Evaluating the Cyber Security Skills Gap relating to Penetration Testing

A thesis submitted in fulfillment of
the requirements of the degree of

MASTER OF SCIENCE
of
RHODES UNIVERSITY

By Dirk Johannes Beukes

December 2019

Abstract

Information Technology (IT) is growing rapidly and has become an integral part of daily life. It provides a boundless list of services and opportunities, generating boundless sources of information, which could be abused or exploited. Due to this growth, there are thousands of new users added to the grid using computer systems in a static and mobile environment; this fact alone creates endless volumes of data to be exploited and hardware devices to be abused by the wrong people. The growth in the IT environment adds challenges that may affect users in their personal, professional, and business lives. There are constant threats on corporate and private computer networks and computer systems. In the corporate environment companies try to eliminate the threat by testing networks making use of penetration tests and by implementing cyber awareness programs to make employees more aware of the cyber threat. Penetration tests and vulnerability assessments are undervalued; are seen as a formality and are not used to increase system security. If used regularly the computer system will be more secure and attacks minimized.

With the growth in technology, industries all over the globe become fully dependent on information systems in doing their day-to-day business. As technology evolves and new technology becomes available, the bigger the risk becomes to protect against the dangers which come with this new technology. For industry to protect itself against this growth in technology, personnel with a certain skill set is needed. This is where cyber security plays a very important role in the protection of information systems to ensure the confidentiality, integrity and availability of the information system itself and the data on the system. Due to this drive to secure information systems, the need for cyber security professionals is on the rise as well. It is estimated that there is a shortage of one million cyber security professionals globally. What is the reason for this skills shortage? Will it be possible to close this skills shortage gap? This study is about identifying the skills gap and identifying possible ways to close this skills gap.

In this study, research was conducted on the cyber security international standards, cyber security training at universities and international certification focusing specifically on penetration testing, the evaluation of the need of industry while recruiting new penetration testers, finishing with suggestions on how to fill possible gaps in the skills market with a conclusion.

Acknowledgements

First and foremost, I want to thank my Heavenly Father who gave me the strength, courage, patience and perseverance to successfully complete my studies. I would like to acknowledge and thank my wife Tienie Beukes and my daughters Isa and Luka for their support throughout the duration of this research. Without your support and encouragement this journey would have been significantly more challenging. I would also like to thank my family for their continued understanding during my studies.

I want to thank my supervisor, Prof Barry Irwin, for the supervision, support, patience and guidance he provided throughout the entire degree. His feedback and insight have played a major part in shaping the final product of this research. His constant drive to produce perfect work pushed me to the limit and guided me to the success and completion of this research.

This work was undertaken with financial support from the South African National Defence Force. The author acknowledges that any opinions, findings and conclusions or recommendations expressed here are those of the author and that none of the above-mentioned sponsors accept any liability whatsoever in this regard.

Contents

List of Tables

List of Figures

Glossary of Terms

The following list describes the various abbreviations and acronyms used throughout this document. Citations to research related to these areas listed below can be found in the text to better retain the context upon which the citation relies.

3G Third generation of wireless mobile telecommunications technology

4G Fourth generation of broadband cellular network technology

5G Fifth generation of cellular wireless network technology

IEEE802.11x. Institute of Electrical and Electronic Engineers original wireless specification

ARPA Advanced Research Project Agency

ARPNET Advanced Research Projects Agency Network

ASTD American Society for Training and Development

BYOD Bring Your Own Device

CEO Chief Executive Officer

JCSE-IITPSA Johannesburg Center for Software Engineering - Institute of Information Technology Professionals South Africa

CNST Centre for Nan-scale Science and Technology

CTL Communications Technology Laboratory

CISA Certified Information Systems Auditor

CISM Certified Information Security Manager

CISSP Certified Information Systems Security Professional

CISO Chief Information Security Officer

CSO Chief Security Officer

CTF Capture The Flag

DMZ Demilitarized Zone

EL Engineering Laboratory

ESG Enterprise Strategy Group

GSM Global System for Mobile communication

ICT Information Communication Technology

IEC International Electro technical Commission

ISA Information Security Architects

ISACA Information Systems Audit and Control Association

ISMS Information Security Management Systems

ISSA Information System Security Association

IP Internet Protocol

ISO International Organization for Standardization

IT Information Technology

ITL Information Technology Laboratory

JTR John The Ripper, a password cracking tool

KPI Key Performance Indicator

LMCKC Lockheed Martin Cyber Kill Chain

MEP Manufacturing Extension Partnership

MICT SETA Media Information and Communication Technologies Sector Education and Training Authority

MML Material Measurement Laboratory

MSF Metasploit Framework

NCNR NIST Centre for Neutron Research

NSA National Security Agency

NIST National Institute of Standards and Technology

OAM Office of Advance Manufacturing

OS Operating System

OWASP Open Web Application Security Project

PCIDSS Payment Card Industry Data Security Standard

PTES Penetration Testing Execution Standard

PHD Doctor of Philosophy

PML Physical Measurement Laboratory

PT Penetration Testing

RAND Research ANd Development

RFID Radio-Frequency IDentification

SABS South African Bureau for Standards

SATAN Security Administrator Tool for Analyzing Networks

SETA Sector Education and Training Authority

SP Special Publication

USA United States of America

WiFi Wireless Fidelity (A trademarked phrase that means IEEE 802.11x).

1 Introduction

When looking back at the history of cyber security, the discipline started as a research project. Robert H. Thomas developed the first self-replicating program called Creeper in 1971. In the modern day a self-replicating program is called a worm. Creeper was launched on the Advanced Research Projects Agency Network (ARPNET), developed in 1969 by the United States Department of Defence and four partnering universities. This network was known as *the world's first operational packet switching network*, and was the predecessor of the Internet. Creeper was known as the first computer virus (Dalakov, 2006; Press, 2015; SentinelOne, 2017).

Ray Tomlinson, who invented email, wrote a program called Reaper known as the first antivirus software. Reaper was the first developed antivirus software to delete Thomas's Creeper. When taking this into consideration, Thomas launched one of the first cyber attacks and Tomlinson countered the attack. Without knowing it, the two gentleman started the cyber concept which evolved into the modern day cyber security (Dalakov, 2006; Press, 2015; SentinelOne, 2017).

When analyzing the definitions of cycer security, one can make the assumption that the goal of cyber security is to protect any device connected to a network, a private network or the internet, against cyber attacks. This includes the protection of hardware, software and data against unauthorized access or exploitation (Kremling and Parker, 2017; Web Finance, 2017; Rouse, 2018).

Cyber security includes security elements such as network security, information

security, application security, operational security, business continuity planning, disaster recovery and end-user education such as cyber awareness training (Rouse, 2018; NIST, 2018b).

Organizations need to protect themselves against cyber incidents by ensuring that their information systems are protected. Organizations need to protect themselves against threats such as exploitation, malware, ransomware, identity theft, phishing and loss of information (Rouse, 2018). To protect against cyber incidents means that cyber professionals need to be hired or be part of the organization. Such professionals called penetration testers are needed to fulfill this task.

This is where the skills shortage problem starts. There is a global cyber skills shortage, and most organizations do not know how to approach and handle the shortage. There are currently 1 million unfilled cyber security jobs globally (Culbertson *et al.*, 2017). According to recent estimates by Cybersecurity Ventures, there will be a global shortfall of 3,5 million cyber security jobs by 2021 (NeSmith, 2018). Therefore, organizations cannot stay abreast of the growing cyber threat; this leads to the vulnerability of their information systems and data (Morgan, 2017; Kennedy, 2018). As the cyber threat grows, the demand for skilled cyber security experts increases (Parsons, 2017; Lynch, 2017; NeSmith, 2018).

There are no instant solutions to fix the global cyber security skills shortage and skills gap; however, implementing Cyber Security Awareness to build knowledge in the current workforce, and rolling out of safety software can be a start in being more secure (Lynch, 2017).

1.1 Problem Statement

Cyber attacks are on a rapid increase, and the cyber criminals are the only beneficiary thereof. By making use of freely available tools and ingenious advanced methods, cyber criminals make it difficult for industry to protect themselves. Thus cyber security professionals need all the help they can get to protect information systems against cyber attacks (Lynch, 2017; NeSmith, 2018).

This puts organizations in a predicament, as skilled cyber professionals are hard to find and expensive. Skills and remuneration are a huge factor to consider when recruiting cyber professionals. Firstly, it has to be determined if a person has the required skills and secondly the experience needed must be measured (Parsons, 2017; Lynch, 2017).

According to NeSmith (2018), cyber criminals take advantage of the cyber skills gap in industry and of industries ability to detect, respond and prevent cyber incidents. The cyber skills gap is a big concern which is already showing its effect in industry. The skills gap needs to be identified and measures need to be put in

place to close the cyber skills gap to make sure the industrial need for skilled cyber specialists is satisfied.

The following specific research questions were identified:

- What are the skills needed to become a cyber security specialist?
- How can education contribute to building the required skills needed in cyber security in industry?
- Will a recruiting framework help industry to identify competent candidates for cyber security positions?
- Will it be possible to close the cyber skills gap currently in industry?

1.2 Research Goals

This research aimed to investigate and achieve the following goals:

- In order to set the background to the research an overview will be conducted on cyber security and cyber security concepts defined.
- The outcome of penetration tests varies according to the standards and/or the methodologies they leverage. During the process of attempting to secure IT infrastructure and prevent and fix vulnerabilities, companies look for the latest, relevant and most popular penetration testing methodologies, standards and tools to fight cyber attacks. Popular penetration testing standards and methodologies available are, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115 (NIST, 2018b), Open Source Security Testing Methodology Manual (OSSTMM) (Shanley and Johnstone, 2015), Information System Security Assessment Framework (ISSAF) (Shanley and Johnstone, 2015), Payment Card Industry Data Security Standard (PCI DSS) (King, 2017), Open Web Application Security Project (OWASP), International Organization for Standardization (ISO) 27001 series (ISO, 2017), the Lockheed Martin Cyber Kill Chain (Lockheed Martin Corporation, 2015) and the Penetration Testing Methodologies and Standards (PTES) (Shanley and Johnstone, 2015).
- During the research the focus will be on cyber security with the emphasis on penetration testing. An analysis will be done on the well-known and most preferred cyber security standards, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115 (NIST, 2018b), Payment Card Industry Data Security Standard (PCI DSS) (King, 2017), International Organization for Standardization (ISO) 27001 series (ISO, 2017)

and the Lockheed Martin Kill Chain (Lockheed Martin Corporation, 2015) as mentioned above. The penetration testing skills prescribed by each standard will be analyzed. A framework will be proposed indicating the skills needed by a penetration tester. The framework will act as a guideline for the penetration tester to do proper planning before executing the test (Guarda *et al.*, 2016).

- Research was done in terms of cyber qualifications presented at formal academic institutions (Universities), international certification organizations and informal qualifications and skills gained through self taught skills. During this process an analysis will be done on cyber security skills prescribed by industry, by advertised cyber positions through recruiting companies or by the organization itself. A recruitment proposal will be suggested to determine the skills and experience level of a candidate applying for a cyber security job.

- Lastly the cyber skills prescribed by international standards, the skills gained at educational institutions and the skills prescribed by industry will be aligned to be able to determine a possible solution in closing the cyber security skills gap.

1.3 Research Objectives

The following specific objectives will be addressed:

- To identify the cyber skills by analyzing International Standards, focusing on penetration testing.

- Suggest a penetration testing framework to be able to identify the required skills and expertise needed for penetration testing.

- To discuss the skills gained in the education system versus the skills requirements prescribed by industry.

- To align the skills prescribed by International Standards and the skills prescribed by industry to close the cyber skills gap.

1.4 Methodology

A qualitative study will be undertaken in conducting this research, using document analysis techniques. Quantitative research methodology is defined as a methodology that studies things in their natural settings and attempts to make sense of or

interpret phenomena in terms of the meanings people bring to them. International Standards are the main documents used to determine what the world prescribes in term of a specific environment. Using what is prescribed in International Standards will give a baseline on how to determine and manage the cyber skills gap.

1.5 Scope and Limits

Although there are standards and frameworks (such as the Open Web Application Security Project (OWASP) and Penetration Testing Execution Standard (PTES)) other than NIST, PCI DSS and ISO 27000 in regards with cyber security and penetration testing, only documented features within the selected standards were used when analyzing cyber security skills and penetration testing framework. During the research on industry requirements for penetration testing, job advertisements from industry were used to determine the skills needed for a specific position. The job advertisements are available as an electronic folder as the advertisements are removed from the internet after a predetermined time. Two of the job advertisements were analyzed and form part of the appendices of this document. Research on skills gained and programs presented by education institutions may differ from the time the research was done and what is presented currently, as new programs are introduced regularly and older programs taken out.

1.6 Document Structure

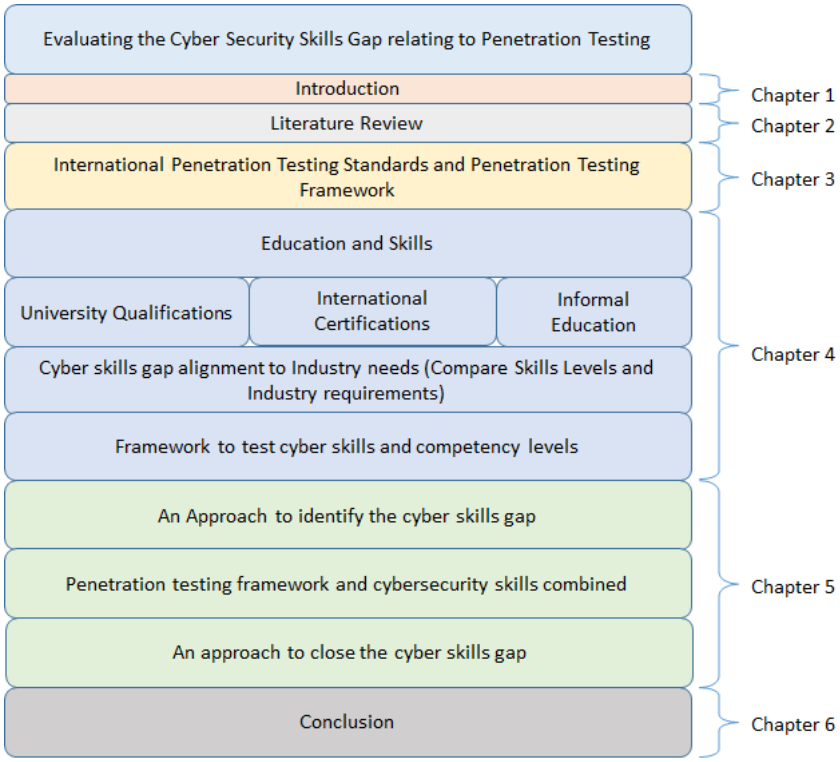

Figure 1.1: Research Approach.

The remainder of this document is structured as depicted in Figure 1.1. **Chapter 2** gives a literature review, to provide an overview of cyber security concepts and definitions to indicate the vastness of cyber security and setting the focus on penetration testing as a specific discipline in cyber security. Chapter 2 will lay the baseline of cyber security concepts covered in the thesis.

Chapter 3 consists of the analysis of well-known cyber security standards to determine the skills needed by a cyber security professional. By determining the skills, a penetration testing framework will be proposed. Proposing the penetration testing framework, will give an indication of what type of qualifications, formal or informal, skills and practical experience a cyber security professional needs to execute the cyber security function.

Chapter 4 consists of the types of education and qualifications in the cyber security field. The cyber security skills gap will be aligned with industry standards where after a framework will be proposed on how to confirm skills and experience levels.

In **Chapter 5** a comparison will be done by aligning the penetration testing framework suggested in Chapter 3 with the skills needed by industry to identify if it will be possible to close the cyber security skills gap. Possible suggestions on how to close the skills gap will then be deducted.

Chapter 6 concludes the research and gives an indication on further research on the cyber security skills shortage problem.

2 Literature Review

Chapter 2 provides background on cyber security with definitions of all the cyber concepts to set a baseline and get the reader in the right frame of mind to understand concepts which are focused on. Section 2.1 provides an overall introduction to cyber security which might be well known but not understood. Section 2.2 give a full background on Cyber security, including Information Security, Security Awareness and Cyber security Awareness. Section 2.3 focus on Penetration Testing with a full explanation on Penetration Testing. In sections 2.4 and 2.5, Red and Blue Teaming and Capture The Flag (CTF) are discussed.

Section 2.6 defines the cyber security terms and explains some of the cyber security terminologies. The chapter concludes with section 2.7 which provides a summary of the chapter.

2.1 Introduction

Information Technology (IT) is growing rapidly and has become an integral part of daily life. It provides a boundless list of services and opportunities, generating boundless sources of information, which could be abused or exploited (Jai and Mehtre, 2015). Due to this growth, there are thousands of new users added to the global grid using computer systems in a static and mobile environment; this fact alone creates endless volumes of stored data to be exploited and hardware devices to be abused by the wrong people. The growth in the IT environment adds chal-

lenges that may affect users in their personal, professional, and business spheres. In the process of protecting IT devices and its users, cyber security has to be implemented as a protection method to ensure the confidentiality, integrity, and availability of information (Rouse, 2018). This means that individual users have to become cyber-wise or cyber aware.

There are constant threats on corporate and private computer networks and computer systems. In the corporate environment companies attempt to eliminate the threat by testing networks making use of penetration tests, vulnerability assessments and implementing cyber awareness programs to make employees more aware of the cyber threat (Lynch, 2017). Penetration tests and vulnerability assessments are undervalued; they are seen as a formality and are not used to increase system security. If used regularly the computer network will be more secure and attacks minimized (Jai and Mehtre, 2015).

Penetration tests are performed by professional penetration testers in a defensive manner and, in the same light, offensive penetration tests can be executed by unwanted individuals and groups outside a company. These individuals or groups are known as hackers. The overarching question normally remains on what are the skills levels needed, which are the best penetration testing framework/tools out there, how are they used and what are the risks involved when executing penetration tests on live systems (Guarda *et al.*, 2016).

During the research done for this thesis, cyber security was analyzed with all aspects coupled to it and focusing specifically on the skills gap in penetration testing.

2.2 Cyber security

Cyber security is a combination of technologies, processes, procedures and practices which is designed to protect computers, data, information, networks, and programs from attack, damage and unauthorized access. Cyber security is a critical part of any government's or organization's security strategy (Von Solms and Van Niekerk, 2013; Guarda *et al.*, 2016; CISCO, 2019; Kaspersky, 2019).

Cyber security aims to achieve and maintain the cyber properties in an organization. It is the processes and procedures put in place to protect assets against cyber risks. Cyber incidents compromise the availability, confidentiality and integrity, which may include non-repudiation and authenticity (Von Solms and Van Niekerk, 2013; Buch *et al.*, 2018; Toch *et al.*, 2018).

Cyber Security has three main groups as shown in Table 2.1. (Von Solms and Van Niekerk, 2013; Taylor *et al.*, 2014; Baloch, 2015).

Table 2.1: Cyber Security Groups

Group	Description
Cyber Terrorism	The disruptive use of information technology by terrorist groups to advance their political agenda.
Cyber Warfare	Involves non-states using information technology to penetrate another nation's networks to cause damage or disruption.
Cyber Espionage	The practice of using information technology to obtain secret information without permission from its owners or holders. It is used to gain strategic, political, military and economic advantage. Cracking techniques and malware are used for cyber espionage.

2.2.1 Information Security

Information security is the protection of the confidentiality, integrity and the availability of information on devices with the capability of storing, processing and transmitting information and is accomplished through policies, procedures, people and products (Ciampa, 2014; Rouse, 2018). The information security components are depicted in Figure 2.1.

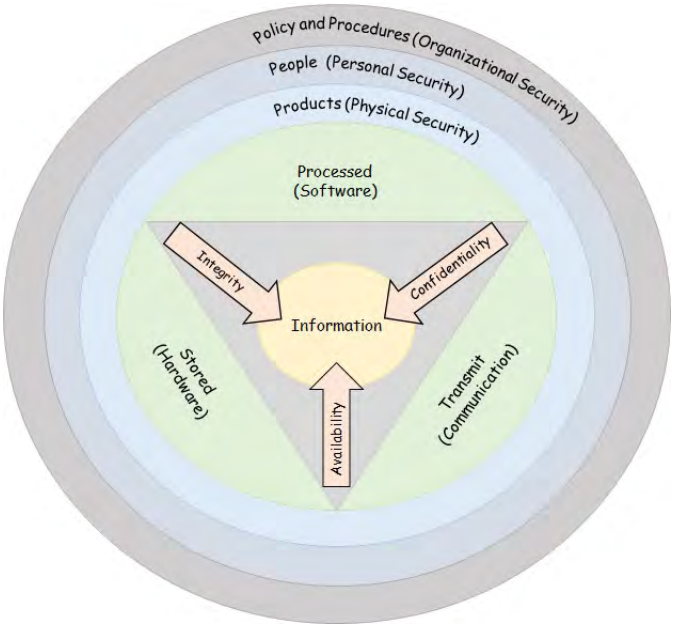

Figure 2.1: Information Security Components (Goldstein *et al.*, 2007; Ciampa, 2014).

The main aim of information security is the attempt to avoid data and identity theft, to avoid legal actions due to not securing information, to sustain productiv-

ity and to prevent cyber terrorism. Information security attacks increase yearly despite the effort and allocated budgets spent to secure these systems. There are no computer systems which will be 100% secure or which are immune to cyber attacks. It is extremely difficult to secure against cyber attacks. Aspects contributing to the struggle to secure networks or devices are that almost all devices have an connection to the internet, the speed at which attacks are executed, the complexity of attacks, access to freely available tools which are easy to use, attackers having the ability to detect vulnerabilities more quickly, security updates not done regularly, attackers making use of distributed attacks using multiple sources, and users who are confused and not skilled (Ciampa, 2014).

2.2.2 Cyber security Awareness

A few basic processes and procedures have to be implemented before executing penetration tests. These processes and procedures are important to ensure that effective results are received. Government, industry and private computer users realized that security is a huge concern in their daily work and private life (Jaeger, 2018). Although the standard computer user has limited skills and basic knowledge on how to secure a computer and to keep it safe, the real threats, vulnerabilities and damages are not clear. Cyber Security Awareness programs play a vital role in teaching the right skills to computer users on different levels to make them aware (Ciampa, 2014; Chandarman and van Niekerk, 2017; Bada *et al.*, 2019).

Due to the lack of and limited cyber knowledge and skills of the standard computer and mobile user, it is clear that there are numerous dangers in the cyber, IT environments which would target these vulnerabilities. This has a big influence especially on the personal life of adults, young people, children and senior citizens, not to mention the effect of cyber incidents on government and the corporate environment. Keeping that in mind, it is evident that the population of a country such as South Africa must be made aware of the danger of cyber attacks. If one looks at the ways to make the citizens of a country like South Africa, cyber aware, one will find that there are a few factors to be looked at. These factors might include aspects like the age of the person, the skills of a specific person, the geographical area, access to physical devices and access to network connectivity (Ciampa, 2014; Chandarman and van Niekerk, 2017).

Past projects on getting society involved in cyber awareness programs show that people do not have knowledge with regard to cyber. They have very limited skills regarding how cyber works, and what the dangers are when using mobile devices and computers. The citizens staying in remote geographical locations who do not have access to TV, radio or sometimes data networks will not be able to be part

of cyber awareness programs except if awareness programs are presented in their geographical area. This means that it is a difficult process to reach all the citizens of a country like South Africa by presenting awareness projects. This unfortunately means that there will always be members of society who are unaware of the good and bad of cyber (Ciampa, 2014; Jaeger, 2018).

The picture in the government and corporate environment looks a little bit different, but there will be challenges as well. Government and the corporate environment do have cyber awareness programs running to make employees more cyber savvy. These environments have started to realize that cyber has big risks to deal with and if their employees are not informed or made aware of the dangers, it will have a big impact on the corporate environment. On the other hand, you can have the best awareness programs in place and the most informed employees, and it will take only one disgruntled employee to cause a huge cyber security breach. Cyber Security Awareness has six different parts that cover the whole spectrum of security awareness (Ciampa, 2014). These six parts are as follows:

- Personal Security. The term personal security, in this sense, refer to a person's security measures put in place on a computer system, to keep them safe from exploits, attacks and vulnerabilities. It is believed in cyber security circles that people are the weakest link in any security model (Tipton and Krause, 2007). The biggest security aspect to be in place with regard to personal security is authentication, to confirm that you are the right person working on the computer system (Ciampa, 2014). To be able to access a computer system or secure web sites, a user has to authenticate; this is done by means of a password. Weak passwords mean that the attacker will easily get access to your computer system. Due to security reasons there have to be policies in place to ensure that passwords are strong and not easy to break. The stronger the password the more difficult to break/crack the password. This is where cyber awareness plays a vital role (Ciampa, 2014).

- The biggest attack against personal security is social engineering. Social engineering is the process of gathering information to be used during an attack by exploiting the weaknesses of an individual (Aldawood and Skinner, 2019). There are a few techniques to be used during a social engineering attack. Some of these techniques are; pretending to be someone you are not, hoaxes, spear phishing, dumpster diving, shoulder surfing, piggy back, identity theft and analyzing Face Book and other social media sites (Ciampa, 2014).

- Computer Security. Computer security focuses on the security of the software loaded on the computer system. One of the biggest threats is malicious software that enters the computer system without the owner knowing it. This

causes all kinds of damage or theft of information. The best way to secure against computer security attacks is to keep the software security patches up to date, make use of good quality anti-virus programs and keep the virus data base up to date (Abousen, 2015). It is wise to load a software firewall for more protection. Backups are critical, to be able to recover after a computer attack (Ciampa, 2014).

- Internet Security. Internet security focuses on the security aspects when accessing the internet, specifically internet-based threats (Edwards, 2019). The internet consists of computers, servers and networks which are interconnected worldwide. It is a collection of networks to which devices are attached. Industry, government, universities, schools and individuals make use of this network called the internet. To stay secure on the internet the user has to make sure that security features on web browsers are activated and updated (Ciampa, 2014). Internet security includes hacking, the unauthorized access to computer systems, email accounts or websites, viruses and other malicious software (malware), damage of data or making systems vulnerable to other threats, and identity theft, when hackers steal personal details such as credit card numbers and bank account information (Edwards, 2019). Internet security is a way to protect against the above mentioned threats.

- Mobile Security. Mobile security focuses on the mobile device itself, devices such as mobile phones, tablets and laptops. It also includes the communication types used by mobile devices such as WiFi, Bluetooth, 3G, 4G and new 5G (Curran *et al.*, 2015). The security on the device includes encryption, passwords, auto lock features, the software used on the device such as the operating system and applications. The standard security software and the correct activation thereof is very important (Ciampa, 2014).

