strengthen the cybersecurity of the Namswitch system, the study provided a Namswitch Safe Financial Exchange (NAMSAFE) Protocol which is an algorithmic process aimed at remedying identified vulnerabilities and improving existing processes. It further outlines remedial strategies, risk mitigation steps, and compensating controls for vulnerabilities that could not be eliminated. Successfully implemented, NAMSAFE provides a prescriptive methodology for maintaining ongoing reliability and robustness to the Namibian banking system.

Keywords: cybersecurity, banking sector, pen testing, vulnerability assessments.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABREVIATIONS AND ACRONYMS IN THIS THESIS

Acronym/abbreviation	Description
AI –	Artificial Intelligence
APP –	Application
ATM –	Automated Teller Machine
BID-30 –	BoN Determination of Information Security
BoN –	Bank of Namibia
CEH –	Certified Ethical Hacker
CERT –	Computer Emergency Response Team
CGEIT –	Certified in the Governance of Enterprise
CGTF –	Corporate Governance Task Force
CIS –	Center for Internet Security
CISSP –	Certified Information Systems Security Professional
CISWG –	Corporate Information Security Working Group
CMSPSM –	Common Minimum Standards of Protective Security Measures
COBIT –	Control Objectives for Information and Related Technology
CPMI –	Committee on Payments and Market Infrastructures
CVE –	Common Vulnerabilities and Exposures.
CVSS –	Common Vulnerability Scoring System.
CPMI –	Committee on Payments and Market Infrastructures
CRISC –	Certified in Risk and Information Systems Control
CSIRT –	Computer Security Incident Response Team
DMZ –	Demilitarized Zone
DNS –	Domain Name Server
DDoS –	Distributed Denial of Service
EFT –	Electronic Funds Transfer
FIA –	Financial Intelligence Act
FMI –	Financial Market Infrastructures (
FFIEC –	Federal Financial Institutions Examination Council
GDPR –	General Data Protection Regulation
HTTPS –	Hypertext Transfer Protocol Secure
ICT –	Information and Communication Technology
IoT –	Internet of Things
IOSCO –	International Organization of Securities Commissions
IPS –	Intrusion Prevention System
IEC –	International Electrotechnical Commission
IT –	Information Technology
ITIL –	Information Technology Infrastructure Library
MITM –	Man-in-the-middle
MPLS –	Multiprotocol Label Switching,

NBCF – Namibia Banking Cybersecurity Framework
NDA – Non-Disclosure Agreement
NIST – National Institute of Standards and Technology
OWASP – Open Web Application Security Project (OWASP)
PAN – Payment Association of Namibia
PCI-DSS – Payment Card Industry Data Security Standard
POPI – Protection of Personal Information
POS – Point of Sale
PTC – Penetration Testing Framework
SIEM – Security Information and Event Management
SSL – Secure Socket Layer
SSO – Single Sign On
SIT – System Integration Testing
TLS – Transport Layer Security
SQL – Structure Query Language
UAT – User Acceptance Test
VPN – Virtual Private Network

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation and gratitude to the following people:

First and foremost, I want to express my gratitude to the heavenly Father, the Lord our God, the Almighty, for his unwavering love, protection, and provision of abundant health during my studies. Secondly, I would like to express my gratitude to Professor William Sverdlik, my supervisor, for his excellent assistance, guidance, encouragement, and counsel during the crafting of my thesis. Thirdly, I want would like to express my gratitude to the Namswitch system's IT personnel who agreed to take part in the research for their contribution to my research. I value their enthusiasm as well as their knowledgeable contributions.

I would also like to thank my fellow postgraduate students for their motivation, and inspiration during the course of my research. Finally, I would like to thank my family, with a special mention of my brother Severen Nghoshi, and close friends for their encouragement, understanding, and unwavering support.

To anybody else who has helped me directly or indirectly, I say thank you.

DEDICATION

To God Almighty, my mother Meme Paulina, my siblings, and my wife Bertha.

DECLARATION

I, Sion Nghoshi, hereby declare that this study is my own work and is a true reflection of my research, and that this work, or any part thereof has not been submitted for a degree at any other institution.

No part of this thesis/dissertation may be reproduced, stored in any retrieval system, or transmitted in any form, or by means (e.g., electronic, mechanical, photocopying, recording or otherwise) without the prior permission of the author, or The University of Namibia in that behalf.

I, Sion Nghoshi, grant The University of Namibia the right to reproduce this thesis in whole or in part, in any manner or format, which The University of Namibia may deem fit.

Full Name: Sion S. Nghoshi

Signature: __  _____ Date: ___April 2023_____

CHAPTER ONE

INTRODUCTION

This chapter introduces the study and provides an overview of the research topic, research problem, objectives, and significance of the study. The chapter further presents a brief overview of the research methodology used in this study. The chapter is concluded with an outline of the chapters in the thesis as well as a summary of this chapter.

1.1. Background of the study

As financial services grow exponentially in the cyber environment, the nature and the scale of the underlying cyber risks are evolving rapidly. The major contributing factors include the changing nature of technologies, increases in the deployment of financial technology commonly referred to as FinTech, aggressive lead times for launching electronic financial services, as well as the expanding roles of FinTech and IT service providers often operating outside the local regulatory ambit (TorontoCenter, 2018). According to a report by IBM X-Force Threat Intelligence Index, the financial sector alone was responsible for nearly a fifth of all cyberattacks in 2018. Moreover, financial services also face the highest costs amongst all industries while dealing with cyberattacks and their repercussions (IBM, 2019).

Namswitch, Namibia's inter-banking system, links several of the country's financial institutions. According to Tait (2017), Namswitch provides an Information Technology (IT) network that allows consumers to conduct inter-banking electronic transactions known as "Off Us" transactions. The system has been recognised as an Internet Service Provider (ISP) to the Namibian financial industry by the Namibian

Payment System (NPS). Tait (2017), highlights that any IT risk or vulnerability on the Namswitch system has the potential to disrupt the entire Namibian banking industry. As such, it is evident that the Namswitch system together with the banking systems create an IT ecosystem. Dragan (2017) states that IT is growing increasingly significant and more influential in all modern-day organisations. Dragan further states that while IT is paramount to every organisation, cyber threats resulting from the introduction of IT infrastructure and new skill sets are also on the increase. The key factor to the safe operation of any IT system is the protection from external and internal cyber threats (Godwin & Engebretson, 2014). Cybercriminals are everyday advancing their data exfiltration techniques and they are able to monetise data in several ways. IT systems may pose vulnerabilities, which are a weakness in an IT system that can be exploited by an attacker to compromise either integrity, availability or confidentiality of data (Reddy, 2018). Common types of vulnerabilities includes weak passwords, bugs, use of broken algorithms, missing or weak data encryption, the reliance on untrusted inputs in a security decision, misconfigured system components, etc.

Organisations wishing to ensure the security of their systems may look towards adopting appropriate measures to protect themselves against potential security breaches. Some of the measures are cybersecurity assessments, which are aimed at finding vulnerabilities present in an organisation's network, and providing recommendations as to how best to mitigate such risks. Cybersecurity assessments are crucial instruments that are used to prevent or minimise attacks on IT systems, through identifying possible vulnerabilities posed on IT systems. In addition, they also assist with predicting the impact of threats as well as to provide threat recovery options in order to mitigate future risks.

There exists a number of different types of security assessments such as IT audit, IT risk assessments, VPN assessments, social engineering assessments, Red teaming, vulnerability assessments, penetration tests, etc. However, due to limited time and the amount of work it would require performing all assessments, this study focused on assessing the Namswitch system through conducting a vulnerability assessment and a penetration test.

It pays to be proactive and having a preventive plan in place through periodically assessing IT security which is a great recipe for avoiding data breaches and consequently business disasters. The purpose of this study was to act proactively by analysing Namswitch system's security posture by conducting a penetration test and vulnerability assessment on the Namswitch system. The identified vulnerabilities were addressed with a sequence of remediation techniques. The research also created a NAMSAFE Protocol, which is an algorithmic procedure that is aimed at remediating the exposed flaws as well as improving current procedures and methodologies. Within the Namswitch ecosystem and the Namibian financial industry, the research also established and ensured a tested and secured cyber environment. Finally, the study was aimed at improving the Namswitch system's security posture.

1.2. Statement of the problem

The reliance of modern organisations on IT is growing every day. Many organisations require around-the-clock terms of service. This dependence on IT implies that security is paramount to the success of the enterprise since financial institutions are frequent targets of attacks (Izagirre et al., 2017). Although this might be the case, some institutions are oblivious to how vulnerable their systems are to attacks, while other

organisations fail to conduct frequent and periodic security checks on their systems and network infrastructures. It has been documented that enterprises often respond to security incidents rather than proactively testing and protecting their systems (Khari, 2015). Some financial institutions do not test their systems' tolerance to real-world attack patterns or they underestimate the wide range of easily available sophisticated tools to accomplish the mission with little expertise on the attacker's side.

While there are lots of different types of attacks, according a report published Fortinet (2021), denial-of-service (DoS), which is an attack that is designed to overwhelm the resources of a system to the extent where it is unable to reply to legitimate service requests and a distributed denial-of-service attack (DDoS). The DDoS is initiated by a vast array of malware-infected host machines controlled by the attacker and this appears to be the most common type of cyberattacks. The report further indicates that Man-in-the-middle (MITM) types of cyberattacks, in which an attacker eavesdrops on the data sent between two devices appears to be the second most common type of attack. Malware attacks, which can be any malicious software viruses including worms, spyware, ransomware, adware, and Trojans that breaches a system through a vulnerability. Examples of cyberattacks are unauthorised access, electronic fraud, identity theft, etc.

Attacks on the financial systems in Namibia are not uncommon, particularly in light of the rise in cybercrimes and the adoption of new systems (Tait, 2017). As such, it is crucial and essential to be predictive and proactive rather than reactive. Similarly, there is a vital need to verify the strengths and weaknesses of the Namswitch system in terms of its ability to detect cyberattacks and to ensure that it is protected from current threats

such as ransomware, etc. which usually have catastrophic effects on systems. There is also a need to validate the Namswitch system's ability to respond appropriately to attacks, and to deploy countermeasures to mitigate threats. Thus it is evident that there is a need to remain current with hacking practices, compile the latest cyber defence approaches, and find the latest compensating controls to mitigate and protect against cyber threats. In this study, proactive measures aimed at identifying vulnerabilities were employed and the study devised remediation strategies to mitigate the identified vulnerabilities.

1.3. Objectives of the study

The objectives of this study were to:

a) Develop a pen test and vulnerability assessment methodology for the Namswitch system;
b) Conduct a penetration test to expose vulnerabilities in the Namswitch system's architecture and report potential impact.
c) Assess the security of the Namswitch system's configurations against best practices, standards, and current practices; and
d) Investigate and suggest appropriate mitigation strategies to remediate issues identified and provide a standard practice protocol on security for Namswitch.

1.4. Significance of the study

The study was aimed at enhancing Namswitch system's security posture by proactively identifying vulnerabilities within the system. Through conducting pen tests and vulnerability assessments, this study determined the security posture of the Namibian inter-banking system. Furthermore, the study provided corrective measures

which were aimed at removing the identified vulnerabilities. The study further aided Namswitch officials to implement the developed standard practice protocol named the NAMSAFE Protocol, which can periodically and proactively mitigate the cyber threats to the Namswitch system and ensuring the long-term viability and reliability of the Namibian banking system.

1.5. Limitations of the study

The study was limited to all the Namswitch systems and networks in the development environment known as the system integration testing (SIT) environment. All the systems and networks in testing environment called the user acceptance testing (UAT) environment, as well as some systems and networks in the production environment which are not publicly accessible. This was due to security, confidentiality, and time constraints. The results obtained from these environments imply the security posture of the production environment, since the security configurations on the SIT and UAT environment systems and networks replicate those of the production environment.

Access to certain data was restricted due to the sensitivity of the information and fear of compromising confidentiality and integrity. All these factors hindered the access to sufficient and comprehensive data.

1.6. Delimitation of the study

This study was limited to Namibian financial institutions, primarily those connected to the Namswitch inter-banking system.

1.7. Research methodology

To achieve the study's goals, the study was designed to use both qualitative and quantitative research methods. For this reason, a hybrid research approach was employed.

This research used quantitative research methods by employing correlational research approaches in order to identify and categorise aspects of the many threats and vulnerabilities discovered, as well as to create statistical models and figures to illustrate the study's findings. Furthermore, quantitative methods were used to conduct pen tests and vulnerability assessments to establish how securely the Namibian interbank systems are configured, as well as the security posture of the Namswitch systems using an experimental approach.

Finally, qualitative approaches were also employed in this study by means of the grounded theory research approach, which was used to collect the extensive data required to create a pen test and vulnerability assessment. The research approach was also used to gather data for the development of appropriate mitigation methods and compensating controls.

The Network mapper (Nmap), OpenVAS and the OpenSSL tools were used to conduct a pen tests and vulnerability assessments. The severity of the common risks and vulnerabilities discovered was graded using the Common Vulnerability Scoring System (CVSS).

1.8. Definition of terms

This section consists of the core terminologies used in the thesis. Although the terminologies may have multiple definitions in the literature, for the purpose of this study, the following definitions apply.

Cybercrime: is referred to as any illegal behaviour targeting the security of computer systems and the processed data directed by means of electronic operations (Ayofe & Irwin, 2010).

Cyber security: is the collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that could be used to protect the cyber environment, organisation, and user assets (ITU, 2019).

Risk: is the potential loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability. A risk is the likelihood of something unpleasant happening.

Threat: is an object, person, or other entity that represents a constant danger to an asset (Whitman & Mattord, 2021). It is anything that could exploit a vulnerability, intentionally or accidentally and could damage or destroy an asset.

Vulnerability: is a weakness or gap in our protection efforts. It is a defect or weakness in an information asset, security procedure, technical design or control that a threat might exploit on purpose or even accidentally, in order to breach a security system (Jounia et al., 2014).

1.9. Outline of the thesis

The thesis is organised into seven chapters as follows:

Chapter one introduces the research carried out, the statement of the problem, research objectives, significance of the study, and limitations of the study, followed by a summary of the research methodology, the definition of terms, and lastly the outline of the mini-thesis.

Chapter two reviews literature relating to the study.

Chapter three discusses the research methods used in the study.

Chapter four provides the tests conducted and also presents the results of the security assessment.

Chapter five provides an in-depth discussion of the research findings.

Chapter six discusses the risk mitigations, compensating controls, and remediation steps that could be implemented in order to eliminate or mitigate the identified vulnerabilities and it provides recommendations for future studies.

Chapter seven concludes the study.

1.10 Chapter summary

The study was introduced in this chapter. The background to the study, the problem description, the aims, and the significance of this study were all addressed in this chapter. The research objectives and methods were also summarised in this chapter. The next chapter reviews related literature to understand inter-banking systems and the threats and vulnerabilities against financial systems.

CHAPTER TWO

LITERATURE REVIEW

This chapter provides a description of the Namswitch system, as well as the various security tools and methodologies used in the financial sector for IT risk evaluations and penetration testing. The chapter also discusses the different kinds of cyber-attacks, and different types of IT security audits. The chapter is then concluded with a rundown of the benefits of security assessments, as well as a discussion of security reviews and regulatory enforcements.

2.1 Introduction

This chapter examines related works of literature in terms of the topic in discussion. It also serves as a foundation for sources of expertise on conducting and analysing the study's results. Reviewing the literature entails a thorough and objective examination of prior studies. It is a summary and analysis of a specific research field and enables readers to read the paper and assess whether a particular study is being undertaken (Fouton & Krainovich-Miller, 2016). The chapter summarises different literature on the different types of security assessments and methodologies, security policies, and best security practices for IT systems. Lastly, the chapter summarises vulnerability and weakness analysis, and classification.

2.2 Overview of Namswitch

Previously, the South African switching system, SAswitch, was responsible for switching Namibia's domestic electronic interbank transactions as part of the South African clearing and settlement process (Tait, 2017). As a sovereign state and

autonomous entity, Namibia began to monitor and manage its domestic risks and exposure in the financial sector (Alweendo, 2010). In 2000, the Bank of Namibia (BON) assigned a National Payment Reform programme to the Bankers Association of Namibia (BAN) which serves all commercial banks in Namibia. The reform project's goals were to abolish SAswitch from the NPS and replace it with an in-house interbank settlements mechanism which would come to be known as Namswitch. Namswitch is a Namibian clearing system that resolves all domestic interbank transactions through the Namibia inter-bank Settlement System (Tait, 2017).

In 2001, Namibia's Namswitch system, which cleared and settled domestic interbank cards transactions under the name Namibia's Card System, was implemented. Namswitch launched in two parts since the transactions, services, and processes involved were complex (Alweendo, 2010). Specifically, the Automated Teller Machines (ATM), which switches transactions done at ATMs and Point-Of-Sale (POS), switches transactions made at POS machines across the country. Namswitch expanded the NPS to include the clearing and payment of cheques in addition to card purchases.

The Namswitch expanded the list of its operations to include the clearing and settling of Electronic File Transmission (EFT) transactions, which include features like Enhanced Electronic File Transmission (EEFT) and Near Real Time Clearing (NRTC). However, in June 2019, the BON and the Payment Association of Namibia (PAN) declared that cheques would no longer be accepted as a form of payment under the NPS. Cheques have risks that are associated with them, including the possibility

of theft, hence their use as a payment method had to be discontinued (Tait, 2017). Namswitch was subsequently listed by the NPS as an Information Service Provider (ISP), enabling interbank transactions between Namibian financial institutions.

2.3 Namswitch ecosystem

The Namswitch IT ecosystem consists of the infrastructure of all banks in Namibia. This includes systems, applications, and networking equipment interconnected via a Multiprotocol Label Switching (MPLS) backbone network. In a nutshell, the ecosystem is made up of various instruments, processes, and technologies. All the banks apply similar infrastructural and security configurations based on agreed upon and predefined standards, even though each bank uses a different technology (Tait, 2017). The inter-banking ecosystem is made up of various information technology infrastructures that work together to achieve a shared goal, which is to interconnect banking systems, enable and facilitate seamless transactions between banks.

2.4 Cybersecurity threats, attacks, vulnerabilities and solutions in general

Cybersecurity threats continue to grow and evolve in complexity, vector and frequency (Ozkaya, 2019). The numerous ways in which computer systems and data can be compromised has made cyber security a growing field. Furthermore, Obotivere and Nwaezeigwe (2020) confirm that ever-more sophisticated cyberattacks involving malware, phishing, machine learning and artificial intelligence, cryptocurrency and more have placed the data and assets of corporations, governments and individuals at constant risk. The progress of digital transformation has inevitably led to new cybersecurity threats posing high risk to organisations and specifically with regards to

exfiltration of data. The consequences of cyber security or data breaches can be severe. McDonough (2019) confirm that cybersecurity breaches can have dire consequences such as reputational damages that can potentially lead to loss of customers, loss of sales and reduction in profits. McDonough (2019) went on to discuss additional effects, including the potential loss of intellectual property. Moreover, the General Data Protection Regulation (GDPR) and Data Protection Act (2018) require appropriate technical and organisational security and the consequences of non-compliance often results in a fine, again incurring financial loss on an organisation.

2.4.1 Cyber attacks

Mostly, cyberattacks succeed due to the presence of vulnerabilities in a system. Some of the most common software vulnerabilities includes injections flaws such as the Structured Query Language (SQL), Operating Systems (OS) and Lightweight Directory Access Protocol (LDAP) injections occur when suspicious or infected data is unknowingly received by a user as part of a request or order. Additionally, notable common vulnerability includes the broken authentication and session management vulnerabilities caused by wrongly implemented codes which provides a way for attackers to compromise credentials such as passwords and logins, keys, or session tokens (Maistry et al., 2019).

There exists nine prime threat groups as published by a report by the European Union Agency for Cybersecurity (2021). These include, Ransomware, Cryptojacking, Threats against data, Malware, Disinformation/misinformation, Non-malicious threats, Threats against availability and integrity, Email-related threats and Supply chain threats. Obotivere and Nwaezeigwe (2020) concur that the latest common types

of cyberattacks are injection attacks, session hijacking which is a security attack on a user session over a protected network. Web applications attacks are another form of attack that create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

Phishing is another type of cyberattack. It happens when an attacker is masquerading as a trustworthy entity in electronic communication, and attempts to steal sensitive information like user login credentials and credit card number. Furthermore, brute force is an attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organisation's network security.

DNS Spoofing is an attack in which data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer. Denial of Service (DOS) is another attack which is meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending in information that triggers a crash. Malware is a system-based attack which is intended to compromise a computer or a computer network.

2.4.2 Cybersecurity solutions

Traditional security controls can be employed to protect against cyberattacks. Maistry et al. (2019) indicate some of the countermeasures to cyberattacks. Firstly, it's the user's awareness training to be aware of the kinds of attacks that are likely to occur within their cyber space. Secondly, are legal responses which prohibit all attacks.

Thirdly, is patching which ensures that security updates are installed to protect against known vulnerabilities. Fourthly, is the use of strong cryptography to ensure that data in transit or at rest is encrypted with strong algorithms and access controls such as the use of two-factor authentications. Lastly, is the use of intrusion prevention systems to periodically and automatically detect instructions.