- Workplace / Physical Security. Physical / work space security involves the restriction of access to facilities and computer systems (Parmar, 2018). The access to facilities focuses on hardware locks, proximity readers, man-traps and video surveillance systems. The access to systems focuses on tokens, smart cards containing integrated circuit chips and bio-metric authentication. User restrictions have to be implemented to give users access only to specific areas and files on computer systems according to their job description and functions. Security policies and sub-policies have to be put in place to manage this (Ciampa, 2014).

2.3 Penetration Testing

Penetration testing is a term used when a party has authorization to determine the risk areas and the vulnerabilities on a targeted environment or an specific application, (wired or wireless networks, mobile devices, computer hardware and software) with the sole purpose of taking control over a system or to secure the system; this sometimes means that real attacks are launched on real systems by making use of the same tools and techniques which hackers use (Kim, 2018; Najera-Gutierrez and Ansari, 2018). This means that when doing penetration testing you target a specific organization's defensive systems (an organization who gave permission or who requested a penetration test) which consist of all the computer systems and infrastructure of the organization. Before a penetration test is executed it is well planned, otherwise the opposite effects will be reached, and the penetration test may be turned into a vulnerability (Engebretson, 2013; Baloch, 2015; Cyberdegrees.org, 2017).

A penetration test is executed by a penetration test expert who is contracted to find vulnerabilities and risk areas in a computer network. The penetration tester does the tests as a pro-active measure by a company to find vulnerabilities before the real hackers do. On completion of the penetration test the penetration tester will provide the company with a report with all the vulnerabilities found to be rectified (Engebretson, 2013; Epling *et al.*, 2015). Penetration testing is sometimes confused with Ethical Hacking; these two concepts are often referred to as the same (Najera-Gutierrez and Ansari, 2018).

2.3.1 History of Penetration Testing

Computer network have been tested by security specialists (penetration testers/white hat hackers) for almost 50 years, since the mid-1960s, trying to defend networks and information against hackers with malicious intent (Scott-Jackson, 2016). As computer systems grew to be able to communicate to each other and share information over various communication lines, the urge to protect information and information systems grew as well.

Government and industry started to realize that there was an opportunity for a hacker to compromise systems, steal data and influence communication lines. There are currently hundreds of terabytes of data flowing around each day, every minute, and every second. This makes the risk even bigger; with all this data flying around, there is an abundance of information to be stolen and all this information needs to be protected (Information Security Institute, 2016).

In 1965 a group of security specialists warned government and industry against

the dangers involving IT systems. Due to the rapid growth in the IT environment, communication between information systems and the sharing of information pose a big risk that computer systems might be compromised, communication channels influenced and information stolen. Due to this, computer and information systems need to be protected.

In 1967 the first annual Joint Computer Conference was held where 15 000 security specialists came together to discuss the possibility that information systems could be compromised and information stolen. A company called the Research ANd Development (RAND) Corporation then identified the need to protect computer systems by doing security scanning and the actual testing of systems. RAND Corporation joined with the Advanced Research Project Agency (ARPA) in the United States of America and created an important report called The Willis Report, which identified the security problems and suggested some technical considerations and policies that laid down the basis for security measures,some of which are still used today. Due to this report organizations, including governments, started building teams who did security scans to look for vulnerabilities in networks and computer systems to protect these systems against unethical hacking and penetration. The security teams were named after specialized military teams and called tiger teams (Information Security Institute, 2016).

The first penetration testing software was developed by James P. Anderson in 1972, to be used by tiger teams to find vulnerabilities in computer systems, to identify threats, to identify attacks, to find weaknesses during an attack and ways to defuse the threat. The skills used to perform such a penetration test are still used today (Information Security Institute, 2016).

Research and development on how to create secure systems continued during the 1970s and 1980s. Ground-breaking work was done during these years and several techniques that were identified form part of the standard system protection today. Multiple developers started developing software to assist the penetration testing teams in their work. Some of the concepts used in the early years of penetration testing are still relevant and used today. Some developments used for penetration testing were:

- Multics (Multiplexed Information and Computing Service), used by military, government and corporate entities from 1965 to 2000. Some of these concepts are still used today. Multics were a cross- platform development which allowed secure computing services to reach remote users in remote locations.

- Security Administrator Tool for Analyzing Networks (SATAN), developed in 1990. The tool executed a series of tests on its own networks to be able to identify vulnerabilities and while the tests were executed it built a report to

explain the issues identified. The types of scans and functionality of SATAN are the reason it is not in use any more. Development on SATAN was stopped and tools like Nessus and NMap replaced SATAN.

- Today, there are several penetration testing operating systems consisting of numerous tools to be utilized during security tests. Penetration tests are highly specialized; penetration testers need skills and special software to be able to execute security scans. Kali Linux[1] is an example of the specialized software used by penetration testers. Due to the introduction of new communication methods security tools need to be developed to be able to secure these methods. Some of the communication methods include, but are not limited to, Wired communication, Wireless communication which includes Bluetooth, GSM, normal WiFi and RFID (Information Security Institute, 2016).

2.3.2 Role of a Penetration Tester

The role of a penetration tester is critical due to the fact that he/she has to test, analyze, give guidance and recommendations on how to protect critical data and systems against vulnerabilities and risks found during the execution of a penetration test. A minor mistake will put the tester and the organization at risk. Keeping that in mind, a penetration tester must be a well-trained, skilled, competent individual. Therefore the roles of a penetration tester are as follows:

- Must identify infective allocation and use of tools and technology.
- Execute tests across core security systems.
- Protect critical data by identifying vulnerabilities and risks.
- Identify vital knowledge of risks and vulnerabilities throughout the tested infrastructure.
- Report and give priority to recommendations to make sure that the security team uses their time effectively while protecting the most important security risks.

2.3.3 Types of Penetration Testing

The important types of penetration testing as depicted in Figure 2.2, are as follows (Baloch, 2015; Jai and Mehtre, 2015; Guarda *et al.*, 2016):

- Black Box Penetration Testing.

[1] http://www.kali.org

- White Box Penetration Testing.
- Grey Box Penetration Testing.

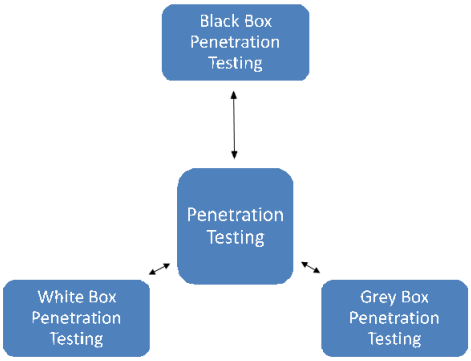

Figure 2.2: Types of Penetration Testing.

2.3.4 Black Box Penetration Testing

When doing Black Box Penetration Testing the tester has no information or prior knowledge of the system and network architecture to be tested. The main focus is on gathering information on the system to be tested. This means that the tester is only informed on what the expected outcome should be and there is no examining of programming code. Normally Black Box Penetration Testing is executed from an external network to the internal network where the tester has to rely on his skills and expertise to reach the objectives (Alisherov and Sattarova, 2009; Jai and Mehtre, 2015; Baloch, 2015; Guarda *et al.*, 2016). Advantages of Black Box Penetration Testing are:

- Due to the fact that the tester does not have to know a specific programming language, the tester does not necessarily have to be an expert, but needs to be skilled.
- The tests are executed from the viewpoint of a user and not the designer.
- The tester confirms conflicts in the specifications and the actual system.

2.3.5 White Box Penetration Testing

White Box Penetration Testing is a full and thorough test where the tester is given all the information needed about the system to be tested, which includes network

diagrams, operation systems used, source code and IP address ranges (Najera-Gutierrez and Ansari, 2018). This test is executed from inside the network to be tested. It can be seen as a simulation of an internal source attacking the network. White Box Penetration Testing gives better results than Black Box Testing (Alisherov and Sattarova, 2009; Baloch, 2015; Jai and Mehtre, 2015; Guarda *et al.*, 2016). Advantages of White Box Penetration Testing are as follows:

- Design errors are identified due to the difference in the logical flow of the software program and the actual execution.
- Typographical errors are identified and syntax checking is done.

2.3.6 Grey Box Penetration Testing

When doing Grey Box Penetration Testing the tester is provided with limited information on the network or system to be tested. Grey Box Testing is a combination of Black and White Box Testing. The test is executed from inside or outside the network to be tested. The test is seen as an hacking attempt from outside the organization by an attacker who has unauthorized access to network infrastructure and documentation (Alisherov and Sattarova, 2009; Baloch, 2015; Jai and Mehtre, 2015; Guarda *et al.*, 2016). Grey Box Testing is normally used for web application testing with the focus on finding the vulnerability within the application itself and not on the host server or the network (Najera-Gutierrez and Ansari, 2018). Advantages of Grey Box Penetration Testing are as follows:

- Not all internal information on network structures, program functions and operations is provided.
- The access to source code is not required which means that it is not intrusive and unbiased.

2.3.7 Areas of Penetration Testing

Penetration Testing is grouped in the following areas and is executed as such (Baloch, 2015).

- Network Penetration Testing. To ensure the security in a network, the physical structure is tested to identify vulnerabilities and risks. There are two types of network penetration testing, namely internal and external tests. When conducting internal tests, the tester becomes part of the internal network and tests the network. When conducting external tests, public IP addresses are tested. The areas in the company's network where the tester

identifies security weaknesses are in the design, implementation and operation. Physical devices to test include modems, routers, computers, mobile devices and remote access devices.

- Application Penetration Testing. Tests are done on the logical structure of the system. Vulnerabilities and risks are identified by simulating and attacking to expose the effectiveness of an application's security controls. Normally firewalls and other monitoring systems are used to protect security systems; in-depth testing needs to be done on network traffic which is allowed through the firewall.

- Web Application Penetration Testing. This is one of the well-known, very common and fastest growing tests. Due to the fact that the application host stores critical personal information of the user, web application testing is more common than a normal network penetration test. Critical data stored by the web application includes data such as passwords, pin numbers, usernames and credit card numbers.

- Mobile Application Penetration Testing. Since companies introduced the Bring Your Own Device (BYOD) concept, this type of testing is the newest, most rapidly growing test because organizations provide services to employees and customers via iOS and Android based applications. These tests are rapidly growing as companies want to ensure that their systems are secure and trusted by their users.

- Response or workflow. The response or workflow of the system is tested by making use of Social Engineering. Social Engineering is used to gather information by interacting with humans, by unauthorized access to classified documents which are not locked away or documents in waste bins that have not been shredded. Valuable information is gathered on the organization and systems by making use of Social Engineering attacks like phishing and spear phishing.

- Physical Penetration Testing. This form of testing is not that popular and is rarely done by the tester. This test is done when the tester is asked to physically walk into a building and test the physical security controls.

2.3.8 Manual Penetration Testing

Manual Penetration Testing is executed by a human being. A penetration testing expert is testing a machine for security risks and/or vulnerabilities. There are two types of Manual Penetration Testing.

- Focused Manual Penetration Testing. When executing Focused Manual Penetration Testing the penetration tester will focus on specific risks and vulnerabilities. This type of test cannot be done automatically; it has to be done by a human who examines specific application vulnerabilities within targeted systems.

- Comprehensive Manual Penetration Testing. Comprehensive Manual Penetration Testing is done on whole systems which are connected to each other to identify risks and vulnerabilities.

The approach towards manual penetration testing is generally divided into four phases.

Phase 1: Data Collection. Data collection plays a vital role when doing penetration testing. Data is collected manually by making use of data collection tools. The results received during data collection have an impact on how the rest of the penetration test is executed.

Phase 2: Vulnerability Assessment. Testers use the data collected to identify risks and vulnerabilities on a targeted system and take defensive steps to protect against vulnerabilities.

Phase 3: Actual Exploit. The expert tester will launch attacks on the targeted system and at the same time reduce the possibility of an attack by outsiders.

Phase 4: Report Preparation. On completion of the above-mentioned phases, the tester will prepare a report with full descriptions of everything found on the targeted system. As a final step the report is analyzed and corrective measures are put into place to protect the system tested.

2.3.9 Automated Penetration Testing

Automated Penetration Testing is an automated process testing for risks and vulnerabilities which is much faster, more efficient, very easy and trustworthy. If executing this type of testing there is no need for an expert tester, as a person with limited knowledge of the technology can run these tests. Some of the well-known Automated Penetration Testing tools are EnCase [2], Nessus [3], OpenVas [4] and Metasploit [5].

[2]https://www.guidancesoftware.com
[3]https://www.tenable.com/products/nessus/nessus-essentials
[4]http://www.openvas.org
[5]https://www.metasploit.com

Table 2.2: Automated Penetration Testing Tools.

Tool	URL	Description
EnCase	https://www.guidancesoftware .com	OpenVAS is a full-featured vulnerability scanner. Its capabilities include unauthenticated testing, authenticated testing, various high level and low level internet and industrial protocols, performance tuning for large-scale scans and a powerful internal programming language to implement any type of vulnerability test.
Nessus	https://www.tenable.com /products/nessus/ nessus-essentials	Nessus is a vulnerability scanner for network infrastructure with automatic scan analysis for remediation prioritization. Nessus includes web application, cloud environment and mobile device scanning. The Nessus vulnerability scanner family provides malware detection, auditing of control systems such as SCADA and embedded devices, configuration auditing and compliance checks.
OpenVas	http://www.openvas.org	OpenVAS is a framework of services and tools that provides a comprehensive and powerful vulnerability scanning and management package.
Metasploit	https://www.metasploit.com	Metasploit verifies vulnerabilities, manages security assessments, and improves security awareness; it empowers and arms defenders to always stay one step ahead of the game.

2.3.10 Manual vs. Automated Penetration Testing

Table 2.2 list the important differences between Manual and Automated Penetration Testing.

Table 2.3: Difference between Manual and Automated Penetration Testing.

Manual Penetration Test	Automated Penetration Test
An expert is required to execute the test.	A person with limited knowledge can execute the test due to automated tools.
Different tools are required for testing.	Make use of integrated tools.
Results vary from test to test.	It has fixed results.
The tester needs to clean up memory.	Does not need cleaning of memory.
It takes time and is extensive.	It is fast and efficient.
Has advantages, the tester can analyze the situation, think how an attacker thinks, decide on the steps to follow, and how to protect and secure the system.	Cannot analyze the situation
The tester runs multiple tests according to the requirement.	Cannot run multiple tests like in manual process.
More reliable in critical environments.	Less reliable in critical environment.

2.3.11 Penetration Testing workflow.

The penetration testing workflow is all the processes to be followed during an penetration test. This includes the process from gathering the initial information right through to retesting to confirm that all risk areas are protected (DataArt, 2018; Vectra, 2018). The penetration testing workflow is depicted in Figure 2.3. When planning the execution of a penetration test the first action will be the gathering of information of the network or system to be tested. After analysis of the information gathered a vulnerability analysis will be executed. During the vulnerability analysis the information gathering process will continue. The next step is attack modelling; by understanding the attack model the penetration tester will get some insight into the vulnerabilities found during the vulnerability analysis. When the attack modelling is understood the information can be used to protect the tested network from future attacks. While executing the attack modelling the information gathering and vulnerability analysis is a continuous process. After the attack modelling the attack execution will follow, while the first three steps continue. After

the attack execution step full reporting will take place. This includes report writing and physical reporting to the management team of the organization tested. After reporting, the final step will be retesting to ensure the risk areas are protected.

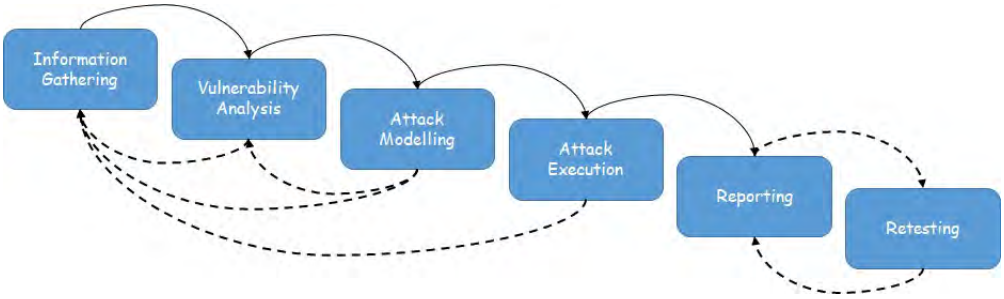

Figure 2.3: Penetration Testing Workflow after (DataArt, 2018; Vectra, 2018).

2.3.12 Penetration Testing Tools

In the penetration testing world there are multiple tools to be used. The tools used during a penetration test are absolutely the preference of the tester. The penetration tester will use tools that he/she feels comfortable with and they will use the best tool for the specific part of the test (Engebretson, 2013; Verma, 2016; Cybersecurity, 2017).

Penetration testing tools are software applications which assist the penetration tester in executing the task at hand. These tools include manual and automatic tools. Normally the tools consist of information gathering tools, vulnerability and risk analysis tools, exploits to test for vulnerabilities and report writing tools. The tester has to know the features of the specific tools he/she is using to utilize them at full capacity. Penetration testing tools are platform dependent. They are mostly freeware, although some of the well-known tools have a trial version, and a license fee has to be paid for the full version. Linux Operating System distributions are available, which have a combination of tools incorporated into the Operating System. Kali Linux [6], BackBox [7] and Parrot [8] are examples of such Operating Systems (Banks, 2016; Cybersecurity, 2017).

During an online poll it was found that there are preferred penetration testing tools also known as the most used tools in the environment, and the list of preferred tools was confirmed by cyber security experts (Vonnegut, 2016; Verma, 2016; Banks, 2016; Cybersecurity, 2017). A table containing the list of the most used penetration testing tools is attached to this thesis as Appendix D.

[6] https://www.kali.org.
[7] https://www.blackbox.org.
[8] https://www.parrotsec.org.

2.3.13 Penetration Testing Report Writing

According to Henry (2012), the ultimate goal of penetration testing is to help an organization to secure their networks, systems and databases. The penetration tester has the responsibility of providing meaningful information to the organization being tested. This information will enable the organization to compile a rectification plan for mitigating any vulnerabilities and to put security strategies in place. Baloch (2015, pg 8-9) is of the opinion that penetration testing report writing is a skill that needs to be developed by a penetration tester. A penetration testing report is a comprehensive task which includes the methodology used, procedures, clear explanations on the report design and the content, a detailed explanation on the tests done, and the tester's personal experience. After publishing the report to the company CEO, senior management staff and the technical team, the rectification plan needs to be written with target dates for when rectifications need to be completed (Henry, 2012; Baloch, 2015).

Overall the report has to be simple, clear and understandable, well presented, well organized, without spelling and grammar mistakes. Due to the extensive writing process, penetration testing report writing is divided into four stages, namely:

1. Report Planning.
2. Information Collection.
3. Writing the First Draft.
4. Review and Finalization.

The typical content of a penetration testing report is listed in Appendix C, Penetration Testing report writing framework.

2.3.14 Penetration Testing Limitations

Due to the rapid change in cyber and information technology, the penetration testing success stories are fairly short lived. Organizations will more easily build more protection into systems than perform penetration tests to prevent possible successful attacks. Some of the major limitations of penetration testing are as follows:

- **Time**. Penetration testing should not be a time-bound process; however penetration testing experts allocate a fixed amount of time for each test. On the other hand, an attacker has no time limits; they plan their attacks in a week, a month or even years.

- **Scope**. Because of organization's own limitations, such as budget constraints, limited resources, and security constraints, not all aspects can be tested. Similarly, penetration testers have limitations as well; they sometimes have to skip parts of the penetration test that might be a big risk or vulnerability that might be exploited by an attacker.

- **Access**. Penetration testers are given restricted access to the target environment to be tested, for instance, if the De-Militarized Zone (DMZ) is tested from across its internet networks, but no tests were done through the normal internet gateway.

- **Methods**. During a test, when making use of specific attack methods there is a possibility that the target system may crash; to avoid target system crashes the penetration tester will circumvent attacks that may cause downtime.

- **Skill sets**. Professional penetration testers are limited as they have limited and scarce skills acquired during past experience and their expertise. Penetration testers focus on a specific technology and have rare knowledge of other fields of expertise.

- **Known Exploits**. Many of penetration testers only know exploits which are public, and they do not think the way attackers think. An attacker's imaginative thinking is better than a tester's which means the attacker has the ability to discover the vulnerability or risk to attack.

- **Experiment**. Some testers are time bound and work by a tight schedule to reach the customer's requirements. When working on a tight time schedule the tester does not have time to try something new, they do not think outside the box, and they only follow the customer's instructions, whereas attackers think outside the box, they are free to think, free to experiment and free to develop a new attack path.

2.3.15 Penetration Testing Legal Issues

Before a penetration tester executes a test, he/she has to get proper authorization before conducting the test. In the case of testing sensitive data, the tester has to ensure that the company takes measures with regards to the confidentiality, integrity and availability of data. The following are some of the legal issues between the tester and the client:

- In most of the cases the tester is not known to the client, so the decision has to be made if the tester may have access to sensitive data. If data is lost,

who will take responsibility for the lost data? This may play a big role in the confidentiality, integrity and availability of sensitive data.

- The tester has to confirm who is the owner of the system to be tested, and inform the client that tests may have an effect on the company's systems.
- Permission has to be given to the tester in writing, which clearly defines the parameters.
- The details of the tester have to be given to the company with a declaration that no sensitive or confidential data will be leaked.
- A legal agreement is critical for both parties.
- The law with regard to penetration testing differs from country to country. The tester has to ensure that he/she is familiar with the laws in the respective country.
- The penetration tester has to ensure that he/she knows the law in a respective country before signing agreements.

2.4 Red and Blue Teaming

Red and Blue teams is a term which is used in the military, where members of the red team will attack a target (the blue team) and the members of the blue team will defend against attacks. The cyber security/information security environment adapts this method as well where red team members attack a network or system and blue team members have to defend or protect the network or system. If the implementation of Red and Blue teams is functioning properly, continuous knowledge sharing between the red and the blue teams is very important for continuous improvement on both sides. During Red and Blue team exercises the members of the Red and Blue teams must use the opportunity to improve their skills and to see it as a training opportunity (Sangster *et al.*, 2009; Carlin *et al.*, 2010).

- **Red Team**. The term Red Team is used to identify opposing forces also known as the enemy. Red teams normally want to cause damage, infiltrate or pretend to be something they are not. Red teams try to gain access by making use of hacking skills and can also be seen as penetration testing. Red teams find flaws in network defenses and exploit them with authorization from the organizations they are working for (Miessler, 2016; Applebaum *et al.*, 2016).
- **Blue Team**. Blue Team refer to own forces or friendly forces, to protect or defend. Blue team is a good opportunity to ensure that the members of an

organization adhere to policies and procedures. Blue teams defend against red teams or real attackers. Blue teams defend against exploitation or cyber-attacks and will constantly update and try to improve security (Pack and Rowe, 2013; Miessler, 2016).

- **Purple Team**. A big problem within an organization and between organizations is the sharing of information. During Red and Blue team events the sharing of information might become a challenge as well. A Purple team is not needed if information and experiences are shared among Red and Blue teams. Keeping that in mind, a Purple team is a group of security experts who make sure that Red and Blue teams function to their full capacity with maximum effectiveness. The Purple team will accomplish this by combining the defensive strategies, skills and controls of Blue teams with vulnerabilities, risk areas and threats identified by Red teams, build all these aspects into a single narrative and confirm that all efforts are applied to the maximum. If the Purple team functions properly the value of the Red and Blue team will be visible. The whole purpose of the Purple team is to share knowledge between Red (offensive) and Blue (defensive) teams. A Purple team is not needed when Red and Blue teams function properly (Miessler, 2016).

2.5 Capture the Flag

Capture The Flag (CTF) exercises originated in defence forces all over the world where there are two teams competing in battle exercises against each other with the main purpose of capturing a flag situated in the opposing force's territory. The teams were also known as red and blue teams only to identify teams. The team who captures the opposing force flag first is the winner. A cyber CTF works on the same principle where the only difference is that a digital flag needs to be captured (Mirkovic and Peter, 2014). There are three types of CTFs, namely:

- Jeopardy CTF - A couple of scenarios / challenges are set up over a wide spectrum of IT aspects, for example, password cracking, hashes, forensics, encryption, hacking skills. Points are gained for each completed task. Easy challenges count for fewer points than complicated challenges. Participants/teams can only proceed to the next challenge if the current challenge is solved. At the end of the game time the participant / team with the highest points/most digital flags captured, is the winner.

- Attack - Defense CTF - Each team has its own network/host with vulnerable services. Each team gets time to patch vulnerabilities on their own

network/host and also to develop exploits and confirm strategies. The CTF organizers connect all participants on a network and the war game starts. Participants earn defence points by protecting their own services and earn attack points by hacking opponents. This type of CTF was historically the first type of CTF.

- Mixed CTF - Mixed CTF competitions are normally a mixture of jeopardy and attack-defence CTFs.

CTF activities and exercises have a multi-functional purpose. In some environments CTF is used as an awareness training session for the more advanced computer user in the organization. On the other hand, it is used to train your cyber warriors and to keep them up to scratch with new cyber security trends and vulnerabilities (Eagle and Clark, 2004; Mirkovic and Peter, 2014). Cyber warriors are people who are involved in cyber warfare, either for personal reasons or patriotic or religious beliefs. Cyber warfare is conducted defensively or offensively against computer and information systems. Cyber warriors have different roles depending on the individual's expertise and skills area in computer and information security (Leenen *et al.*, 2018).

2.6 Terminology / Definitions.

Numerous concepts are referred to in the research. Section 2.6 give clarity on terminology and definitions used by the researcher to put everything into perspective. This section gives the researchers perspective on the terminology and definitions used during the research.

2.6.1 Skill

A skill is a type of work or activity which requires special training and knowledge. It is an ability and capacity acquired through deliberate, systematic, and sustained effort to smoothly and adaptively carry out complex activities or job functions involving ideas (cognitive skills), things (technical skills), and/or people (interpersonal skills).

2.6.2 Skills Gap

A skills gap is defined as "a significant gap between an organization's skill needs and the current capabilities of its workforce". A skill gap is the difference in the skills required on the job and the actual skills possessed by the employees. A skills

gap presents an opportunity for the company and the employee to identify the missing skills and try to gain them. The American Society for Training and Development (ASTD) defines a skills gap as a significant gap between an organization's current capabilities and the skills it needs to achieve its goals.

2.6.3 Formal Education

Formal education is any training which is structured, in a classroom (physical or online), and any topic can be taught (Champion *et al.*, 2014).

2.6.4 Informal Education

Informal education is seen as self-taught and outside the classroom concept. It is the extent to which a person explores a subject although the nature of the subject might originate from a classroom (Champion *et al.*, 2014).

2.6.5 Offensive Cyber

Offensive cyber is defined as operations to manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks.(Uren *et al.*, 2018).

2.6.6 Defensive Cyber

Defensive cyber consists of a wide range of activities which are important to enable an organization to protect itself from an attack and to be able to rapidly respond to any threat. Defensive cyber includes the capability to detect any threat and to detect when you are targeted, the capability to react and respond to any threat, preventative controls and cyber deterrents to reduce your appeal to the attackers (Bateman, 2014). If these measure are in place it will ensure the integrity, availability, confidentiality and non-repudiation of the protected information (Uren *et al.*, 2018).

2.6.7 Cyber Security

Cyber security is a combination of technologies, processes, procedures and practices which is designed to protect computers, data, information, networks, and programs from attack, damage and unauthorized access. Cyber security is a critical part of any government's or organization's security strategy (Ciampa, 2014). According to the National Institute of Standards and Technology, Computer Security Resource Centre, cyber security also includes the protection and prevention of damage to

information on computer and communication systems to ensure the availability, integrity, authentication, confidentiality, and nonrepudiation thereof (NIST, 2019).

2.6.8 Cyber Threat

According to Ciampa (2014) a threat is an event or an action that represents a danger or could cause harm to information assets, which is something that has value.

2.6.9 Threat Agent

According to Ciampa (2014) a threat agent is a person or element that has the power to carry out a threat, usually by exploiting a vulnerability, which is a flaw or weakness.

2.6.10 Risk

A risk is the probability that a threat agent will exploit the vulnerability. According to Baloch (2015, pg 3) a risk is defined as the impact or damage caused by the successful compromise of an asset. A risk is normally calculated by using the equation Risk = Threat x Vulnerabilities x Impact.

2.6.11 Cyber Risks

A cyber risk is not only one specific risk. A cyber risk is rather a group of risks that differ in technology, attack vectors, etc. These risks are addressed as a group due to two similar characteristics, potential great impact and considered improbable. A cyber risk can be seen as any risk (or loss) on any technological storage device, network, personal data or any type of transaction while connected to the internet (Ciampa, 2014). According to Baloch (2015, pg 3)'s definition of a risk, the assumption can be made that a cyber risk is then the impact or damage that will be inflicted on the successful compromise of an information technology system or infrastructure.

2.6.12 Information security

Information security is the protection of the confidentiality, integrity and the availability of information on devices with the capability of storing, processing and transmitting information and is accomplished through policies, procedures, people and products (Ciampa, 2014).

2.6.13 Penetration Testing

Penetration testing is a term used when someone has authorization to determine the risk areas and the vulnerabilities on a targeted environment or a specific application (Najera-Gutierrez and Ansari, 2018), (wired or wireless networks, mobile devices, computer hardware and software) with the sole purpose of taking control of a system or to secure the system. This sometimes means that real attacks are launched on real systems by making use of the same tools and techniques which hackers use (Wai, 2002; Baloch, 2015; Epling *et al.*, 2015; Falah *et al.*, 2017; Cyberdegrees.org, 2017).

2.6.14 Framework

There are many different definitions of a framework, but all these definitions boil down to one idea. According to two of the biggest online dictionaries, The Merriam-Webster and the Business Dictionary, a framework is an open structure, a frame, an outline or a skeleton of combined ideas, supporting a specific method to reach an identified or specific objective. It can be seen as a guide which if necessary, can be adjusted by removing and adding items (Web Finance, 2017; Webster, 2018).

2.6.15 Methodology

The most important steps in a penetration test is the methodology and reporting. A methodology is a process or map which is used by the penetration tester to guide him/her to reach their desired results to meet the customers' requirements. The methodology contains all the steps to be followed by the tester and the tools to be used during testing (Alisherov and Sattarova, 2009; Zitta *et al.*, 2014).

2.6.16 Social Engineering

Social Engineering is the processes / techniques / skills (such as digital, in person, over the phone) used to target a human, a group of humans or an organization / company in order to find or steal sensitive information, money, company secrets, intellectual property (Ciampa, 2014)

2.6.17 Vulnerability

A weakness in a security system which allow a penetration tester or a hacker to compromise or break into the system. The weakness can exist in the network protocols, the operating system or the application software (Singh *et al.*, 2018).

2.7 Summary

The logical flow of this chapter followed the outline provided by the goals set in Section 1.2. This chapter began by clarifying the cyber concept. It is important to understand the cyber concepts first and then delve deeper into specific areas in cyber security. Due to the focus of this research, penetration testing is an in-depth discussion to identify the purpose, skills and experience needed to be a professional.

This chapter provides background on cyber security with definitions of all the cyber concepts to set a baseline and get the reader in the right frame of mind to understand concepts which are focused on. Section 2.1 provided an overall introduction to cyber security which might be well known but not understood. Section 2.2 gave a full background on cyber security, information security and information system security awareness which included Cyber Security Awareness. Cyber Security Awareness is further discussed with a full explanation on penetration testing. In section 2.4, Red and Blue teaming and Capture The Flag (CTF) were discussed.

Section 2.6 defined the cyber security terms and explained some of the cyber security terminologies.

In Chapter 3 an analysis is presented on the history and concepts in International standards aligned with the Lockheed Martin Kill Chain and a Penetration Testing Framework is suggested.

3

International Penetration Testing Standards and Frameworks

Chapter 2 contained the literature study to lay the baseline with regards to cyber security concepts and cyber security definitions. Chapter 3 contains a history of cyber security standards with a proposed framework focusing on penetration testing. Section 3.1 contains an introduction to cyber security standards focusing on penetration testing, where after the history and usage of the three most used cyber security standards are analyzed. The three standards analyzed are the National Institute of Standards and Technology 800-115 (NIST 800-115), the International Organization for Standardization 27000 series (ISO 27000) and the Payment Card Industry Data Security Standard (PCI DSS), with an overview of the history of the Lockheed Martin Cyber Kill Chain. Section 3.2 contain an in dept analysis of the mentioned standards. Section 3.3 contain an analysis of prescribes skills needed to do penetration testing according to the analyzed standards and framework. A hybrid penetration testing framework is proposed in Section 3.4. Chapter 3 ends with a summary in Section 3.5.

3.1 Cyber Security Standards focusing on Penetration Testing

Cyber security dates back to the 1970s when the United States federal government for the first time identified the possibility of a security breach. The Federal Computer Systems Protection Act was proposed, but did not pass approval by government. From the 1970s to the mid-1990s cyber security was not a top priority and only from the 2000s was more attention given to cyber security. As cyber incidents increased measures were put in place in the form of Acts, national and international standards to address all aspects in the cyber security field. One of these cyber security fields was identified as penetration testing as a proactive measure to a cyber incident (Kremling and Parker, 2017).

A penetration tester is an IT expert with a thorough understanding of a wide range of IT concepts such as networks, computer hardware and software and programming. A penetration tester executes penetration tests on a network with the aim of finding vulnerabilities or risk areas to secure the network before real hackers find and exploit vulnerabilities. Penetration testers are authorized individuals or groups of professionals contracted and appointed by an organization to perform a penetration test (Epling *et al.*, 2015; Cyberdegrees.org, 2017).

Penetration testers sometimes launch real attacks on live systems by making use of the same tools and techniques which hackers use. This means that when doing penetration testing you target a specific organizations defensive system (an organization who gave permission or who requested a penetration test) which consists of all the computer systems and infrastructures of the organization. Before a penetration test is executed it is well planned, otherwise the opposite effects will be reached, and the penetration test may be turned into a vulnerability (Baloch, 2015; Cyberdegrees.org, 2017).

The penetration tester does the tests as a pro-active measure. On completion of the penetration test the penetration tester will provide the company with a report with all the vulnerabilities found or risk areas to be worked into a rectification plan by the company's IT department (Epling *et al.*, 2015).

The most important step in a penetration test is the methodology followed by the penetration tester. A methodology is a process or map which is used by the penetration tester to guide him/her to reach their desired results to meet the customer's requirements; the methodology contains all the steps to be followed and tools to be used during testing (Alisherov and Sattarova, 2009; Zitta *et al.*, 2014).

Penetration testers adopt methodologies or use a combined methodology according to their preference. These methodologies are part of international standards which include The International Organization of Standards (ISO), the Payment

Card Industry (PCI DSS) and the National Institute of Standards and Technology (NIST). A methodology is used to plan properly to ensure that a test is conducted professionally, is less time consuming, and is effective (Alisherov and Sattarova, 2009; Baloch, 2015).

International Standardization organizations give organizations in industry an option to comply with their standards, normally when an organization has in-house penetration testers. There are specific processes to follow and be evaluated against to be compliant with a chosen international standard.

International standards date back to 1120 AD where the first measurement standard was identified as the ell. International Cyber Security standards were used as a guideline from as early as 1990, from where new standards were developed and because of the rapid growth in technology were updated on a regular basis. In Chapter 3 the history of International Standards and specifically cyber security standards will be discussed with the focus on Penetration Testing. A comparison was done on three of the big Standardization bodies, namely The National Institute of Standards and Technology (NIST), The International Organization for Standardization (ISO) and The Payment Card Industry Data Security Standard Counsel (PCI DSS). A comparison is done by comparing the International Standards with the Lockheed Martin Cyber Kill Chain (Lockheed Martin Corporation, 2015) to identify an penetration testing framework to help penetration testers to accomplish their goal. By suggesting a penetration testing framework, the required skills level will also be indicated.

3.1.1 History of Standards

During the writing up of the history of the world the presence of standards is clearly visible. In some instances, royal judgments were the cause of the creation of some standards. For example, King Henry I of England created a standard for measurement in 1120 AD by introducing the ell, which was the same length as his forearm, from the bend of the elbow to the tip of the middle finger (about 18 inches or 457mm); later the ell was replaced by the foot which was based on a booted foot rather that the naked foot (1 foot = 304,8mm). Some standards were an extension of man's wish to harmonize his accomplishments with important changes in a specific environment. Others were produced in response to the requirements of an increasingly complex society (Quigley *et al.*, 2015).

Ancient civilization recorded one of the earliest instances where a standard was standardized when the calendar was created. During the Industrial Revolution, the US Government and US Department of Defence introduced the standard for a common railroad gauge which measured the track size: this was adopted from

England. This standard was implemented for use in the Transcontinental Railroad in 1886.

In the 20th century as cities expanded rapidly, bringing wealth, more and more people started moving to urban areas as cities became more sophisticated and their infrastructures more complex. To make sure that city dwellers were safe it became apparent that a set of specialized national standards would be necessary. For example, after a fire incident in America in 1902 where reinforcements from different cities were requested, it was realized that the fire hose couplings of the different cities fire department's were not the same size, which had a devastating effect on fighting the fire. Afterwards, on completion of an investigation it was found that there were 600 different types of couplings used all around America (Quigley *et al.*, 2015).

A year after the incident a national standard was created to ensure uniform fire safety equipment and the safety of Americans nationwide. It is clear that through the history of the world the development of standards was necessary. Standards are very important in the international community especially when different countries are working together during a joint international attempt. The importance of standards is of utmost important in industries like engineering, information technology, medical, architecture and defence, to name just a few.

3.2 Information Technology Standards.

The public is constantly made aware of cyber incidents and information security breaches taking place all over the world. The average public observers might think that information security is a new concept, lately getting widespread attention. On the contrary, the information security aspect has been an area of concern and interest for almost as long as the digital age.

Three of the big cyber security role players in the standardization community were analyzed. The cyber security standards which were analyzed were the National Institute of Standards and Technology 800-115 (NIST 800-115), Payment Card Industry Data Security Standard (PCI DSS), International Organization for Standardization 27001 (ISO 27001). These three standards were selected due to the focus placed on penetration testing.

3.2.1 National Institute of Standards and Technology (NIST).

The National Institute of Standards and Technology is a United States of America National Standard; it is a measurement laboratory standard with activities divided into laboratory programs which include Information Technology.

Between 1901 and 1988 the National Institute of Standards and Technology was known as the National Bureau of Standards (NBS). Although the National Institute of Standards and Technology is a United States national organization, international organizations are adapting to the National Institute of Standards and Technology standards across multiple industries. The National Institute of Standards and Technology was established on 03 March 1901, by Dr Samuel Wesley Stratton, who also served as the founding director. Dr. Stratton was the first director of the National Institute of Standards and Technology and held the position for 21 years (NIST, 2017).

According to the National Institute of Standards and Technology, their mission, is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

According to the National Institute of Standards and Technology's vision, they aim to be the world's leader in creating critical measurement solutions and will promote equitable standards (NIST, 2017; Alexander D and Panguluri, 2017).

According to the National Institute of Standards and Technology's core values they ensure a high performing environment safe and respectful to all. These values are:

- Perseverance: Take a holistic approach in planning the future with scientific knowledge and imagination to ensure continued impact and relevance.
- Integrity: ethical, honest, independent and provide an objective perspective.
- Inclusivity: People diversity and ideas inside and outside the National Institute of Standards and Technology are considered to attain the best solutions to multidisciplinary challenges.
- Excellence: Rigor and critical thinking are applied to achieve world class results and continuous improvement in everything that is done (NIST, 2017).

As the National Institute of Standards and Technology is organized into laboratory programs and extramural programs, these programs were realigned and reduced from ten to six laboratories with effect from 1st October 2010. These laboratories include (NIST, 2017):

- Centre for Nan-scale Science and Technology (CNST).
- Communications Technology Laboratory (CTL).
- Engineering Laboratory (EL).
- Information Technology Laboratory (ITL).

- NIST Center for Neutron Research (NCNR).
- Material Measurement Laboratory (MML),
- Physical Measurement Laboratory (PML).

The National Institute of Standards and Technology, Major Programs include: (NIST, 2017)

- Office of Advance Manufacturing (OAM).
- Baldrige Performance Excellence Program.
- Manufacturing Extension Partnership (MEP).
- Special Programs Office.

A shortened history of the National Institute of Standards and Technology series Special Publications standards are depicted in the timeline figure below.

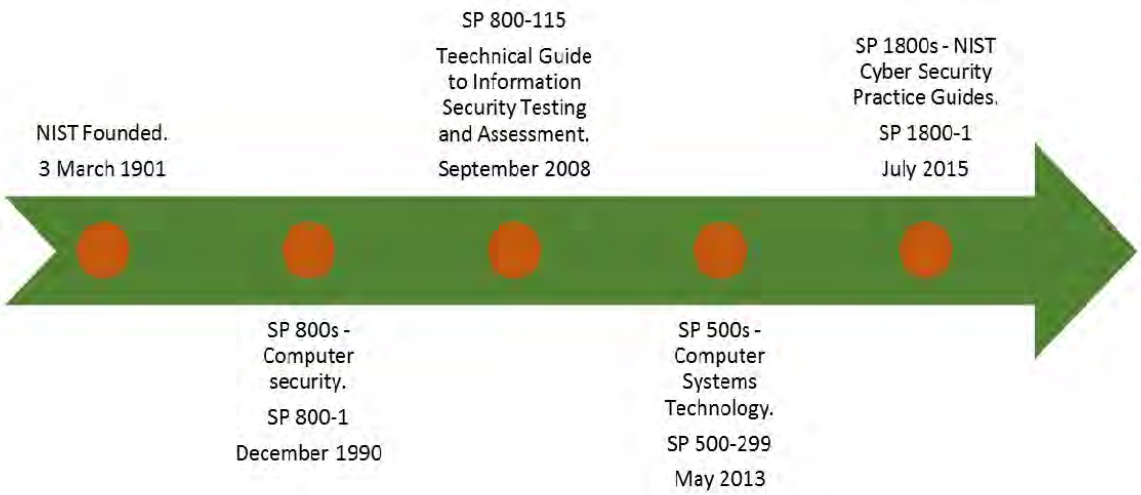

Figure 3.1: National Institute of Standards and Technology shortened timeline (NIST, 2017).

The National Institute of Standards and Technology make use of three different Special Publication sub-series to publish all cyber, information and computer security aspects covering guidelines, reference materials and recommendations. The three Special Publication sub-series are as follows (NIST, 2017).

- Special Publication (SP) 800 - Computer Security, ranging from SP 800-1 to SP 800-193. The first Special Publication (SP 800-1) was presented in December 1990; the National Institute of Standards and Technology makes use

of this sub-series as its primary mode of publishing cyber, computer and information security recommendations, guidelines and reference materials. In this paper a deeper analysis of SP 800-115 will be done.

- Special Publication (SP) 1800 - National Institute of Standards and Technology, Cyber security Practice Guides, ranging from SP 1800-1 to SP 1800-8, the first Special Publication (SP 1800-1) presented in July 2015. The 1800 sub-series were created to compliment the 800 sub-series. The 1800 sub-series were created to focus on specific cyber security challenges in the private and public sectors. The 1800 sub-series consisted of practical user friendly guides to be used in the adoption of standards based on approaches to cyber security.

- Special Publication (SP) 500 - Computer Systems Technology. There are only two publications in this sub-series, namely SP 500-299 and SP 500-304; the first publication was presented in January 1977 and revised in May 2013 as indicated on the timeline above, Figure 3.1. This is the general IT sub-series which is more broadly used by the National Institute of Standards and Technology Information Technology Laboratory (ITL). The 500 sub-series were used for computer security publications before the 800 sub-series came into existence.

Other than the International Organization for Standards, the National Institute of Standards is a United States based organization and does not have international members. International industries and organizations use NIST as an industry best practice and only adopt parts of their standards (Alexander D and Panguluri, 2017).

The National Institute of Standards and Technology, SP 800-115 specifically, prescribes a framework to be used when doing security testing; this includes review techniques, target identification, target vulnerability, validation techniques and report writing.

3.2.2 Payment Card Industry Data Security Standards Council (PCI DSS)

The Payment Card Industry Data Security Standards Council was established by the five globally used payment brands giants, namely: (King, 2017)

- American Express.
- Discover Financial Service.
- JCB International.

- MasterCard.
- Visa Inc.

The organizational structure consists of and is led by a policy-setting Executive Committee, presented by the five founding global payment brands and strategic members. Participating organizations forms a Board of Advisors who provides inputs and feedback on the development of the Payment Card Industry Standard. There are management committees comprised of founding and strategic members and employees of the council. The management committees are responsible for: (King, 2017)

- Maintenance of the Payment Card Industry Standard.
- Maintenance of the Council technical work product.
- Development and management of new work groups, Special Interest Groups and task forces on technical matters.
- Management of day-to-day functions.

The Payment Card Industry Data Security Standards Council is a global open body established to develop, enhance, disseminate and assist in understanding the security standards for payment account security. The Payment Card Industry Security Standards Council maintains, evolves and promotes the Payment Card Industry Security Standards. For the implementation of the standard the Council provides important tools such as: (King, 2017)

- Assessment and scanning qualifications.
- Self-assessment questionnaires.
- Education and training.
- Product certification programs.

The history of the Payment Card Industry Data Security Standard Council standard releases are depicted in the timeline figure below (Parizo, 2013; Innovative Solutions, 2016; King, 2017).

Figure 3.2: Payment Card Industry Standard timeline.

3.2.3 International Organization for Standardization

The International Organization for Standardization (ISO) is an International organization; therefore the name has different meanings or other acronyms in different languages. The founders took the acronym ISO which was taken from the Greek "isos", which means "equal". From there the slogan "Whatever the country, whatever the language, we are always ISO" (ISO, 2017).

The ISO as it is known today was known as the International Federation of the National Standardizing Associations (ISA) from 1926 until 1942. During this time the focus was heavily on mechanical engineering. ISA was disbanded in 1942 during the Second World War, and re-organized as the ISO in 1946 (Martincic, 1997).

The ISO started in 1946, at the Institute of Civil Engineers in London, where 65 delegates from 25 countries met. During this meeting delegates discussed the future of international standardization. The ISO formally started operations on 23 February 1947, with 67 technical committees (experts focusing on a specific subject). Today the ISO Central Secretariat is situated in Geneva, Switzerland, with more than 135 full-time employees, members from 163 countries and 781 technical bodies looking after standard development. The ISO is the world's largest developer of voluntary International Standards. Since 1947 till today, the ISO has published 21655 International standards covering aspects of technology and business (Martincic, 1997; ISO, 2017; Alexander D and Panguluri, 2017).

The ISO has members worldwide. Each country has only one member to represent the ISO in that country. Individuals or companies cannot become members of the International Organization for Standardization. The ISO member in South Africa is known as the South African Bureau of Standards (SABS), with Information Security Standards, SANS 27000:2018/ISO/IEC 2700:2016 (ISO, 2017; SANS,

2018).

Three membership categories exist, each with a different level of access and influence into the ISO system. The three membership categories and their involvement are as follows: (ISO, 2017)

- Full members/Member bodies - Participating and voting in the International Organization for Standardization technical and policy meetings. Sell and adopt the International Organization for Standardization International Standards nationally.

- Correspondent members - Attend the International Organization for Standardization technical and policy meetings as observers. Sell and adopt the International Organization for Standardization International Standards nationally.

- Subscriber member - Can only keep up to date with regards to the International Organization for Standardization's work but cannot participate in it. Cannot sell or adopt the International Organization for Standardization International Standards nationally.

In 2015 the International Organization for Standardization had 162 members from all over the world: 119 countries were full members, 38 countries were correspondent members and 5 countries were subscriber members. The figure below shows the International Organization for Standardization membership of countries in the world as well as their membership category (ISO, 2017).

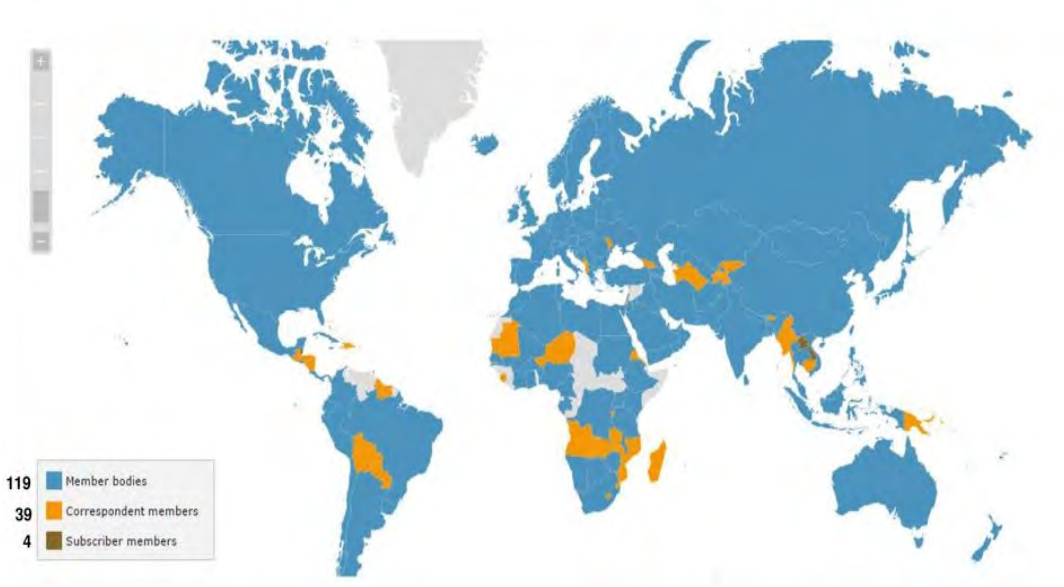

Figure 3.3: ISO member states and membership category.

To develop an International Organization for Standardization standard is a time-consuming process consisting of professionals in the specific field. To develop an International Organization for Standardization standard from the first proposal until final publication takes about 3 years. The development process has 6 steps, as follows (ISO, 2017):

- Step 1: Preliminary work is done where the initial feasibility for a standard is assessed, and the proposal for the new work item is proposed.
- Step 2: Expert consensus is built with a First working/Committee Draft (CD) and an International Organization for Standardization Publicly Available Specification (PAS) as deliverable.
- Step 3: Consensus is built in the TC/SC. Technical Specifications and technical report as deliverable.
- Step 4: The international standard is drafted, final text for processing is added with the Final Draft International Standard (FDIS) as a deliverable.
- Step 5: All the international bodies have a formal vote on the standard and submit their comments. The secretariat proof checks the draft document and final recommendations are added.
- Step 6: The international standard is published.

The ISO and the International Electro technical Commission (IEC) developed and published the ISO/IEC 27000 series (also known as ISO 27000 family) of mutually supporting information security standards (ISO, 2017).

Cyber/information security will and will always be one of the most critical aspects in organizations. As information systems evolve and more sensitive data is stored, it is critical that organizations protect their most important data assets, to ensure client, customer and partner confidence, and for their own operational needs (Wang, 2011; ISO, 2017).

As the International Organization for Standardization Standards is seen as the top international standard, providing a sound baseline for guidance, organizations use the International Organization for Standardization 27000 series international standard as the critical guideline when implementing comprehensive Information Security Management Systems (ISMS). The first International Organization for Standardization working group started their efforts in information security standards in 1993; since then the International Organization for Standardization 27000 series standard continued to evolve and mature to the documents it is today and serves as the basis for the ISMS international certification. With the involvement and knowledge of experts in the information security environment and

the history of continuous revising and updating (improvement) of the International Organization for Standardization 27000 series, the utilization of this standard as a foundation for information security management systems is necessary. This does not mean that International Organization for Standardization 27000 series of standards is the ultimate international standard; the other cyber/information security standards must be kept in mind as well (Wang, 2011; ISO, 2017; Alexander D and Panguluri, 2017).

The history of the International Organization for Standardization 27000 series standards is depicted in Figure 3.4.

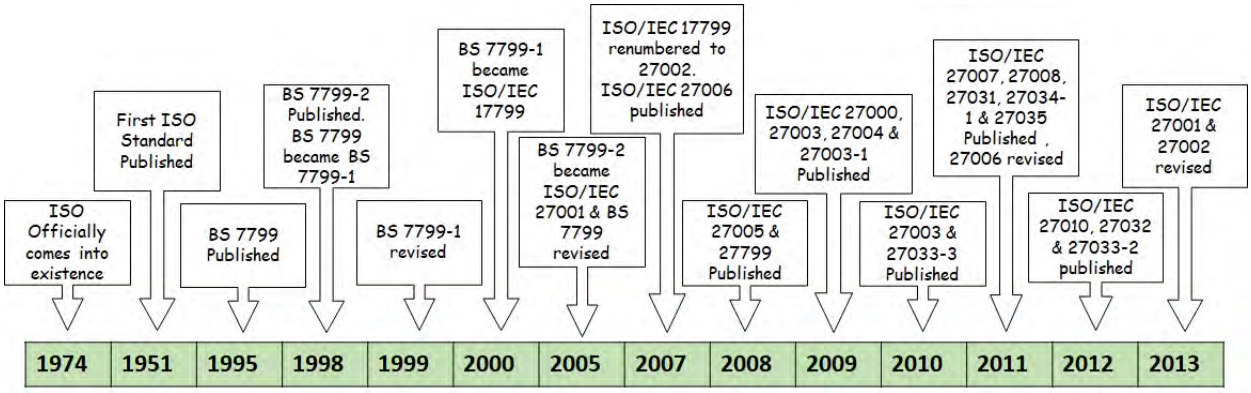

Figure 3.4: International Organization for Standardization 27000 series.