Tiirmaa-Klaar (2011) emphasise that in addition to the traditional controls, it is imperative to conduct security audits in order to test the strength of any IT system. These include risk audits, pen test and vulnerability assessments. This enables an organisation to test and proactively enhance the security of their systems through the identified security gaps.

2.4.2 Cybersecurity in emerging technology

The new systems or applications and technologies often come with security enhancements and security features such as strong cryptography, identity controls and software mediated contracts. They regularly offer significant levels of data protection and integrity. However, despite these security enhancements, there has been rife with security concerns within new technologies. New technologies come with new tools and methods for exploitation (Obotivere & Nwaezeigwe, 2020). A new class of cyber threats is emerging, involving tactics that are unique to new technologies. These include Blockchain authentication in cryptocurrency systems such as Bitcoins, Artificial Intelligence (AI) systems and Internet of Things (IoT). Where there is money, there are hackers, and blockchain networks are proliferating both. Decentralised finance-related breaches constitute 76% of all major hacks in 2021, with

over $1 billion being lost in the third quarter alone (Atlas VPN, 2021). As such, attackers are becoming a great concern in the cyberspace.

Blockchain technology is based on principles of cryptography, decentralisation and consensus or verifiability. Data is structured into blocks that connect to each other in a cryptographic chain in such a way that it's nearly impossible to tamper with. In addition, James (2019) states that blockchain networks are not immune to cyberattacks and fraud. Common attacks include phishing attacks, whereby an attacker sends wallet key owners emails that are designed to look as though they're coming from a legitimate source. Another well-known form of attacks is the routing attack and the 51% attacks which attack public blockchains. Moreover, Nath (2021) states that despite improvements, the blockchain industry has been plagued by security concerns. The most common blockchain related attacks are the Exitscam, which occurs when a cryptocurrency exchange mysteriously leaves with user funds, restricting them from retrieving funds from their wallets (Spiceworks, 2021). Other common attacks are the Exchange hack, DeFi and Phishing. Some of the security incidents are the Wormhole incident in which a communication hub for Solana was attacked through a faulty account validation. Another incident was the BitMart, where attackers compromised the encryption of two hot wallets (Spiceworks, 2021).

Traditional or conventional security controls and technology-unique controls can be employed to secure blockchain technology against know cyberattacks. These include Identity and access management, Key management, Data privacy, Secure communication, Smart contract security, Transaction endorsement, etc.

The internet of things is one of the most versatile technologies in existence today. The ubiquity of the internet, the growing capacity of network connection, and the diversity of connected devices make the IoT scalable and adaptable (Chang & Li, 2019). The IoT industry does not have one clear set of security standards for developers and manufacturers to build in consistent security. The IoT attack surface areas includes the devices in which vulnerabilities can come from are its memory, firmware web interface or network services. The second surface area is the communication channel where by attacks can originate from the channels that connect IoT components to one another. The last attack surface area is the applications and software. The security guidelines to IoT includes ensuring that each device connected to any network should be securely connected so as to change the factory default credentials and to regularly update all software. Lastly, are disabled features which allow devices to be accessed remotely or grant access to known remote connections.

It is therefore, imperative and necessary to ensure that any cyberspace is protected to the best level from cyberattacks. It is evident that new forms and types of security threats are manifested daily and evolving and thus there's a need to tighten cybersecurity defences from all attacks. This includes employing a number of security solutions and keeping on par with security tools and strategies to protect against cybercrimes. With fast-evolving cyberattacks and the rapid multiplication of devices happening daily, this study can help to keep abreast with cybercriminals, automate threat detection, and respond more effectively than conventional software-driven or manual techniques. The following section provides a summary of the cybersecurity threats and attacks in Namibia.

2.5 Cybersecurity threats, attacks, vulnerabilities and solutions in Namibia

A report published by the United Nations Specialised Agency for ICTs (2021) shows that in Africa, many countries have seen a rise in reports of digital threats and malicious cyber activities. The results include sabotaged public infrastructure, losses from digital fraud and illicit financial flows, and national security breaches involving espionage and intelligence theft by militant groups. This is an indication that African countries are not exempted from cyberattacks. There's however, little literature on cyber incidences and specifically cybercrimes in Namibia. This could be due to security reasons and this could be an effort to protect organisations from reputational damages. Nonetheless, a report by CheckPoint (2020) shows that multiple attack attempts targeted Namibia, although the report doesn't indicate whether these attacks were successful or not. A survey report by Delloit (2018) on Cyber security in Namibia indicates that although Namibia in general is not a high risk target for cybercrime, there are organisations that were breached through cyberattacks. The report further highlighted that in Namibia, budget for IT infrastructure including cybersecurity is too low for strategic development and security of IT infrastructure. Furthermore, there's room for improvement on skills and training on IT and it was revealed that there was a lack of awareness of cyber risk and accountability for cyber security was not correctly assigned.

It is against this background that while there's little budget on IT and skills shortage amongst others, the present study carried out a cybersecurity assessment which can be useful to assist Namswitch to proactively assess the strength of its security systems. The following section discusses compliance and standards imposed by regulators to enforce and make organisations comply with in an effort to tighten cyber security.

2.6 Compliance requirements, international standards on security and best practice frameworks

Cybersecurity frameworks and standards provide the structure, approach and methodology needed to protect important and critical digital assets. In addition, they provide sets of best practices for measuring risk tolerance and establishing controls. A security framework provides a series of documented processes that define policies and procedures around the implementation and ongoing management of information security controls (Sem, 2020). These frameworks are a blueprint for managing risk and reducing vulnerabilities. On the other hand, compliance requirements are guidelines, laws and regulations that an organisation must adhere to. In cybersecurity, these are essential functions that are aimed at mitigating cybersecurity risks.

The US National Institute of Standards and Technology (NIST) is a complex and broad in scope framework that provides cybersecurity functions that follow the basic pattern of cyber defence, to identify, detect, protect, respond and recover. It also provides a mechanism for identifying IT risks and assets that require protection. NIST has developed an extensive library of IT standards, many of which focus on information security. The goal is to ensure a protected cyberspace.

The Committee on Payments and Market Infrastructures (CPMI) works together with the International Organisation of Securities Commissions (IOSCO) to enhance the coordination of standard and policy development and implementation, regarding clearing, settlement and reporting arrangements including financial market infrastructures (FMIs) worldwide (IOSCO, 2021). They are designed to help ensure the safety, efficiency and resilience of these infrastructures supporting global financial

markets. In 2016, it issued regulation on cyber resilience for financial sector infrastructures (Crisanto & Prenio, 2017).

The ISO/IEC 27000 series was developed by the International Organization for Standardization. It is a flexible information security framework that can be applied to all types and sizes of organisations (ISO, 2018). It establishes the requirements and procedures for creating an information security management system that requires the systematic management of the organisation's information security risks, taking threats and vulnerabilities into account.

The Center for Internet Security (CIS) Critical Security Controls, which was built in the late 2000 and formerly the SANS Top 20, lists technical security and operational controls that can be applied to any environment. CIS is a great option if you want an additional framework that can coexist with other industry-specific compliance standards (such as NIST) (NIST, 2020). CIS provides security benchmarks and hardening guideline based on commonly used standards. An organisation can be following these guidelines to ensure that best security standards are applied.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards that are designed to ensure that all institutions that accept, process, store or transmit credit card information maintain a secure environment. Institutions that handles credit card data are expected to undergo through the PCI DSS compliance certification and reviewed annually. PCI DSS version 4.0 is the latest version and all institutions handling PCI data are expected to comply before 2025 (PCI DSS Council, 2022). The 12 set of requirements for PCI DSS are aimed at providing a secure credit

card data environment. Institutions that fails PCI DSS compliance face severe penalties that results in heavy fines. On the other hand keeping up with these regulations and compliance requirements means that organisations will need a heavy budget.

In the Namibian context, the Bank of Namibia (BoN) provides a Determination on Information Security (BID-30) documentation that seeks at improving cybersecurity within the Namibian banking industry. BID-30 covers a broad range of areas that include information security governance, risk management and reporting requirements. The purpose is to provide guidance for banking institutions to enhance their information security resilience (Bank of Namibia BID-30 2017). Furthermore, BID-30 is principles based and the banks do not prescribe specific information security standards to be used by the banking institutions, however, institutions should take into account relevant industry information security standards and sound international best practices as appropriate (Bank of Namibia BID-30 2017).

Ultimately, some of the goals of cybersecurity frameworks are to provide a baseline group of security controls, to prioritise the implementation of security controls, to construct a cybersecurity programme and to identify, measure, and quantify the organisation's security risks. The standards and frameworks can be a lot and confusing to choose from. However, selecting which one is appropriate for a firm may be challenging. Furthermore, many legislations refer to more than one standard or framework. The aim is to protect organisations from cyber threats, to help improve their cybersecurity posture and to improve cyber resilience.

Recent high-profile cyber-attacks on financial institutions have focused attention on the need to strengthen cyber-security. Banks have the most public-facing products and services, and they are thus significantly vulnerable to potential cyber-attacks. Consequently, cyber-risk is a major concern for most bank supervisors. However, only a handful of jurisdictions have specific regulatory and supervisory initiatives that seek to address banks' cyber-risk (Crisanto & Prenio, 2017). Given the background on cybersecurity frameworks, standards and best practices on security, this research thus adds value through reviewing and ensuring that best practices are followed and enforced. This study was also aimed at performing an assessment that proactively measures cybersecurity resilience of Namswitch in an effort to ensure a hardened security cyberspace. The following section provides the cybersecurity strategies that can be employed within a cyberspace.

2.7 Cybersecurity strategies

Cyber-strategy is a high-level approach towards various aspects of how an organisation will secure its cyberspace (O'Reilly, 2019). The approach describes and lists what and how to implement solutions that safeguard IT infrastructure and services. In a constantly changing cyber threats environment, EU Member States need to have flexible and dynamic cybersecurity strategies that meet new global threats (ENISA, 2019). This usually involves a collaboration of many key stakeholders. A cyber strategy aims to build resilience to cyber threats and to ensure that citizens and businesses benefit from trustworthy digital technologies.

Organisations are becoming deeply concerned with their ability to protect themselves from data breaches, cyberattacks, and insider threats in today's age of digitalisation

and cybercrime. The Australian Government invested US$1.67 billion over 10 years on a Cyber Security Strategy to achieve its vision of creating a more secure web experience for its people (SANS, 2020). This emphasises the importance of investing in, and formulating cybersecurity strategies. The information security industry is one of today's fastest-growing economies with a forecasted growth of 7% from U$86.3 billion in 2017 to U$93 billion in 2017 (Gartner, 2018). Yeo (2017) agrees with Gartner (2017) that cybersecurity spending will reach a total of $1 trillion between 2017 and 2018, with a compound annual growth rate of 12% to 15%. Ayofe and Irwin (2010) contributed that businesses often fail to determine the best cybersecurity approach for their organisations. In support of the above, the NAMSAFE Protocol considered the importance of cybersecurity strategies and approaches and incorporated them into its design to help enhance the security of the Namswitch system. To assist with enforcing the cybersecurity strategy, a cybersecurity analysis or assessments can first be employed to evaluate and measure the level of protection applied. The section that follows discusses a few of the assessments.

2.8 Penetration testing

IT infrastructure have become susceptible to security threats and it is vital to reduce security breaches and use effective preventive measures to validate the security of an enterprise (Thomas, 2021). There are many cybersecurity assessments that have been conducted, which help to detect major risks and threats in infrastructure, and further enable organisations to take vital precautions to avoid security breaches. Penetration tests, security audits, risk assessments, and threat assessments are a few examples of cybersecurity assessments. The current study focuses on the use of pen tests to expose and remediate vulnerabilities in the Namswitch system.

2.8.1 Penetration test defined

Penetration testing is formally defined as a collection of practices that are used to identify and exploit security flaws (Bacudio et al., 2011). It is not always directed at a programme, host, or network device (Shewmaker, 2008), but it may also be directed at several users or an office (Bishop, 2011). Another fascinating perspective on penetration testing is an ethical cybersecurity assessment conducted to identify, safely exploit, and help eliminate vulnerabilities that reside across a cyber-environment (Tran & Dang, 2016). The following sections focus on the types of pen tests.

2.8.2 Types of penetration tests

A penetration test can either be performed externally or internally. External testing targets assets that are available on the internet or from the public domain. In contrast, internal testing is performed within an organisation's network. There are many types of penetration tests, including a) network penetration testing; b) application penetration testing; c) periodic assessment of network weaknesses; and d) physical penetration testing (Osborne, 2016). The following paragraphs elaborate on each of these types of penetration tests.

a) A network penetration test examines the entire network, with a focus on essential network resources including firewalls, database servers, web servers, and workstations. Testing methods employed in order to simulate a real-world network-based attack include port scanning, IP spoofing, session hijacking, Denial of Service (DoS) assaults, and buffer overflow attacks (Naik et al., 2009).

b) Application penetration testing entails uncovering vulnerabilities in applications through code analysis, injection attacks, and broken access controls (Yeo, 2017). Web systems are vulnerable to hackers because they are available to the public, and process information elements from HTTP requests (Melbourne & Jorm, 2010). As a result, web servers require significant security against a variety of well-known exploits, especially on port 80 which is the destination for most web traffic. Most bugs result from default or unpatched operating system settings or other installed software. As such, ensuring that web servers are up to date with the latest patches is essential (Midian, 2012).

In addition to the above, injection attacks, which are caused by a lack of input validation, are often the root cause of vulnerabilities in web applications. SQL injections are an example of injection attacks. These attacks allow an attacker to exploit the underlying database by providing input into an application which can change the underlying SQL query (Melbourne & Jorm, 2010). The Open Web Application Security Project (OWASP) is a non-profit organisation dedicated to the security of web applications. The OWASP has listed SQL injections and cross-site scripting (XSS) as the most common vulnerabilities (Antunes & Vieira, 2013).

c) A periodic network risk assessment is non-intrusive assessment which is typically used to augment a complete penetration assessment (Osborne, 2016). This operation entails scanning IP ranges on a quarterly or monthly basis and logging any deviations from established security measures. The assessment also scans for newly developed vulnerabilities and exposures.

d) Physical penetration testing assesses the company's physical security. It is a means of exposing a breach of the physical integrity of a customer's network and systems security (Allsopp, 2009). Analysis and testing of operational security, a physical penetration test could include a variety of techniques such as intelligence gathering, general deception, psychological engineering, night time infiltration, and lock breaking according to the Open Source Security Testing Methodology Manual (OSSTMM). There are standards that guide pen tests, these are discussed below.

2.8.3 Penetration Testing Standards (PTES)

The Cyber Kill Chain framework, developed by Lockheed Martin, is part of the Intelligence Driven Defence (IDD) model for the identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective (Martin, 2018). It provides steps that enhance visibility into an attack and enriching an analyst’s understanding of an adversary’s tactics, techniques and procedures. The steps are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.

Penetration Testing Framework (PTF) provides a combination of tools with a script designed to create functions for a pentester. The framework offers a database of exploits, tools and scanners required to perform a pen test. Developed by researchers and designed for Debian, Ubuntu and ArchLinux systems, it removes the hustle for amateurs to install the basic tools. Furthermore, pen tests have styles or types that can be conducted and they are discussed below.

2.8.4 Penetration testing styles

Three styles of tests are often used for network penetration testing, namely black-box testing, white-box testing, and grey-box testing (CPNI, 2016). In black-box testing, the tester has little to no knowledge of the target, whereas in white-box testing, the tester is given full information about the target. Grey-box testing, however, is a form of hybrid test which allows the tester partial knowledge of the target. Some details such as a typical user's login credentials to a system are shared, but not all. A black-box test is used to determine what an attacker with no knowledge of the target might accomplish. A white-box test, on the other hand, is useful for uncovering as many flaws and attack vectors as possible, in order to conduct more focused attacks to expose more details about the system under testing. Grey-box testing aims to determine how much access a trusted person would have to an organisation’s computing resources (CPNI, 2016). For security and confidentiality reasons, only a limited number of credentials could be obtained during this study, hence a grey-box test was conducted. Furthermore, grey-box testing was favoured as it provides the best balance between efficiency and authenticity by eliminating potentially time-consuming reconnaissance activities. The proposed NAMSAFE Protocol was, designed to accommodate any or all of the three (3) penetration testing styles discussed herein. The methodologies for conducting pen tests are discussed in the following section.

2.8.5 Penetration testing methodologies and phases

Penetration tests are generally divided into three phases which represent the steps carried out during an attack (Vacca, 2010). The first phase is the pre-attack stage which aims to investigate the target. The second phase, known as the attack stage, is where the attacker compromises the target. Finally, the testing team arrives at the post-attack

phase which aims to restore systems to the states they were in before the penetration test was conducted. Figure 2.1 below illustrates three activities that take place in each of the three phases of a penetration test. Reconnaissance takes place in the pre-attack phase, enumeration takes place in the attack phase, while exploitation takes place in the post-attack phase (Cheim, 2014).

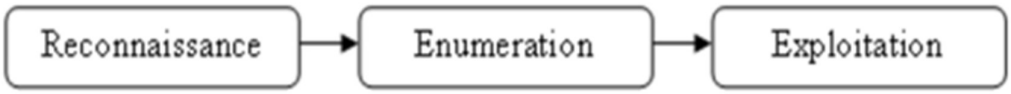


Figure 2.1 A simple penetration testing methodology
Source: A study of penetration testing tools and approaches (2014)

A more standardised or formal penetration test might contain more sub-activities within the three phases mentioned above. Figure 2.2 below provides an illustration of a more detailed penetration test process, which include additional phases such planning, bootstrapping, maintaining access, reporting and cleaning up.

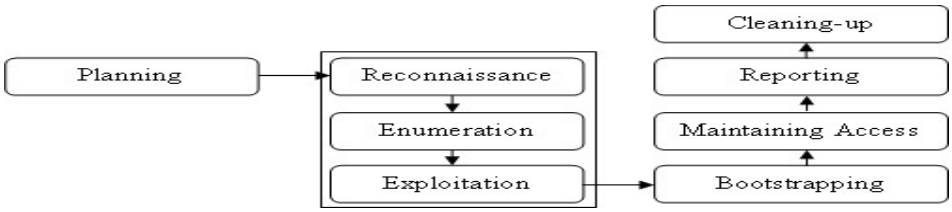


Figure 2.2 A formal penetration testing methodology
Source: A study of penetration testing tools and approaches (2014)

A formal penetration test usually starts with the initial planning and preparation stage which has a huge impact on the penetration test's outcome (Tiller, 2011). This stage details specifics of the test such as security procedures, programmes, postures, and threats, as well as their positions in forming a controlled attack. Unlike a simple approach, a formal penetration test includes further measures after the manipulation stage, such as bootstrapping the penetration, maintaining control, monitoring, and cleaning up. Bootstrapping refers to the process of launching an attack from a different

vantage point in order to detect new bugs (Shewmaker, 2008). The pen test phases therein were discussed and summarised as presented below:

2.8.5.1 Reconnaissance

Reconnaissance or recon, is the method of looking for available information to use in a penetration test and is also known as the information gathering phase (Tiller, 2011). Depending on the context of a penetration test, reconnaissance activities could include ping sweeps to locate IP addresses on a network, rummaging through dumpsters to locate telephone service receipts, tapping telephone lines and networks, and lastly, employing social engineering activities by lying to customers and employees in order to extract valuable information. The passive research approach may also be used to gather as much organisational data as possible, such as DNS archives, name registries, and IPS glass-looking directories (Osborne, 2016).

Within the reconnaissance phase, there are several open-source and several commercial tools that can be used in a pen test such as the Nmap, Nessus, Spiderfoot and SQLmap. These tools are further explained below.

a) **Network Mapper** or **Nmap**, is a powerful network security scanning application that uses crafted packets to probe target networks in order to discover open ports, services, and other host details, such as the operating system type (Engebretson, 2011).

b) **Nessus** is a proprietary vulnerability scanner that specialises in delivering comprehensive mappings of target system vulnerabilities, including web and network vulnerabilities, misconfigurations, weak passwords, and non-compliance to standards such as HIPAA and PCI (Faircloth, 2011).

c) **Spiderfoot** is a continuous cyber reconnaissance tool that searches over 100 public data sources automatically. This tool collects data about IP addresses, domain names, and email, among other information (Automate OSINT for Asset, 2021).

d) **sqlmap** is an open-source penetration testing tool for discovering and exploiting SQL injection flaws and taking control of database systems. It includes a robust detection engine and performs database fingerprinting, data retrieval from databases, access to the underlying file systems, and out-of-band command execution on operating systems (SQLMAP, 2021).

2.8.5.2 Enumeration

The enumeration phase relates to the construction of a representation of an environment. The data used in this phase is obtained directly from target processes, services, and networks using techniques available to the attacker. Host enumeration describes utilities that are accessible on various devices such as firewalls, routers, and web servers, and exposes their functionality and open ports that may be used to access the system. Network enumeration on the other hand creates a layout of the target network (Shewmaker, 2018).

The aim of this phase is to gain access to the target and to discover vulnerabilities. A vulnerability is a possible security flaw, such as design problems, glitches, or misconfigurations, which may lead to security policy violations (Vacca, 2010). A vulnerability assessment is the process of identifying threats and security vulnerabilities on a target, quantifying and analysing them based on predefined risks (Vacca, 2010). Vulnerability assessments are activities that are conducted as part of an enumeration phase. These activities are explained in the following section.