The main standard in the International Organization for Standardization 27000 series is the ISO/IEC 27001:2013, known as ISO 27001. This part of the standard set out the requirements against which an information security management system can be certified and audited. All the other ISO 27000 series standards support ISO 27001. This paper focuses on penetration testing and is therefore only focusing on ISO 27001.

3.2.4 Lockheed Martin Kill Chain

Lockheed Martin is a global company based in America. They specialize in aerospace, defence, security and advance technologies sought after from a global perspective. The Lockheed Martin Company was formed by merging the Lockheed Corporation and Martin Marietta in March 1995; their headquarters are in Bethesda, Maryland in Washington DC (Lockheed Martin Corporation, 2015).

The kill chain is originally a military concept associated with the structure of an attack ranging from the identification of the target to the destruction of the target. The Lockheed Martin Kill Chain is a framework used as an Intelligence Driven Defence model to identify and prevent cyber intrusions (Hutchins *et al.*, 2011; MITRE, 2014; Lockheed Martin Corporation, 2015; Filkins, 2017).

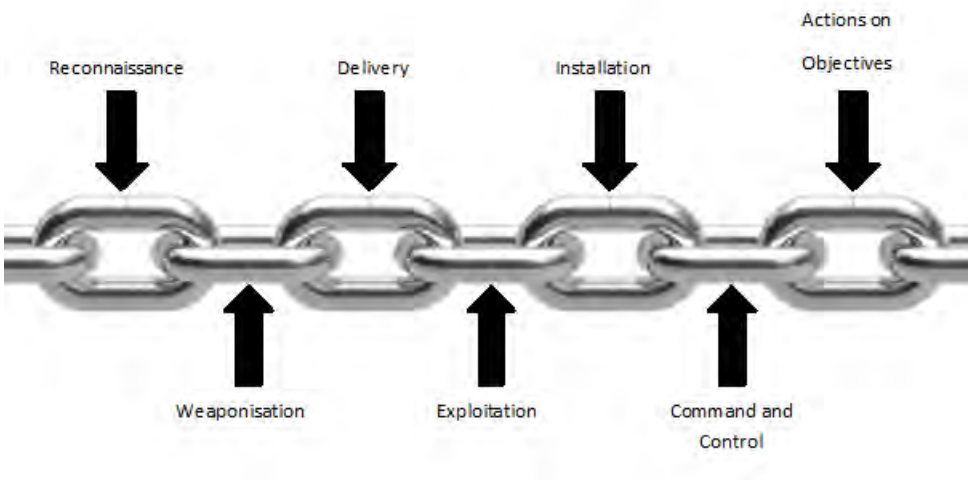

Figure 3.5: Lockheed Martin Kill Chain.

As depicted above the Lockheed Martin Kill Chain (LMKC) framework contains seven important steps which can be adapted by cyber specialists to identify key areas in a cyber attack determining the weak link in the chain, preventing a breach before the chain breaks. The Lockheed Martin Kill Chain increases the visibility of an attack by increasing a cyber specialist's understanding of the techniques, procedures and tactics used to launch an attack. The seven Lockheed Martin Kill Chain steps include, in sequence, Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control and Actions on Objectives (Bamford *et al.*, 2013; Zitta *et al.*, 2014; Lockheed Martin Corporation, 2015; Information Security Institute, 2016; Filkins, 2017).

The seven phases of the Cyber Kill Chain are:

- **Reconnaissance**. The gathering of open source / publicly available information. This can be done on the internet and by social engineering. The attacker will do reconnaissance before the attack start.

- **Weaponization**. By using vulnerabilities or exploits found during the reconnaissance phase, the attacker will create malicious payloads and send them to the victim. This step will take place on the attacker side.

- **Delivery**. By using intrusion methods, the attacker will send his payload to his victim by email or any other method.

- **Exploitation**. When the attacker is making use of an exploit it will be executed.

- **Installation**. If the attacker makes use of malware as part of his attack the malware installation takes place on the infected computer. This phase

will take place when executed and may take months to activate as this phase forms part of the whole extensive hacking process.

- **Command and control**. After gaining access to the targeted machine or network the attacker will create a command and control channel such as a backdoor to be able to connect to the target and work remotely.

- **Action on objectives**. For the attacker to achieve his goals on the targeted network he will work through these phases. This is a complicated and intense process which takes months and multiple small steps in order to achieve the goal.

The Cyber Kill Chain was developed by Lockheed Martin based on the original Lockheed Martin Kill Chain to be used as a model to identify and prevent cyber intrusions (Bamford *et al.*, 2013; Zitta *et al.*, 2014; Franco, 2016). The Lockheed Martin Cyber Kill Chain is depicted below.

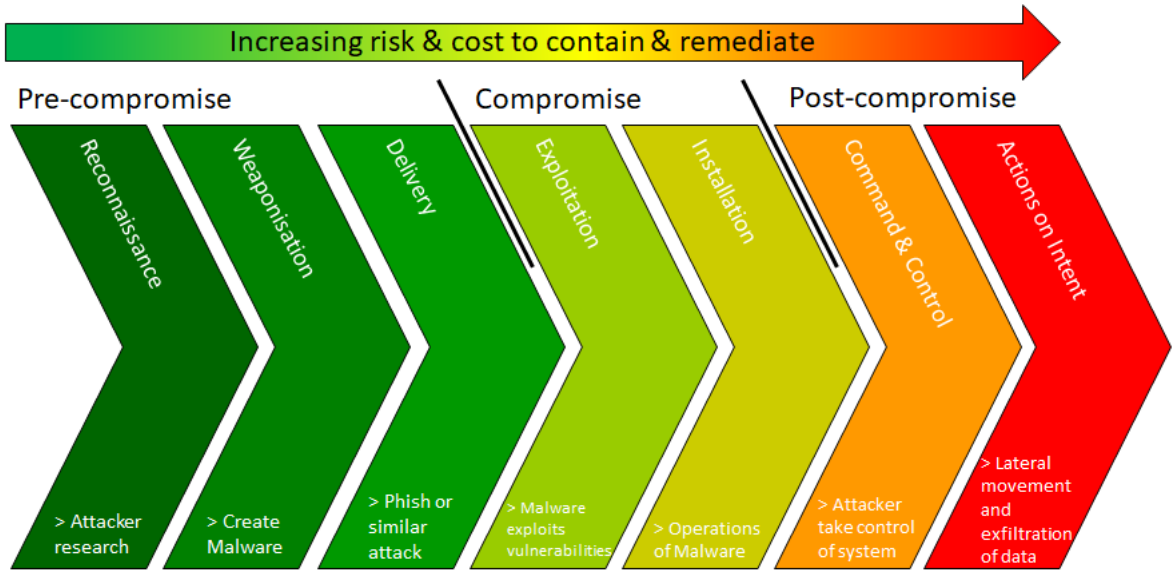

Figure 3.6: Lockheed Martin Cyber Kill Chain.

According to Lockheed Martin "An intruder will only succeed when launching an attack, if they work through steps one to six and reach the final stage of the Cyber Kill Chain". The Lockheed Martin Kill Chain, when adapted by penetration testers, will strengthen processes, and assist in enabling methods to be proactive in protecting computer systems and networks to ensure that cyber attacks are prevented at the same time. The Lockheed Martin Kill Chain is used for offensive and defensive cyber. Utilizing the Lockheed Martin Kill Chain or part thereof in the penetration testing environment will be beneficial to the penetration tester. Usually the attacker's tactics will be to focus on the most vulnerable area of a net-

work or system; they will usually not go directly for the target (Zitta *et al.*, 2014; Lockheed Martin Corporation, 2015).

By using the LMKC the vulnerable areas on a network or system will be identified before an attack. The identification of vulnerable areas depends on the skills level of the penetration tester, and the attacks on networks or systems will also be different due to the skills level of an attacker. The Lockheed Martin Kill Chain is only a guideline when planning an attack or a penetration test. An attack will not exactly match the steps in the LMKC, but the Kill Chain will help to identify the risks and vulnerabilities to be secured (Zitta *et al.*, 2014).

3.3 Skills recommended by international standards

According to the three international standards analyzed, each has their own methodologies which are followed and especially the National Institute of Standards and Technology suggests which tools and skills a person needs if they want to become a penetration tester. The standards can be adopted individually or a combination of specific parts, according to requirements, from different standards are combined to develop a standard fitted for a specific environment. With all the standards one needs a sound penetration testing methodology to achieve successful results. The analyzed standards are compared with the Lockheed Martin Kill Chain in the matrix below according to their suggested methodology. It is evident that the methodologies suggested by the international standards are basically the same, giving the same results.

3.3.1 Standards aligned with Lockheed Martin Kill Chain Matrix.

The international standards have different focus areas which make them unique. These focus areas indicated are as follows:

- National Institute of Standards and Technology. The National Institute of Standards and Technology, NIST 800-115 gives a clear indication of what skills a penetration tester must have in order to successfully complete the steps according to their methodology (Thomas, 2017). According to the National Institute of standards a penetration tester needs to have skills in the following areas as depicted below in Figure 3.7.

Figure 3.7: National Institute of Standards and Technology prescribed skills.

- Payment Card Industry Data Security Standard Council. The Payment Card Industry Data Security Standard Council has a very specific methodology to be followed by security testers who comply with their standard. There is a very specific guideline on courses to be done by a security tester to comply with the standard. The Payment Card Industry methodology concentrates on the following areas as depicted below in Figure 3.8.

Figure 3.8: Payment Card Industry Data Security Standard prescribed skills.

- International Organization for Standardization. According to the International Organization for Standards methodology the following processes are followed during a penetration test, as depicted below in Figure 3.9.

Figure 3.9: International Organization for Standardization prescribed skills.

The three international standards each has their own indication on skills needed for penetration testing. The National Institute of Standards and Technology suggests which tools and skills a person needs to become a penetration tester. The International Standards can be adopted individually or a combination of standards can be used to develop a framework for a specific environment to achieve the desired results. A skills matrix was set up to compare the international standards with the Lockheed Martin Cyber Kill Chain. As a result, an accurate framework to cover all aspects can be proposed for use in any environment (Bamford *et al.*, 2013; Harris *et al.*, 2013; Mattern *et al.*, 2014; Franco, 2016).

Table 3.1: Penetration Testing skills matrix.

Lockheed Martin Cyber Kill Chain	**NIST 800-115**	**ISO 27001**	**PCI DSS**
Reconnaissance (Identify Targets)	Review Techniques	Information Gathering	Host and Service Discovery
Weponization (Prepare the operation)	Target Identification	Target Modelling	Vulnerability Identification and verification
Delivery (Launch the operation)	Target vulnerability Validation Techniques	Vulnerability Analysis, Exploitation, Post-exploitation	System exploitation and Compromise
Exploitation (Gain access to the target)			
Installation (Establish presence)	NA	NA	NA
Command and Control (Remote access and control)	NA	NA	NA
Actions on objective (Achieve the goal and report)	Report writing	Reporting	Report writing

Table 3.1 presents a comparison of skills needed according to the three interna-

tional standards analyzed and the Lockheed Martin Cyber Kill Chain. It is evident that not one international standard covers the whole spectrum of the penetration testing process according to the Lockheed Martin Cyber Kill Chain. As mentioned earlier, if one link in the chain is not covered the chain is broken. Thus, a combination of the processes in the standards can be used to strengthen the process. Figure 3.10: International Standards aligned with Lockheed Martin Cyber Kill Chain, depicts the alignment of standards with the cyber kill chain.

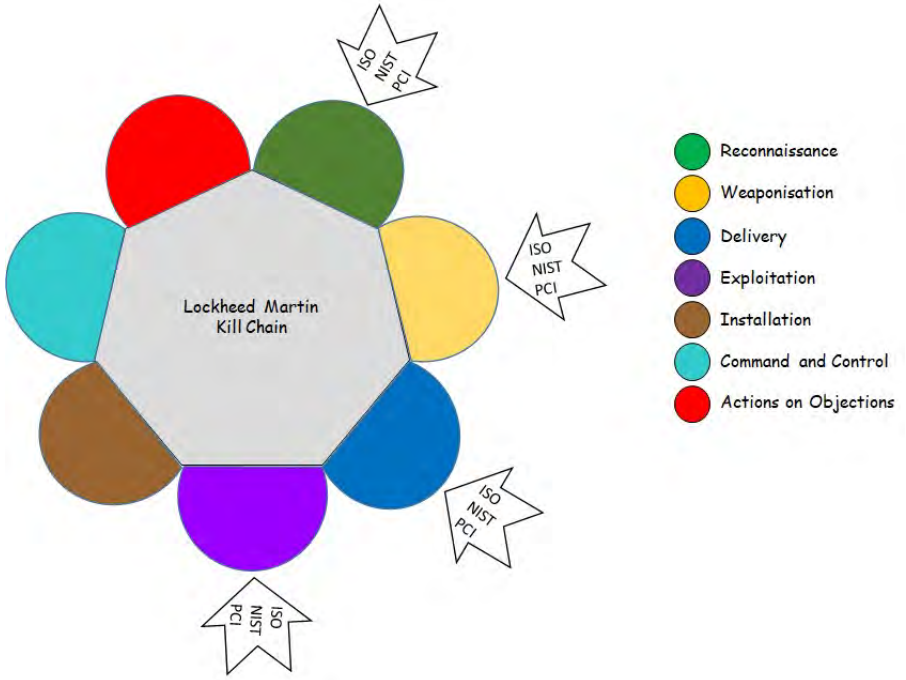

Figure 3.10: International Standards aligned with Lockheed Martin Cyber Kill Chain.

3.4 Penetration Testing Frameworks

To be able to identify and manage vulnerabilities and risk areas on a networks or devices, it is important to understand cyber security (also known as information security), and the link it has towards the availability, integrity, and confidentiality of infrastructure and information. Cyber security specifications differ from one organization to another, which mean that risks and vulnerabilities are not treated with the same urgency across the board. Due to this approach by IT specialists in organizations, the cyber incident rate will continue to grow and have a huge impact on business (Guarda *et al.*, 2016; Creasey and Glover, 2017).

Many organizations do have policies in place regarding cyber security, but they are not always enforced. Because not all organizations treat cyber security with the same level of urgency, penetration testing frameworks used by organizations

will differ. The penetration testing framework suggested will lay down a baseline, and can easily be adapted (Guarda *et al.*, 2016; Creasey and Glover, 2017).

As explain in the previous section, three international standards and the Lockheed Martin Cyber Kill Chain were analyzed. The results thereof were aligned with the basic penetration testing processes in order to come to a conclusion for a possible basic penetration testing framework. There is no silver bullet when conducting a penetration test due to the fact that not all organizations networks will look the same. The penetration testers will be able to develop their own framework from this basic generic framework (MITRE, 2014; Guarda *et al.*, 2016; NIST, 2018a).

The framework will provide a common classification and mechanism for an organization to:

- Identify and define their current cyber security level;
- Identify and prioritize risks and vulnerability areas for improvement and rectification within the context of a continuous and reliable process;
- Build security levels towards the required target state;
- Share identified risks and vulnerabilities, with proposed counter measures with internal and external stakeholders.

The suggested framework can easily be changed to fit the organization's needs. The approach for this penetration testing framework is for it to be flexible, performance based, easy to use and cost effective. The framework is designed to provide guidance in performing a successful penetration test. The framework can contribute to developing a common language used by penetration testers internationally (Creasey and Glover, 2017; NIST, 2018a).

3.4.1 Overview of the frameworks

This framework is based on a basic network penetration test. Most functions can be used for web and software penetration tests. The approach to the framework is based on risk to identify and manage cyber risks and vulnerabilities. The framework consists of two parts: the core of the framework and implementation levels. Each component of the framework supports the connection between cyber security activities and IT infrastructure, hardware, software and the skills of the penetration tester (NIST, 2018a; MITRE, 2014). An explanation of the framework components is as follows:

Framework Core: the framework core is a set of cyber security activities, desired outcomes and valid references that are common across the penetration testing processes and functions. The core provides clear understanding and communication from the executive level to the operations level with regard to international standards, good practices and guidelines. This framework does not include the initial planning phase and authorization (Bamford *et al.*, 2013; Harris *et al.*, 2013; Mattern *et al.*, 2014; MITRE, 2014; Zitta *et al.*, 2014; Jai and Mehtre, 2015). The core contain six functions, namely:

1. Reconnaissance.

2. Target Evaluation (Weaponization and Delivery).

3. Exploitation.

4. Privilege Escalation (Installation).

5. Maintaining a Foothold (Command and Control).

6. Reporting (Actions on Objectives).

These six functions give an organization a strategic view of the cyber security risk management life cycle. The framework core will identify the essential categories and subcategories for each function. Each subcategory will then be matched with useful references such as international standards, guidelines and methodologies (NIST, 2018a; Cybersecurity, 2017). The structure of the framework core is depicted in Table 3.2 and explained thereafter.

Table 3.2: Penetration Test Framework Core Structure.

Function	Categories	Subcategories	References
Reconnaissance			
Target Evaluation			
Exploitation			
Privilege Escalation			
Maintaining a Foothold			
Reporting			

The Framework Core Structure has four main focus points as shown in Table 3.2.

1. **Functions** - Relates to the steps the penetration tester needs to follow during execution. The functions are aligned with Standards and Methodologies to aid the penetration tester in the management of the process (ISO, 2017; NIST, 2017; King, 2017; Cyberdegrees.org, 2017; NIST, 2018a).

2. **Categories** - Subdivides functions into groups of outcomes to be reached by penetration tester. This will basically identify what needs to be done and how the goal can be reached.

3. **Subcategories** - Divides categories further into specific outcomes of technical activities which provide results to support the achievement of the outcome of each category.

4. **References** - For this framework four standards were evaluated which include the Lockheed Martin Kill Chain, NIST 800-115, ISO 27001 and PCI DSS, which will act as a guide to reach the objective (Lockheed Martin Corporation, 2015; NIST, 2017; King, 2017; ISO, 2017).

Implementation levels: The implementation level is greatly dependent on the skills level and experience level of the penetration tester him/herself. The functions and categories identified in the Framework Core make up a sequence of events to follow. The skills and experience level of the penetration tester will determine how far the penetration test will progress and how successful the test will be. The functions can be executed by only one very experienced penetration tester or by a team of penetration testers specializing in a specific function. Depending on the size of the organization, a penetration test will be executed by a team of penetration testers specializing in a specific function during the test, due to the high level of skills and experience needed to conduct a successful penetration test. Any penetration tester, regardless of their expertise level, has to be a good report writer. Every step done during the functions of penetration testing needs to be recorded to ensure a chain of events to protect the penetration tester.

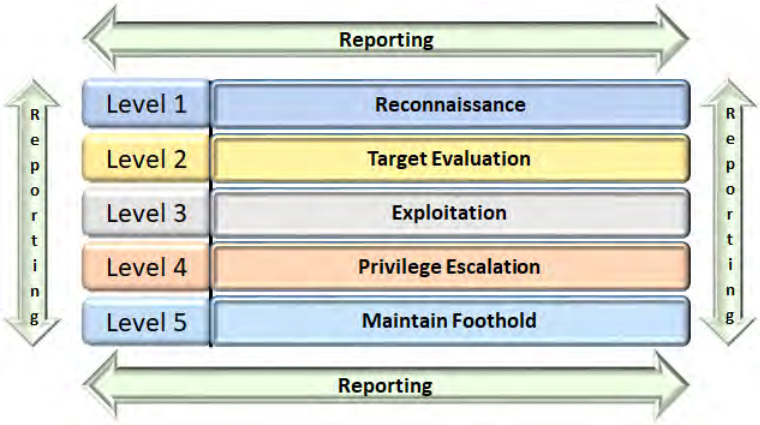

Figure 3.11: Penetration Testing Framework implementation levels.

As indicated in Table 3.3, a penetration test execution can be done by a very experienced individual or by a team of experts specializing in a specific area. Take note that reporting is crucial in all the levels. The implementation levels are explained as follows (Bamford *et al.*, 2013; Harris *et al.*, 2013):

1. **Reconnaissance** – Gathering information on the target by making use of public information sources such as the internet, social engineering and physical connection to the target network. All information available is collected during this phase. The reconnaissance phase is divided into passive and active functions (Lockheed Martin Corporation, 2015; NIST, 2017).

2. **Target evaluation** (Weaponization and Delivery) – After completion of the reconnaissance phase the penetration tester will have enough information to execute the target evaluation. The penetration tester must have the skill to identify which vulnerability is exploitable and which tools to use for that. Using the right tool will shorten the execution time and will make it difficult to detect (NIST, 2018a).

3. **Exploitation** – Exploitation is the process where identified vulnerabilities are used to gain unauthorized access to the target. Authorization is needed from the organization to do exploitation. Exploitation can be a manual or automated process (NIST, 2018a; Lockheed Martin Corporation, 2015; King, 2017; NIST, 2017).

4. **Privilege Escalation** (Installation) – After initial access to the target is established in the exploitation phase on most likely a guest account, the next step is to gain administrator privilege through additional exploiting. This is called privilege escalation.

5. **Maintaining a Foothold** (Command and Control) – This is the process where the penetration tester looks for alternative ways to get access to the targeted system. In this step the penetration tester will cover his steps by leaving no traces behind (NIST, 2018a; Lockheed Martin Corporation, 2015).

6. **Reporting** (Actions on objectives)– Reporting is one of the most important functions during a penetration test. This is the method of communication between the penetration tester, the organization's IT department and the CEO and other executives of the organization. Reporting lists and describes each potential risk and vulnerability discovered, how and to what extent it may be exploited, and possibilities on how to counter the risks and rectify the problems (King, 2017).

Proposed Framework: The Framework Core indicates the categories and functions to be use in the Proposed Framework. Indicated in Table 3.3, and Table 3.4, for ease of use, all of the functions and categories in the Framework Core were given a unique identifier. The subcategories are given the same sequence identifier coupled to the correlating category. These identifiers will help in the process of structuring your own basic penetration testing framework (Thomas, 2017).

Table 3.3: Function and Category identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
RC	Reconnaissance	RC.PR	Passive Reconaissance
		RC.AR	Active Reconaissance
		RC.DF	Document findings
TE	Target Evaluation	TE.ET	Evaluate target for weakness
		TE.IP	Identify and prioritise vulnerable systems
		TE.MVS	Map vulnerable systems to aset owners
		TE.DF	Document findings
EP	Exploitation	EP.EV	Exploit vulnerabilities
		EP.OF	Obtain foothold
		EP.CUD	Capture unauthorised data
		EP.ASE	Aggresively social engineer
		EP.AS	Attack other systems or applications
		EP.DF	Document findings
PE	Privilege Escalation	PE.OA	Obtain escalated level access
		PE.UA	Uncover other user account information
		PE.AO	Access other systems with escalated privileges
		PE.DF	Document findings
MF	Maintain Foothold	MF.EA	Establish multipal access methods
		MF.RE	Remove evidence of authorised access
		MF.RS	Repair systems
		MF.ID	Inject false data
		MF.HC	Hide communication
		MF.DF	Document findings
RP	Reporting	RP.ES	Executive Summary
		RP.MT	Methodology
		RP.DF	Detail Findings
		RP.RF	References

Table 3.4 is an example of a penetration testing framework. The framework will change according to the objectives and outcomes of the penetration test to be conducted. The framework will give the penetration tester the opportunity to plan all necessary areas to be tested, identify if advanced skills and tools are needed during execution, and will contribute to the success of the penetration test.

Table 3.4: Penetration Testing Framework, Level 1 - Reconnaissance.

Function	Category	Subcategory	Reference
Reconnaissance (RC)	Passive Reconnaissance (RC.PR): To gather information in such a manner not to draw the attention of the target.	**RC.PR-1**: Identify Targets, public network information such as IP address, DNS name, Contact Information, Bussiness address, Social websites.	Lockheed Martin Kill Chain, NIST 800-115, ISO 27001, PCI DSS
		RC.PR-2: Identify System Tipes, by making use of banner grabing.	
		RC.PR-3: Passive Social Enginering Information.	
		RC.PR-4: Footprinting.	
		RC.PR-5: Document findings.	
	Active Reconnaissance (RC.AR): To gather information while interacting with the target, this method will draw attention.	**RC.AR-1**: Discover network and hosts.	Lockheed Martin Kill Chain, NIST 800-115, ISO 27001, PCI DSS
		RC.AR-2: Identify Available Ports and Services through scanning with Nmap.	
		RC.AR-3: Search for unpublished directories, files and servers	
		RC.AR-4: OS Fingerprinting, Banner grabing, web server application scan.	
		RC.AR-5: Document findings.	
	Document findings (RC.DF)	**RC.DF-1:** Scope of work.	
		RC.DF-2: Summary of findings.	
		RC.DF-3: Summary of recommendations.	

Table 3.5: Penetration Testing Framework, Level 2 - Target Evaluation.

Function	Category	Subcategory	Reference
Target Evaluation (TE)	Evaluate target for weakness (TE.ET)	**TE.ET-1:** Identify weaknesses by using scanners such as Nessus and GFI.	Lockheed Martin Kill Chain, NIST 800-115, ISO 27001, PCI DSS
	Identify and prioritise vulnerable systems (TE.IP)	**TE.IP-1:** Identify vulnerabilities by using CVE database.	
		TE.IP-2: Use Nessus vulnerability scan results to prioritise vulnerabilities.	
	Map vulnerable systems to aset owners (TE.MVS)	**TE.MVS-1:** Visualise network map by making use of an network mapper.	
		TE.MVS-2: Compare Network Map with network diagram and asset list.	
		TE.MVS-3: Aset owner versus network priviliges.	
	Document findings (TE.DF)	**TE.DF-1:** Scope of work.	
		TE.DF-2: Summary of findings.	
		TE.DF-3: Summary of recommendations.	

Table 3.6: Penetration Testing Framework, Level 3 - Exploitation.

Function	Category	Subcategory	Reference
Exploitation (EP)	Exploit vulnerabilities (EP.EV)	**EP.EV-1:** Use vulnerabilities to bypass security restrictions.	Lockheed Martin Kill Chain, NIST 800-115, ISO 27001, PCI DSS
		EP.EV-2: Minimise risk to target, maximise possible success.	
		EP.EV-3: Identify main entry points.	
		EP.EV-4: Identify high value target assets.	
	Obtain foothold (EP.OF)	**EP.OF-1:** Identify configuration settings.	
		EP.OF-2: Identify communication channels.	
		EP.OF-3: Identify relationships with other network devices.	
		EP.OF-4: Identify methods of accessing the network at a later time.	
	Capture unauthorised data (EP.CUD)	**EP.CUD-1:** Network sniffing.	
		EP.CUD-2: Packet sniffing.	
		EP.CUD-3: Honeypots.	
		EP.CUD-4: Social engineering.	
	Aggresively social engineer (EP.ASE)	**EP.ASE-1:** Phishing attack.	
		EP.ASE-2: Pretexting attack.	
		EP.ASE-3: Media dropping	
		EP.ASE-4: Tailgating and physical information gathering.	
	Attack other systems or applications (EP.AS)	**EP.AS-1:** Identify other targets on network with same vulnerabilities.	
		EP.AS-2: Identify priviledged users.	
		EP.AS-3: Identify vulnerable applications to be exploited.	
	Document findings (EP.DF)	**EP.DF-1:** Scope of work.	
		EP.DF-2: Summary of findings.	
		EP.DF-3: Summary of recommendations.	

Table 3.7: Penetration Testing Framework, Level 4 - Privilege Escalation.

Function	Category	Subcategory	Reference
Privilege Escalation (PE)	Obtain escalated level access (PE.OA)	**PE.OA-1:** Password Cracking.	Lockheed Martin Kill Chain, NIST 800-115, iSO 27001, PCI DSS
		PE.OA-2: DLL preloading, replace shared folder DLL with malicious DLL.	
	Uncover other user account information (PE.UA)	**PE.UA-1:** Dumping SAM or Config file.	
		PE.UA-2: Identify sensitive information stored in shared folders.	
		PE.UA-3: Change system settings.	
	Access other systems with escalated privileges (PE.AO)	**PE.AO-1:** Create new system users.	
		PE.AO-2: Install tracking cookies.	
		PE.AO-3: Remote user logon.	
	Document findings (PE.DF)	**PE.DF-1:** Scope of work.	
		PE.DF-2: Summary of findings.	
		PE.DF-3: Summary of recommendations.	

Table 3.8: Penetration Testing Framework, Level 5 - Maintain Foothold.

Function	Category	Subcategory	Reference
Maintain Foothold (MF)	Establish multiple access methods (MF.EA)	**MF.EA-1:** Install Rootkits.	Lockheed Martin Kill Chain, NIST 800-115, ISO 27001, PCI DSS
		MF.EA-2: Install backdoors.	
		MF.EA-3: Establish communication ports.	
		MF.EA-4: Install key loggers.	
	Remove evidence of authorised access (MF.RE)	**MF.RE-1:** Anti- incident response procedures.	
		MF.RE-2: Anti - Ferensic measures.	
	Repair systems (MF.RS)	**MF.RS-1:** Ensure target is in original state.	
		MF.RS-2: Change everything back as originally found.	
		MF.RS-3: Cover tracks.	
		MF.RS-4: Secure communication links.	
	Inject false data (MF.ID)	**MF.ID-1:** Inject malicious file.	
		MF.ID-2: Adding fake entries to log files.	
		MF.ID-3: SQL injection.	
		MF.ID-4: Cross-site Scripting.	
	Hide communication (MF.HC)	**MF.HC-1:** Use automated tools.	
		MF.HC-2: Do not open shells.	
		MF.HC-3: Don't be to noisy on the network.	
	Document findings (MF.DF)	**MF.DF-1:** Scope of work.	
		MF.DF-2: Summary of findings.	
		MF.DF-3: Summary of recommendations.	

Table 3.9: Penetration Testing Framework, Level 6 - Reporting.

Function	Category	Subcategory	Reference
Reporting (RP)	Executive Summary (RP.ES)	**RP.ES-1:** Scope of the work that was done.	NIST 800-115, ISO 27001, PCI DSS
		RP.ES-2: Objectives for Penetration Test.	
		RP.ES-3: Assumptions made.	
		RP.ES-4: Timelines.	
		RP.ES-5: Summary of findings.	
		RP.ES-6: Summary of recommendations.	
	Methodology (PR.MT)	**PR.MT-1:** Planning.	
		PR.MT-2: Exploitation.	
		PR.MT-3: Reporting.	
	Detail Findings (RP.DF)	**PR.DF-1:** Detail on system information.	
		PR.DF-2: OS Server information	
	References (RP.RF)	**PR.RF-1:** Appendixes.	

Not all penetration tests will be the same, but the basics of penetration testing will stay the same. The proposed penetration testing framework is a baseline to be used by the penetration tester to help identify the functions to be performed during a test. As indicated in the proposed framework, reporting is added at all functional levels. This will help the penetration tester to maintain a chain of evidence throughout the process and will save time in the writing of the final report especially when working with a penetration testing team. As indicated, the penetration tester's skills play a vital role in the successful execution of the penetration test. The penetration tester will determine the framework structure to be used according to objectives to be reached during planning.

3.5 Summary

It is important to understand the origin of International Standards and what is prescribed in these standards to be able to implement the standards in an organization. Although the basics prescribed in the three standards are basically the same a penetration testing framework was suggested taking into consideration the international standard prescribed and the Lockheed Martin Cyber Kill Chain.

Chapter 3 gave an introduction to cyber security standards focusing on penetration testing, there after the history and usage of the three most used cyber security standards were analyzed. The three standards analyzed were the National Institute of Standards and Technology 800-115 (NIST 800-115), the International Organization for Standardization 27000 series (ISO 27000) and the Payment Card Industry Data Security Standard (PCI DSS), and include an overview of the history of the Lockheed Martin Cyber Kill Chain. Section 3.2 gave an in dept analysis of the mentioned standards. Section 3.3 contain an analysis of prescribes skills needed to do penetration testing according to the analyzed standards and framework. A hybrid penetration testing framework were proposed in Section 3.4. Chapter 3 ends with a summary in Section 3.5.

4

Education and Skills

In Chapter 3 an analysis was done of three of the main cyber security international standards, namely the National Institute of Standards and Technology, the International Organization for Standards and the Payment Card Industry Data Security Standard and compared to the Lockheed Martin Cyber Kill Chain.

In Chapter 4 an analysis is presented on the available tertiary education available for cyber professionals, with a particular focus on penetration testers. Section 4.1 includes an introduction to the concerns with regard to the cyber skills gap in industry. The cyber skills gap is identified by analyzing the value of university degrees, international certifications and practical skills as prescribed in job advertisements. An educational roadmap on penetration testing skills is proposed and aligned with what industry needs as advertised in job advertisements in real life, in Section 4.1. In Section 4.2 a possible solution will be proposed to help industry to successfully appoint cyber professionals. Thereafter Chapter 4 concludes with a summary in Section 4.3.

4.1 Educational Roadmap

As new technology becomes available it brings with it new trends and vulnerabilities. Technology grows yearly, and in some cases monthly, depending on the rate that technology changes. The scale of connected devices in the digital world gives an indication on how cyber crime has grown. As new technology becomes available

it brings with it new security risks. Thus, the importance of cyber security is an undeniable fact (Silensec, 2017).

According to the premier global market intelligence provider, International Data Corporation (IDC), security technology worldwide revenue will exceed $100 Billion in 2020. The security training and certification market will be worth more than two billion dollars. However, there is still an outcry from employers all over the world indicating the shortage of skilled cyber security professionals (Silensec, 2017).

South Africa was not always in the sights of cyber criminals, but as new Information Technology communication technology was upgraded and introduced, and better connectivity made available, cyber criminals start to build an interest in South Africa's digital world. This communication technology made it easier to connect to the internet, which introduced new threats to normal citizens and organizations who are not aware of the dangers and who are not security conscious.

Research has been done on the development of expertise in cyber security. Systems are designed to accelerate expertise but the value of these systems needs to be evaluated by cyber professionals (Champion *et al.*, 2014). However, little research has been done to compare the benefit of informal (self-taught) learning to traditional formal education (Champion *et al.*, 2014). To keep up with the ever-growing cyber security demand, the educational roadmap and the development cycle for cyber security professionals need to be understood. This is where the problem lies. There are contradictions within organizations with regard to job requirements which are needed for a cyber security position. One may follow the formal educational and certification route to become a penetration tester. But it might not fully prepare a person for an actual position. Factors contributing to this include aspects such as limitations in the scope of curricula, limited practical experience, or improper practical experience (Champion *et al.*, 2014).

This chapter takes a closer look at the cyber security skills gap and what can be done to try to re-mediate the gap.

4.1.1 Identify the Cyber security skills gap

According to Kampoor (2018), practice head of Cyber security and GRC at In2IT Technologies, South Africa is ranked 3rd out of 117 countries for the most cyber attacked country in the world. The situation is looking grim as the immense cyber security skills shortage is exploited by cyber criminals. Cyber security skills shortage is a global crisis, as it is a South African crisis. As new technology expands, cyber security professionals have to play catch up, while the growth of cyber security skills lag behind and organizations will need all the help they can get (EC-Council, 2019). This results in the shortage of cyber security specialists and widens the gap

as there are not enough skilled people capable of accurately identifying threats and risk as they grow, which means that networks are not protected properly from intrusions (Kampoor, 2018). The EC-Council (2019) reports that there two major reasons for the cyber skills shortage; the lack of required cyber skills and organizations who underinvest in their cyber security solutions. The mistakes made in the past contribute to the giant gap that we have in the cyber skill supply chain today.

According to Lapena (2019), Tripwire reports that according to their research published, in October 2018, there was an worldwide shortage of 2,93 million cyber security professionals. This is an indication that the cyber security skills gap is continuing to worsen. The need for skilled cyber security professionals grows rapidly and the demand for new skills grows as the threat landscape evolves and attack surfaces change. As threats and vulnerabilities grows, industry struggles to find skilled resources to maintain a strong basis of security (EC-Council, 2019; Lapena, 2019).

According to Adrian Schofield (2018), academia and business have to partner and influence governments to have a better understanding of the future skills needed in the cyber security domain, in order to be able to incorporate critical skills development in academia (Schofield, 2018).

In order to close the skills gap, measures have to be put in place to build skills and close the gap. According to the 2018 Joburg Centre for Software Engineering – Institute of Information Technology Professionals South Africa (JCSE-IITPSA)[1] Information Communication Technology (ICT) Skills Survey, there were many private sector initiatives to address the skills gap due to the failure of the education departments to do so. Although programmes were introduced to close the gap, the focus was once again on the theoretical skill and not the practical experience to align with industry's requirements. As commented by Moira de Roche (a director of IITPSA) "One can't just churn out experts, instead they need some specialist skills which are only built by experience of about five to eight years" (Schofield, 2018).

According to the Career Junction Index Executive Summary for January 2019, the number one job with the highest demand in South Africa is Information Technology followed by Finance (Career Junction, 2019).

Career Junction statistics were compared and depicted in Figure 4.1, on vacancy levels across various sectors. The indication of demand (the blue bar on the graph) portrays where the majority of employment takes place. The indication of supply (the orange bar on the graph) portrays what positions active job seekers look for (Career Junction, 2019).

[1]https://cj-marketing.s3.amazonaws.com/CJI_Executive_Summary.pdf

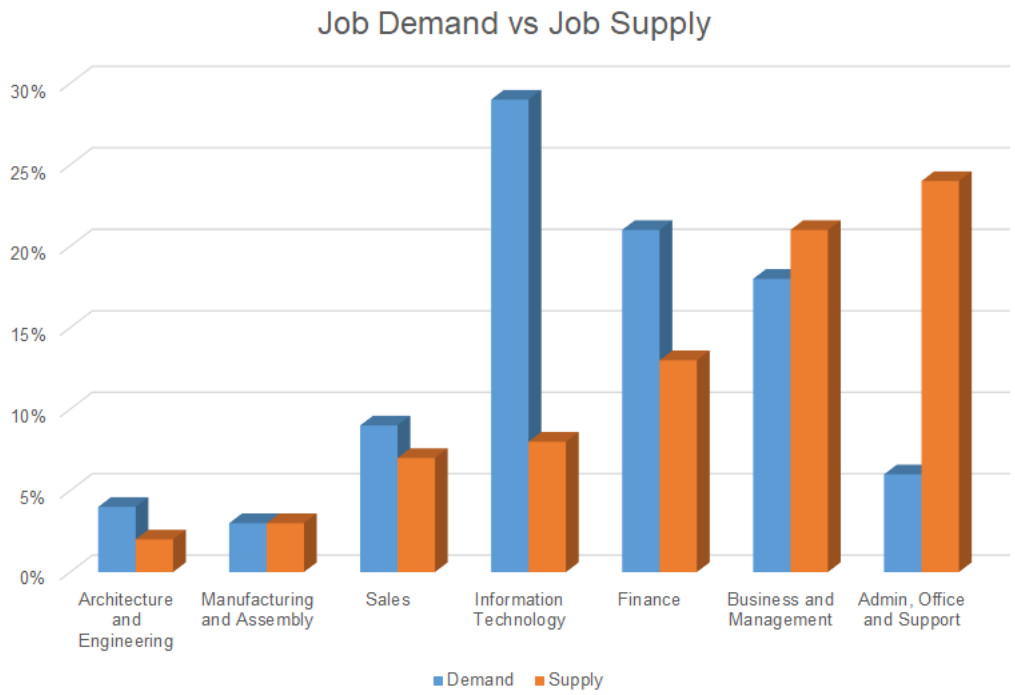

Figure 4.1: Job demand vs. job supply (Career Junction, 2019).

According to Career Junction Index Executive Summary January 2019, (Career Junction, 2019), the information system sector has a job demand of almost 30% whereas the supply only indicates 9%, as indicated in the graph in Figure 4.1. The rapid change in digital transformation caused a growth in the use of cloud and web applications and services, which in turn has created an increase in the demand for more IT professionals and in this instance skilled cyber professionals (EC-Council, 2019).

According to the Media, Information and Communication Technologies Sector Education and Training Authority (MICT SETA) ICT security specialist is one of the top ten "hard to fill" vacancies in the MICT sector. Statistics indicate that there was an increased demand for employees to be multi-skilled. This shows that the employment opportunities are for highly skilled professionals (SETA, 2017).

The cyber security skills gap is a great concern. To close the gap will not be an easy task as the process in becoming a skilled cyber security professional takes time. Becoming a knowledgeable cyber security expert takes time to build knowledge in (Kampoor, 2018):

- Technologies and systems
- Understand how technologies and systems integrate
- Spend time in classrooms
- Theoretical knowledge

- Practical knowledge

The profile of a cyber security expert is rather different from the normal IT professional. Firstly, the person must have the right mind set, something between the thirst for knowledge of security threats and the distinct knowledge of how a cyber criminal thinks. This ensures that the cyber expert not only understands how to protect a network, but also knows what to protect the network from. This is the link between theoretical knowledge and skills built in the class room and the practical knowledge and skills acquired in the real environment.

The challenge for business and recruiting companies is to find individuals who possess the full package:

- Proper cyber security certifications and qualifications,
- Experience within multiple environments,
- The security-centric mind set (Silensec, 2017; SETA, 2017).

To close the security skills gap, the problem has to be defined clearly to identify the challenges to overcome to fill the gap (Silensec, 2017).

To determine the cyber security skills gap accurately, the size of the problem needs to be identified. The ongoing cyber security skills shortage has been studied and reports published to determine the core of the skills shortage. One of the organizations conducting these studies is the international professional organization, ISACA. ISACA has published a yearly Global Cyber Security Status report, from 2015, providing information on cyber security threats and skills gaps. The main factors in the two most current reports, 2017 and 2018, influencing the cyber security skills gap are as follow:

1. Organizations find it difficult to find skilled individuals for cyber security job advertisements. For an open position an organization may receive more than 10 applicants, but fewer than half of the applicants are qualified. Even after a skilled individual is placed, that individual still needs time and training before functioning at the required skill level. The time spent in finding the appropriate candidate to fill a position widens the skill gap and sometimes the position stays open. (ISACA, 2017, 2018)

2. The expansion of the cyber security budget is growing slowly. Organizations start realizing that cyber security is an important factor in the organization and is seen as an investment. With the increasing of funding levels, organizations will start with investment in skills development (e.g., training) and talent retention may increase. (ISACA, 2017, 2018)

3. Gender disparity is an emerging factor contributing to the cyber security skills gap but it can be mitigated. (ISACA, 2017, 2018)

4. Organizations are concerned that, although skilled professionals are placed in open positions, it will still be difficult to mitigate the threat. Some organizations would rather hire skilled professionals for a limited time than fill positions.

5. With skills come qualifications, practical experience and work experience. It is said that the biggest skills gap in today's cyber security professionals is the ability to understand business, technical skills and communication skills. (ISACA, 2017, 2018)

When considering the above-mentioned factors influencing the cyber security skills gap, it is predicted that there will be at least one point five million vacant cyber security jobs by 2019 (Silensec, 2017).

4.1.2 University Qualifications

According to Rowe *et al.* (2011), the rapid continuous growth of cyber threats puts a big responsibility on academic institutions to graduate skilled students in the concepts and technologies of cyber security. (The role of cyber security in Information Technology education). Because of the growing shortage of qualified cyber security professionals in the public sector, it is proposed that academic institutions add wider research emphasis in cyber security focus on advanced topics which should add value to existing IT programs. Cyber security needs to be implemented throughout IT programs. If it is not part of IT curricula students are educated that security is not necessary during development and production which will lead to massive security vulnerabilities. Cyber security should have its own advanced curriculum as an undergraduate qualification.

Rowe *et al.* (2011), refer to five pillars which are all critical prerequisites for cyber security. The five pillars they refer to are; networks, human computer interaction, data bases, programming and web systems. As key knowledge areas, these five pillars provide a student with the important key knowledge cornerstones as a prerequisite for cyber security education. Education methods go hand in hand with building the cyber security skills gained by a student in preparation to enter the work force. These critical methods are hands on exposure, collaboration with experts, industry and job shadowing and lastly case studies (Rowe *et al.*, 2011).

Universities have started developing new specialized degrees specially in cyber security and information security. Looking at degrees it is mostly post graduate

studies such as Master's degrees. To accommodate basic level cyber security qualifications, some universities developed learning opportunities such as a certificate or diploma in cyber security. According to Porup: "Cyber security training will continue to mature, and international certificates alone will no longer be enough to take the next step in a security professionals career." Porup continues saying that cyber security master's degrees are popping up all over, including at prestigious universities, and more and more companies will be looking to hire Chief Security Officers (CSO's) and Chief Information Security Officers (CISO's) with the cross-disciplinary skills acquired from a master's degree.

4.1.3 International Qualifications

International qualifications and certifications pose a big gap in the cyber security job market. The ratio of certification holders versus openings requiring certifications are relatively low, the reason being that after passing the certification exam, certifications such as CISSP, CISM and CISA require that professional experience is needed to attain the certification (Silensec, 2017).

4.1.4 Informal Education

Informal education or self-taught skills are an area that is not recognized or not looked at in the employment process. A big aspect in the skills gap might be closed when analyzed closely. During informal education the emphasis is not that much on the theory of the subject but more on the practical side of the subject. As seen in my research, one of the biggest areas in the skills gap is practical experience (Champion *et al.*, 2014).

4.1.5 Cyber skills gap alignment to Industry needs

In the process of recruiting specifically only security expertise the process is loaded with other challenges. Large organizations have the means to budget more efficiently to hire cyber security professionals than smaller firms. But the smaller firms are not only easy targets, but they also provide passage to gain access to the digital space of larger organizations (EC-Council, 2019).

After analyzing the job requirements from recruitment agencies globally, it was evident that most cyber security jobs required a bachelor degree in computer science, engineering, programming or preferably in information system security. Experience is a main requirement in cyber security; a candidate may possess the necessary qualifications but lack experience which hampers the appointment in a specific position (Silensec, 2017).

Job advertisements from all over the world were analyzed to look at the education and skills needed for penetration testing and vulnerability testing. Web sites used for job searches on penetration testers and vulnerability testers are shown in Table 4.1. South African and International job advertisements were used during research to compare the requirements needed in a global perspective. It were found that requirements in South Africa and internationally is the same, thus only South African advertisements were used.

Table 4.1: Websites used for job searches.

www.cybersecurityjobs.net
www.google.com
www.monster.com
www.careers24.com
www.careerjunction.co.za
www.indeed.com

During the analysis of open positions at different organizations, a deduction was made that most advertisements for cyber specialists are very generic and do not focus on a specific skill. Although some specific skills are mentioned, it is evedent that in the requirement description in the adverticements, more skills are needed than listed. A total of 11 advertisements were analyzed from the websites as mentioned in Table 4.1. These adverticements were specifically targeted for a penetration tester and were for the international job market as documented in the matrix in Figure 4.2. The job advertisements are attached as Appendix A. A Cyber Penetration Tester Matrix was compiled on the 11 positions and shown in Figure 4.2. During the analysis it was found that the job advertisements were basically similar with differences in the years of experience, formal education (degree's) and international certifications as prefered by the organisation. The advertisements have four categories, indicating the skills and education needed for the job. The categories are as follow.

- Requirements. A requirement is a quality or a performance demanded of an individual or group in accordance with certain fixed regulations: in this case the requirements for a specific job function (McKean, 1995).

- Required Skills. Are the ability and competency developed through considered, logical, and continuous efforts to easily and adaptively carry out difficult activities or job functions involving ideas (cognitive skills), things (technical skills), and/or people (interpersonal skills) (McKean, 1995).

- Nice-to-have skills. There are additional skills to have to build the competency and ability level and are an addition to required skills

- Responsibilities. A thing which one is required to do as part of a job, role, or legal obligation (McKean, 1995).

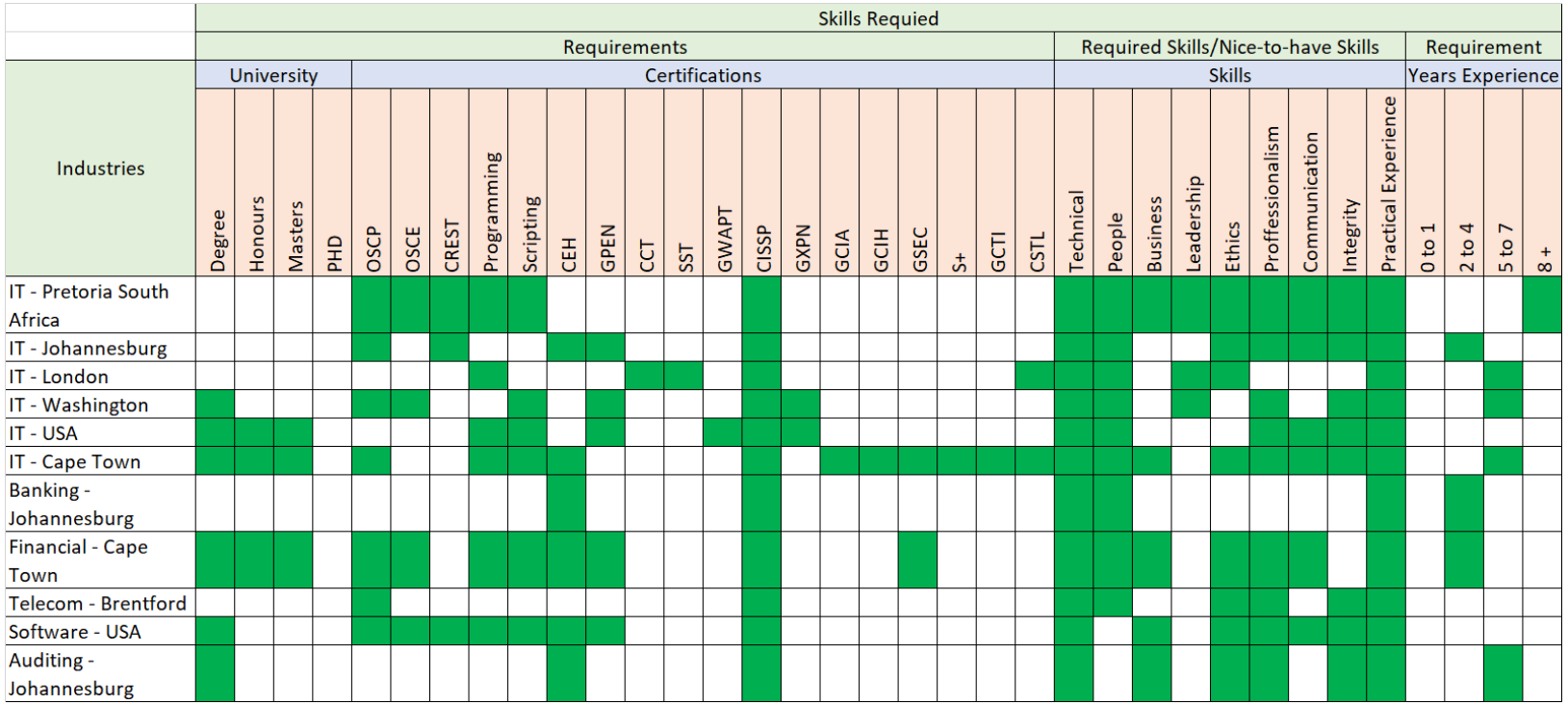

Figure 4.2: Job Requirement Matrix.

During the analyzing of the advertised jobs, it is evident that a person who wants to apply for a job in the penetration testing environment needs work experience in the field for at least two years for junior positions and five plus year for medium and senior level positions. This has an influence in the skills gap and shortage of professionals in the cyber security and information security. Not one of the advertised jobs mentioned self-taught skills or informal training.

4.2 Proposed solution

While analyzing the skills needed for specific positions in the cyber environment, specific skills are required for an individual to be a successful applicant. When screening a person for a position in the cyber environment there are specific aspects to rate a person against. In the proposed solution three phases are identified. These phases are, the Human Resource selection as required by the employer which will be addressed by as qualification, test and evaluation, and thirdly, validation.

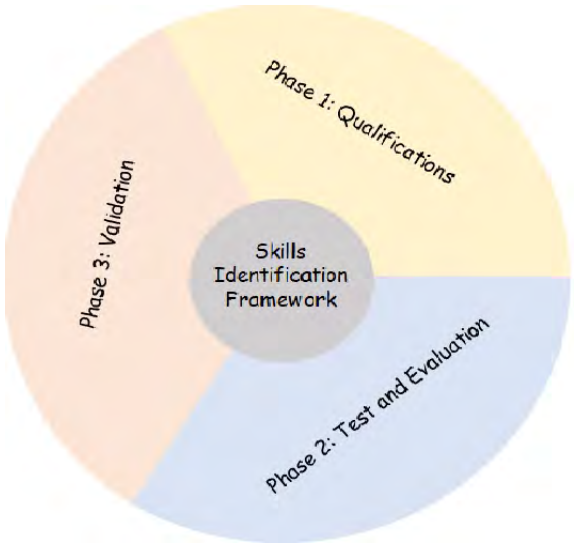

Figure 4.3: Phases to identify skills.

To be able to make a sound selection or evaluation on how a candidate might be suitable for a specific position in a company according to skills, it would only make sense to work according to a specific framework. The framework developed will fit into the three phases mentioned above.

Positions at eleven different companies were analyzed as an example. These advertisements are attached as Appendix A, and a matrix combining the skills needed for the positions as in Figure 4.2. The requirements for the analysed position are summarized in Table 4.2.

Table 4.2: Information Security Specialist Requirements.