The tools used in the enumeration phase are such as OpenVAS, OpenSSL, Nexpose, Enum4Linux. These tools are further explained below.

a) **NeXpose** is an enterprise-grade vulnerability assessment tool used to identify many common vulnerabilities in both physical and virtualised systems (Engebretson, 2011).

b) **OpenVAS and OpenSSL** are open-source vulnerability scanners that include a variety of built-in tests. The scanner obtains the tests for detecting vulnerabilities from a feed that has a long history and daily updates (Greenbone, 2021).

c) **Enum4Linux** is a tool for enumerating operating systems (NIST, 2020).

The IT industry typically includes vulnerability assessment as one step in the pen testing process. This is necessary to discover the loopholes in a system that can be exploited. The following sections discuss this further.

2.8.5.2.1 Types of vulnerability assessments

Network-based scans

Network-based scans combine the enumeration of vulnerabilities with host and service discovery. The discovery component of a network-based scan aids the evaluator in identifying the devices on a network and potential attack points. The scanning tool analyses a target's actions and reactions in order to generate a fingerprint that contains the device's details. This aids the tool in compiling the host's characteristics with varying degrees of precision. To decide the form and version of the host or computer, the tool could, for example, list operating services, search for a set of open Transmission Control Protocol (TCP) ports, or inspect system banners, amongst other information (Murugiah, Scarfone, Cody & Orebaugh, 2008). Most modern scanning tools can reliably detect the target's operating system and network applications, and perform focused tests based on known vulnerabilities and common misconfigurations for those operating systems and applications.

Host-Based Scans

Since network-based scans are designed to search for externally exploitable vulnerabilities, they can overlook flaws that can only be exploited by a user signing into the system, also known as local exploits. Host-based scans are executed from the target computer or managed centrally using an authenticated account with connections to the target device (Murugiah, Scarfone, Cody & Orebaugh, 2008). These scans can provide more insight into a system's settings and patch information, while also covering ports and resources that are noticeable in network-based scans. As a result, host-based scans are more extensive than network-based scans, which can result in additional latency, making them more difficult to set up and execute.

Wireless Network Scans

Wireless network scans are used to detect potential points of attack on an organisation's wireless network infrastructure. Wireless scans also verify the security configurations on an organisation's wireless networks. This includes assessments aimed at detecting rogue access points which can pose as legitimate wireless networks for the organisation, or as a hotspot at a nearby coffee shop, in order to trick victims into connecting to the attacker's network (NIST, 2018).

Network-based, host-based, and wireless network scans were all performed in this study. This was necessary to ensure coverage of the entire eco-system, to ensure all possible vulnerabilities were identified and remediated, to ensure that the objectives of this study were met, and ultimately to ensure the cyber-resilience of Namswitch.

2.8.5.2.2 Benefits of vulnerability assessments

Vulnerability assessments, like most information management controls and procedures, are guided by two factors: security advantages and regulatory responsibilities (NIST, 2020). Conducting vulnerability tests meets all of these requirements. The following are some benefits of vulnerability assessments.

a) **Security benefits**

Vulnerability assessments are often used in industry processes and best practice recommendations. For example, one of the top five CIS controls to minimise the bulk

of enterprise security risks is to conduct continuous vulnerability analyses and remediations (CIS, 2018). Similarly, under its control category, the NIST Cybersecurity Framework (2017) calls for asset risk monitoring and reporting. The results of vulnerability analyses may be used not only to prioritize remediation activities but also to identify structural problems including patch management flaws and resource life cycle management. Network vulnerability scans can detect rogue assets attached to a company's network and locate unauthorised devices on internal networks. The findings of vulnerability assessments can also be incorporated into incident correlation by cross-referencing irregular incidents with established vulnerabilities in more advanced organisations which use centralised logging. These use cases may boost security detection capabilities and increase the likelihood of identifying a malicious attacker while executing device identification or exploitation (NIST, 2020).

b) **Compliance requirements**

The conditions for compliance are split into two categories: compulsory and non-compulsory. Compulsory requirements are government or industry-mandated conditions that a corporation must adhere to, such as a law or regulation. Common examples of compulsory requirements include the Health Insurance Portability and Accountability Act (HIPAA), the CIS standard, the General Data Protection Regulation (GDPR), and the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS is an example of a contractual provision imposed by the industry, which although not required by the government, is a requirement that all credit card retailers and suppliers must comply with. Compulsory requirements almost always

include a financial penalty for non-compliance. Non-compulsory drivers are not mandated, however, for some companies, the expectations of customers or business partners might require compliance to certain standards such as ISO / IEC 27001:2013.

Further insight on the vulnerabilities was provided and the section below focused on the classifications of vulnerabilities that can be found on a system.

2.8.5.2.3 Ranking of vulnerabilities

The MITRE Corporation introduced the Common Vulnerabilities and Exposures (CVE) database in 1999. The database provides a list of common identifiers for publicly known vulnerabilities and exposures, and was intended to assist different entities during the process of associating, categorising, and classifying different types of software and firmware vulnerabilities. The aim was to provide a single archive that could be pointed to when discussing the same issue in order to prevent cybersecurity discrepancies and to serve as the foundation for a cybersecurity standard for classifying and listing vulnerabilities. According to Konstantinos et al. (2010), the CVE also seeks to standardize names of publicly known bugs and security disclosures. The CVE listing also offers fixes for these bugs and vulnerabilities (NIST, 2018). This aids businesses in establishing baselines for assessing the coverage of their security tools.

The CVSS was founded and is operated by the Forum of Incident Response and Security Teams (FIRST), a non-profit organisation headquartered in the United States, which seeks to support cybersecurity incident response teams. The CVSS is used as a vulnerability scoring system as it provides open guidelines for assigning a numerical rating for the severity of a vulnerability in order to determine its magnitude

(Konstantinos et al., 2010). It is meant to convey the seriousness of application, hardware, and firmware flaws that create vulnerabilities. The scoring system places a premium on technology, with network being the first metric in the attack vector metric. The CVSS may be a suitable choice for experts who need a structure to identify non-technical vulnerabilities (Konstantinos et al., 2010). In short, the CVSS aids in the identification and prioritization of IT risks and determines how easy it is to circumvent a flaw and how dangerous it can be if exploited.

The CVE differs from the CVSS in that the CVE assigns a unique identifier to each vulnerability listed in the NIST NVD, while the CVSS assigns a severity rating to each CVE. CVSS calculations were used in this study to classify and provide vulnerability scoring in order to determine the magnitude and severity of vulnerabilities. This was useful in determining the security posture of the Namswitch system.

The CVSS scoring scheme is now in its third version, known as CVSSv3.1. The CVSSv3.1 score has three values for rating a vulnerability (FIRST, 2021), namely the base, the temporal, as well as the environmental score. The base score indicates how easily the vulnerability can be exploited and how much harm an exploit targeting the vulnerability could cause. The temporal score determines how well people are aware of the risk, the actions that are being taken to address it, and whether threat actors are exploiting it. The environmental score is a customized measure that is unique to an organization and is calculated using various matrices. It is used to determine an asset's business criticality. The last phase of the pen test deals with intruding systems. The section that follows deals with this.

2.8.5.3 Exploitation

Finally, exploitation uses various automated methods, procedures, and fine-tuned manual measures to exploit a device through the identified bugs or other open channels exposed during the information gathering phase (Tiller, 2011). The process's ultimate goal is to gain access to organisational resources through vulnerable devices (Engebretson, 2011). Tools that are used in an enumeration phase are Metasploit and SQLmap. One of the tool is further explained below.

a) **Metasploit** is a modular, expandable toolset designed for rapidly discovering and exploiting vulnerabilities in a target system. It allows assessors to easily enumerate and exploit real-world vulnerabilities, as well as discover their potential danger and significance (Faircloth, 2011).

The most significant output of a penetration test is documentation. An effective report provides a detailed listing of the vulnerabilities found, as well as their potential impact to the organization. The report should also provide a safety ranking of the vulnerabilities, as well as recommendations for mitigating the risk associated with the vulnerability (Osborne, 2016). Furthermore, the report should be readable and understandable by both technical and non-technical personnel. The final phase, which is the clean-up phase aims to return the device under scrutiny to its original state so that it can resume regular operations (Tran & Dang, 2016).

In this study, a formal penetration testing methodology was adopted as it was more appropriate with the gray-box pen test approach and it contains more sub-activities built around the three core measures, this aids in the acquisition of valuable data to

cover all systems. The tools used at the different stages were the Nmap, OpenVAS, OpenSSL and the SQLmap.

2.9 Chapter summary

The review of the literature offered further information on penetration tests and vulnerability assessments. It also explained that the Namswitch system interconnects banking systems in Namibia and is therefore considered a critical component of the Namibian banking industry. As such, the Namswitch cyberspace needs to be safeguarded to ensure continuous operations of all Namibian banking systems.

The literature reviewed also looked at cyber security assessments that could be employed to safeguard an entity, such as penetration tests and vulnerability assessments. Although a number of penetration testing styles exist, the grey-box pen test was preferred for this study as not all credentials on Namswitch could be availed owing to confidentiality and security reasons. In addition to this, only partial information could be provided.

The formal penetration testing methodology was chosen as it contains more sub-activities built around the three core measures, which are reconnaissance, enumeration, and exploitation. This aids in the acquisition of valuable data to cover all systems. Open-source tools were preferred due to ease of accessibility and lack of financial implications. Furthermore, most tools used were chosen because some could be used in more than one pen test phase.

Lastly, the chapter briefly discussed the tools used to classify and rank vulnerabilities, such as the CVE database which provides a list of common identifiers for publicly known vulnerabilities and exposures, as well as the CVSS which provides a numerical rating of the severity of a vulnerability in order to determine their magnitude.

As indicated in section 1.3, the objectives of this study were to determine the security resilience of this ecosystem by identifying vulnerabilities, and to develop mitigating measures to address the flaws uncovered in the ecosystem, as well as compensating controls for vulnerabilities that could not be addressed. Furthermore, the NAMSAFE Protocol was created to achieve the study's objectives by proactively strengthening the security and resilience of the Namswitch IT infrastructure and services.

The next chapter explains the research methodology employed for this study.

CHAPTER THREE

RESEARCH METHODOLOGY

This chapter outlines the methodology used for the study. The chapter provides an overview of the research design, research instruments, procedure, and the data analysis techniques used. The chapter further highlights the ethical considerations adhered to throughout the study. The chapter is concluded with a summary of the discussion.

3.1 Introduction

The chapter details the research methods used to conduct the study in order to address the research objectives. The research methodology is in line with the research objectives of the study. The research paradigm was deliberated to point out various aspects of this study. This research aimed to assess the security posture of the Namswitch system by conducting a pen test and a vulnerability assessment. The outcomes of this study consists of results that were further analysed in proposing mitigating strategies in accordance with the aims of the research. This chapter presents how a pen test methodology was developed, how it was used to conduct a pen test and vulnerability assessment on the Namswitch system. To achieve the objectives of the study, reliable data collection methods, research procedures and data analysis and research ethical considerations are also presented.

3.2 Research approach

There are three different approaches to conducting research, namely quantitative, qualitative, and mixed-methods. The mixed methods research approach is a

combination of both quantitative and qualitative research approaches (Creswell, 2013). A mixed methods approach was used in this study since the study incorporated both quantitative and qualitative aspects.

The qualitative research approach associated with the interpretivism paradigm was used to conduct a penetration test to determine how secure the Namibian inter-banking system was, by uncovering security concerns in the inter-banking system. The qualitative research approach was also used to identify and categorise different vulnerabilities based on their characteristics. The quantitative research approach was used to develop statistical models and figures to illustrate the study's findings. Quantitative research designs were also used to assess the security of the Namswitch system against industry best practices.

3.3 Research design

A research design is a plan for carrying out a study. This study employed a diagnostic research design combining both qualitative and quantitative research methods. A diagnostic research design is one that focuses on the particular traits and existing social difficulties with the goal of discovering out what is happening, why it's happening, and what can be done to avoid/prevent it (Bernardo et al. 2019). This design consists of three research stages, which are; inception of the issue, diagnosis of the issue and solution for the issue. The design was primarily selected to conduct a penetration test to determine how secure the Namibian inter-banking system was, by uncovering security concerns in the inter-banking system. Vulnerabilities were then discovered in the Namswitch system and solutions were discovered.

In-depth interviews, case studies, ethnographic research focus groups, content analyses, and combinations of these techniques are all examples of qualitative research methodologies (Creswell, 2013). Qualitative approaches produce more descriptive findings, allowing conclusions to be drawn from the data (Oates, 2006). This study employed qualitative research techniques in the form of a case study to conduct an exploratory research that are simulation or emulation in quantitative in nature in order to acquire data through IT scans which could be analysed to derive the security posture of the Namswitch system. This provided an in-depth understanding of the Namswitch system's vulnerabilities and security posture. The IT scans were further utilized to evaluate the Namswitch system's security in comparison to best practices and security standards. For example, an Nmap scan was employed in this study which provided a list of vulnerabilities found on the Namswitch system as well as a CVSS rating of these vulnerabilities in order to determine the severities of their impact.

An experimental testbed is a network consisting of the attacker, who in this case is the researcher; as well as the target, which in this case is the Namswitch system. The research took place in two steps. The first step was to develop a model to conduct the penetration test as well as the vulnerability assessment. Secondly, was to use tools such as Nmap, OpenSSL and OpenVAS to collect statistical information about the number of services discovered, the number of vulnerabilities detected, and the types of vulnerabilities detected. The tools were also used to quantify the risk rating of the vulnerabilities identified, and subsequently carry out a penetration test. The data was then evaluated to determine the security posture of the Namswitch system as well as to provide remedial steps and compensating controls. On this basis, effective recommendations for addressing these security flaws were made.

Convenience sampling is a sort of nonprobability sampling in which participants are chosen because they are "convenient" data sources for researchers (Oates, 2006). The convenience sampling technique was used to select the target IP addresses from Namswitch's development, testing and production environments. The researcher deems this necessary with the aim to ensure all essential services are covered. The IPs used in the test were known to the tester ahead of time and were selected in a manner that ensured the availability of the production infrastructure and systems, as well as the confidentiality of the banking institutions. This IPs were selected because they consists of all the entities that are interconnected and make up the Namswitch system. Seven (7) public IPs and at least fifty (50) internal IPs from Namswitch were targeted for the attacks and the results were objectively analysed by enumerating and rating vulnerabilities using CVSS, in order to determine Namswitch's cyber resilience.

The experimental design of this study comprised of a setup of the pen tester and the Namswitch environment. The pen tester used a laptop installed with Kali Linux Tools combined and followed a pen testing frame work that also offers pen testing tools. This was used to conduct both the internal and external pen tests.

3.4 Data requirements

Many fingerprinting techniques were used in the first stage of the experiment to classify the services running on the hosts within the digital environment known as User Acceptance Testing (UAT). The UAT is a replica of the production environment and is used to test solutions before deployment to the production environment. Since the UAT consists of identical configurations to the production environment, it was used in this study to safely conduct the penetration tests which exposed weaknesses in the

security configurations of the production environment. The parameters or metrics evaluated are: (i) the devices' response time, (ii) number of detected applications, (iii) active services, iv) open ports, (v) patching or missing updates, and (vi) the number and severity of vulnerabilities discovered where required.

3.5 Research procedure

There are a variety of industry-accepted methodologies referred to as testing models, which can guide a pen testing or vulnerability assessment exercise. The researcher identified a few testing models that are often utilized in the financial field. Among these are the OWASP, the PTES, the OSSTMM, and the NIST – SP800-115. These models were then used to construct the testing model. Much of the developed testing model was derived from the NIST SP800-115 which is the PCI DSS council's recommended testing guide (PCI DSS, 2020). This is because the banking industry is governed by the PCI DSS standard, hence the proposed testing model is influenced immensely by this standard. Figure 3.1 below shows an overview of the testing model that was developed through combining the PTES (2019) and NIST SP800-115 (2020) models and applied in this study. The model extends a formal penetrating test model by including additional steps such as the signing of the Non-Disclosure Agreement (NDA) and providing remedial steps. The model includes step-by-step procedures that pen testers may follow in order to conduct a pen test on Namswitch and can be extended to other financial institutions.

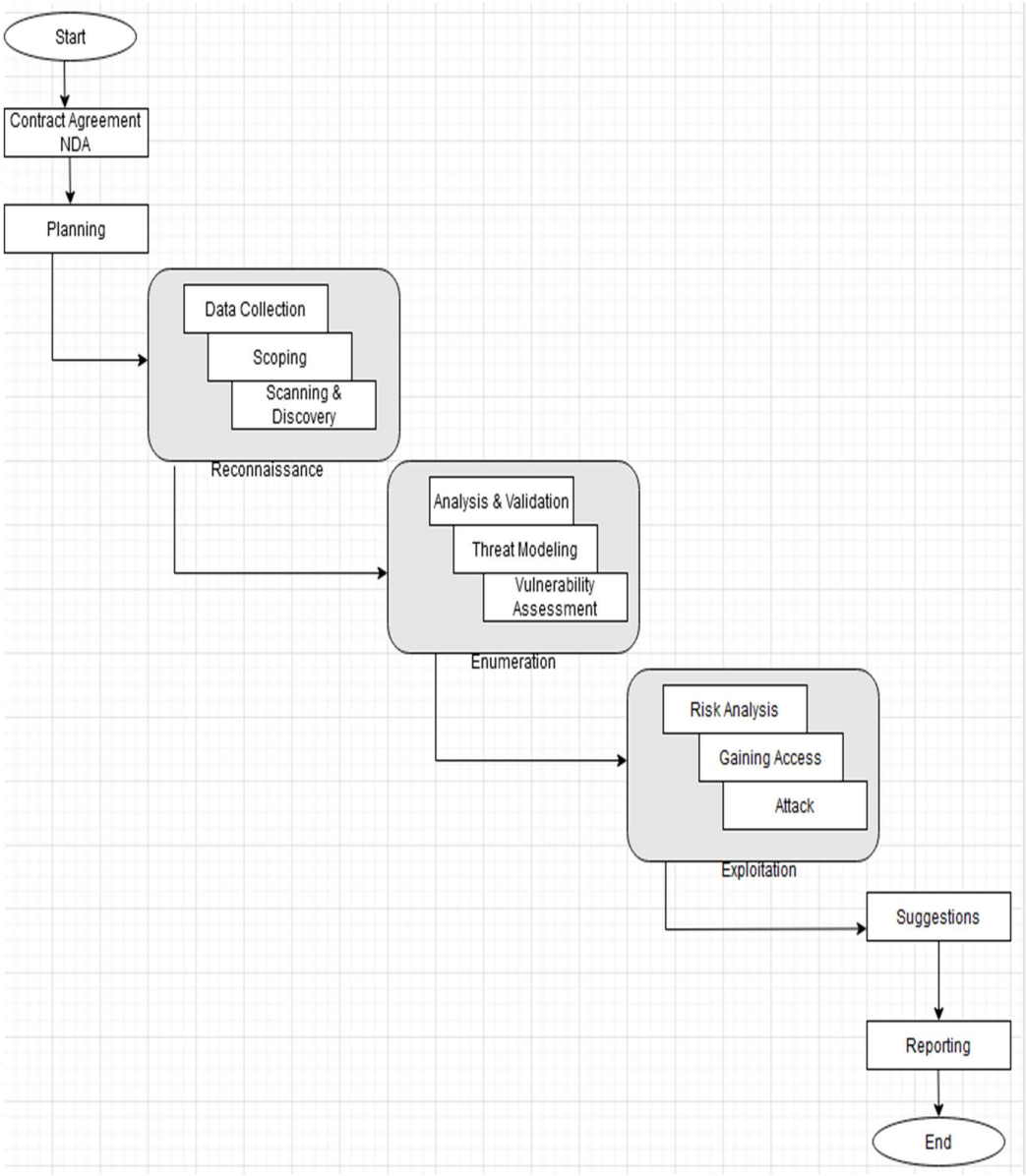


Figure 3.1 *Pen testing model adopted in this study.*

3.5.1 NDA

The first and most important step was to obtain approval from Namswitch to perform the test before the pen test commenced. The researcher and the Senior Official signed a Non-Disclosure Agreement which served as a legal agreement binding both parties on confidentiality (Refer to Appendix D).

3.5.2 Planning

Prior to the commencement of the pen test, a discussion was held with Namswitch to define the scope and the goals of the test. The researcher sought information regarding Namswitch's network diagrams, and networks to be tested. This phase also included the identification of security tools such as Nmap, OpenSSL and OpenVAS that were used during the scanning, threat modelling, validation and attack sections. Furthermore, this stage involved intelligence gathering to understand the architecture of the Namswitch system. This includes the network devices (switches, and routers), servers (virtual and physical hosts), databases, applications and security systems or appliances.

The testing model covered Namswitch essential resources such as applications, networks, and databases. Internal IP addresses and Fully Qualified Domain Names (FQDNs) associated with critical network infrastructure, such as network components, servers, workstations, and peripherals were included in the internal scope. This included partial information, especially with regards to credentials. Additionally, all Namswitch public IPs were disclosed. A list of all services and ports that were to be available as well as the methods by which approved users were granted access to vital systems were detailed and provided for testing.

3.5.3 Reconnaissance

Scanning and discovery

Scanning tools were used to analyse ICT resources specified in the scope such as the network devices (switches, and routers), servers (virtual and physical hosts),

databases, applications and security systems or appliances. During this stage, the Nmap port scanning tool was used to identify Namswitch's IP addresses and associated listening services and firewall rules. Fingerprinting tools examined listening services to identify the nature and function of listening services. This stage also involved the use of packet sniffing tools to capture various samples of the network traffic for analysis. Furthermore, Domain Name Service (DNS) interrogations were performed to queries Namswitch DNS server with the intent to identify targets and verify ownership. Lastly, the same tools were also used to identify Operating System (OS) versions. Figure 3.2 below shows the port scan results for the external IPs. This indicates that only two of the IPs were accessible from the public domain. See Appendix F for the complete table.

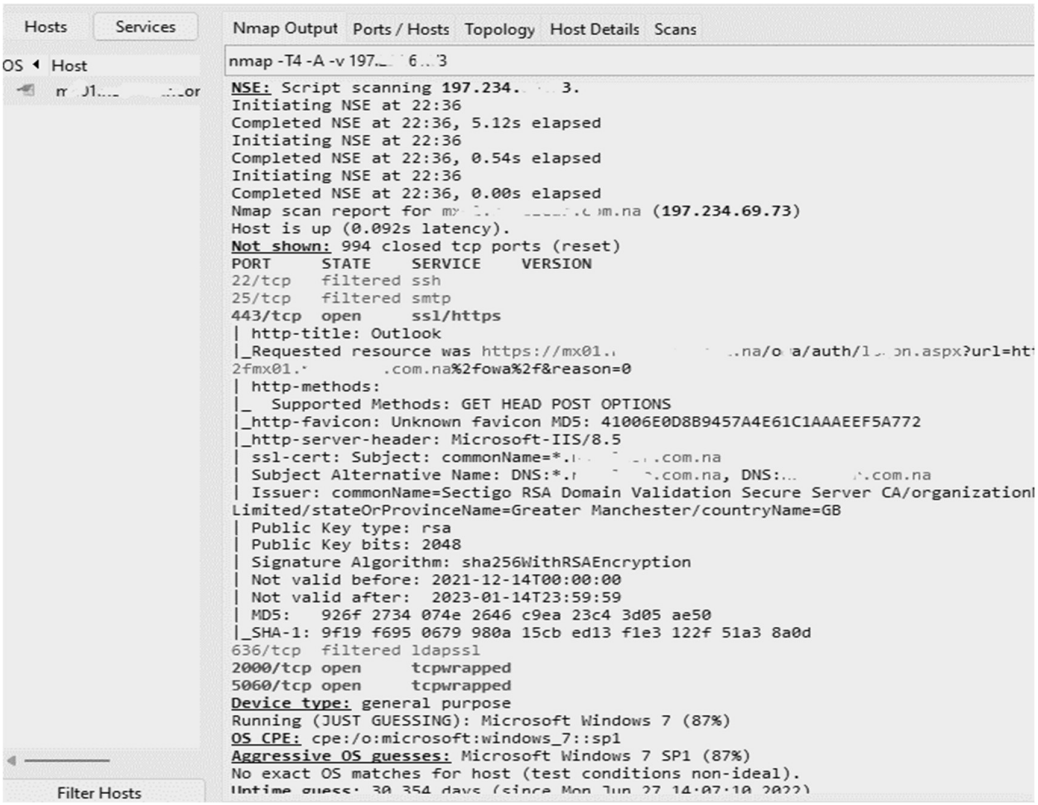


Figure: 3.2 External port scan results

The output of the port scan that shows partial results on the Namswitch internal systems are presented in Table 3.1 entitled Internal port scan results below. The scan findings shows that there are open ports that requires to be further examined for possible vulnerabilities. Open ports are an indicator that there's a service listening on that port. See Appendix F for the complete table.

Table: 3.1 Internal port scan results

Address of Host (Hostname)	Protocol/Port/Service/Status
10.XX.XX.7	TCP / 22 / SSH / OPEN TCP / 1720 / H323Q931 / OPEN TCP / 2000 / TCPWRAPPED / OPEN TCP / 5060 / SIP-PROXY / OPEN UDP / 123 / NTP / OPEN *Output truncated..*
192.XX.XX.150	TCP / 22 / SSH / OPEN TCP / 443 / HTTP / OPEN TCP / 2000 / TCPWRAPPED / OPEN TCP / 5060 / TCPWRAPPED / OPEN *Output truncated..*

3.5.4 Enumeration

Vulnerability assessment, threat modelling and validation

The researcher used insights from the reconnaissance phase to further understand the threat landscape by categorising various assets and constructing custom threats to

penetrate the Namswitch system. During this phase, vulnerability assessments were carried out using enumeration tools, such as the sqlmap, OpenVAS and OpenSSL to perform unauthenticated vulnerability scans to identify vulnerabilities in operating systems and network services. Furthermore, this stage involved an analysis of packets captured, that involved examining traffic samples by looking at protocols with known vulnerabilities. For example, the DNS server was responding to queries for third-party domains that do not have the recursion bit set, that can be further exploited. The Namswitch system was also subjected to vulnerability verification to confirm and validate findings from the scanning tools in order to consolidate findings and remove false positive findings.

During this phase, the researcher looked at the applications and systems within the testing scope and compared the setups and configurations against best practices, standards and current practices set out by the vendors or as set out by CIS security hardening guides. This information was necessary to assess the Namswitch system's security. This phase also involved analysing, classifying and rating vulnerabilities using Nmap, OpenVAS & OpenSSL. All this information was crucial for the exploitation phase.

The following tables (Table 3.3, Table 3.4 and Table 3.5) are the observations which were noted during the assessment. The tables provide the findings regarding the service, associated to the affected resources and the observations made. The tables below present's results obtained from the external facing systems. See Appendix F for the complete table.

Table 3.2 Enabled SSL medium strength cipher suites

3.2 SSL Medium Strength Cipher Suites Supported	
Port	TCP 443
Observation	The researcher observed that the remote service supports the use of medium strength SSL ciphers
Affected Resources	197.234.74.11 & 197.234. 69.73
Results	

Table 3.3 TLS/SSL certificate vulnerabilities

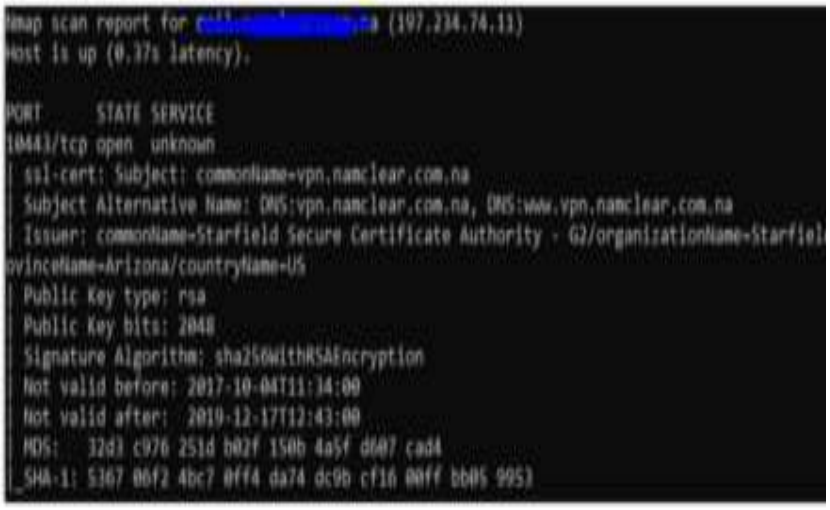
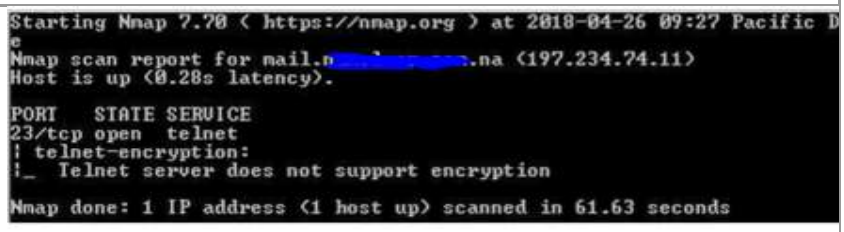
3.3 TLS/SSL certificate vulnerabilities	
Ports	TCP 10443
Observation	The researcher observed that the affected systems are vulnerable to the following vulnerability: 1. X.509 Server Certificate Is Invalid/Expired 2. X.509 Certificate Subject CN Does Not Match the Entity Name
Affected Resources	197.234.69.73 & 197.234.74.11
Results	

Table 3.4 Unencrypted Telnet Server

3.4 Unencrypted Telnet Server	
Port	TCP 23
Observation	The researcher observed that remote Telnet server transmits traffic in clear text.
Affected Resource	197.234.74.11 & 197.234.69.73
Results	

3.5.5 Exploitation

Risk analysis, gaining access and attack

At this stage, the researcher identified attack avenues by reviewing findings from the enumeration phase in order to identify plausible attacks with a chance of succeeding. The researcher used the Metasploit tool to probe Namswitch's vulnerabilities to ascertain that they are exploitable. This tool was also used to exploit the vulnerabilities found. Post exploitation was the last step of the exploitation phase. It involved removing any change added to the Namswitch system as part of the assessment in order to return systems to their pre-assessment states. The following subsections detail the internal and external pen tests performed.

3.5.5.1 Web application and database testing

The Nmap tool was used to examine the application to understand its logic and potential entry points. The Metasploit tool was used to monitor all HTTP requests and responses. An active attack was conducted in the form of session management in order to determine how the Namswitch web applications handle and manage sessions to protect communications from attacks such as session hijacking, etc. The attack was conducted using Metasploit, OpenSSL and OpenVAS tools on a set of active tests that had been separated into 11 subcategories for a total of 91 controls, including input validation testing, which prevents poorly constructed data from entering an information system. Injection flaws such as SQL injection attacks were performed in order to determine how databases handled insertion of data through URLs. Appendix C, the full set of controls, under the Web applications and databases, lists the entire control sets. The pen test tools follows or uses a logical flow when performing an attack. Figure 3.3 below is an example of a logical flow of an attack process (Emagined, 2021).

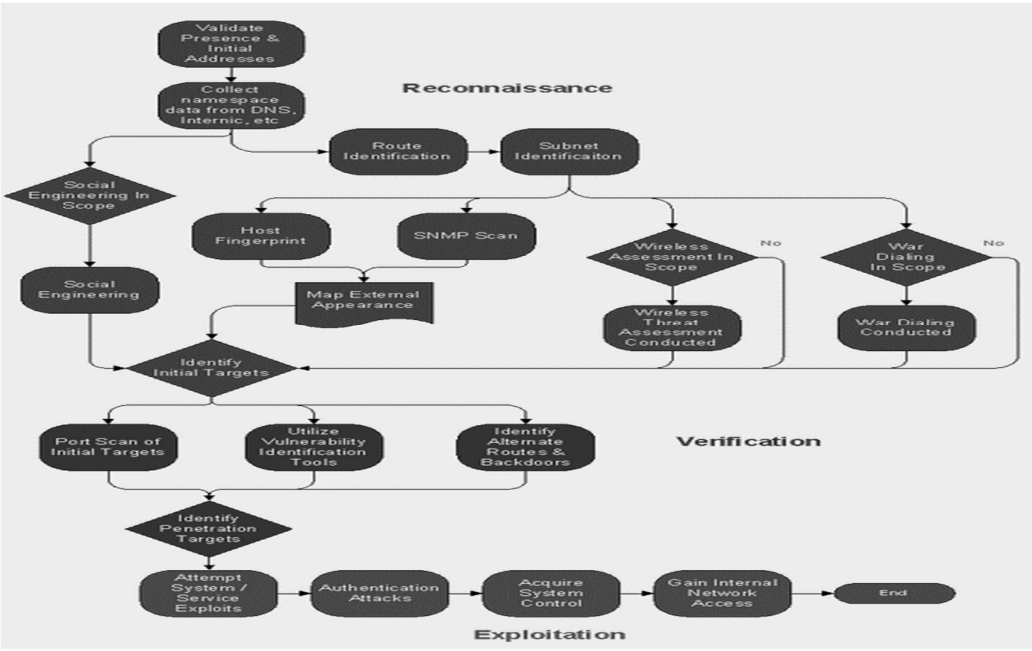


Figure: 3.3 Logical flow of the attack process

Figure 3.4 below show a sample output of OpenSSL results that indicates CVE-2000-0649 detected vulnerability, in which a web server was disclosing its internal IP address to the public. The figure reveals a successful attack of this vulnerability on an email server that disclosed its internal IP configuration information. Further, Figure 3.4 below exposes the server name *DC01* while internal IP info is masked due to security reasons. Successful exploitation of this vulnerability results in the disclosure of the internal IP address or internal network name, which could then be used in further attacks against the target.

Figure: 3.4 OpenSSL results of internal IP disclosure attack on an email server.

3.5.5.2 Network testing

The Metasploit, Nessus, OpenVAS and OpenSSL tools were used to perform the following test on server OS, network devices and security appliances. The researcher performed session management testing on the servers and network devices for flaws such as session fixation, session hijacking and unprotected session keys. Based on previous tasks findings, the researcher performed network protocol exploitation on the network to test for denial of services attack and determine whether these devices will be inaccessible or will not be able to function during the attack. The logical flow of the attack process for a network testing is similar to web applications or database pen testing with minor distinct steps.

Figure 3.5 below shows a sample output of the performed the File Transfer Protocol (FTP) Brute force or Dictionary attack login, which indicates that it was possible to login to the application with the root credentials. The figure reveals successful access to this system by using the username: *root* and password: *root* which are default credentials.

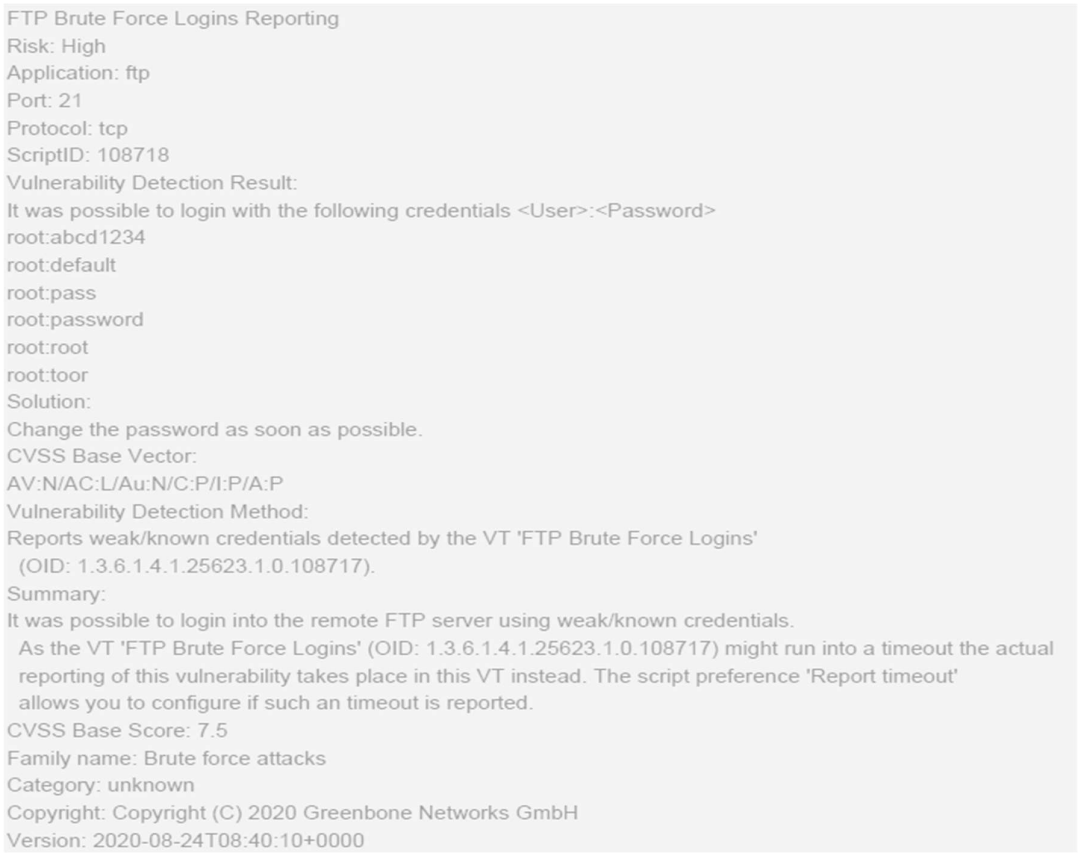


Figure: 3.5 FTB Brute force attack results

Authentication tests were also performed on the network for default user accounts and devices configured with weak login credentials. Moreover, information extracted from SNMP enumeration were used to perform SNMP reflection attack, which is reminiscent of earlier generation of DNS attacks. Other tests performed were disclosure of information attack performed on publicly accessed devices. Figure 3.6 below demonstrates a sample output of vulnerabilities identified during the Metasploit

scan. The scan reveals the most common vulnerabilities found and the most common vulnerabilities per category such as Microsoft, Web, Mail, etc. Furthermore, from the figure, it can be seen that about 30 systems contained the password never expires vulnerabilities. Other vulnerabilities shown in the Figure 3.6 below were the use of lower suite ciphers such as the use of TLS version1.0, SSL DES ciphers and SSL static key ciphers.

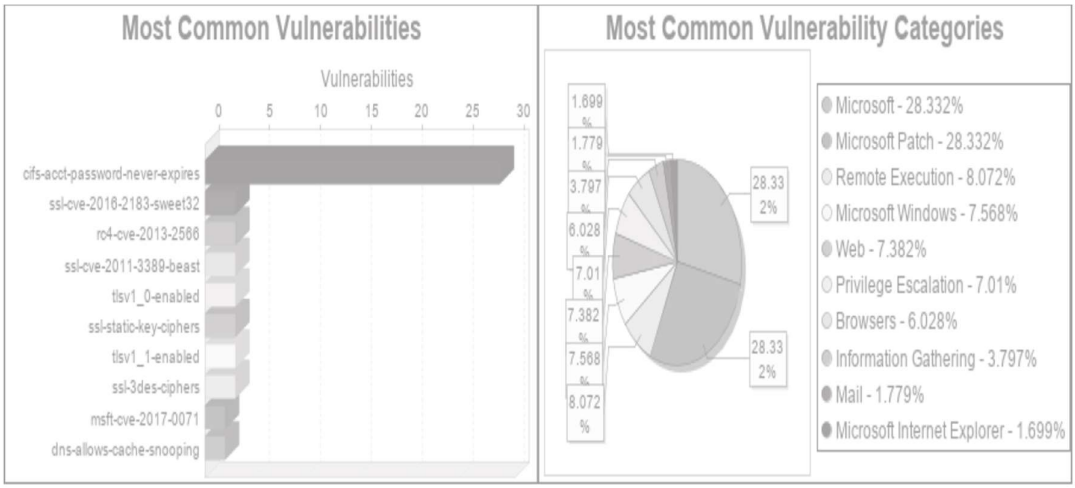
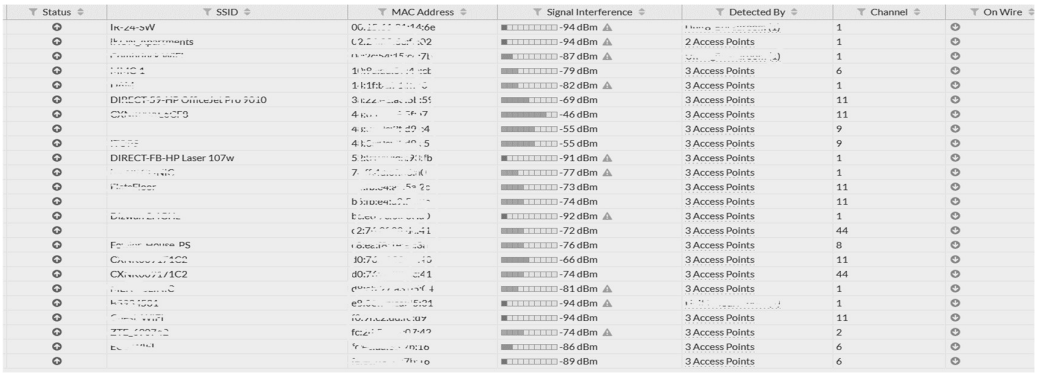


Figure: 3.6 Metasploit detected vulnerabilities

3.5.5.3 Network access scanning

Wired-side scanning: this is a type of scanning that performs an infrastructure scans via a devices that is physically connected to the network, usually by using a network cable. An infrastructure scan with OS fingerprinting was enabled so as to reveal any rogue wireless access points. The results indicates that presence of access points however, none was on the wire or could be classified as a rogue access point. Due to confidentiality reasons some information is masked. Figure 3.7 below show results of the detected wireless access points revealed through a device connected to the network via a cable.