Mission/ Core purpose of the Job	Cyber Penetration Tester.
	Simulate cyber attacks to check for exploitable vulnerabilities.
	Do tests to breach application systems (e.g. Front/back-end servers, application protocol interfaces (APIs))to uncover vulnerabilities.
	Reporting.
Requirements	Two+ years of Ethical Hacking experience.
	Relevant certifications (OSCP, CASS, CEPT, CPT, CCTHP, CRTOP, CISSP, CCEH, GPEN, OSCE).
	Strong technical background and knowledge.
	Exposure to red team testing.
	Exposure to threat hunting.
	Exposure to identifying and exploiting attack paths to critical assets.
	Exposure to cyber attack frameworks (MITRE, Cyber Kill Chain) Technologies.
Required	Knowledge of C++, C, C#, Python, Scripting.
	Good coding ability.
	Technical Cyber attack frameworks.
Nice to Haves	Knowledge of CBEST, CREST and TIBER
	Banking experience
	Technical IT qualification at Bachelors/Masters Level
	Hobbies - hacking things
Responsibilities	Reverse engineering, coding, finding bugs in software/hardware.
	Help establish a red team in the bank.
	Ethical person.
	Have theoretical knowledge of hacking.
	Have practical experience in hacking.
	Deep technical understanding in Linux and Windows operating systems.

4.2.1 Scoring methodology.

The scoring methodology used during the 3 phases of recruiting for an specific position, will be based on the Key Performance Indicator (KPI) method. The KPI

methodology were used as an guideline and adapted for scoring for an specific instance (Gabcanova, 2012; Parmenter, 2015). The scores used in this research is generically allocated as this solution can be used as a recruiting tool in all industries. The scores will vary from a low score of 1 which indicate that the KPI was not met, a score of 3 which will indicate that the KPI is met, and a score up to 5 which indicate that a candidate has met the KPI with skills higher than needed according to the skills prescribed by the organization. Scores will be indicated during the 3 phases.

4.2.2 Phase 1 - Qualifications and skills.

During the Human Resource Selection there are certain qualifications that the applicant has to adhere to. These qualifications include formal university degrees, international qualifications and years of experience. The qualifications and skills framework will be used as depicted in Figure 4.4.

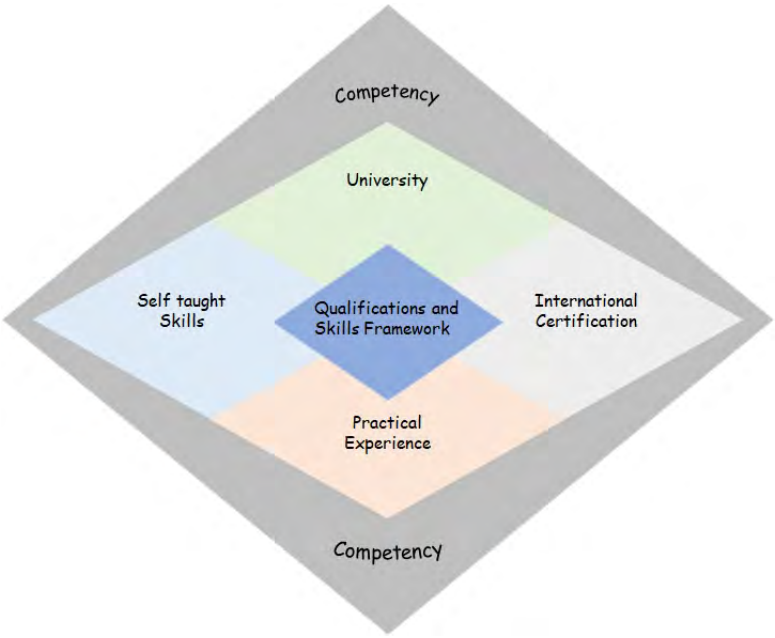

Figure 4.4: Qualifications and Skills Framework.

In order to measure competency, there are two essential items to consider, namely skills and qualifications. Ability and desire are used to measure skills, and personal knowledge is used to measure qualifications (Conklin *et al.*, 2014). For an organization to effectively execute business functions and reach its objectives the desired competency is required which is a combination of the right knowledge, ability and desire.

Knowledge is gained through study and experience, the understanding of information (Conklin *et al.*, 2014). This is the understanding, memorization and the

ability to grasp the theoretical facts of a subject. A subject knowledgeable person, is a person who may be able to describe a subject related concept clearly and in detail, even if there is no practical experience or exposure to that specific subject (Skills Base, 2016).

Self-taught skills or informal training on the other hand will contribute extensively to the practical skills of an individual. The individual might not have the necessary theoretical knowledge but has extensive exposure to the practical knowledge of a subject.

According to the Oxford Dictionary, "an ability is a measure of how well a person is able to carry out or perform a given skill. It is a measure of proficiency, talent, and the practical application of a skill within a reasonable amount of time and with a reasonable amount of energy."

To measure desire a person's interest in a given skill is evaluated. This is the interest of a person to perform, develop and maintain a skill (Skills Base, 2016). Desire enhances both ability and knowledge. A person must have a genuine desire to perform at a high level, and continually develop, manage and maintain skills.

A candidate will be rated against an scoring system. Scores will be allocated to qualifications obtained by the candidate. The candidate will be rated and compared with an ideal score to be able to determine the candidate's competency level.

Scoring will be done in levels as shown in Table 4.4.

Table 4.4: Scoring Levels.

University Degree	No Degree	1	International Certification	No Certification	1
	Degree	2		Level1 Certification	2
	Honours	3		Level 2 Certification	3
	Masters	4		Level 3 Certification	4
	PHD	5			
Self-Taught Skills	None	1	Years Experience	None	1
	1 to 2 Years	2		1 to 2 Years	2
	3 to 4 Years	3		3 to 4 Years	3
	5+ Years	4		5 to 7 Years	4
				8+ Years	5

Scores will be allocated in categories of very low, low, medium, high and very high. Scores allocated are classified as very low equal to one, low equal to two, medium equal to three, high equal to four and very high equal to five. Scores between the main scoring allocated will be allowed. These scores will be allocated if a candidate does not have a B-Degree, then the score will be 1 or if the candidate is busy with a B-Degree then the score of 1,5 will be given. If the candidate has a B-Degree and is busy with an Honours degree then a score of 2,5 will be allocated. The same will apply for a score between 3 and 4, and, 4 and 5. The scores will be

indicated on a bar graph compared with the ideal score from the Human Resource Section.

Scoring of qualifications will be done as follow:
Formal University Degree (Deg)

- Very Low (1) - No Degree.
- Low (2) - B-Degree.
- Medium (3) - Honours Degree.
- High (4) - Master's Degree
- Very High (5) - PHD.

International Certification (IC)

- Very Low (1) - No Certification.
- Low (2) - A+/N+/S+/Linux+/CIPP/CISA/CISSP/CISM.
- Medium (3) - CS Analyst/ CS Consultant/Pen Tester/ CEH/ CISSP.
- High (4) - CS Manager/ CS Engineer/ CS Architect.

Self-taught skills

- Very Low (1) - No self-taught skills.
- Low (2) - 1 to 2 years.
- Medium (3) - 3 to 4 years.
- High (4) - 5+ years.

Year's experience (YE)

- Very Low (1) - No experience.
- Low (2) - 1 to 2 years.
- Medium (3) - 3 to 4 years.
- High (4) - 5 to 7 years.
- Very high (5) - 8+ years.

Scoring will be applied as follow.

1. Very Low (1) - There are no qualifications in the specific area.

2. Low (2) - Means that candidate does not have the required qualifications or has only some of the required qualifications.

3. Medium (3) - Means that the candidate has all the required qualifications.

4. High (4) - Means that the candidate has more than the required qualifications.

5. Very high (5) - Means that the candidate's qualifications are higher than expected.

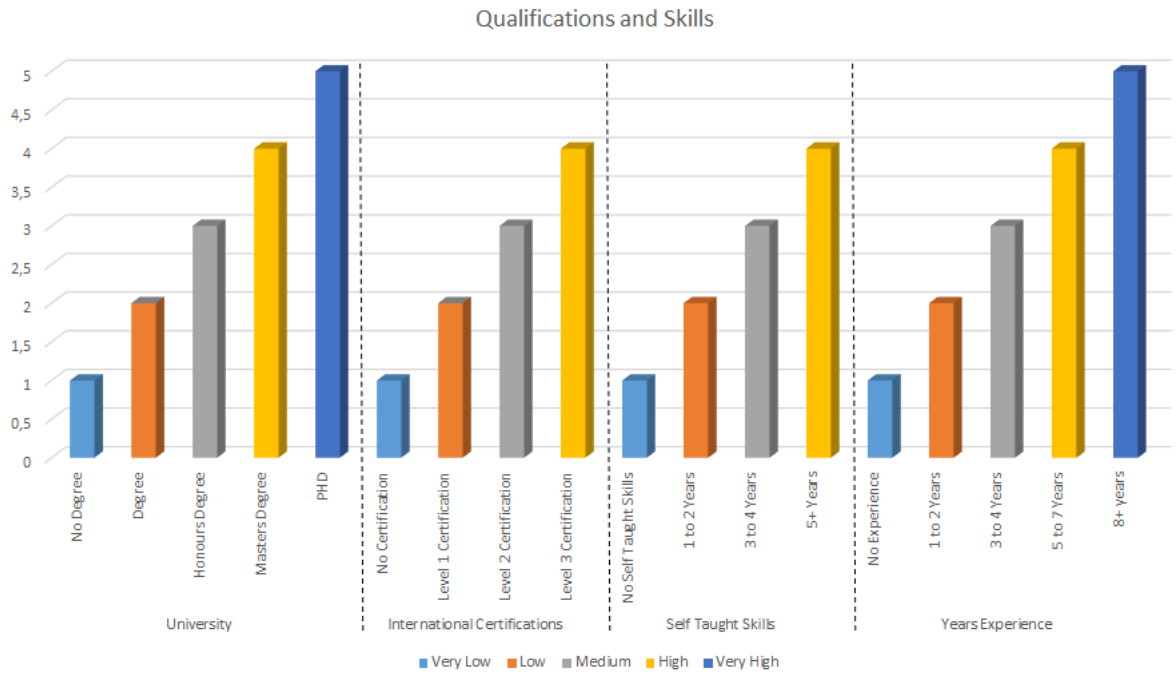

Figure 4.5: Qualification and Skills Matrix

.

After completion of the scoring for phase one, a value has to be allocated. This value will be used in the final sore of all three phases to be able to determine the over all tested skills and competency. A simple addition mathematical equation for skills is applied and looks as follow:

- University qualification + International Certification + Self Taught Skills + Years Experience = Skills.

- 2+3+1+2= 8

- The total of 8 will be transferred to the final score calculation at the end of phase 3.

4.2.3 Phase 2 - Test and Evaluation.

Phase 2 will consist of testing and evaluation. Testing and evaluation may consist of a questionnaire given to the applicant and short practical problem-solving scenarios. Tests and evaluations will be done to determine the competency level of an individual. The required competencies would be measured and not limited by using the competency framework as illustrated in Figure 4.6. The purpose of the competency framework is to understand people's behaviors in the working environment to be able to succeed in working roles and in certain environments (Bartram, 2006). The specific competency skills are adapted in the specific working environment for an individual to be successful (Petersen *et al.*, 2020). Due to the cyber security environment, especially penetration testing, being an specialist environment an individual need to be competent or have skills in all areas in an company, thus the competency framework in figure 4.6 below (Bartram, 2006; Petersen *et al.*, 2020).

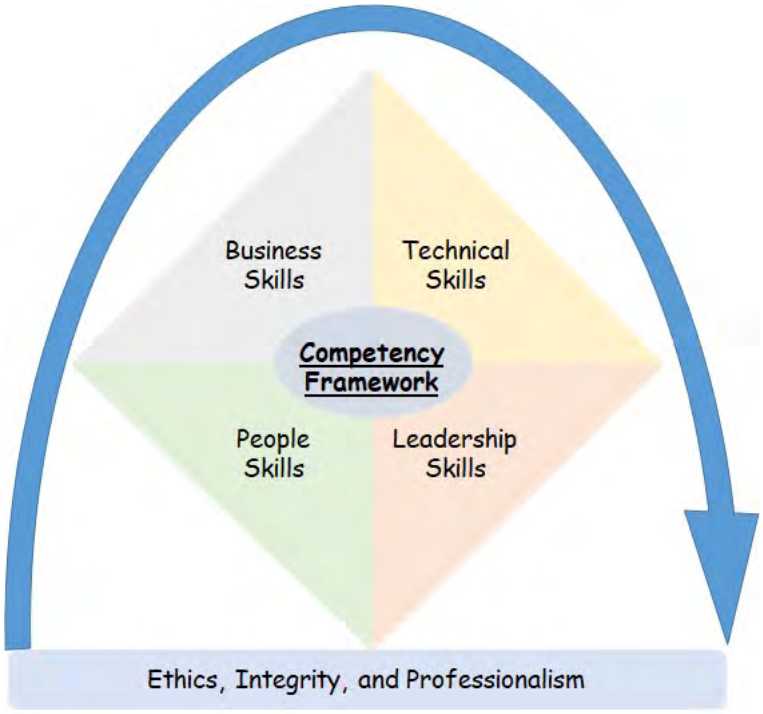

Figure 4.6: Competency Framework.

During this phase the applicant's IT technical skill and knowledge, leadership skills and knowledge, people skills and knowledge and business skills and knowledge are rated against a score. The applicant's ethics, integrity and professionalism will be tested as an overarching factor over the other mentioned skills. The Human Resource manager will have an ideal score which the candidate will be rated against.

The same scoring principal as in phase 1 will be use in phase two. The areas to be tested and evaluated are as indicated in Table 4.5.

Table 4.5: Test and evaluation.

Test and Evaluation	Technical Skills
	Leadership Skills
	People Skills
	Business Skills
	Ethics
	Integrity
	Professionalism

All the skill areas will be tested by means of a questionnaire or a scenario. This process will test the candidate's theoretical knowledge and problem-solving skills. The outcome of the test will be scored on the same principle as in phase 1, and the outcome is shown in Figure 4.7.

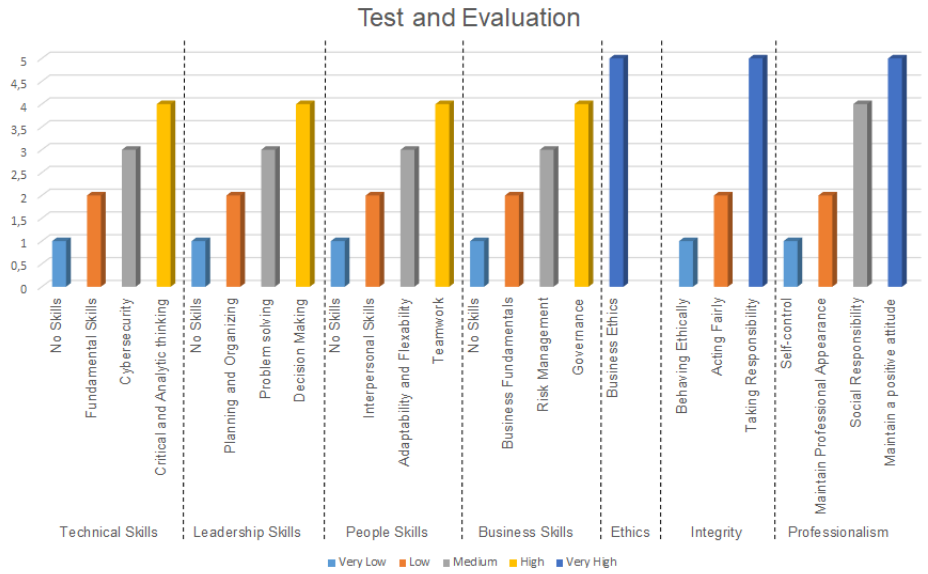

Figure 4.7: Phase 2 Test and Evaluation

After completion of the scoring for phase two, a value has to be allocated. This value will be used in the final score of all three phases to be able to determine the overall tested skills and competency. A simple addition mathematical equation for test and evaluation is applied and looks as follow:

- Technical Skills + Leadership Skills + People Skills + Business Skills + Ethics + Integrity + Professionalism = Competency
- 10+10+10+10+5+8+12=65
- The total of 65 will be used in the final bar chart to indicate the competency level.

4.2.4 Phase 3 - Validation

Phase 3 will be the final validation to confirm the candidate's knowledge and ability for a position. The Validation Framework will be used to validate skills.

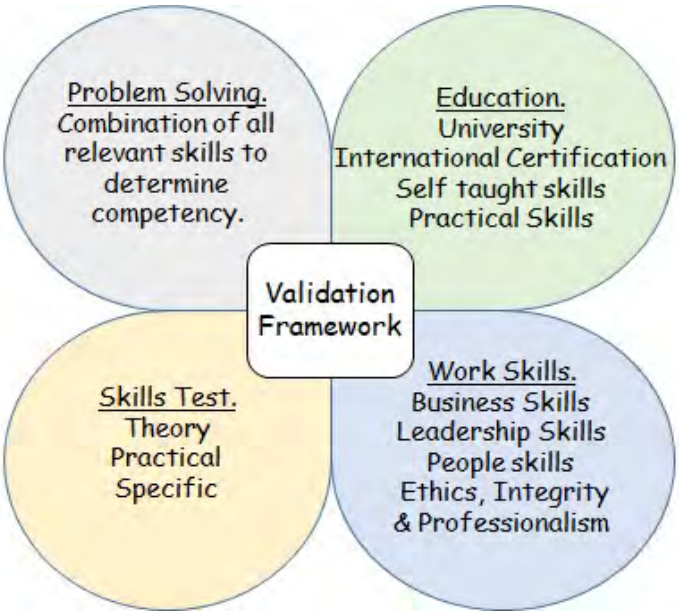

Figure 4.8: Validation Framework.

Validation will be focused on practical knowledge and work experience. All the areas as shown in the validation framework will be covered during this phase. It will be scenario-based problem solving and feedback in the form of presentation. A final score will be given to the candidate on the result of the ability to solve problems and the outcome of the result of the scenario to be solved. During this process the reading, writing and communication skills will also be tested. Reading will be tested in the ability to read what is expected, and to understand the tasks and outcome. Writing will be tested on the written product that has to be produced, either

document or presentation. Communication will be tested during the presentation and feedback to be given according to the scenario. Figure 4.9 shows the score card for Validation.

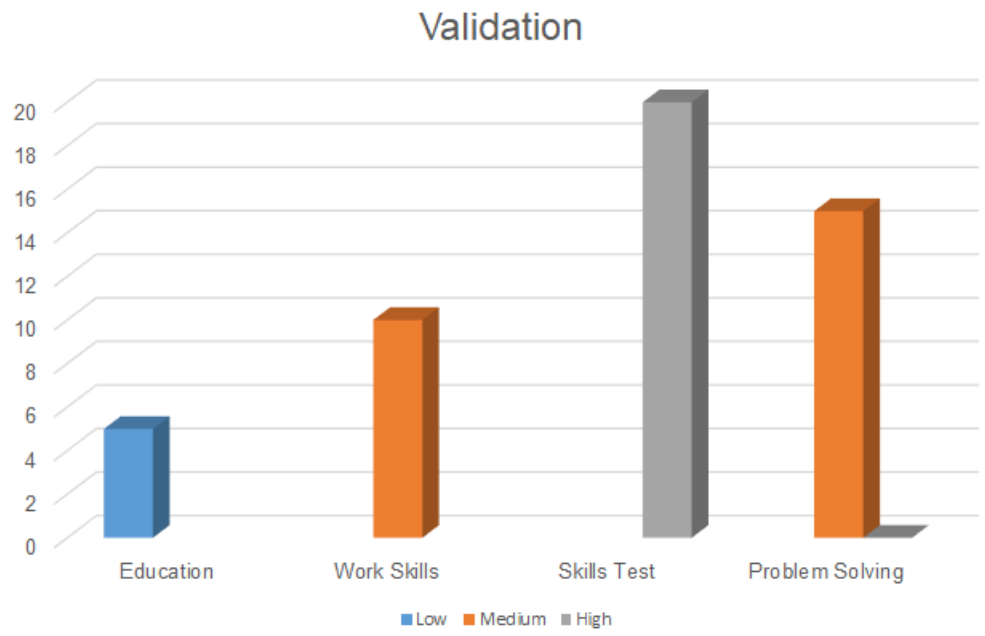

Figure 4.9: Phase 3 Validation.

After completion of the scoring for phase three, a value has to be allocated. This value will be used in the final sore of all three phases to be able to determine the overall tested skills and competency. A simple addition mathematical equation for the validation phase is applied and looks as follows:

- Education + Work Skills + Skills Test + Problem Solving = Validation
- 5+10+20+15=50
- The total of 50 will be used in the final bar chart to indicate the competency level.

To bring all the scores from phase one, two and three into perspective, the outcome from the three phases will be consolidated into one bar graph to give the final picture on the competency level of an individual. The consolidation of the three phases is shown in Figure 4.10.

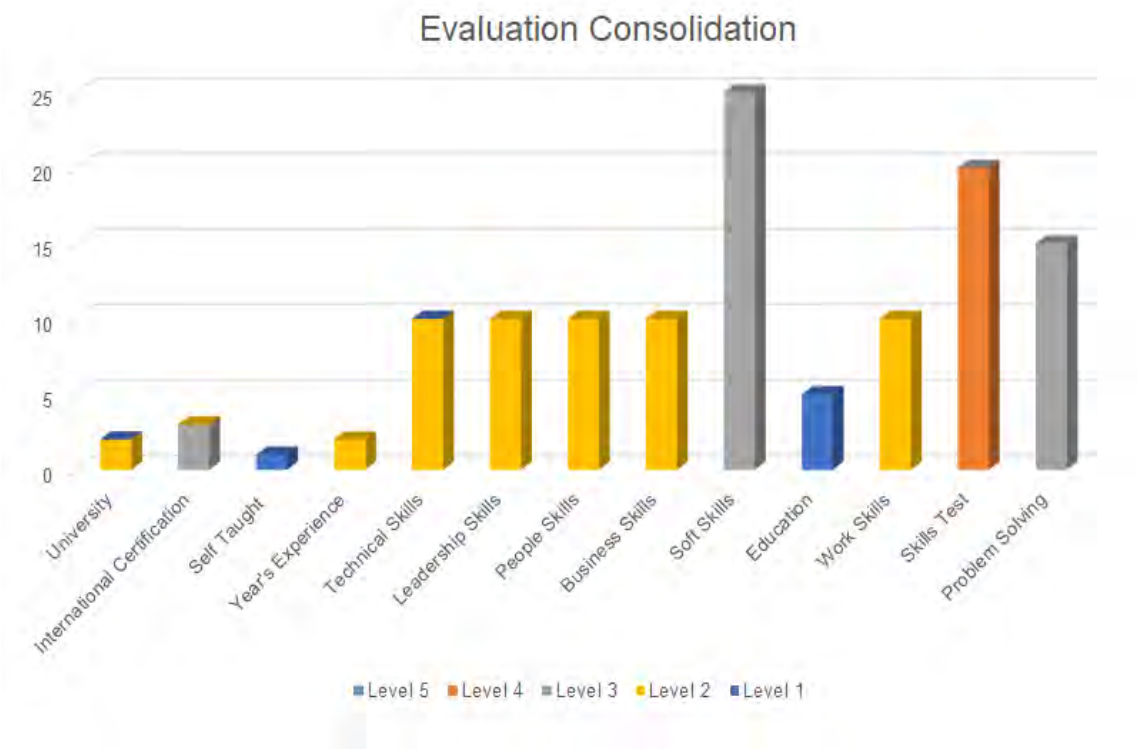

Figure 4.10: Evaluation Consolidation

In phase one it was mentioned that rating of skills will be done against an ideal score. During the finalization of each phase a value was given by means of a mathematical equation. The total score of each phase will now be compared with the predetermined overall ideal scores. This will give an indication on which level the individual is and a deduction can now be made if the person is the right one to consider for employment.

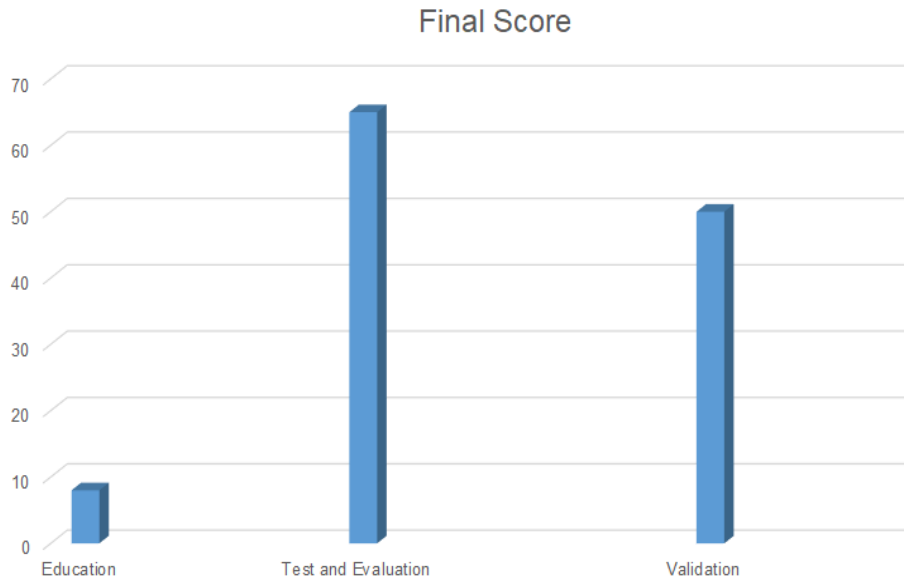

Figure 4.11: Final Score

4.3 Summary

Chapter 4 give a analysis presented on the available tertiary education available for cyber professionals, with a particular focus on penetration testers. Section 4.1 include an introduction to the concerns with regard to the cyber skills gap in industry. The cyber skills gap was identified by analyzing the value of university degrees, international certifications and practical skills as prescribed in job advertisements. An educational roadmap on penetration testing skills was proposed and aligned with what industry needs as advertised in job advertisements in real life, in Section 4.1. In Section 4.2 a possible solution was proposed to help industry to successfully appoint cyber professionals. Thereafter Chapter 4 concludes with a summary in Section 4.3.

In Chapter 5 an analysis will be done on identifying possible ways to close the cyber skills gap. Section 5.2 will explain the penetration testing framework versus cyber security skills and Section 5.3 will look into an approach to close the cyber skills gap where after Chapter 5 will be concluded with an summary.

5

Cyber Security Skills Gap

In Chapter 4 the cyber security skills gap was analyzed by using a scoring technique to get to a solution. In Chapter 5 the penetration testing framework will be aligned with the skills needed by industry to determine a possible method to close the skills gap in industry.