Status	SSID	MAC Address	Signal Interference	Detected By	Channel	On Wire
			-94 dBm		1	
			-94 dBm	2 Access Points	1	
			-87 dBm		1	
			-79 dBm	3 Access Points	6	
			-82 dBm	3 Access Points	1	
	DIRECT-59-HP OfficeJet Pro 9010		-69 dBm	3 Access Points	11	
			-46 dBm	3 Access Points	11	
			-55 dBm	3 Access Points	9	
			-55 dBm	3 Access Points	9	
	DIRECT-FB-HP Laser 107w		-91 dBm	3 Access Points	1	
			-77 dBm	3 Access Points	1	
			-73 dBm	3 Access Points	11	
			-74 dBm	3 Access Points	11	
			-92 dBm		1	
			-72 dBm	3 Access Points	44	
			-76 dBm	3 Access Points	8	
			-66 dBm	3 Access Points	11	
			-74 dBm	3 Access Points	44	
			-81 dBm	3 Access Points	1	
			-94 dBm		1	
			-94 dBm	3 Access Points	11	
			-74 dBm	3 Access Points	2	
			-86 dBm	3 Access Points	6	
			-89 dBm	3 Access Points	6	

Figure: 3.7 Detected wireless access points

Wireless-side scanning: this is a type of scanning that performs an infrastructure scans via a devices that is wirelessly connected to the network, usually by using a Wi-Fi connection. A walkthrough of the Namswitch system using wireless sniffing tools such as AirMagnet or ViStumbler to gather information about access points that are within the range of the tools. The network was scanned for actively broadcasting SSIDs, hidden SSIDs, as well as passive listening for transmitted SSIDs. The discovered SSIDs were recorded and compared to a list of known legitimate SSIDs within Namswitch. Once more, no rogue access point was identified. Figure 3.8 below indicates the presence of detected wireless access points, however, they are not classified as rogue access points upon system verification.

Action	Message	SSID	Channel
rogue-ap-detected	AP DIRECT-DB-HP DeskJet 2600 series c	DIRECT-DB-HP DeskJet 2600 series	6
rogue-ap-off-air			1
client-ip-detected	Client		52
client-authentication	Client		52
rogue-ap-detected			11
rogue-ap-detected	AP Guest_		11
rogue-ap-changed			1
rogue-ap-changed			1
rogue-ap-changed			1
rogue-ap-changed			1
rogue-ap-detected			1
rogue-ap-off-air	AP Guest_ 9:9f:c2: chan 11 live 7641328 age 928	Guest_	11
rogue-ap-detected	AP NON_Apartments 02:2 7666460		1
rogue-ap-off-air			11
rogue-ap-off-air			1
rogue-ap-off-air			11
rogue-ap-detected			1
rogue-ap-changed	chan 1 live 7665867		1
rogue-ap-detected	AP Gu 9:9f:c2: chan 11 live 7640411		11
rogue-ap-changed	chan 1 live		1

Figure: 3.8 Verifying rogue access points

3.5.5.4 Segmentation testing

Nmap and Metasploit tools were used to perform segmentation testing in order to confirm the success of segmentation controls from untrusted network zones into protected and trusted networks. Segmentation testing was performed after the reconnaissance and the enumeration phases and falls under the exploitation phase. From the network scope provided, segmentation testing was carried out to test access entries from SIT and the UAT environments into the production environment. The results of this test are important indicators of how well access controls are enforced, and to test Namswitch's logical and physical network security. The attack perspective of the engagement was defined as internal users having access in the out-of-scope network (SIT and UAT) and what the user can exploit in the production environment. The results as can be seen in Figure 3.9 below. The segmentation test results show that no open ports or services were accessible running in the production environment from the out-of-scope networks such as the UAT, the figure reveals.

Figure: 3.9 Segmentation test results

3.5.6 Suggestions and reporting

Based on the result of the pen testing exercise, the researcher provided proposed remedial suggestions for identified vulnerabilities. These remedial suggestions were based on established security best practices and remedial actions stipulated in the NVD (2020) database. The suggestions are detailed in Chapter six.

The researcher also developed a standard practice protocol which will periodically and proactively mitigate the cyber threats to the Namswitch system and ensure the long-term viability and reliability of the Namibian banking system. This was done by running a script that will use the Nmap tool to periodically scan the system for vulnerabilities and perform segmentation testing and report the findings to Namswitch for remedial actions.

Finally, as part of the Reporting stage, a technical report of the pen test was shared with relevant persons at Namswitch. The report covered information from all steps and phases of the pen test. Through the initial discussion covered within the NDA, a conclusion detailing how and what data was to be exposed to parties other than Namswitch was also provided.

3.6 Data analysis

Data analysis is the process of systematically applying statistical and or logical techniques to describe, recap, condense, illustrate and evaluate data (Shamoo & Resnik, 2003). Additionally, it is an analysis of data that is derived through logical and analytical reasoning in order to identify patterns, trends, or correlations. In this study, an exploratory analysis was used on the collected data to explore the cybersecurity

strength of the Namswitch system. This was achieved through criteria's that were used to evaluate whether certain security parameters or policies are enforced. Moreover, scores were used to evaluate the severity of the vulnerabilities identified.

3.6.1 Pass/Fail criteria

An entity is said to have passed an internal or external penetration test scan if all critical and high vulnerabilities, as measured by the CVSSv3 score, are addressed, deleted, or protected by other compensatory safeguards. For example, an external facing system that could allow an authenticated, remote attacker with access to the management network to log in to the affected device using default credentials present on the system. This system would pose a severity rating of 8.8, which is high according to the CVSSv3 score, would fail a security assessment. Table 3.5 below that is based on the NIST Vulnerability Database (NVD) of 2008 and the Vulnerability Severity Ratings standard, illustrates the vulnerability rating scale used to determine the threat level rating of the vulnerabilities found. Table 3.5 provides the CVSSv3 ratings ranging from Informational to the Severe rating which is Critical.

Table 3.5 CVSSv3 Scores

CVSSv3 score	**Rating**
9.0 – 10.0	Critical
7.0 – 8.9	High
4.0 – 6.9	Medium
0.1 – 3.9	Low
0	Information

3.6.2 Automatic failures

Internal and external vulnerability scans are automatically considered as failed when certain conditions or criteria's are met or exposed. Conditions such as unsupported operating system versions, open access to databases via the Internet, the presence of built-in or default accounts and passwords. Other conditions include, the presence of any malware such as rootkits, backdoors, or Trojan horses, as well as services that do not require authentication, automatically warrant the system's failure of the penetration test. Appendix C provides the complete list of prerequisites or scores that will automatically warrant a failed assessment.

3.6.3 CVSS calculations

The Nmap tool, amongst others, were used to carry out the security tests and to provide the computation for CVSS ratings. The CVSS ratings were used to determine the severity of vulnerabilities using a numerical number called the Base Score that ranges from 0 to 10. The CVSS score dictates whether the discovered vulnerabilities are low, medium, high, or critical. Scores range from 0 to 3 for low vulnerability, 4 to 5 for medium vulnerability, 7 to 9 for high vulnerability, and 10 for critical vulnerability. Vulnerabilities that pose either high or critical scores often indicate that an attacker could potentially cause damage to the target. The Base, Temporal, and Environmental are the three metric categories in the CVSS. The Base group shows a vulnerability's inherent features. The Temporal group displays a vulnerability's characteristics that fluctuate over time; and the last metric, the Environmental group represents a vulnerability's characteristics that are specific to a user's surroundings (FIRST.Org., 2020).

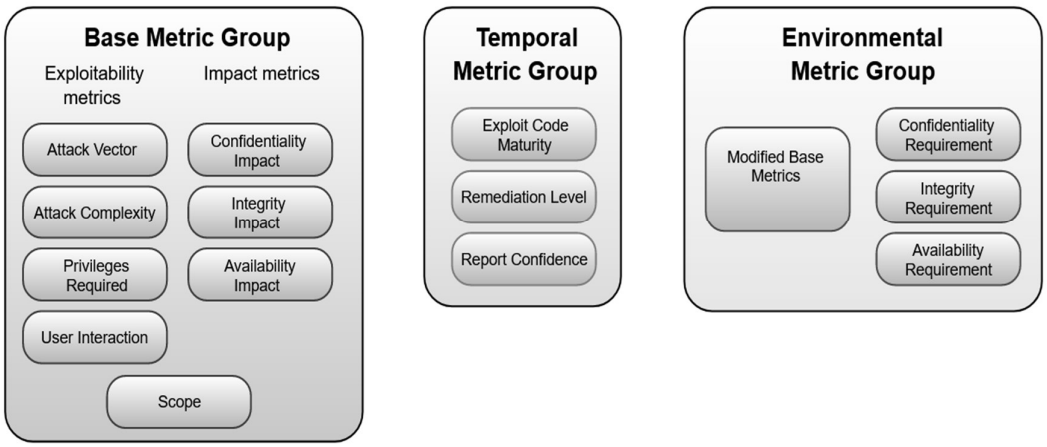


Figure 3.10 Metric Groups (*CVSS v3.1: Specification Document*, 2021)

Figure 3.10 above depict the three metric groups that made up the CVSS. Each metric group has its sub matrices. The Base Metric Group is composed of the Exploitability metrics which include the Attack Vector, Attack Complexity, Privileges Required, User Interaction and the Scope. The Impact metrics include the Confidentiality, Integrity and Availability impacts. The Temporal Metric group is composed of the Exploit Code Maturity, Remediation Level and the Report Confidence. Lastly, the Environmental Metric group is composed of the Modified Base Metrics, Confidentiality, Integrity and Availability requirements. The following section contains formulae snippet sets that are adapted from FIRST.Org for computing the Base scores, Temporal scores and Environmental scores.

3.6.4 Base Metric Group

The Base Metric Group properties represent characteristics that are unaffected by exploitability in the real world and do not change over time. There are two sets of metrics used in the Base metric group. The first metric is the Exploitable metrics which focuses on the vulnerable item, independent of any setup or other compensatory

measures. The exploitable metric is made up is made up of four components which are, the Attack vector, Attack complexity, Privileges required, and User interaction. The second metric of the Base metric group is the Impact metrics, is the ultimate determinant of the outcome of exploitation. The impact metric consists of the Confidentiality impact, Integrity effect, and Availability impact as shown in Figure 3.10 above.

3.6.5 Temporal Metric Group

The Temporal Metrics Group evaluates the present state of exploit techniques or code availability, as well as the presence of any patches and the credibility of a vulnerability's description. Exploit Code Maturity, Remediation Level, and Report Confidence are the three metrics that make up this metric category.

3.6.6 Environmental Metric Group

The Environmental Metrics category reflects the susceptibility characteristics that are impacted by the user's environment. This metric category is made up of the Modified Base metrics and Security requirements. When an organisation applies compensating controls or mitigation measures, it decreases the likelihood that a vulnerability may be exploited. Security needs, which are measured in terms of Confidentiality, Integrity, and Availability, are an indicator of an asset's business criticality.

3.6.7 CVSS v3 Scoring

The Common Vulnerability Scoring System is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat (FIRST.Org., 2020). Figure 3.11 below illustrates how the CVSS is calculated by combining the different values from the 3 groups of matrices. The Base metrics are assigned values by the pen tester, the Base equation computes a score ranging from 0.0 to 10.0. A base equation is derived from two sub equations: the Exploitability sub score equation, and the Impact sub score equation. The Exploitability sub score equation is derived from the Base Exploitability metrics, while the Impact sub score equation is derived from the Base Impact metrics. The Base score can then be refined by scoring the Temporal and Environmental metrics in order to more accurately reflect the risk posed by a vulnerability to a user's environment (FIRST.Org., 2020).

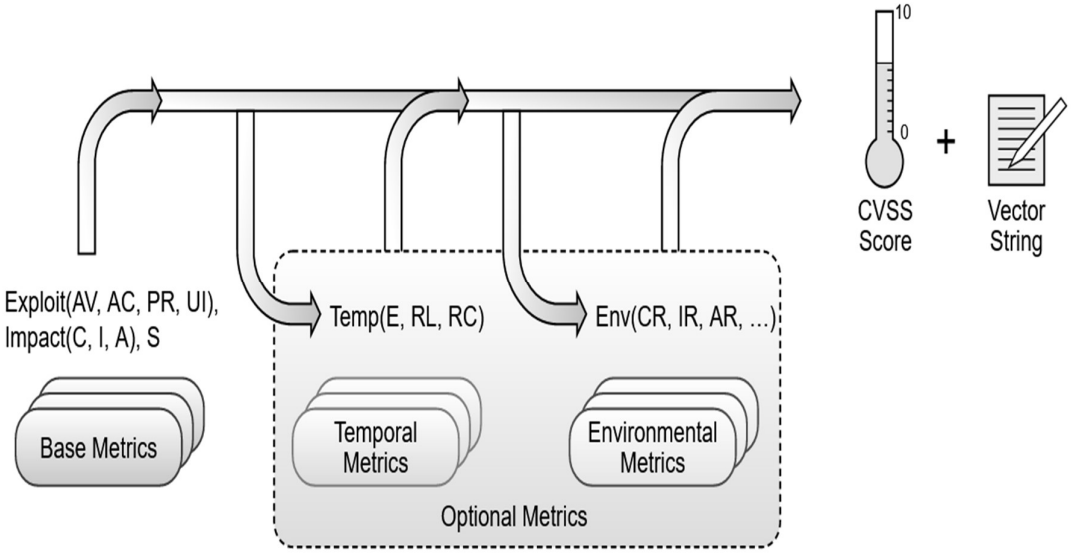


Figure 3.11 Metrics and Equations (*CVSS v3.1: Specification Document*, 2021)

Table 3.6 below lists the values that are used in the CVSS equation. Based on these values, the score is calculated to determine the severity of the vulnerability. This score varies, depending on the vulnerability.

Table 3.6: CVSSv3.1 Metrics (*CVSS v3.1: Specification Document*, 2021)

Base Vector	Temporal Vector	Environmental Vector
AV = Attack Vector AC = Attack Complexity PR = Privileges Required UI = User Interaction S = Scope; C = Confidentiality I = Integrity A = Availability	E = Exploit Maturity Code RL = Remedial Level RC = Report Confidence	CR = Confidentiality Requirement IR = Integrity Requirement AR = Availability Requirement MAV = Modified Attack Vector; MAC = Modified Attack Complexity MPR = Modified Privileges Required MUI = Modified User Interaction MS = Modified Scope MC = Modified Confidentiality MI = Modified Integrity MA = Modified Availability

The CVSS calculator equation:

CVSS:3.1/AV/AC/PR/UI/S/C/I/E/RL/RC/CR/IR/AR/MAV/MAC/MPR/MUI/MS/MC/MI/MA

Equation (3.1)

The **Base Score** is a function of the sub-score formulae for Impact and Exploitability. In this case, the Base score is calculated as:

If (Impact sub score <= 0) *0 else,*
Scope Unchanged[4] $Roundup(Minimum[(Impact + Exploitability), 10])$
Scope Changed $Roundup(Minimum[1.08 \times (Impact + Exploitability), 10])$

The Impact sub-score (ISC) is calculated as follows:

Scope Unchanged $6.42 \times ISC_{Base}$
Scope Changed $7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$
Where,
$ISC_{Base} = 1 - [(1 - Impact_{Conf}) \times (1 - Impact_{Integ}) \times (1 - Impact_{Avail})]$
And the Exploitability sub score is,
$8.22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction$

Equation. (3.2)

The **Temporal score** is calculated as follows:

$(BaseScore \times ExploitCodeMaturity \times RemediationLevel \times ReportConfidence)$

Equation. (3.3)

The environmental score is defined as,

If (Modified Impact Sub score <= 0) *0 else,*
If Modified Scope is Unchanged *Round up(Round up (Minimum [(M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)*
If Modified Scope is Changed *Round up(Round up (Minimum [1.08 × (M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence*)

Equation. (3.4)

And the modified Impact subscore is defined as:

If Modified Scope is Unchanged $6.42 \times [ISC_{Modified}]$
If Modified Scope is Changed $7.52 \times [ISC_{Modified} - 0.029] - 3.25 \times [ISC_{Modified} \times 0.9731 - 0.02]^{13}$

Where,

$ISC_{Modified} = Minimum\ [[1 - (1 - M.IConf \times CR) \times (1 - M.IInteg \times IR) \times (1 - M.IAvail \times AR)], 0.915]$

The **Modified Exploitability** sub score is,

$8.22 \times M.AttackVector \times M.AttackComplexity \times M.PrivilegeRequired \times M.UserInteraction$

4 Where "Round up" is defined as the smallest number, specified to one decimal place that is equal to or higher than its input. For example, Round up (4.02) is 4.1; and Round up (4.00) is 4.0.

CVSS Metric Levels

Table 3.7: Metric Levels, Source (*CVSS v3.1: Specification Document*, 2021)

Metric	Options	Value
Attack Vector (AV)	Network (N) Adjacent (A) Local (L) Physical (P)	0.85 0.62 0.55 0.20
Attack Complexity (AC)	Low (L) High (H)	0.77 0.44
Privileges Required (PR)	None (N) Low (L) High (H)	0.85 0.62 (0.6 if scope is changed) 0.27 (0.5 if scope is changed)
User Interaction (UI)	None (N) Required (R)	0.85 0.62
Scope (S)	Unchanged (U) Changed (C)	—
Confidentiality (C) / Integrity (I) / Availability (A)	High (H) Low (L) None (N)	0.56 0.22 0.00

Table 3.7 above depicts the metric values used in calculating the CVSS scores. Each metric value has an associated constant or numeric value which is used in the formulas

as shown in the table. The value for the Network (N), which falls under the Attack Vector metric (AV) is 0.85. While the Adjacent (A) has a value of 0.62 and the Local (L) is value to 0.55.

Sample calculation

A website running on a Linux server that can be hacked via the internet in which the hacker with bare minimum skills does not require access credentials and uses a script to perform the attack and gained full control of the system.

To begin with, this is a vulnerability that may be exploited via the network and the vulnerable component in this attack is a web server. **Attack Vector** is a **Network** and the **Attack Complexity** is equals to **Low**, since the vulnerability may be exploited with no additional skills.

Secondly, **Privileges Required** is equals to **None**, since the hacker does not need any privileges to exploit the vulnerability. In this case, the scope won't change because the vulnerability is caused by a script and all the impact is on the OS, as a result, **Scope** is **Unchanged**.

Furthermore, since the hacker gained full control of the system, then Confidentiality, Integrity and Availability is under high risk and so, **Confidentiality, Integrity, and Availability Impact** are equals to **High**

Lastly, **User Interaction** is **None**, because the vulnerability may be exploited without the need for a user interaction. The vulnerability may be exploited with a HTTP request crafted specifically for exploits.

In this example, the CVSSv3 Vector string will be:

CVSS v3.1 Vector String: **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**

By using the CVSSv3.1 calculator as shown in Figure 3.12 below, the **CVSS v3.1 Overall Score: 9.8.** The figure displays and highlights the values (AV, AC, PR, UI & S) used in computing the CVSS score for this vulnerability.

Figure 3.12 *Score of sample calculation*

3.6.8 Reporting

All observations were reported using the Nmap standard reporting template. The penetration test reports showed vulnerabilities and their classification according to the CVSSv3 ratings. The vulnerabilities that could adversely affect critical operations and assets were documented, classified, and associated with threats and the possible impact they had on systems according to their likelihood of occurrence and the potential damage.

Tables were used to classify asset compliance, indicate the number of vulnerabilities per host, as well as the remediation time according to the vulnerability severity. Each vulnerability was explored and a CVSSv3 severity rating was associated with each vulnerability. This data was then used to perform the penetration tests. The vulnerability ratings were further used to determine the security posture of the Namswitch system.

3.7 Research ethics

Prior to the commencement of the study, approval to conduct the penetration tests and vulnerability assessments was sought from a Namswitch senior official, on behalf of Namswitch. Furthermore, ethical clearance was sought from UNAM's Research Ethics Committee (UREC) as well as approval from the Centre of Postgraduate Studies (CPGS) (refer to Appendix D). The purpose of this research was fully explained to the owners of the systems prior to carrying out the research. Since this study was conducted on highly sensitive data, confidentiality was ensured by applying strong encryption during the storage and transmission of data. Sensitive information was also masked and sanitised.

3.8 Chapter summary

This chapter provided a detailed outline of the research approach used in order to achieve the research objectives. Furthermore, the chapter presented the mixed methods research techniques employed in this research. The chapter also provided a brief introduction to the approach and design used to develop the penetration testing and vulnerability assessment model for the Namswitch system. Moreover, an overview of how the research was carried out to determine and evaluate the security of the Namswitch systems against current cyber-attacks was outlined.

Ethical considerations were observed. The methodology used considered ethical standards in the design of the study, selection of research tools, and testing procedures. In summary, the chapter introduced the procedures followed to accomplish the aims and objectives of this research by ethically penetrating or hacking the Namswitch system. The next chapter analyses the results obtained and present the findings of the analysis process.

CHAPTER FOUR

RESULTS

This chapter presents the results of the pen test. The findings were divided into two sections namely the external pen test, and the internal pen test. Some configuration information was censored in order to preserve organizational security and confidentiality. The chapter is concluded with a thorough presentation of the Namswitch system's outcomes, as well as a summary of the chapter.

4.1 Results of the external pen test

An external pen test was conducted and seven (7) IP addresses associated with 7 external facing Namswitch systems were submitted for the pen test. Of the 7 IP addresses, only two (2) IPs reserved for the mail and VPN servers were accessible from the public domain. As such, the pen test could only be conducted on these two systems. The pen test revealed the presence of open ports on these systems, which suggests that the systems were listening for a connection and were therefore actively accepting TCP connections, User Datagram Protocol (UDP) datagrams, or Stream Control Transmission Protocol (SCTP) associations. These systems did not, however, publish crucial information, specifically information that could be used to compromise the confidentiality, integrity, or availability of Namswitch resources. Furthermore, the target IP addresses were neither registered in well-known public databases as spamming hosts, nor banned as known malicious IP addresses. Table 4.1 below illustrates the results of the port scans on the mail and VPN servers in terms of types of protocols, port numbers, and services running on these hosts.

Table 4.1 – Results of the Nmap scan on the external networks

Address of Host	Protocol/Port/Service/Status	Comments
197.234.74.11	TCP / 23 / TELNET / OPEN TCP / 25 / SMTP / OPEN TCP / 80 / HTTP / OPEN TCP / 443 / HTTP / OPEN TCP / 10 / UNKNOWN / FILTER TCP / 11 / SYSTAT / FILTERED	All ports on the target host not specified here are in a CLOSED state.
197.234.69.73	TCP /3/COMPRESSNET / FILTERED TCP / 7 / ECHO / FILTERED TCP / 9 / DISCARD / FILTERED TCP / 10 / UNKNOWN / FILTER TCP / 11 / SYSTAT / FILTERED TCP / 80 / SMTP / OPEN TCP / 23 / SMTP / OPEN TCP / 10443 / SMTP / OPEN UDP / 161 / SNMP / OPEN,	All ports on the target host not specified here are in a CLOSED state.

The data from Table 4.1 above shows the results of the Nmap scan on the external networks which reveals that from the two (2) IPs that were scanned, 8 were open ports, 7 were filtered ports and some ports had unknown status, while the rest of the ports were in a closed state.

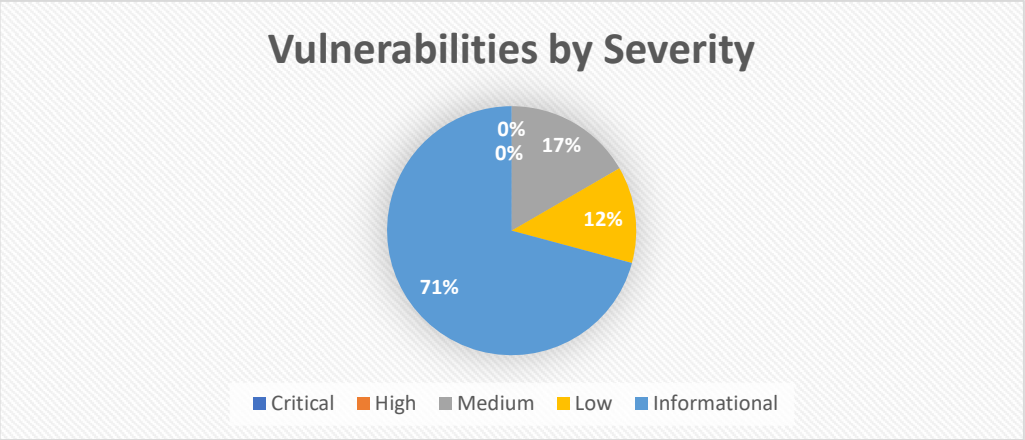


Figure 4.1 Total number of vulnerabilities identified on the two external facing systems

Figure 4.1 above shows that there were no vulnerabilities classified as Critical or High. Further, the figure illustrates that there were four vulnerabilities, accounting for 17% of the total vulnerabilities were classified as Medium, three vulnerabilities, accounting for 12% of the total were classified as Low, while the 17 vulnerabilities, accounting for 71% of the total vulnerabilities detected were Informational.

The results in Figure 4.1 above illustrate that the Namswitch system was secured from most external threats, despite the fact that the scan status attestation would be non-compliant due to the presence of a Medium vulnerabilities with a severity rating score of 6.4. One of the medium vulnerabilities found was the use of an expired SSL certificate on the VPN server. It is paramount that this vulnerability be addressed as they can have catastrophic effects if not remediated. Vulnerabilities on external facing system could be infiltrated by malicious intruders from the public domain. These intruder's attack systems to compromise confidentiality, integrity and availability of systems in order to damage reputation, steal confidential information, or for personal gains, etc.

4.2 Results of internal pen test

An Nmap scan of the internal network was also conducted in order to determine the resilience of the Namswitch system from insider threats. Vulnerabilities on internal systems are often more exposed to malicious internal users or intruders who have already gotten past the initial network security or physical security. The internal scans revealed the presence of vulnerabilities with varying severity ratings. The partial results are as shown in Table 4.2 below.

Table 4.2 – Results of the Nmap scan on the internal networks

Address of Host (Hostname)	Protocol/Port/Service/Status	Comments
10.XX.XX.7	TCP / 22 / SSH / OPEN TCP / 1720 / H323Q931 / OPEN TCP / 2000 / TCPWRAPPED / OPEN TCP / 5060 / SIP-PROXY / OPEN UDP / 123 / NTP / OPEN	All ports on the target host not specified here were in a CLOSED state.
192.XX.XX.150	TCP / 22 / SSH / OPEN TCP / 443 / HTTP / OPEN TCP / 2000 / TCPWRAPPED / OPEN TCP / 5060 / TCPWRAPPED / OPEN	All ports on the target host not specified here were in a CLOSED state.

The data from Table 4.2 above reveals that from the fifty (50) IPs that were scanned, there were a number of open ports and a number of filtered ports. The rest of the ports were in a closed state. The results further reveal that there were certain common and default ports among the open ports discovered, such as port 22 for SSH, port 443 for HTTPS and port 80 for HTTP.

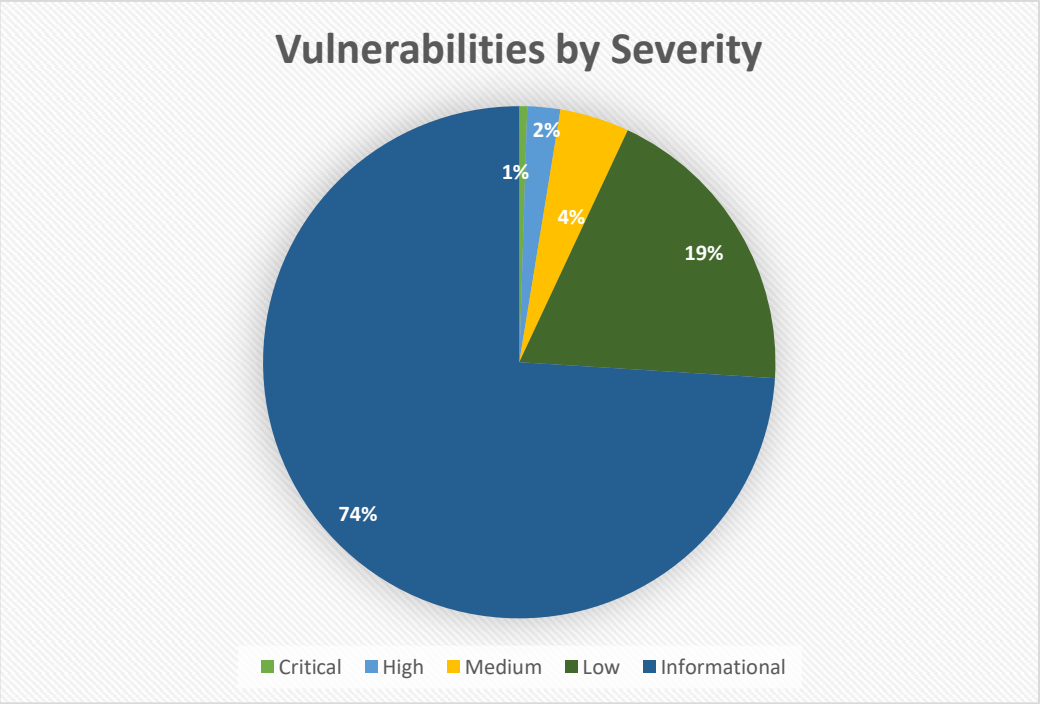


Figure 4.2 A pie chart of the total number of vulnerabilities identified on 50 systems

Figure 4.2 above illustrates that during the nMap scan, 1593 vulnerabilities were found. Of the total 1593 vulnerabilities, eight vulnerabilities, accounting for 1% were Critical, 33 vulnerabilities, accounting for 2% were High, and 70 vulnerabilities, accounting for 4% were Medium. Vulnerabilities classified as Low and Informational accounted for 303 (19%) and 1179 (74%) of the total vulnerabilities detected.

Vulnerabilities with a critical rating require immediate attention as they are relatively easy for attackers to exploit and may grant full control of the affected systems. Twelve (12) Namswitch internal systems contained critical vulnerabilities, making them most vulnerable to attack. In contrast, vulnerabilities with a high severity rating are often harder to exploit and may not provide the same access to affected systems as vulnerabilities with a critical rating do. The pen test discovered vulnerabilities rated high on 16 systems. Vulnerabilities with a medium security rating often provide information that can assist attackers in mounting attacks on other systems and

networks. Medium vulnerabilities were found on 16 systems. Medium vulnerabilities similarly require to be mitigated in a timely manner; however, they do not require urgent attention as those with a critical or high severity rating do. Lastly, six systems did not have any vulnerabilities. Below is a discussion of the vulnerabilities discovered. The vulnerabilities are grouped and presented according to the types of devices found such as windows servers, the network, and network segments.

4.2.1 Windows servers

The results of the internal scans revealed the presence of vulnerabilities such as default ports and services, including services that are not required on those hosts. The results also revealed the security configurations made on the hosts and it was observed that some servers contained unmanaged or default user accounts. Furthermore, it was discovered that some hosts had no security hardening configurations such as disabling of insecure protocols, removal of default credentials, or configuration of security policies. This was detected on some of the running services such as the DNS and Network Time Protocol (NTP) servers which used default configurations. The results also exposed hosts with weak security configurations such as the use of the Data Encryption Algorithm (DES) encryption algorithm and the Rivest Cipher (RC4) ciphers which are flawed. Finally, it was noted that the servers operated different versions of the Windows Server operating system, ranging from Windows Server 2008 to Windows Server 2019.

4.2.2 Network device and wireless scan

The results from the network devices revealed default SNMP configuration information. The Metasploit scan results exposed the CVE-2019-1752 Denial of Service vulnerability which can allow an unauthenticated remote attacker to reload a device. Other results indicated transmission of management traffic in clear text, which can potentially allow information leakage through attacks such as through the man-in-the-middle attack. Moreover, results from the wireless scans revealed the presence of rogue wireless access points.

4.2.3 Segmentation test results

It was discovered that there existed entry points from the untrusted network into the trusted networks. This is a strong indication of the existence of some poor segmentation control policies. The next chapter provides and discusses these vulnerabilities in detail.

4.3 Chapter summary

Seven (7) IP addresses assigned to the external scope were scanned and assessed. The results indicate that only two of the publicly available IPs were accessible through the internet. Open ports and the types of running services and their versions were discovered and explored further for possible exploitation. In contrast, there were at least 50 internal IP addresses scanned and the findings revealed the presence of several vulnerabilities. In the next chapter, the results presented in this chapter are further analysed and discussed, as well as the risk and CVSS ratings of these findings.

CHAPTER FIVE

DISCUSSION

The results of the penetration test and vulnerability assessment performed on the Namswitch system are discussed in this chapter. The chapter also includes additional information which an attacker may leverage to further their attack, as well as conclusions and summaries of the discussion.

5.1 External pen test

The vulnerabilities discovered on the two external facing systems were further explored and their severity ratings were calculated. The two external facing systems were the VPN and the mail server.

5.1.1 VPN Server

It was observed that the VPN server made use of an expired Secure Sockets Layer (SSL) certificate. In addition, the installed SSL certificate's subject name did not match the name of the entity, Namswitch. This vulnerability allows potential attackers to create fake sites identical to the organisation's VPN site. While an SSL certificate proves the validity of a trusted owner of the domain, an expired SSL certificate cannot be trusted. Moreover, an expired certificate may cause serious damage to the organisation's credibility (OWASP, 2020). By exploiting this vulnerability, an attacker could launch a man-in-the-middle attack and obtain user account credentials to launch additional attacks, such as accessing the VPN server. An expired SSL certificate has a medium severity rating and a CVSS score of (AV:N/AC:L/Au:N/C:P/I:P/A:N) is equals to a 6.4.

5.1.2 Mail server

It was observed that this system had several vulnerabilities. Firstly, the system was found to be disclosing its private IP information which should ideally be hidden or masked. Exposure of such IP information creates an information disclosure vulnerability which a remote, unauthenticated attacker can exploit to learn about the server's internal IP address. This information can be used by an attacker to increase knowledge of the internal systems.

Secondly, further evaluation of the services revealed other vulnerabilities such as the application of medium to low security ciphers. These ciphers included the MD2 and MD4 weak hashing algorithms, as well as the DES for encryption of data. These security protocols use a key of insufficient length which makes it easier for the encryption scheme to be broken. This can result in compromised data confidentiality. It was also discovered that the mails server system used SSLv2/v3 and TLS1.0. These technologies provide minimal security and can be easily compromised within reasonable time to reveal confidential information (OWASP, 2020).

A malicious user can leverage these vulnerabilities to perform attacks such as man-in-the-middle attacks, data stream manipulation, or sensitive information disclosure. These attacks could compromise the integrity and confidentiality of communications. This vulnerability has a low severity rating and a CVSS score of (AV:N/AC:M/Au:N/C:P/I:N/A:N) which is 4.3.

Figure 5.1 below demonstrates the low strength ciphers configured on the email server, such as *MD2 and MD4*, RC4 which are deprecated.

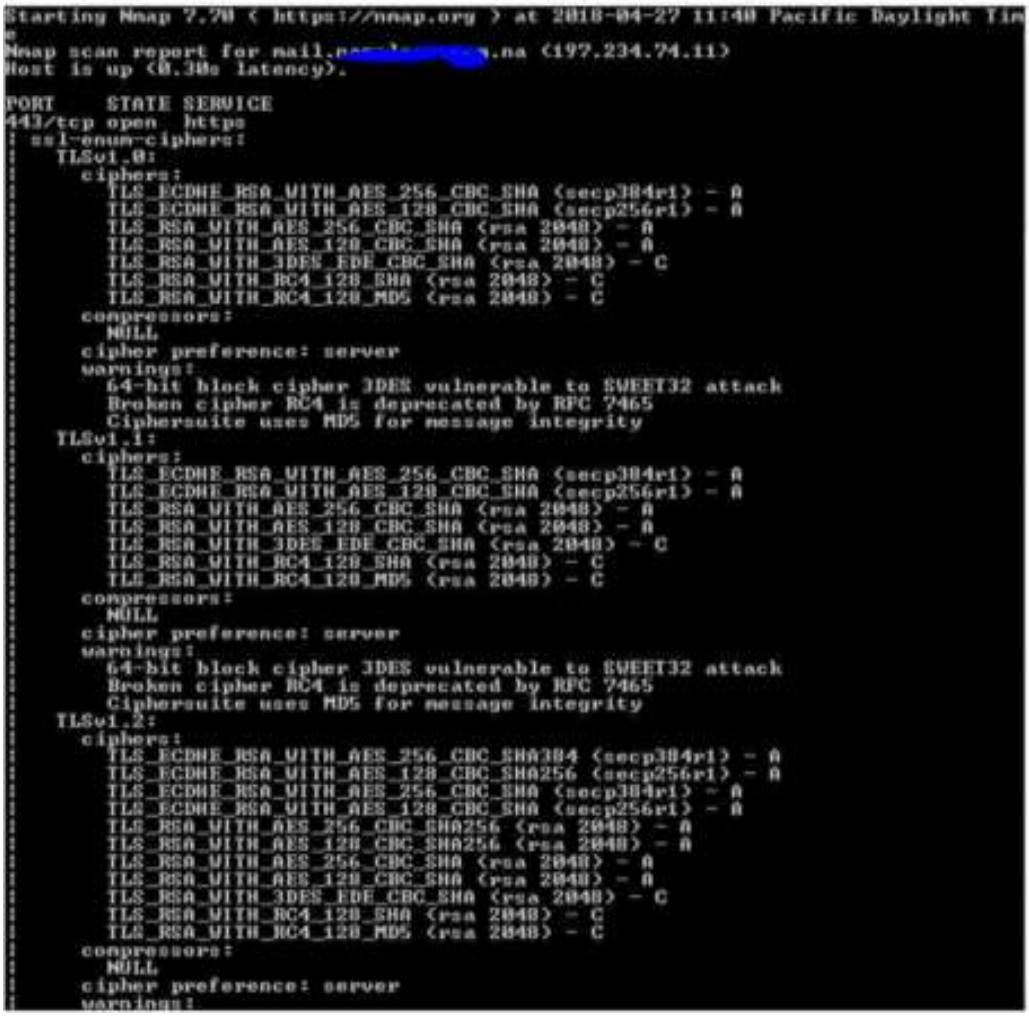


Figure 5.1 Low strength ciphers such as MD2 & MD4 used on the email server.

5.2 Internal pen test

This section details the vulnerabilities found and the attack options which an attacker can employ in order to compromise an internal network. The vulnerabilities are grouped in terms of the type of devices covered such as Windows servers, network devices, and segmentation testing.

5.2.1 Windows servers

a) Default credentials

A system was found to be using an SNMP service running a default community name which could potentially allow attackers to guess the credentials of the default account and gain access to this device. Default credentials are built-in accounts provided by the manufacturer (Microsoft, 2020). These accounts are used to configure the infrastructure and are intended for first time use. These accounts can, however, be used to gain access to systems and often attackers use these credentials to create other accounts (Sarala & Angel 2011). Figure 5.2 below shows a sample output of the successful connection to a machine after logging in with default SNMP credentials and the attacker could further use this information to attempt to login into this system with the accounts provided and possibly gain full access and perform further attacks. This vulnerability had a high severity rating and a CVSSv3 score of: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L which is 7.3.

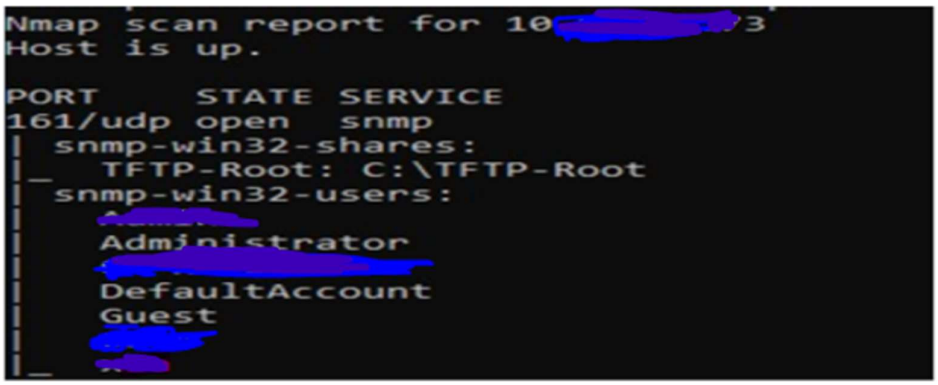


Figure 5.2 Successful connection to a host with default credentials

Similarly, other systems were found using root accounts with no password, this was revealed through telnet login with the user account called 'root' and without a password and to execute the 'id' command. This method would enable attackers to

gain full access to these systems and can perform any kind of malicious acts on these systems. This vulnerability had a Critical severity rating and a CVSSv3 score of: AV:N/AC:L/AU:N/C:C/I:C/A:C which is 9.8.

b) SMB signing

It was observed that some hosts did not allow SMB signing. SMB signing allows the recipient of an SMB packet to confirm their authenticity and helps prevent man-in-the-middle attacks targeted against SMB servers (Hackdefense, 2019). Without SMB signing an attacker can spoof an SMB client, perform a session hijack by modifying the client-server data stream, pose as the client device using a legitimate authentication session, and then gain unauthorized access to data (Grangeia, 2004). This vulnerability has a medium severity rating and a CVSS rating of CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N which is 5.9.

c) DNS Server Cache Snooping

It was observed that a DNS server was responding to queries from third-party domains that do not have the recursion bit set. An attacker can make non-recursive queries to a DNS server in order to look for records potentially already resolved by this DNS server for other clients. Depending on the response, an attacker can use this information to potentially launch other attacks (Grangeia, 2004). This creates an opportunity for attackers to determine which domains have recently been resolved through these name servers and subsequently the hosts that were recently visited (Grangeia, 2004). This vulnerability had a medium severity rating and a CVSSv3 score of: AV:N/AC:L/Au:N/C:P/I:N/A:N which is 5.0.

d) NTP amplification attacks

The research identified that the NTP server was responding to mode 6 queries. An attacker could potentially exploit this vulnerability via crafted mode 6 queries and execute a Denial of Service (DOS) attack. Moreover, devices that respond to these queries have the potential to be used in NTP amplification attacks (Grangeia, 2004). This vulnerability has a medium severity rating and a CVSSv3 score of:

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L which is 6.5

5.2.2 Network Devices

a) SSH Server CBC Mode Enabled

It was established that some network devices running the SSH service were configured to support Cipher Block Chaining (CBC) encryption. This enabled the use of low strength security protocols such as RC4, MD5 and DES-CBC. This may allow an attacker to recover the plaintext message from its cipher text. When the attacker performs a man-in-the-middle attack and captures SSH traffic, the captured traffic can be deciphered with minimal effort (NIST, 2020). This is classified as a vulnerability with a low severity rating and a CVSS score of: AV:N/AC:H/Au:N/C:P/I:N/A:N which is 3.0.

b) NAT64 denial of service vulnerability

It was discovered in some network devices that the Network Address Translation 64 (NAT64) function allowed an unauthenticated, remote attacker to cause either an interface queue wedge, or a device reload, which can result in a denial of service (DoS) (NIST, 2020). An attacker could exploit this vulnerability by sending specific IPv4

packet streams through the device. This was a high severity vulnerability rated: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H which is 7.5

Other significant flaws such as the use of insecure services such as the use of Telnet service and File Transfer Protocol (FTP) services, services that have not been updated or patched, the use of low-security ciphers and encryption methods, as well as misconfigurations that might lead to the disclosure of sensitive information were also discovered. Mitigation controls were provided for these vulnerabilities as well.