In Chapter 3 a penetration testing framework was suggested. According to this framework a penetration tester needs certain skills as indicated by the Lockheed Martin Cyber Kill Chain and the International Standards analyzed. These skills include Reconnaissance, Target Evaluation, Exploitation, Privilege Escalation, Maintaining a Foothold and Reporting. In Chapter 4 education and skills were analyzed to be able to determine a person's skills and competency level. The cyber skills gap needs to be closed. To close this skills gap, the skills needed by industry need to be aligned with the skills built at training institutions, experience and self-taught skills.

According to the Lockheed Martin Cyber Kill Chain, there are seven steps to adhere to for the penetration testing cycle to be successful (Lockheed Martin Corporation, 2015). If one of the steps is left out and not completed the cycle will not be completed.

When analyzing the skills wanted by industry it is clear that a wide range of knowledge and expertise is needed when searching for someone to fill an position in an organization. Although positions for a penetration tester are advertised, the core purpose and experience of the position do not only prescribe the skills

for penetration testing. The requirement by industry is much higher. During the research it was found that one needs a wide range of skills and experience to be truly recognized in the cyber security community.

5.1 An approach to identifying the cyber skills gap

Skills levels associated with cyber security personnel appear to be far more advanced than those of regular IT operations. Due to the risk related with cyber security operations, the complexity of determining the skills requirements increases (Conklin *et al.*, 2014). Cyber security professionals have access to critical data and systems, therefore recruitment in respect of skills and abilities require greater scrutiny. Cyber security skills go further than degrees, certifications, prior experience and practical experience, and companies have an old style entitlement interpretation for qualifying as a security professional. It is now required for industry to change their original hiring processes by changing their view on their criteria when qualifying a cyber security professional (EC-Council, 2019).

Outlining cyber skills is challenging. This is due to the constant technology changes in the digital revolution, and, traditionally cyber security has a huge cost coupled to it and has to take the back seat until it is too late.

A cyber security specialist needs a deep understanding of the technology and security principles, and when fitted into an organizational structure, there is a need for the so-called soft skills which include business, people, leadership skills and professionalism (EC-Council, 2019). That is why it is a multi-year plan to grow a cyber security capability from ground level. To build the required knowledge, abilities and skills takes years of experience to develop; thereafter complex security tasks can be performed.

According to Roy (2019), during studies conducted by the Information Systems Security Association (ISSA) and analyst firm Enterprise Strategy Group (ESG), it was found that there are key indicators for the worsening cyber security skills shortage which include, existing staff being overworked, the lack of knowledge and skills to learn and use security technologies effectively, hiring and training junior employees and limited time to work with business units. The cyber security skills shortage affects the cloud security, application security and security investigations and analysis, which includes penetration testing areas, the most (Roy, 2019). Figure 5.1 depicts a high level classification of the cyber skill levels (SANS, 2018). Figure 5.1 give an suggested road map to be followed by someone who want to specialize in the cyber security as an career. The road map starts at the basic level to an intermediate level and end at the advance level. Figure 5.1 indicate the high level specialist areas one can pursue up to an advanced level.

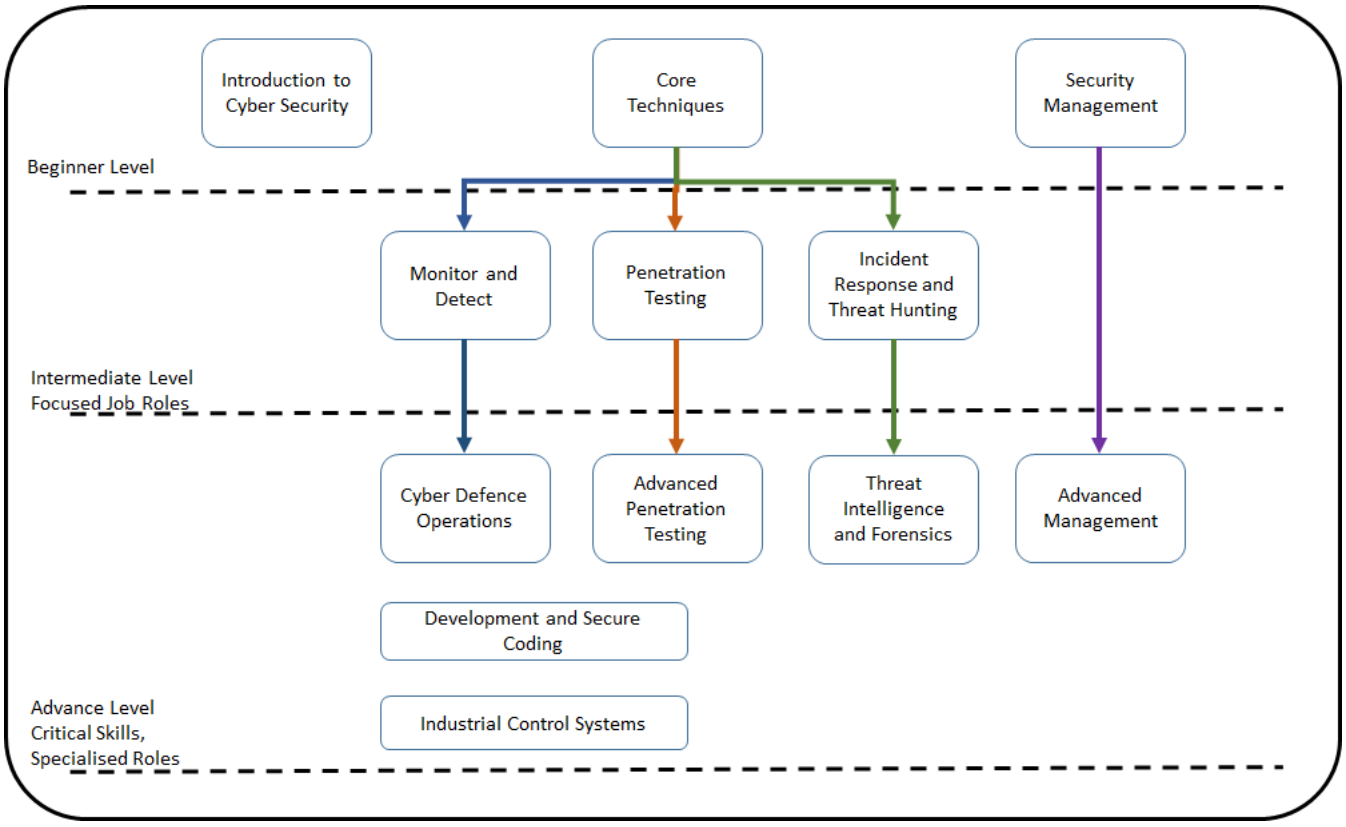

Figure 5.1: Cyber skills level classification (SANS, 2018).

Organizations put too much weight on certifications and do not really know what cyber security skills they need; they need to map requirements back to a framework to identify their needs (Roy, 2019).

As in all other professions, there are different levels of knowledge and skills needed. In some instances, a lower level of knowledge and skills is needed, while others need more advanced levels of skills. One person might have a wide field of knowledge but will never be able to cover the whole cyber security spectrum. Due to this, education needs to be aligned properly with the industry needs.

According to Conklin *et al.* (2014), "One of the biggest current gaps in alignment between education and industry is a complaint that graduates do not have sufficient hands-on skill sets to make them ready to perform jobs. Highly noted in the recent DHS Cyber Skills Report, one proposed remedy is the tightening up of criteria associated with NSA/DHS certifications, so that programs will respond with more hands-on content."

Hands-on experience was identified as a long-standing criticism of many higher education programs. It can be due to training versus education. Training is focused on the how and focuses on current technology and methods, while education focuses on the why, the theory and the mechanisms behind the material (Furnell *et al.*, 2017). Industry is in need of candidates who are able to walk into a position and

know how to perform certain tasks based on their knowledge and practical skills on how to apply their knowledge. It is important to learn the theory (the why), and have the skill to implement the theory on current equipment (the how). Figure 5.1 illustrates the relationship of training to education.

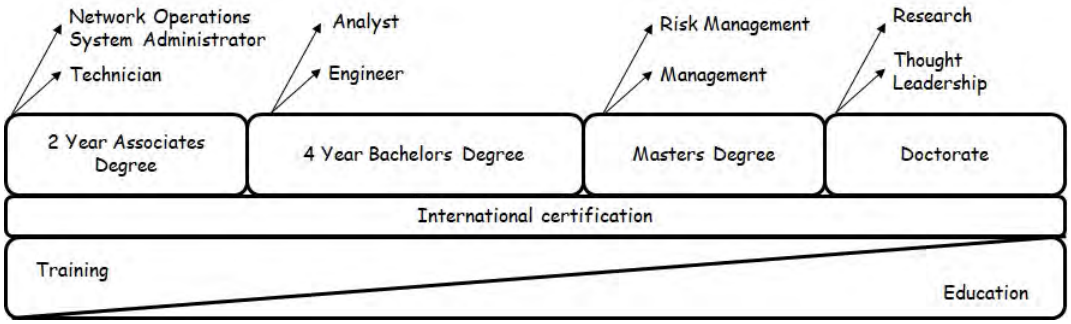

Figure 5.2: Relationship of training to education (Conklin *et al.*, 2014; Furnell *et al.*, 2017).

Figure 5.2 illustrates a roadmap from a national certificate or diploma up to doctoral programs in information and cyber security. Aligned with university studies, international certifications are indicated in different levels from basic to advanced certifications. Several programs are presented at universities and international certifications to provide cyber security workers to industry. The importance behind these different programs is to provide a wide range of cyber security skill sets to industry (Conklin *et al.*, 2014).

This ensures that education provides what industry needs and gives students some opportunities at the end of their education, and in return supports student success. The main gap in education is still, hands-on experience, as education is typically grounded in theory.

5.2 Penetration testing framework and cyber security skills combined

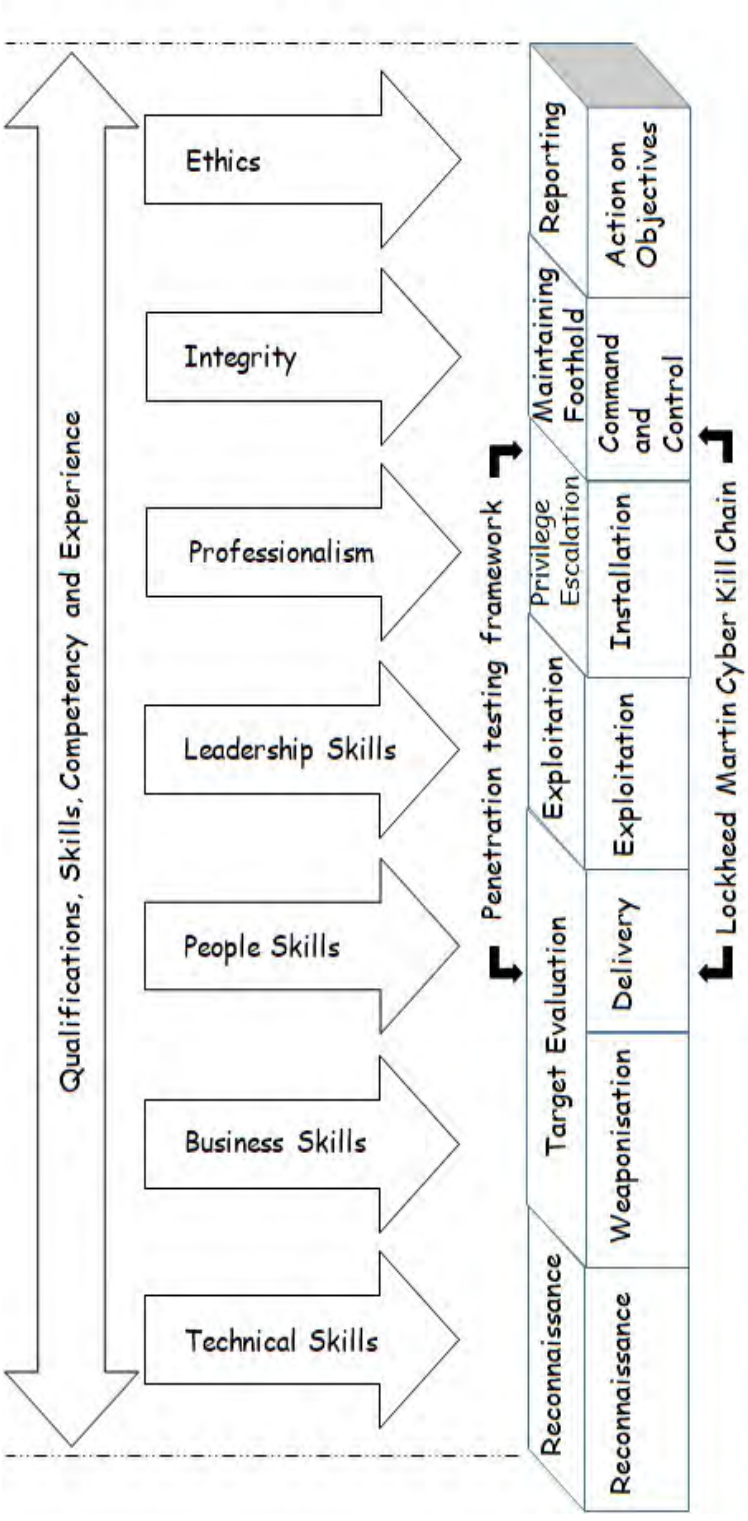

Figure 5.3: Penetration Testing Framework versus Cyber Competency

Figure 5.3 is an integration of the penetration testing framework which is aligned with the Lockheed Martin Cyber Kill Chain and the skills needed to be able to execute the steps in the framework. As seen in Figure 5.3, it is not only information technology and cyber security skills which are needed for an position in industry but a whole range of work experience in different areas in business. It does not matter the level of the position in an organization, an individual needs some knowledge in all areas depicted in Figure 5.3, which include the proposed penetration testing framework combined with the identified skills needed in the environment.

Qualifications, skills and experience are needed to build the required competency level. In this instance technical skills are the most important of all. It is important to know that you need to have holistic insight with regard to information technology to be successful in cyber security, in this instance penetration testing. Theoretical knowledge is vital in cyber security but practical experience plays just as vital a role in being able to implement theoretical skills. Sometimes things work a bit different in practice than in theory. Technical skills are needed throughout all the steps of the penetration testing framework.

Business skills are needed to understand the working of the organization. Things such as business continuity plans, disaster recovery plans, intrusion detection and prevention plans, IT and cyber security policy, need to be understood to do successful tests. Business skills are needed in the reconnaissance, target evaluation and reporting steps. Business skills include business intelligence. Business intelligence consists of a sound understanding of business operations, an interest in knowing business processes, an ability to understand information communication systems used by any organization, and the ability to stay abreast and be aware of changing business technologies and to deal with rapidly growing business threats.

People skills are needed right throughout the penetration testing process. Effective communication skills are needed when working in a team or when communicating with an organizational executive team (EC-Council, 2019). Hand in hand with effective communication is the ability to listen and explain eloquently and to develop high interpersonal skills and soft skills in collaboration with technical experience. One also needs the ability to sense cyber security threats and the ability to interlink points in order to create a clear scenario when reporting. These will prove to be effective psychological abilities. People skills form part of all the steps of the penetration testing framework.

Leadership skills are needed for all the steps of the penetration testing framework. The decisions made in the leadership role may result in the success of the test. This includes the ability to view things “out of the box”, which is the ability to consider security matters from a different perspective and to creatively consider

technology developments. This includes the ability to predict things prior to them actually happening and the inborn interest in evaluating facts on critical knowledge.

Throughout the testing process the tester must maintain a professional presence. Self-control is of importance to maintain composure and keep emotions in check. A key factor of professionalism is to deal calmly and effectively with stressful or difficult situations and to accept criticism tactfully and attempt to learn from it. To maintain a professional appearance one has to dress appropriately for occupational and worksite requirements, and maintain appropriate personal hygiene. One must maintain a positive attitude and project a professional image of oneself and the organization, and show a positive attitude towards work and take pride in one's work and the work of the organization.

Integrity is the foundation on which relationships, and trust is built with coworkers or team members. If a person has integrity, then integrity lives in the values in relationships with team members. Key factors of integrity are honesty and trust. A person with integrity draws other team members to them because they are trustworthy and dependable (Heathfield, 2019). People with integrity form a superior workforce, which is needed to be successful in the framework steps.

Ethics play a vital role throughout the framework steps. The tester has to abide by a strict code of ethics and behaviour. An ethical course of action has to be chosen and one must do the right thing, even in the face of opposition. One must encourage others to behave ethically and utilize company time and property responsibly. One must perform work-related duties according to laws, regulations, contract provisions, and company policies, and one must have an understanding that behaving ethically may go beyond what the law requires.

During analyzing and the explanation of Figure 5.1 it is evident that a wide skill set is needed when one wants to be professional and successful in the cyber security community. As indicated in Chapter 4, education, formal and informal training, self-taught skills and practical experience are needed to execute the steps in the penetration testing framework successfully. It is important to take note that a group of professionals who specialize in a specific area of the framework is better than searching for one person who claims to know everything.

5.3 An approach to close the Cyber Skills gap

There are substantial methods which, when put in place, will address the cyber security skills gap, such as (EC-Council, 2019):

5.3.1 Public-private partnership

The cyber skills shortage is a worsening situation, therefore it is necessary for the private and the public sector to come together to rectify the situation (EC-Council, 2019). In the United States there was an attempt to bridge the cyber gap by trying to come up with a partnership between Silicone Valley and Washington. Israel implemented an effective model of bridging relationships between the military, government agencies, academic institutions, cyber security vendors, and venture capitalists (Oltsik, 2019). As reported by Phakathi (2017), in South Africa there is a need for government to promote public-private partnerships to bridge the cyber gap to be able to counter cyber incidents. It is also mentioned, as indicated in the Global Economic Crime Survey, that in SA, the fourth-most reported economic crime is cyber crime (Phakathi, 2017). It is time to seriously establish public-private partnerships.

5.3.2 Combined effort from industries

It is time that large technology and cyber security vendors stop working alone and rather stand together and build an industry-wide organization to develop strategies and programs to conduct effective cyber training to overcome the skills gap (EC-Council, 2019; Oltsik, 2019). An industry-wide organization will have the power to successfully introduce and implement such a capability (Phakathi, 2017; Oltsik, 2019).

5.3.3 Establish of interactive tools

It is vital that the impact of the industry wide cyber security skills gap is monitored. When public-private partnerships are successfully implemented and industry combines their cyber security efforts, tools can be developed to quantify the long term effects on industry (EC-Council, 2019).

5.4 Summary

In Chapter 5 the penetration testing framework was aligned with the skills needed by industry to determine a possible method to close the skills gap in industry. The cyber security skills gap was identified in an effort to identify ways to close the skills gap. Thereafter the proposed framework as discussed in Chapter 3 was aligned with the cyber skills needed in industry. It was evident that a wide range of skills is needed to be successful in cyber security.

6 Conclusion

The research presented in this document has compared, assessed and proposed solutions on the cyber security skills shortage which is a world-wide problem. In order to be successful in proposing solutions for the problem, the first goal is to determine the cyber security skills gap. Due to the fact that cyber security is such a broad discipline the focus of this research was on cyber penetration testing. The main aim of the research was firstly to determine what skills the international standards prescribe for a penetration tester to have. For this research three of the big standardization bodies standards were analyzed. The second goal was to determine if education satisfy the skills required, and the third goal was to align the skills needed for cyber security between industry and education. The fourth part of the research was to suggest a requirement model to successfully identify and test for the right skills needed for a position in industry. The last part of the research was to identify methods as a suggestion to close the cyber security skills gap. To close the skills gap will not be an overnight process, but will take years to accomplish.

6.1 Document Recap

Chapter 1 - Introduced the research itself, defined its scope and gave a layout of the document to come.

Chapter 2 - Introduced the literature study (Section 2.1) where after the cyber

security concepts were laid out to get an view on how broad cyber security is (Section 2.2). Cyber security is narrowed down to specifically cyber penetration testing where the history, types of penetration testing, how to conduct penetration testing, the tools used in the environment, report writing and finally the limitations with regard to penetration testing (Section 2.3) were discussed. Red and Blue teaming (Section 2.4) and Capture the Flag (Section 2.5) are discussed as the two concepts which can be seen as types of penetration testing procedures. In Section 2.6 the terminology used throughout the research was defined to get the reader in the right frame of mind, and understand the terminology in the same manner as the researcher.

In **Chapter 3**, the history of cyber security standards focusing on penetration testing, Information Technology Standards and the Lockheed Martin Cyber Kill Chain is introduced and discussed (Section 3.1 and 3.2). A penetration testing framework is suggested to give an indication on how complex the penetration testing environment is and what skills are needed in the environment (Section 3.3 and 3.4).

Chapter 4 gived a look at the educational roadmap and what cyber security and penetration testing qualifications are presented at training institutions. A proposed framework on how to select the right candidate for the right position is suggested for the recruitment of new candidates.

Chapter 5 combines the penetration testing framework suggested in Chapter 3 with the skills testing framework in Chapter 4 (Section 5.1 and 5.2). It also discusses an approach to close the cyber skills gap (Section 5.3).

6.2 Research Objectives

In Section 1.3, a number of research objectives were listed and the following reports on the progress towards those objectives:

- The first goal of this research was to identify the cyber skills by analyzing International Standards, focusing on penetration testing. Chapter 2, specifically Section 2.3, works through a full background on what penetration testing entails, where after an analysis were done on three of the main International Standards (Chapter 3, Section 3.1 and 3.2). The standards analyzed were the National Institute of Standards and Technology 800-115 (NIST 800-115), Payment Card Industry Data Security Standard (PCI DSS) and International Organization for Standardization 27001 (ISO 27001). In Section 3.2 the skills as prescribed by the international standards were compared with the Lockheed Martin Cyber Kill Chain to bring the processes into perspective.

- A penetration testing framework was suggested in Chapter 3, Sections 3.3 and 3.4. The framework was suggested to identify the skills and expertise that are needed for penetration testing. This is a basic penetration testing framework to show some of the skills needed to conduct a penetration test successfully. It must be understood that not all the objectives of penetration tests are the same. The suggested framework functions as a guide and has to be adjusted according to the detailed objectives of the test at hand.

- The skills gained in the education system, formal education, international certifications and self-taught skills were compared with the skills requirements needed by industry (Chapter 4, Sections 4.1.1 to 4.1.4). After analyzing the skills gained through training, an in-depth analysis was done on the need in industry (Section 4.1.5). Current advertisements in the job market were analyzed and the information used to compare. A framework was suggested which can be used by industry recruitment to test for specific skills as needed for a specific position (Section 4.1.6).

- Lastly the penetration testing framework (Chapter 3) and the skills testing framework (Chapter 4) were combined in Chapter 5 to come to a conclusion on a possible approach to mitigate or close the cyber skills gap and skills shortage. The cyber skills gap is a global problem in industry.

The above mentioned research objectives were researched and according to the outcome of the research all the research objectives were met.

6.3 Summary of Research

The outcome of the research showed that the cyber security skills shortage/gap is a global problem which needs to be looked at to avoid a catastrophe. There are programmes in place at formal educational institutions and numerous international certifications to be obtained, but, the training programmes and the needs of industry are not aligned. There is a lot of research being done, articles being written and presentations being given at international conferences with regard to the cyber skills gap, but once again no one put words into action. There are work groups that have been formed to take on the skills problem,

International standards prescribe penetration testing skills. During research it was realized that some important steps in the cycle are missing in the international standards when compared with the LMCKC. Industry can comply with a specific international standards penetration testing framework, but during research it was realized that the framework has to be changed to adapt to the outcomes of the

penetration test. The LMCKC's seven steps fit into any situation, but they are only the executional part; the physical work needs to be done that will adapt to the current situation.

There are limited penetration testing only job opportunities. Penetration testing is combined with other IT related work. This makes it difficult to select a competent individual for a position, due to the wide range of knowledge and skills required by industry. One of the main skills shortages is years of working experience. The only way in which work experience can be gained is by physically working in a cyber security environment and building knowledge on the working of cyber security tools, being mentored by an cyber professional and building other business skills.

Self-taught skills are an area not looked at and not recognized, due to the fact that no formal proof or paperwork exists to confirm these skills. There is a big difference between theoretical knowledge, practical skills and self-thought skills. The best way to confirm skills is to physically test a person's competency.

When studying the penetration testing framework as suggested in this research (Chapter 3, Section 3.4), one could come to the conclusion that due to the broad spectrum of skills required to perform all the functions, it could be that more than one specialist is needed to focus on specific areas, to perform large-scale penetration tests. The framework suggested in Chapter 4, Section 4.1.6, can be adapted by industries recruiting sections to test the cyber security skills claimed by candidates.

6.4 Future Work

There are multiple areas where future research can be conducted.

Research could be done into a comparison of the qualifications and skills gained at formal educational institutions such as universities. There are post graduate degrees presented at different universities in South Africa. These degrees are normally presented as a Master's degree in Computer Science. Ways in which universities could align their programs in order to give an industry-needed qualification could be investigated.

A comparison of international qualifications to determine the relevance between qualifications from different institutions could be done . The big names in cyber certifications have many different courses that they present. Research could be done into investigating whether the skills and qualification received when doing this training is really so good or whether it is only a money making business.

Practical experience is an aspect that is of great concern in the cyber security environment. Industry needs specialists with the theoretical cyber knowledge and

most important, years of practical experience. Research on how to gain practical experience and skills while busy with the qualification could be done.

A study could be conducted into how educational institutions and industry can work together to align their needs and as a result, the training institutions can send a well-trained knowledgeable person who will be absorbed into the cyber security world.

References

Abousen, D. Computer Security. 2015. Accessed on 11 July 2019.
URL http://www.contrib.andrew.cmu.edu/~dabousen/Default%20-%20Copy%20(4).html

Aldawood, H. and Skinner, G. Reviewing Cyber Security Social Engineering Training and Awareness Programs Pitfalls and Ongoing Issues. *Future Internet*, 11(3), March 2019. ISSN 1999-5903. doi:10.3390/fi11030073.
URL https://www.mdpi.com/1999-5903/11/3/73

Alexander D, R. and Panguluri, S. Cybersecurity Terminology and Frameworks. In *Cyber-Physical Security*, pages 19–47. Springer, 2017. ISBN 978-3-319-32824-9. doi:10.1007/978-3-319-32824-9_2.

Alisherov, F. and Sattarova, F. Methodology for Penetration Testing. *International Journal of Grid and Distributed Computing*, 2(2):43–50, June 2009. ISSN 2005-4262.
URL http://www.sersc.org/journals/IJGDC/vol2_no2/5.pdf

Applebaum, A., Miller, D., Strom, B., Korban, C., and Wolf, R. Intelligent, Automated Red Team Emulation. In *Proceedings of the 32Nd Annual Conference on Computer Security Applications*, volume ACSAC 2016 of *ACSAC '16*, pages 363–373. ACSAC, ACM, New York, NY, USA, 2016. doi:10.1145/2991079.2991111.