5.2.3 Segmentation testing

Although the scan results revealed entry points from the untrusted network into the trusted network, the researcher could not exploit any of the systems other than exploring the vulnerabilities identified. However, it is imperative that segmentation controls be reviewed as attackers with emerging tools could gain access and compromise the entity's confidentiality, integrity, or availability of systems.

5.3 Chapter summary

It was revealed that several vulnerabilities existed on the Namswitch system. Additionally, it appears that the external facing systems had medium to low vulnerabilities, which if exploited could compromised the availability of these systems. Furthermore, vulnerabilities with high severity ratings on the Namswitch's internal systems were analysed and the results suggested that some of Namswitch's internal systems were susceptible to insider threats. All these vulnerabilities can be used to compromise the Namswitch's ICT resources and cause damage to its reputation. As such, these vulnerabilities require immediate attention in order to

prevent cyber intrusions on the Namswitch system. The researcher proposed corrective actions to address the identified vulnerabilities and these actions are listed in the next chapter. The next chapter presents cutting edge and recommended cybersecurity best practices which can be implemented to safeguard the Namswitch system.

CHAPTER SIX

RECOMMENDATIONS

The recommended remediation solutions for protecting Namswitch against cyber-attacks are presented in this chapter. In addition, the chapter includes the NAMSAFE Protocol that was aimed at exposing vulnerabilities and associated threats on a regular and proactive basis as well as to provide remedial actions to identified vulnerabilities.

6.1 External remedial steps

The researcher studied available options that can be implemented to eliminate or mitigate the identified vulnerabilities in order to protect against threats.

6.1.1 VPN Server

a) Expired Certificate on the VPN Server

The vulnerabilities discovered on the VPN server were based on the SSL certificate. A recommendation was provided to Namswitch to obtain a valid certificate from a reputable certifying authority (CA). Namswitch was further encouraged to ensure that certificates are renewed before they expire.

6.1.2 Email Server

a) Low Security protocols on the email server

Several vulnerabilities with severity ratings ranging from low to medium were a result of the use of low to medium strength cipher suites. This puts data in transit at the risk of being decrypted by attackers. It was therefore recommended that the use of TLSv1.1

and its earlier versions, the use of static keys, as well as the use of low to medium cipher suites be discontinued. It was further recommended that the Namswitch team implement strong ciphers such as AES256 algorithms for the encryption of data and SHA256 for password hashing, so as to enhance data security.

b) Internal IP disclosures

To protect the mail server from the exposure of internal IP information, it was advised that the Namswitch team installs the Microsoft patch intended to address this vulnerability. The researcher also provided configuration steps that could be employed to safeguard against this vulnerability.

6.2 Internal system remedial steps

An investigation was also conducted on remedial actions for the vulnerabilities discovered on the internal systems. These recommendations are grouped based on the type of devices and are presented as follows.

6.2.1 Windows Servers

a) Default credentials

It was strongly advised that all system configurations be reviewed to ensure that default user accounts are either removed, disabled, or changed from their default settings. This review should also include default ports.

b) SMB Signing

This vulnerability can be remediated by enforcing message signing on the host through a group policy change. This configuration varies depending on the Operating System. For example, in Windows, this can be implemented through the *'Microsoft network server: Digitally sign communications (always)'* option.

c) SMB DNS server cache snooping

To safeguard against this vulnerability, it was recommended that the DNS server prevents remote clients from performing recursive DNS queries for domains on which the target DNS server is not authoritative (Grangeia, 2004). Appendix C provides step by step configurations that can be applied

d) SMB NTP amplification attacks

To vulnerability can be remediated by hardening configurations on the NTP server through the restriction of NTP mode 6 queries (Cybersecurity & Infrastructure Security Agency, 2016).

6.2.2 Network devices

a) SSH server CBC mode enabled

This vulnerability has a low severity rating. The countermeasures to guard against attacks aimed at this vulnerability vary. Since this vulnerability was addressed in the newer versions of the SSH service such as SSHv2 (NIST, 2020), the researcher

recommended the easier remedial action of upgrading to the latest version of this service, as opposed to the applying fixes.

b) NAT64 Denial of Service Vulnerability

The preferred recommendation to this vulnerability with a high severity rating was to upgrade the software to the latest version of this protocol.

6.2.3 Segmentation testing

It was recommended that segmentation control policies be reviewed to ensure that only necessary services are permitted. The client was also advised to conduct routine assessments on logical access control policies through periodic firewall rule reviews. This ensures that all entry points into trusted areas and areas with critical data are protected with intrusion prevention systems (IPS). Furthermore, it ensures that old rules or rules that are no longer required are removed.

6.3 The NAMSAFE protocol

The NAMSAFE Protocol is a proposed model for the proactive and periodic management of vulnerabilities on the Namswitch system through the active scanning of systems for vulnerabilities. The NAMSAFE Protocol further provides mitigation strategies to remedy the identified vulnerabilities. Implementation of the NAMSAFE Protocol will eradicate the issues highlighted in Chapters three, four and five.

Figure 6.1 below shows a data flow diagram that indicates the different stages within the NAMSAFE Protocol. The data flow diagram below demonstrates and correlates to

the developed pen testing model. Furthermore, the figure indicates that after the asset discovery a vulnerability assessment is carried out, vulnerabilities are classified, researched for remedial actions and finally, a report will be sent to the system owners through email notifications. There's a wide range of available vulnerability management and penetration testing solutions. However, finding the best solution presents some difficulties. The majority of solutions are pricy, yet, most are generic and not produced specifically for the clients. The price of buying a custom made is considerably greater (Deloitte, 2018). This are some of the constraints that inspired the composition of this script.

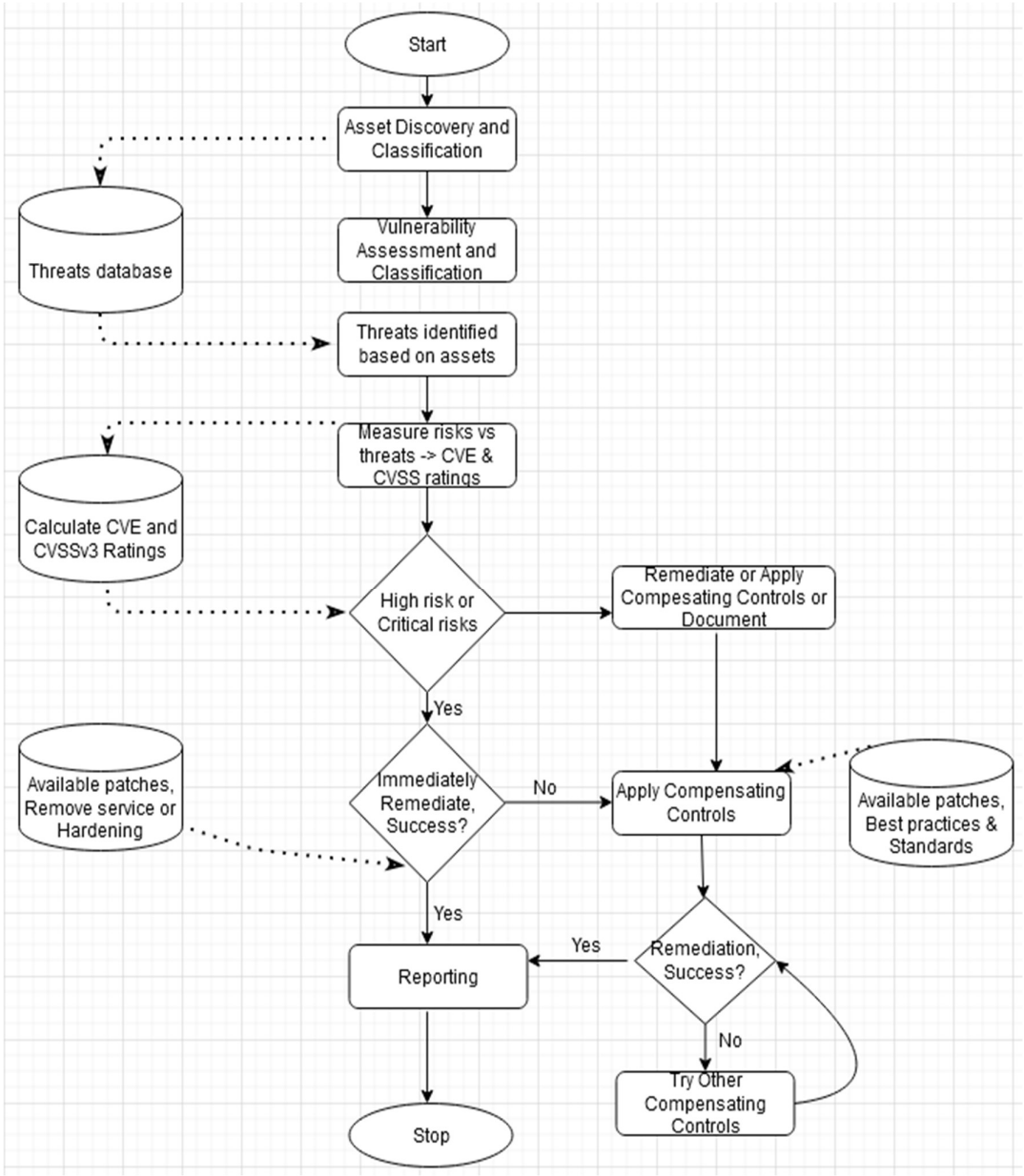


Figure 6.1 Data flow diagram for the NAMSAFE Protocol

The NAMSAFE Protocol was created by combining tools such as the Nmap, OpenVAS and openSSL actioned by a script running on a Linux machine in order to accomplish the automatic execution of scanning. The NAMSAFE Protocol was designed to align to the developed pen test model that followed PTES standard and combining the PTF framework together with the NIST cybersecurity framework. During the discovery phase, the NAMSAFE Protocol was intended to scan target

systems and networks which if hacked, might compromise the Namswitch system's integrity, confidentiality, or availability.

This script was intended to scan for all open ports and identify associated services. The NAMSAFE Protocol was set to run during the reconnaissance, and enumeration processes to identify risks related to vulnerabilities and to determine their risk ratings such as the CVSSv3 scores. Furthermore, the NAMSAFE Protocol will notify system users of vulnerabilities found and will further provide a report and recommendations for mitigation of the identified vulnerabilities. Namswitch will be notified as soon as vulnerabilities with critical, high, medium or low security ratings are discovered.

Finally, the NAMSAFE Protocol was designed to run regularly and proactively at predetermined intervals, sending results or alarms to a predefined email address. In cases when vulnerabilities cannot be immediately remediated, the methodology provides compensating measures to protect against attacks targeting these vulnerabilities. All this will be accomplished through an active connection to the internet CVE database to enable searching of vulnerability ratings and remediation's. The script used by the NAMSAFE Protocol is provided in Appendix E. The NAMSAFE Protocol will be used to conduct both internal and external pen tests as well as network segmentation testing.

6.5 Chapter summary

It was strongly advised that a 360° review of the security policies and hardening guides be done in order to ensure that all system configurations are aligned according to these policies and guidelines. Vulnerabilities that could not be removed must be mitigated by other means such as through the use of IPS or anti-virus solutions. Another means

of mitigating vulnerabilities is through the segmentation of systems, and by ensuring that access to vulnerable systems is controlled by other security features such as the use of Access Control Lists (acl). Furthermore, access to these systems should be granted to users with necessary permissions, often referred to as necessary or least privilege. The NAMSAFE Protocol was design to proactively scan and manage vulnerabilities, while also providing remedial steps for identified vulnerabilities on the Namswitch system. This will ensure a tested and resilient cyber environment for Namswitch. The recommendations provided in this Chapter are not the only viable options to protect Namswitch systems from threats. However, when implemented they can improve the cyber resilience of the internal and external Namswitch systems.

CHAPTER SEVEN

CONCLUSION

This chapter concludes the study. Concluding this study is based on the results of the study, literature and empirical data analysis. In this chapter, suggestions for future research are also presented.

7.1 Research conclusion and contributions

The first objective of this study was to develop a pen testing and vulnerability assessment methodology for the Namswitch system. This objective was achieved through the development of the penetration testing model known as the NAMESAFE Protocol, which was derived from several pen testing models from within the financial industry. The developed pen testing model was tailored to suit the target system. The NAMESAFE Protocol will proactively scan the Namswitch system for vulnerabilities and notify system owners of findings and possible remedial strategies through email notifications.

The second objective was to conduct, a pen test to expose vulnerabilities within the Namswitch system's architecture and report the findings. This was again achieved by using the NAMSAFE Protocol to conduct a pen test on the Namswitch system. The assessment and test included both internal and external systems. The results of the test revealed the presence of Low to Medium vulnerabilities on the external systems while the internal systems posed Low to Critical vulnerabilities. The scan status attestation of the Namswitch system was non-compliant due to the presence of Medium vulnerabilities on the external facing systems, as well as the presence of High and

Critical vulnerabilities on the internal systems as shown in Chapters three, four and five.

The Namswitch system was assessed against configuration best practices and standards on security. This aided in achieving the third objective which was to assess the security posture of the Namswitch system's configurations against best practices, standards and current practices. The findings revealed that the target systems had a few systems that were poorly configured and did not provide adequate protection against cyberattacks this was revealed through the presence of default configurations on some systems, while other systems followed best practices and configuration standards such as the use of strong cryptographic protocols. Specifically, some systems had not fully implemented security hardening guides applied, while other systems were configured with security protocols ranging from low to high. The study also revealed that some internal systems posed no vulnerabilities, and most internal systems were inaccessible from the public network. A few external systems were found with low to medium vulnerabilities.

Finally, an appropriate mitigation strategy to remediate issues identified was developed. To achieve this, the study developed a prescriptive protocol (NAMSAFE), that, when employed regularly, will minimise the occurrences of most vulnerabilities encountered in this study. The system owners were also made aware of other alternatives to the proposed recommendations for protecting Namswitch from cyber-attacks.

7.2 Recommendation for future research

The research can be pursued in a wide range of possible directions. Future studies can focus on improving and adding more information to the developed model in order to cover other systems from various industries such as health, mining, etc. Further studies maybe required on comparing similar reports from within the same industry, which can be used by other institutions for benchmarking the security posture of their systems. Additional research can also be made at a larger scope to include the whole banking ecosystem in Namibia in order to give an overview of the strength of the security of the Namswitch system and the Namibian Payment System at large. Other areas for future research can be the development or integration of the NAMESAFE Protocol into a single vulnerability management solution. Lastly, future research can also focus on adding other cybersecurity assessments that would focus on other areas such as analysing security impacts on business continuity and risk assessments.

7.3 Research contributions

The main contribution of this work was therefore the development and implementation of the NAMSAFE Protocol. The NAMSAFE Protocol was successfully implemented and it provided a prescriptive methodology for maintaining ongoing reliability and robustness to the Namibian banking system. The developed protocol will help to combat cybersecurity issues within the Namibia financial sector. This study serves as the basis to continue to expand and update the locally recognised cyber security body of knowledge. The NAMSAFE Protocol supports efforts to deal with complex and emerging cybersecurity threats within the banking industry through providing the foundation of security objectives and activities that can be employed. The protocol

draws on standard methodologies that are used to assess various types of cyber risks, threats and vulnerabilities and these can be easily applied at the individual and organisational level as implementation guidelines are provided.

The next section presents a list of materials cited in this study.

8. REFERENCES

Alweendo, T. (2010). *Annual report - 2010*. https://www.bon.com.na/Economic-information/Annual-Reports.aspx

Allsopp, J. (2009). *Developing with web standards.* (8th ed.). California. O'Reilly.

Antunes, N., & Vieira, M. (2013). *An integradet tool to detect vulnerabilities inservice-based infrastructures.* Proceedings-IEEE 10th International Conference on Service Computing, SCC 2013, 280-287.

Atlas VPN. (2021). *Businesses were attacked over 700 million times across the world by hackers in the span of only 30 days*. https://www.integraldefence.com/cyber-news/atlas-vpn-recently-published-a-report-documenting-over-720-million-cybersecurity-threats-recorded-over-the-last-30-days-digital-information-world/

Ayofe, A., & Irwin, B. (2010). Cyber security: Challenges and the way forward. *Computer Science and Telecommunications, 6*(29), 5-6.

Bacudio, A. G., Yan, X., Chu, B. B., & Jones, M. (2011). An overview of penetration testing. *International Journal of Network Security & Its Applications, 3*(6), 1-9.

Bank of Namibia (n.d.). *BID-30 information security*. https://www.bon.com.na/CMSTemplates/Bon/Files/bon.com.na/be/be1d4b35-dffc-4c0d-85a1-6faf52e3d836.pdf

Bishop, M. (2007). About penetration testing. *Security & Privacy, IEEE, 5*(6), 84-87. doi:10.1109/msp.2007.159

Chang, Z. & Li, S.. (2019). *The IoT Attack surface: Threats and security solutions.* https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions

Checkpoint. (2020). *Namibia cyber security skills gaps tackled*. https://www.cesict.com/cyber-security-interview-with-namibian-broadcasting-corporation/

Cheim, P. T. (2014). *A study of penetration testing tools and approaches.* https://core.ac.uk/download/pdf/56364552.pdf

CIS. (2018). *Vulnerabillity assessments.* cisecurity.org: https://www.cisecurity.org/services/vulnerability-assessments/

Creswell, J. (2013). *Research design.* Sage.

Crisanto, J.C., & Prenio J. (2017). *Regulatory approaches to enhance bank's cyber-security frameworks.* Financial Stability Institute insights on policy implementation No 2: Bank for international settlements

CPNI. (2016). *Protective security management systems*. www.cpni.gov.uk: https://www.cpni.gov.uk/protective-security-management-systems-psems

Cybersecurity & Infrastructure Security Agency. (2016). *NTP Amplification attacks using CVE-2013-5211*. https://www.cisa.gov/uscert/ncas/alerts/TA14-013A

Dragan, D. (2017). *Vulnerability assessment and penetration tesing in th emilitary and IHL context*. https://dx.doi.org/10.5937/vojtehg65-10761

Deloitte. (2018). *Cyber Security survey for Namibia keeping an eye on what matters.* https://www2.deloitte.com/content/dam/Deloitte/na/Documents/risk/na-Deloitte-Cyber-Security-Survey-for-Namibia.pdf

Deloitte. (2018). *Vulnerability assessment, penetration testing & configuration* https://www2.deloitte.com/hu/en/pages/risk/solutions/cyberrisk-vulnerability.html

Emagined. (2021). *Penetration testing process and methodology*. https://www.emagined.com/clear-path-penetration-testing

Engebretson, P. (2011). *The basics of hacking and penetration testing: Ethical hacking and penetration testing made easy*. http://AUT.eblib.com.au/patron/FullRecord.aspx?p=730200

ENISA. (2019). *ENISA and cyber security strategies*. www.enisa.europa.eu: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-ncss

European Union Agency. (2021). *Cybersecurity: Main and emerging threats in 2021 (infographic)*. https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats-in-2021-infographic

FIRST.Org. (2020.) CVSS v3.0: *Specification Document.* (2020). https://www.first.org/cvss/v3.0/cvss-v30-specification_v1.9.pdf

Fortinet. (2021). *FortiDDoS DDoS protection solution.* https://www.fortinet.com/products/ddos/fortiddos

Faircloth, J. (2011). *Penetration tester's open source toolkit* (3 ed.). http://AUT.eblib.com.au/patron/FullRecord.aspx?p=740483

Fouton, S., & Krainovich-Miller, B. (2016). *Theoretical framework examples research paper*. https://www.myperfectwords.com/blog/research-paper-examples/theoretical-framework-examples-research-paper.pdf

Gartner. (2017). *Gartner says worldwide information security spending will grow 7 percent to reach $86.4 billion in 2017*. https://www.gartner.com/en/newsroom/press-releases/2017-08-16-gartner-says-worldwide-information-security-spending-will-grow-7-percent-to-reach-86-billion-in-2017

Gasevic, D. (2017). *Computer in human behaviour.* sciencedirect.com: https://www.sciencedirect.com/science/article/abs/pii/S074756321830325X

GDPR. (2018). *General data protection regulation.* https://gdpr-info.eu/

Gerson Izagirre, Chrisopher, O & Hardikar, A. (2017). *Penetration testing in the financial services industry.* SANS.

Godwin M. T., Engebretson S. K., (2014). Cyber security: Challenges for society-literature review. *IOSR Journal of Computer Engineering (IOSR-JCE), 2*(12), 67-75.

Grageia, L. (2004). *DNS cache snooping or snooping the cache for fun and profit.* https://pdf4pro.com/view/version-1-1-february-2004-luis-grangeia-c27b7.html

Greenbone. (2021). *OpenVAS - open vulnerability assessment scanner*. https://www.openvas.org/: https://www.openvas.org/

Hackdefense. (2019). *The importance of SMB signing. How criminals can (potentially) take over the entire networ if SMB signing is not enabled.* https://hackdefense.com/publications/het-belang-van-smb-signing/

Hoehl, M., & Brandon, S. N. (2014). *Cyber breach coaching.* SANS.

IBM. (2019). *IBM report: Manufacturing felt brunt of cyberattacks in 2021 as supply chain woes grew.* https://newsroom.ibm.com/2022-02-23-IBM-Report-Manufacturing-Felt-Brunt-of-Cyberattacks-in-2021-as-Supply-Chain-Woes-Grew

IOSCO. (2021). *CPMI-IOSCO.* https://www.iosco.org/about/?subsection=cpmi_iosco

ITU *National Strategies*. (2019). www.itu.int: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx

James, N. (2019) *What is blockchain security?* https://www.ibm.com/topics/blockchain-security

Jounia. (2014). *Vulnerabilities, exploits and threats at a glance*. Rapid7.com: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/

Khan., G. M. (2014). Cyber security: challenges for society-literature review. *IOSR Journal of Comuter Engineering (IOSR-JCE) e-ISSN*, 67-75.

Khari, T., & Dhillon, G. (2015). *What to do before and after a cybersecurity breach?* https://www.american.edu/: https://www.american.edu/cybergov/uploads/what-to-do.pdf

Maistry, N. T., Ramkurrun, N., Cootignan, M., & Catherine, P. C. (2019) *Cyber security: Threats, Vulnerabilities and countermeasures - A perspective on the state of affairs in Mauritius.*

https://www.academia.edu/13578905/Cyber_security_Threats_Vulnerabilities_and_Countermeasures_A_Perspective_on_the_State_of_Affairs_in_Mauritius

McDonough, B. (2018). *Cyber smart: Five habits to protect your family, money, and identity from cyber criminals*. https://consilium-eureka.hosted.exlibrisgroup.com/permalink/f/1onr1f0/32CEU_ALMA513318 0480004371

Melbourne, J., & Jorm, D. (2010). *Penetration testing for web application (Part One).* http://www.symantec.com/connect/articles/penetration-testing-web-applications- part-one

Microsoft. (2020). *Local accounts*. https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts

Midian, P. (2012). Perspectives on penetration testing. *Computer Fraud & Security, 2012*(6), 15-17. doi:http://dx.doi.org/10.1016/S1361-3723(02)00612-7

Murugiah, S., Scarfone, K., Cody, A., & Orebaugh, A. (2008). *Technical guide to information security testing and assessment.* http://dx.doi.org/10.6028/NIST.SP.800-115

Naik, N. A., Kurundkar, G. D., Khamitkar, S. D., & Kalyankar, N. V. (2009). *Penetration testing: A roadmap to network security. Journal of Computing, 1*(1), 187-190.

Nath, O. (2021). top five blockchain attacks & dlt vulnerabilities to know in 2022. https://www.spiceworks.com/tech/tech-general/articles/top-five-blockchain-platforms/

NIST. (2018). *Cybersecurity framework*. https://www.nist.gov/cyberframework

NIST. (2020). *Tools and instruments*. nist.org: https://www.nist.gov/laboratories/tools-instruments

Oates, B. (2006). *Researching information systems and computing.* Sage.

Obotivere, B. A. & Nwaezeigwe, A. O. (2020) Cyber Security threats on the internet and possible solutions. I*nternational Journal of Advanced Research in Computer and Communication Engineering, 9*(9), 2319-5940

Osborne, M. (2016). How to cheat at managing information security. *Scitech Book News, 30*(4). http://ezproxy.aut.ac.nz/login?url=http://search.proquest.com/docview/200176483?accountid=8440

O'reilly. (2019). *What is a cyber strategy*. www.oreilly.com: https://www.oreilly.com/library/view/cybersecurity-attack/9781838827793/Text/Chapter_3.xhtml

OSINT. (2021). *OSINT for security assessments*. https://www.spiderfoot.net/osint-for-security-assessments/

OWASP. (2015). *Open web application security project.* https://www.owasp.org/index.php/Category:Vulnerability.

Ozkaya, E. (2019) *Cybersecurity: The beginner's guide: a comprehensive guide to getting started in cybersecurity*. https://consilium-eureka. hosted.exlibrisgroup.com/permalink/f/1onr1f0/32CEU_ALMA5135599500004371

PCI. (2008). *Information supplement: Requirement 11.3 penetration testing. PCI Security Standards Council*, 11.3. https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf

Reddy, G. J. U. (2018). *A study of cyber security challenges and its emerging trends on latest technologies*. https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

Sarala, S., & Angel, S. (2011). A study on penetration testing. *International Journal of Advanced Research in Computer Science, 2*(5), 0976-5697.

Samant, N. (2011). *Automated penetration testing*. San Jose State University

SANS. (2020). *MGT514: Security strategic planning, policy, and leadership*. https://www.sans.org/cyber-security-courses/security-strategic-planning-policy-leadership/

Sem, T. (2020). T*op 10 IT security frameworks and standards explained*. https://www.pegasusone.com/top-10-it-security-frameworks-and-standards-explained/

Shewmaker, J. (2008). *Introduction to network penetration testing.* http://www.dts.ca.gov/pdf/news_events/SANS_Institute-Introduction_to_Network_Penetration_Testing.pdf

Spiceworks. (2021). *Post event round-up: what was missing at RSA 2022?* https://www.spiceworks.com/it-security/security-general/guest-article/post-event-round-up-what-was-missing-at-rsa-2022/

SQLMAP. (2021). *Automatic SQL injection and database takeover tool*. https://sqlmap.org/: https://sqlmap.org/

Sutherland, I., Konstantinos, X., Blyth, A., & Andrew, J. (2012). *Protective emblems in cyber warefare.* https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1048&context=isw

Tait, F. (2017). *Corporate overview*. http://www.namclear.com.na/payment-services/

Thomas, R. (2021). *6 types of security assessments for enterprises.* https://www.enterprisesecuritymag.com/news/6-types-of-security-assessments-for-enterprises-nid-2215-cid-102.html

Tiirmaa-Klaar, H. (2011). *Cyber security threats and responses*: *At Global, Nation-State Industry and Individual levels*. http://www.ceri-scienes-po.org

Tiller, J. S. (2011). *CISO's guide to penetration testing: A framework to plan, manage, and maximize benefits.* http://AUT.eblib.com.au/patron/FullRecord.aspx?p=826967

TorontoCentre. (2018). *Supervision of cyber risk.* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiDrq-

5br5AhVklFwKHRTSA6AQFnoECAQQAw&url=https%3A%2F%2Fres.torontocentre.org%2Fguidedocs%2FSupervision%2520of%2520Cyber%2520Risk%2520FINAL.pdf&usg=AOvVaw0FldSGZ1PkICuVoKS-cFbQ

Tran, Q. N. T., & Dang, T. K. (2016). Towards side-effect-free database penetration testing. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 1*(1), 72-85.

Vacca, J.R. (2010). *Managing information security.* http://AUT.eblib.com.au/patron/FullRecord.aspx?p=535284

Whitman, M., & Mattord, H. (2021). *Management of information security.* (7th ed.). Cengage Learning.

Yeo, J. (2013). Using penetration testing to enhance your company's security. *Computer Fraud & Security*, *2013*(4),17-20. doi:http://dx.doi.org/10.1016/S1361 - 3723(13)70039-3

APPENDIX A – TCP AND UDP PORTS STATES DEFINITION

The status of a TCP or UDP or SCTP or ICMP or IGMP or ARP connection can have one of the following state:

Open – This indicates that an application is listening for a connection on the port. This also indicates that application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port.

Closed – This indicates that the probes were received but there is no application listening on the port. A closed port is accessible (receiving and responding to probes). A closed port also indicates that the host is up.

Filtered – This indicates that the probes were not received and the state could not be established. A filtered state means the probe device cannot determine whether the port is open due to packet filtering (i.e. access lists) that prevents probes from reaching the port.

Unfiltered – This indicates that the probes were received but a state could not be established. This also indicates that a port is accessible, but the probe device is unable to determine whether it is open or closed.

Open/Filtered– This indicates that the port was filtered or open but the probe device couldn't establish the state. This could also mean that the open port did not give a response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited.

Closed/Filtered – indicates that the probe device is unable to determine whether a port is closed or filtered.

APPENDIX B: SCRIPTS

The following scripts were used to gather the collected data.

ipconfig >> ipconfig_ Name_of_Subnet.txt

nmap --privileged -n -Pn -sS -sU -A --osscan-guess --max-os-tries 1 -p T:1-65535,U:7,9,11,13,17,19,37,53,67-69,88,111,123,135,137-139,161-162,177,213,259-260,445,464,500,514,520,523,623,631,749-751,1194,1434,1701,1812-1813,1900,2049,2746,3230-3235,3401,4045,4500,4665-4666,4672,5059-5061,5351,5353,5632,6429,7777,9100-9102,11211,17185,18233,23945,26000-26004,26198,27015-27030,27444,27960-27964,30720-30724,31337,32771,34555,44400,47545,49152,54321 --max-retries 3 --min-rtt-timeout 500ms --max-rtt-timeout 3000ms --initial-rtt-timeout 500ms --defeat-rst-ratelimit --min-rate 450 --max-rate 5000 --disable-arp-ping -v -oA Nmap_"Name_of_Subnet" <subnet/subnet mask>

nmap -Pn -oA Nmap_"Name_of_Subnet" <subnet/subnet mask>

The following script was used to schedule the scans:

```
#!/bin/sh
TARGETS="<targetIPs>"
OPTIONS="-v –n -T4 -F –sV --privileged -n -Pn -sS -sU -A --osscan-guess --max-os-tries 1 -p "
date=`date +%F`
cd /root/scans
nmap $OPTIONS $TARGETS -oA scan-$date > /dev/null
if [ -e scan-prev.xml ]; then
      ndiff scan-prev.xml scan-$date.xml > diff-$date
      echo "*** NDIFF RESULTS ***"
      cat diff-$date
      echo
fi
echo "*** SEE SCAN RESULTS BELOW***"
cat scan-$date.nmap
ln -sf scan-$date.xml scan-prev.xml
```

The following script sends and email containing the scan output results

$ ./nmap-diff.sh -h

./nmap-diff.sh [options].

REQUIRED

-f|--file: input file with an IP list.
--email: email address.
-o|--output: output directory.

OPTIONAL
-h|--help: Display this help summary.

APPENDIX C: FULL SET OF CONTROLS

Web application and database testing.

Conducted as per OWASP web testing guide version 4 (2016). For web applications and databases, the following tests are mandatory:

- Injection flaws, particularly SQL injection. Also consider OS command injection,
- LDAP and XPath injection flaws, as well as other injection flaws
- Buffer overflows and Insecure cryptographic storage
- Insecure communications and Improper error handling
- All "high-risk" vulnerabilities identified in the vulnerability identification process
- Cross-site scripting (XSS) and Cross-site request forgery (CSRF)
- Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions)
- Broken authentication and session management, and Improper error handling
- Any additional vulnerabilities identified in industry best practice, including the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.

If the application has an authentication system, the application should be tested as an unauthenticated user and then at each of the user levels defined in the application using test accounts. The testing is divided into 2 phases: Passive and Active mode.

The Active mode has a set of active tests has been split into 11 subcategories for a total of 91 controls:

- Information gathering

- Configuration and deployment management testing
- Identity management testing
- Authentication testing
- Authorisation testing
- Session management testing
- Input validation testing
- Error handling
- Cryptography
- Business logic testing
- Client-side testing

Testing for information gathering includes the following test procedures (test procedure numbers indicate OWASP test procedures):

- Conduct search engine discovery and reconnaissance for information leakage (OTG-INFO-001)
- Fingerprint webserver (OTG-INFO-002)
- Review webserver metafiles for information leakage (OTG-INFO-003)
- Enumerate applications on webserver (OTG-INFO-004)
- Review webpage comments and metadata for information leakage (OTG-INFO005)
- Identify application entry points (OTG-INFO-006)
- Map execution paths through application (OTG-INFO-007)
- Fingerprint web application framework (OTG-INFO-008)
- Fingerprint web application (OTG-INFO-009)

- Map application architecture (OTG-INFO-010)

Testing of configuration and deployment management includes the following test procedures:

- Test network/infrastructure configuration (OTG-CONFIG-001)
- Test application platform configuration (OTG-CONFIG-002)
- Test file extensions handling for sensitive information (OTG-CONFIG-003)
- Review old, backup and unreferenced files for sensitive information (OTG-CONFIG004)
- Enumerate infrastructure and application admin interfaces (OTG-CONFIG-005)
- Test HTTP methods (OTG-CONFIG-006)
- Test HTTP strict transport security (OTG-CONFIG-007)
- Test RIA cross-domain policy (OTG-CONFIG-008)

Testing of identity management includes the following test procedures:

- Test role definitions (OTG-IDENT-001)
- Test user registration process (OTG-IDENT-002)
- Test account provisioning process (OTG-IDENT-003)
- Testing for account enumeration and guessable user account (OTG-IDENT-004)
- Testing for weak or unenforced username policy (OTG-IDENT-005)

Testing of authentication includes the following test procedures:

- Testing for credentials transported over an encrypted channel (OTG-AUTHN-001)
- Testing for default credentials (OTG-AUTHN-002)
- Testing for weak lock-out mechanism (OTG-AUTHN-003)
- Testing for bypassing authentication schema (OTG-AUTHN-004)
- Test remember password functionality (OTG-AUTHN-005)
- Testing for browser cache weakness (OTG-AUTHN-006)
- Testing for weak password policy (OTG-AUTHN-007)
- Testing for weak security question/answer (OTG-AUTHN-008)
- Testing for weak password change or reset functionalities (OTG-AUTHN-009)
- Testing for weaker authentication in alternative channel (OTG-AUTHN-010)

Testing of authorization includes the following test procedures:

- Testing directory traversal/file include (OTG-AUTHZ-001)
- Testing for bypassing authorization schema (OTG-AUTHZ-002)
- Testing for privilege escalation (OTG-AUTHZ-003)
- Testing for insecure direct object references (OTG-AUTHZ-004)

Testing of session management includes the following test procedures:

- Testing for bypassing session management Schema (OTG-SESS-001)
- Testing for cookies attributes (OTG-SESS-002)

- Testing for session fixation (OTG-SESS-003)
- Testing for exposed session variables (OTG-SESS-004)
- Testing for cross-site request forgery (CSRF) (OTG-SESS-005)
- Testing for logout functionality (OTG-SESS-006)
- Test session timeout (OTG-SESS-007)
- Testing for session puzzling (OTG-SESS-008)

Testing of input validation includes the following test procedures:

- Testing for reflected cross-site scripting (OTG-INPVAL-001)
- Testing for stored cross-site scripting (OTG-INPVAL-002)
- Testing for HTTP verb tampering (OTG-INPVAL-003)
- Testing for HTTP parameter pollution (OTG-INPVAL-004)
- Testing for SQL injection (OTG-INPVAL-005)
- Oracle testing, MySQL testing and SQL server testing
- Testing PostgreSQL (from OWASP BSP)
- MS Access testing
- Testing for NoSQL injection
- Testing for LDAP injection (OTG-INPVAL-006)
- Testing for ORM injection (OTG-INPVAL-007)
- Testing for XML injection (OTG-INPVAL-008)
- Testing for SSI injection (OTG-INPVAL-009)
- Testing for XPath injection (OTG-INPVAL-010)
- IMAP/SMTP injection (OTG-INPVAL-011)
- Testing for code injection (OTG-INPVAL-012)

- Testing for local file inclusion and Testing for remote file inclusion
- Testing for command injection (OTG-INPVAL-013)
- Testing for buffer overflow (OTG-INPVAL-014)
- Testing for heap overflow and Testing for stack overflow
- Testing for format string and Testing for incubated vulnerabilities (OTG-INPVAL-015)
- Testing for HTTP splitting/smuggling (OTG-INPVAL-016)

Testing for error handling includes the following test procedures:

- Analysis of error codes (OTG-ERR-001)
- Analysis of stack traces (OTG-ERR-002)

Testing for weak cryptography includes the following test procedures:

- Testing for weak SSL/TLS ciphers, insufficient transport layer protection (OTGCRYPST-001)
- Testing for padding oracle (OTG-CRYPST-002)
- Testing for sensitive information sent via unencrypted channels (OTG-CRYPST003)

Business logic testing includes the following test procedures:

- Test business logic data validation (OTG-BUSLOGIC-001)
- Test ability to forge requests (OTG-BUSLOGIC-002)
- Test integrity checks (OTG-BUSLOGIC-003)
- Test for process timing (OTG-BUSLOGIC-004)

- Test number of times a function can be used limits (OTG-BUSLOGIC-005)
- Testing for the circumvention of work flows (OTG-BUSLOGIC-006)
- Test defenses against application misuse (OTG-BUSLOGIC-007)
- Test upload of unexpected file types (OTG-BUSLOGIC-008)
- Test upload of malicious files (OTG-BUSLOGIC-009)

Client-side testing includes the following test procedures:

- Testing for DOM-based cross-site scripting (OTG-CLIENT-001)
- Testing for JavaScript execution (OTG-CLIENT-002)
- Testing for HTML injection (OTG-CLIENT-003)
- Testing for client-side URL redirect (OTG-CLIENT-004)
- Testing for CSS injection (OTG-CLIENT-005)
- Testing for client-side resource manipulation (OTG-CLIENT-006)
- Test cross-origin resource sharing (OTG-CLIENT-007)
- Testing for cross-site flashing (OTG-CLIENT-008)
- Testing for clickjacking (OTG-CLIENT-009)
- Testing Web-Sockets (OTG-CLIENT-010)
- Test web messaging (OTG-CLIENT-011) and Test local storage (OTG-CLIENT-012)

Network testing

Network testing includes all the tests listed below and conducted as per OWASP testing guide version 4 (2016). For web applications and systems including network devices the following tests are mandatory:

- Injection flaws, particularly SQL injection. Also consider OS command injection,

- LDAP and XPath injection flaws, as well as other injection flaws
- Buffer overflows
- Insecure cryptographic storage
- Insecure communications
- Improper error handling
- All “high-risk” vulnerabilities identified in the vulnerability identification process
- Cross-site scripting (XSS)
- Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions)
- Cross-site request forgery (CSRF)
- Broken authentication and session management
- Any additional vulnerabilities identified in industry best practice, including the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.

Router/Switch checks:

- Availability of unnecessary services
- SNMP community strings status and Access lists and interfaces status
- Routing/Switching tables
- Router/Switch administration via Telnet
- Software versions (patching level)
- Egress filtering and Privilege escalation and Router configuration from external view

- TCP and UDP port scans and OS fingerprinting
- Check for common response to ICMP and SNMP requests
- TCP sequence number prediction and Protection against SYN flood attack
- Firewall checks and Availability of unnecessary services
- SNMP community strings status
- Access lists and interfaces status
- [Add other relevant tests/checks]

Firewall/IDS/IPS checks

- VPNC IPsec tunnel connection
- Firewall administration via Telnet and Egress filtering
- Software version
- Firewall configuration from external view
- Privilege escalation
- TCP and UDP port scans and OS fingerprinting
- Check for common response to ICMP and SNMP requests
- TCP sequence number prediction and Protection against SYN flood attack
- BGP querying and other routing protocols querying
- [Add other relevant tests/checks]

Email servers (SMTP)

- SMTP probing, MX records check and Reverse DNS test
- DNSBL (spam blacklist) check
- SPF record verification (server- and client-side)
- Open relay test and email format validation

- SMTP, POP3 and IMAP clear text authentication
- Open relay
- Information leakage/enumeration and Presence and operation of AV
- SMTP server response and SMTP/POP3/IMAP brute-force verification/grinding
- SMTP service assessment and SMTP/POP3/IMAP manipulation
- [Add other relevant tests/checks]

FTP servers

- FTP banner grabbing
- FTP brute-force password checking
- FTP bounce port scanning
- PORT and PASV abuse
- Anonymous access
- Bounce attack
- FTP process manipulation
- [Add other relevant tests/checks]

DNS servers

- Who is Response
- Resource record search (MX, CNAME, NS, HOST)
- Forward DNS querying
- Forward/Reverse DNS grinding
- Zone transfer
- Reverse DNS sweeping
- DNS probing

APPENDIX D: ETHICAL CLEARANCE

APPENDIX E: LANGUAGE EDITOR'S REPORT

ACET Consultancy
Anenyasha Communication, Editing and Training
Box 50453 Bachbrecht, Windhoek, Namibia
Cell: +264814218613
Email: mlambons@yahoo.co.uk / nelsonmlambo@icloud.com

12 September 2022

To whom it may concern

LANGUAGE EDITING – SION S. NGHOSHI

This letter serves to confirm that a **MASTER OF SCIENCE (INFORMATION TECHNOLOGY)** thesis entitled ***PENETRATION TESTING AND VULNERABILITY ASSESSMENT ON THE NAMIBIAN INTER-BANKING SYSTEM: NAMSWITCH*** by SION S. NGHOSHI was submitted to me for language editing.

The thesis was professionally edited and track changes and suggestions were made in the document. The research content or the author's intentions were not altered during the editing process and the author has the authority to accept or reject my suggestions.

Yours faithfully

DR NELSON MLAMBO
PhD in English
M.A. in Intercultural Communication
M.A. in English
B. A. Special Honours in English – First class
B. A. English & Linguistics