Bada, M., Sasse, A. M., and Nurse, J. R. C. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *CoRR*, abs/1901.02672, 2019.
URL http://arxiv.org/abs/1901.02672

Balabanov, T. A Quick Overview of Hashcat and oclHashcat. Internet, August 2016. Accessed on 20 June 2019.
URL https://www.cybrary.it/0p3n/quick-overview-hashcat-oclhashcat/

Baloch, R. Ethical Hacking and Penetration Testing Guide. Taylor & Francis Group, 2015. ISBN 978-1-4822-3162-5.

Bamford, G., Felker, J., and Mattern, T. Operational Levels of Cyber Intelligence. 2013. Accessed on 23 October 2018.
URL https://www.nist.gov/sites/default/files/documents/2017/06/08/20131213_charles_alsup_insa_part3.pdf

Banks, T. The pentest is dead, long live the pentest. Presentation, 2016. Accessed on 12 June 2017.
URL https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-banks-carric.pdf

Bartram, D. The SHL universal competency framework. *SHL White paper*, pages 1–8, 2006.
URL http://www.shl.com

Bateman, A. What is Cyber Defence? March 2014. Accessed on 04 April 2019.
URL https://www.mwrinfosecurity.com/our-thinking/what-is-cyber-defence/

Buch, R., Borad, N., and Kalola, P. World of Cyber Security and Cybercrime. *Recent Trends in Programming Languages*, 4(2):18–23, 08 2018.
URL http://computers.stmjournals.com/

Career Junction. Career Junction Index Executive Summary January 2019. Technical report, Career Junction, 2019. Accessed on 20 February 2019 and 07 March 2019.
URL http://cj-marketing.s3.amazonaws.com/CJI_Executive_Summary.pdf

Carlin, A., Manson, D. P., and Zhu, J. Developing the Cyber Defenders of Tomorrow with Regional Collegiate Cyber Defense Competitions (CCDC). *Information Systems Education Journal*, 8(14):3–10, April 2010. ISSN 1545-679X.
URL https://files.eric.ed.gov/fulltext/EJ1146949.pdf

Champion, M., Jariwala, S., Ward, P., and Cooke, N. J. Using Cognitive Task Analysis to Investigate the Contribution of Informal Education to Developing Cyber Security Expertise. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 58(1):310–314, 2014. doi:10.1177/1541931214581064.

Chandarman, R. and van Niekerk, B. Students Cybersecurity Awareness at a Private Tertiary Educational Institution. *The African Journal of Information and Communication*, 20:133–155, 2017. doi:10.23962/10539/23572.

Ciampa, M. Security Awareness and Applying Practical Security in Your World, volume 4th Edition. Course Technology, 2014. ISBN 9781111644208.

CISCO. What is Cybersecurity? 2019. Accessed on 17 June 2019.
URL https://www.cisco.com/c/en/us/products/security/whst-is-cybersecurity.html

Conklin, W. A., Cline, R. E., and Roosa, T. Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. In *2014 47th Hawaii International Conference on System Sciences*, pages 2006–2014. Jan 2014. ISSN 1530-1605. doi:10.1109/HICSS.2014.254.

Creasey, J. and Glover, I. A guide for running an effective Penetration Testing programme. 2017. Accessed on 20 October 2017.
URL https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf

Culbertson, D., Humphries, D., Ivy, G., Kolko, J., and Rodden, V. The Global Cybersecurity Skills Gap. 2017. Accessed on 16 Oct 2018.
URL https://www.cybintsolutions.com/the-global-cybersecurity-skills-gap/

Curran, K., Maynes, V., and Harkin, D. Mobile device security. *International Journal of Information and Computer Security*, 7:1, 01 2015. doi:10.1504/IJICS.2015.069205.

Cyberdegrees.org. Become a Penetration Tester. 2017. Accessed on 19 March 2017 and 25 March 2017 and 25 June 2019.
URL http://www.cyberdegrees.org/jobs/penetration-tester/

Cybersecurity, C. Hacker Tools Top Ten. Internet article, 2017.
URL https://www.concise-courses.com/hacking-tools/top-ten/

Dalakov, G. First computer virus of Bob Thomas. 2006. Accessed on 16 October 2018.
URL http://history-computer.com/Internet/Maturing/Thomas.html

DataArt. Penetration Testing Services. 2018. Accessed on 11 April 2019.
URL https://www.dataart.com/services/security-testing/penetration-testing

Eagle, C. and Clark, J. Capture-the-Flag: Learning Computer Security Under Fire. 2004. Accessed on 17 July 2017.
URL https://calhoun.nps.edu/handle/10945/7203

EC-Council. The Truth About the Growing Cybersecurity Skill Gap. March 2019. Accessed on 16 July 2019.

URL https://blog.eccouncil.org/the-truth-about-the-growing-_cybersecurity-skill-gap/

Edwards, C. What Is the Meaning of Internet Security? May 2019. Accessed on 10 July 2019.
URL https://www.techwalla.com/articles/what-is-the-meaning-of-internet-security

Engebretson, P. The Basics of Hacking and Penetration Testing - Ethical Hacking and Penetration Testing Made Easy. Syngress, second edition, 2013. ISBN 978-0-12-411644-3.

Epling, Lee, Hinkel, Brandon, Hu, and Yi. Penetration Testing in a Box. In *Proceedings of the 2015 Information Security Curriculum Development Conference*, InfoSec '15, pages 6.1–6.4. ACM, New York, NY, USA, 2015. ISBN 978-1-4503-4049-6. doi:10.1145/2885990.2885996.

Falah, A., Pan, L., and Abdelrazek, M. Visual representation of penetration testing actions and skills in a technical tree model. In *ACSW '17*. ACSW'17, 2017. doi:10.1145/3014812.3014820.

Ferranti, M. What is Nmap? Why you need this network mapper. Internet, August 2018. Accessed on 21 June 2019.
URL https://www.networkworld.com

Filkins, B. Road map to a Secure, Smart Infrastructure. *SANS Institute InfoSec Reading Room*, page 16, August 2017. Accessed on 24 August 2019.
URL https://www.sans.org/reading-room/whitepapers/analyst/road-map-secure-smart-infrastructure-37895

Franco, J. Attack Patterns Aligned to Cyber Kill Chain. Presentation, 2016.
URL http://gauss.ececs.uc.edu/Courses/c6055/pdf/attackpatterns.pdf

Furnell, S., Fischer, P., and Finch, A. Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security*, 2017(2):5–10, 2017. ISSN 1361-3723. doi:10.1016/S1361-3723(17)30013-1.

Gabcanova, I. Human Resource Key Performance Indicators. In *Journal of Competitiveness*, volume 4, pages 117–128. 2012. doi:10.7441/joc.2012.01.09.

Goldstein, N., Newmark, R., Burton, L., May, D., Mcmahon, J., Whitehead, C., and Ghatikar, R. Assessing Security Needs of the Multifaceted Relationships of Energy and Water Providers. Technical report, Office of Scientific and Technical Information (OSTI), 08 2007. doi:10.2172/924955.

Guarda, T., Walter, A., Maria, F., Morillo, G., Navarrete, S. A., and Pintoand, F. M. Penetration Testing on Virtual Environments. In *Proceedings of the 4th International Conference on Information and Network Security*, International Conference on Information and Network Security (ICINS '16), pages 9–12. Association for Computing Machinery (ACM) Digital Library, New York, NY, USA, 2016. ISBN 978-1-4503-4796-9. doi:10.1145/3026724.3026728.

Harris, B., Konikoff, E., and Petersen, P. Breaking the DDoS Attack Chain. 2013. Accessed on 20 February 2018.
URL https://www.cmu.edu/mits/files/breaking-the-ddos-attack-chain.pdf

Heathfield, S. What is Integrity really? February 2019. Accessed on 29 April 2019.
URL http://www.thebalancecareers.com

Henry, K. PREPARING THE REPORT, chapter 9, pages 158–170. IT Governance Publishing, 2012. ISBN 9781849283717.

Hutchins, E., Cloppert, M., and Amin, R. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In **Dr. Edwin (Leigh), E. C.**, editor, *6th International Conference on Information Warfare and Security*, pages 113–124. International Conference on Information Warfare and Security, 2011. ISSN ISBN 978-1-906638-92-4.

Information Security Institute. The history of Penetration Testing. July 2016. Accessed on 08 February 2017.
URL http://resources.infosecinstitute.com/the-history-of-penetration-testing/#gref

Innovative Solutions. History of the Payment Card Industry Data Security Standard (PCI DSS). June 2016. Accessed on 08 August 2017.
URL https://www.sfgnetwork.com/blog/payment-processing/history-of-pci-dss/

ISACA. State of Cyber Security 2017: Current Trends in Workforce Development. Technical report, Information Systems Audit and Control Association (ISACA), 2017. Accessed on 18 June 2018.
URL https://www.isaca.org/cyber/pages/state-of-cyber-security-2017.aspx

ISACA. State of Security Report 2018: Workforce Development. Technical report, Information Systems Audit and Control Association (ISACA), 2018. Accessed 10 January 2019.
URL https://www.isaca.org/cyber/pages/state-of-cyber-security-2018.aspx

ISO. ISO. Technical report, ISO, 2017. Accessed on 19 June 2017.
URL https://www.iso.org/about-us.html

Jaeger, L. Information Security Awareness: Literature Review and Integrative Framework. In *Proceedings of the 51st Hawaii International Conference on System Sciences*, pages 4703–4712. 2018. doi:10.24251/HICSS.2018.593.

Jai, N. G. and Mehtre, B. Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. In **Science, P. C.**, editor, *3rd International Cobference on Recent Trends in Computing (ICRTC-2015)*, volume 57, pages 710–715. 2015. doi:10.1016/j.procs.2015.07.458.

Kampoor, V. Cybersecurity - Mind the skills gap. 2018. Accessed on 20 February 2018.
URL http://www.itnewsafrica.com/2018/01/cybersecurity-mind-the-skills-gap/

Kaspersky. What is Cyber-Security? 2019. Accessed on 17 June 2019.
URL https://www.kaspersky.co.za/resource-center/definitions/what-is-cyber-security

Kennedy, J. Cybersecurity: The 'Zero-Trust' Movement. 2018. Accessed on 16 October 2018.
URL https://www.csoonline.com/article/3258994/data-protection/cybersecurity-skills-shortage.html

Kim, P. The Hacker Playbook 3: Practical Guide To Penetration Testing. Independently published, 2018. ISBN 1980901759.

King, J. Payment Card Industry Data Security Standard (PCI DSS) Security Standard. Technical report, Payment Card Industry Data Security Standard (PCI DSS), 2017. Accessed on 08 August 2017.
URL https://www.pcisecuritystandards.org/about_us/

Kremling, J. and Parker, A. Cyberspace and Cybersecurity and Cybercrime. SAGE Publications, 2017. ISBN 9781506392288.

Krishnan, H. Armitage - Fast and Easy Hacking. April 2012. Accessed on 21 June 2019.
URL https://resources.infosecinstitute.com

Lapena, R. Report 80 percent of IT Security Pros Think the Skills Gap Has Worsened Since 2017. March 2019. Accessed on 16 July 2019.
URL https://www.tripwire.com/state-of-security/security-awareness/security-pros-skills-gap-worsened/

Leenen, L., Aschman, M., Grobler, M., and Van Heerden, A. Facing the culture gap in operationalising cyber with a military context. In *13th International Conference on Cyber Warfare and Security*, pages 387–394. Academic Conferences and Publishing International Ltd, Academic Conferences and Publishing International Ltd., 2018.

Lockheed Martin Corporation. Applying Cyber Kill Chain Methodology. Technical report, Lockheed Martin, 2015.
URL https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Lynch, J. How the UK is Closing the Cybersecurity Skills Gap. 2017. Accessed on 18 October 2018.
URL https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/how-the-uk-is-closing-the-_cybersecurity-skills-gap/

Martincic, C. J. Pitt View, IT Standards, A Brief History of International Organization for Standardization (ISO). 1997. Accessed on 19 July 2017.
URL http://www.sis.pitt.edu/mbsclass/standards/martincic/isohistr.htm

Mattern, T., Felker, J., Borum, R., and Bamford, G. Operational levels of Cyber Intelligence. *International Journal of Intelligence and Counter Intelligence 27:4*, 27:2:702–719, August 2014. doi:10.1080/08850607.2014.924811.

McCauley, B. Introduction to Wireless Security with Aircrack-ng. Internet, September 2018. Accessed on 18 June 2019.
URL https://securityboulevard.com/2018/09/introduction-to-wireless-security-_with-aircrack-ng/

McKean, E. Online English Dictionary. May 1995.
URL https://www.dictionary.com/browse/

Miessler, D. The difference between Red, Blue and Purple teams. 2016. Accessed on 19 February 2017.
URL https://danielmiessler.com/study/red-blue-purple-teams/

Mirkovic and Peter, P. Class Capture the flag exercises. 2014. Accessed on 13 July 2017.
URL https://www.usenix.org/conference/3gse14/summit-program/presentation/mirkovic

MITRE. Threat Based Defense. July 2014. Accessed on 14 September 2017.
URL https://www.mitre.org/capabilities/cybersecurity/threat-based-defense

Mohamed, A. Password Cracking Using Cain and Abel. Internet, January 2018. Accessed on 20 June 2019.
URL https://resources.infosecinstitute.com/password-cracking-using-cain-abel/

Morgan, S. Cybersecurity job market to suffer severe workforce shortage. 2017. Accessed on 22 June 2017 and 16 April 2019.
URL https://www.csoonline.com/article/3201974/it-areers/cybersecurity-job-market-statistics.html

Najera-Gutierrez, G. and Ansari, J. Web Penetration Testing with Kali Linux: Explore the methods and tools of ethical hacking with Kali Linux, 3rd Edition. Packt Publishing, 2018. ISBN 9781788623803.

NeSmith, B. The Cybersecurity Talent Gap Is An Industry Crisis. 2018. Accessed on 18 October 2018.
URL https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/

NIST. National Institute of Standards and Technology (NIST) History. 2017. Accessed on 23 July 2017, 06 August 2017, 08 August 2017.
URL https://www.nist.gov/nist-history

NIST. Framework for Improving Critical Infrastructure Cybersecurity. Technical report, National Institute of Standards and Technology (NIST), April 2018a. doi: 10.6028/NIST.CSWP.04162018. Accessed 20 July 2018.

NIST. NIST. 2018b.
URL https://www.nist.gov/timeline#event-a-href-node-774236david-wineland-_shares-physics-nobel-a

NIST. Computer Security Resource Center Glossary. 2019. Accessed on 03 April 2016.
URL https://csrc.nist.gov/glossary/term/cybersecurity

Obbayi, L. A Brief Introduction to the Nessus Vulnerability Scanner. Internet, November 2018a. Accessed on 20 June 2019.
URL https://resources.infosecinstitute.com/a-brief-introduction-to-the-nessus-_vulnerability-scanner/

Obbayi, L. Introduction to the Nikto Web Application Vulnerability Scanner. Internet, March 2018b. Accessed on 20 June 2019.
URL https://resources.infosecinstitute.com/introduction-to-the-nikto-web-_application-vulnerability-scanner/

Oltsik, J. The Cybersecurity Skills Shortage Is Getting Worse. January 2019. Accessed on 18 July 2019.
URL https://www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-_getting-worse

Ortega, M. Acunetix Web Vulnerability Scanner. Internet, December 2014. Accessed on 20 June 2019.
URL https://hakin9.org/acunetix-web-vulnerability-scanner/

OWASP. OWASP Zed Attack Proxy Project. May 2019. Accessed on 19 June 2019.
URL https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Pack, S. and Rowe, D. C. Training Cyber-Defense and Securing Information Assets Using Student Blue Teams. In **SIGITE**, editor, *SIGITE*, pages 3–6. SIGITE, 2013. doi:10.1145/2512276.2512290.

Parizo, E. The history of the PCI DSS standard: A visual timeline. 2013. Accessed on 08 August 2017.
URL http://www.searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline

Parmar, S. K. Information Resource Guide, Computer, Internet and Network Systems Security, An Introduction to Security. A Security Manual. 2018.
URL http://citeseerx.ist.psu.edu/viewdoc/citations?doi=10.1.1.153.5669

Parmenter, D. Key performance indicators: developing, implementing, and using winning KPI's. John Wiley & Sons, 2015. ISBN 1118925106.

Parsons, B. How can the cyber skills gap be closed? 2017. Accessed on 18 October 2018.
URL https://www.openaccessgovernment.org/can-cyber-skills-gap-closed/33275/

Petersen, R., Santos, D., Smith, C., Wetzel, K., and Witte, G. Workforce Framework for Cyber Security. November 2020. doi:10.6028/NIST.SP.800-181rl. This is an new document as part of rectifications to thesis.

Phakathi, B. Public Private partnerships are key in fight against cybercrime, MPs told. February 2017. Accessed on 18 July 2019.

URL https://www.businesslive.co.za/bd/national/2017-02-28-public-private-partnerships-are-key-in-fight-against-cybercrime-_mps-told/

Porup, J. What is Wireshark? What this essential troubleshooting tool does and how to use it. Internet, September 2018. Accessed on 19 June 2019.
URL https://www.csoonline.com/article/3305805/what-is-wireshark-what-this-essential-troubleshooting-tool-does-and-how-to-_use-it.html

Press, G. The Birth Of The Cybersecurity And Computer Industries. 2015. Accessed on 16 October 2018.
URL https://www.forbes.com/sites/gilpress/2015/11/01/this-week-in-tech-history-the-birth-of-the-cybersecurity-and-computer-industries/#64c7c1e85bcd

Puha, O. John the Ripper. Internet, May 2019. Accessed on 21 June 2019.
URL https://www.softpedia.com/get/Security/DecryptingDecoding/John-the-Ripper.shtml

Quigley, Jon, M., Robertson, and Kim, L. Configuration Management: Theory, Practice, and Application. CRC Press, 2015. ISBN 9781482229356.

Rouse, M. Cybersecurity. May 2018. Rieviewed on 16 Oct 2018 Web page visited on 16 Oct 2018.
URL https://searchsecurity.techtarget.com/definition/cybersecurity

Rowe, D., Lunt, B., and Ekstrom, J. The role of cyber-security in information technology education. In *Proceedings of the 2011 conference on Information technology education*, volume SIGITE'11, pages 113–122. Proceedings of the 2011 conference on Information technology education, October 2011. doi: 10.1145/2047594.2047628.

Roy, M. Effects of cybersecurity skills shortage worsening, new study says. May 2019. Accessed on 21 July 2019.
URL https://searchsecurity.techtarget.com/news/252463186/Effects-of-cybersecurity-skills-shortage-worsening-new-study-says

Sanchez, R. How to Use Maltego to Conduct Threat Research. Internet, July 2017. Accessed on 20 June 2019.
URL https://www.groupsense.io/how-to-use-maltigo-to-conduct-threat-research/

Sangster, B., O'Connor, T., Cook, T., Fanelli, R., Dean, E., Morrell, C., and Conti, G. Toward Instrumenting Network Warfare Competitions to Generate Labeled Datasets. In *Proceedings of the 2nd Conference on Cyber Security Experimentation and Test*, CSET' 09, pages 9–9. USENIX Association, Berkeley, CA, USA, 2009.

SANS. Information technology - Security techniques - Information security management systems - Overview and vocabulary. Technical Report SANS27001, South African National Standards, March 2018. ISBN 978-0-626-31568-9.

Schofield, A. 2018 JCSE-IITPSA ICT Skills Survey. Technical report, Johannesburg Centre for Software Engineering (JCSE) and Institute of Information Technology Professionals South Africa (IITPSA), 2018. Accessed on 07 March 2019.
URL https://www.iitpsa.org.za/wp-content/uploads/2018/10/2018-JCSE-IITPSA-ICT-Skills-Survey-V1.pdf

Scott-Jackson, T. The Evolution Of The Penetration Test. July 2016. Accessed on 9 June 2019.
URL https://www.informationsecuritybuzz.com/articles/evolution-penetration-test/

SentinelOne. The History of Cyber Security, Everything You Ever Wanted to Know. 2017. Accessed on 16 October 2018.
URL https://www.sentinelone.com/blog/history-of-cyber-security/

SETA, M. Sector Skills Plan 2018 to 2023. Technical report, MICT SETA, August 2017.
URL https://www.mict.org.za/downloads/MICTSETASSP2018to2023Draft.pdf

Shaheer. THC Hydra free download 2019 - Best Password Brute Force Tool. March 2019. Accessed on 20 June 2019.
URL https://securedyou.com/download-thc-hydra-password-cracking-tool-free/

Shanley, A. and Johnstone, M. Selection of penetration testing methodologies, A comparison and evaluation. In *13th Australian Information Security Management Conference*, pages 65–72. 2015. doi:10.4225/75/57b69c4ed938d.

Silensec. Addressing the Cyber Security Skills Gap. 2017. Accessed on 19 March 2018.
URL http://www.silensec.com/downloads-menu/whitepapers/item/29-addressing-the-cyber-security-skills-gap

Singh, A., Jaswal, N., Agarwal, M., and Teixeira, D. Metasploit Penetration Testing Cookbook: Evade antiviruses, bypass firewalls, and exploit complex environments with the most widely used penetration testing framework, 3rd Edition. Packt Publishing, 2018. ISBN 9781788629713.

Skills Base. The Skills Base Competency Framework - Maximizing your organizations greatest asset. 2016. Accessed on 15 to 18 April 2019.
URL https://www.skills-base.com/competency-framework

Son, D. Install Social Engineering Toolkit (SET) on Windows. Internet, February 2018. Accessed on 20 June 2019.
URL https://securityonline.info/install-social-engineering-toolkit-set-windows/

Taylor, R. W., Fritsch, E. J., and Liederbach, J. Digital Crime and Digital Terrorism. Prentice Hall Press, Upper Saddle River, NJ, USA, 3rd edition, 2014. ISBN 9780133458909.

Thomas, M. Implementing the NIST Cybersecurity Framework using COBIT 5. Technical report, Information Systems Audit and Control Association (ISACA), 2017. Accessed in February 2018.
URL https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-the-NIST-Cybersecurity-Framework-_Using-COBIT-5.aspx

Tipton, F. and Krause, M. Information Security Management Handbook. CRC Press, May 2007. ISBN 9780429151101. doi:https://doi.org/10.1201/9781439833032. Chapter 13.

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., and Lepri, B. The Privacy Implications of Cyber Security Systems: A Technological Survey. *ACM Comput.ing Surveys*, 51(2):36:1–36::7, February 2018. ISSN 0360-0300. doi:10.1145/3172869.

Uren, T., Hogeveen, B., and Hanson, F. Defining offensive cyber capabilities. July 2018. Accessed on 12 October 2018.
URL https://www.aspi.org.au/report/defining-offensive-cyber-capabilities

Vectra. Penetration Testing. August 2018. Accessed on 11 April 2019.
URL https://www.vectra-corp.com/penetration-testing/

Verma, A. Best hacking tools of 2017 for Windows, Linux and OS X. December 2016. Accessed on 25 March 2017.
URL https://fossbytes.com/best-hacking-tools-of-2016-windows-linux-mac-osx/

Von Solms, R. and Van Niekerk, J. From information security to cyber security. *Computers & Security*, 38:97–102, 2013. doi:10.1016/j.cose.2013.04.004.

Vonnegut, S. A Quick guide to Ethical Hacking and top Hacking Tools. 2016. Accessed on 25 March 2017.
URL https://www.checkmarx.com/2016/05/16/quick-guide-ethical-hacking-_top-hacking-tools/

Wai, C. T. Conducting a Penetration Test on an Organization. *SANS Institute InfoSec Reading Room*, 2002.
URL https://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67

Wang, P. A Brief history of standards and standardization organizations: A Chinese Perspective. Technical Report 117, East-West Center, 2011.
URL https://www.eastwestcenter.org/publications/brief-history-standards-and-standardization-organizations-chinese-perspective

Web Finance. Business Dictionary. 2017.
URL http://www.businessdictionary.com/definition/framework.html.

Webster, M. Merriam Webster Dictionary and Thesaurus. 2018.
URL https://www.merriam-webster.com/dictionary/framework

Zitta, S., Horalek, J., Marik, O., and Neradova, S. Conducting effective penetration testing. In *Proceedings of the 2014 International Conference on Systems, Control, Signal Processing and Informatics II (SCSI '14)*, Recent Advances in Electrical Engineering Series - 33, pages 144–149. Prague, Czech Republic, April 2014. ISBN: 978-1-61804-233-0.
URL http://www.inase.org/library/2014/prague/bypaper/SCSI/SCSI-23.pdf

A

Job Advertisements for Cyber Penetration Tester in South Africa

To be able to test the proposed solution framework in Chapter 4, it was required to test it with real-time job advertisements which were advertised during the write-up of this thesis. The advertisements are only available for a predetermined time where after they are removed from the internet. The two job advertisements analyzed during the study are listed below.

A.1 Sample 1: Penetration Tester

URL: https://www.google.com/search?client=firefox-b-d&q=cyber+penetration+testing+jobs+south+africa&ibp=htl;jobs&sa=X&ved=2ahUKEwiL9LGyusbjAhWPKlAKHR77Af0Qp4wCMAJ6BAgMEAE#htidocid=X77RbrIlFi8XimcvAAAAAA%3D%3D Dudley Zengeza Sandton

Apply on E-Merge IT Recruitment

12 days ago Full–time

Do you believe you are one of the best Ethical Hackers in South Africa? Do you like hacking Systems in your spare time to test your skills? Can you do Penetration Testing in your sleep? If you answered yes to any of these questions, then my client wants you. You will be required to simulate cyber-attacks against the groups' computer system to check for exploitable vulnerabilities. Attempt to breach

a number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

Requirements:

- 5+ years of Ethical Hacking experience
- Relevant certification (OSCP, CASS, CEPT, CPT, CCTHP, CRTOP, CISSP, CEH, GPEN, OSCE)
- Strong technical background and knowledge • Exposure to red team testing
- Exposure to threat hunting
- Exposure to identifying and exploiting attack paths to critical assets
- Exposure to cyber-attack frameworks (MITRE, Cyber Kill Chain) Technologies

Required:

- Knowledge of C++, C, C#, Python, Scripting
- Good coding ability
- Technical Cyber-attack frameworks

Nice to haves:

- Knowledge of CBEST, CREST and TIBER
- Banking experience
- Technical IT qualification at Bachelors/Masters Level
- Hobbies hacking things

Responsibilities:

- Reverse engineering, coding, finding bugs in software/hardware
- Help establish a red team in the bank
- Ethical person
- Have theoretical knowledge of hacking
- Have practical experience in hacking

- Deep technical understanding in Linux and Windows operating systems

Reference Number for this position is DZ50050 which is a permanent position based in Woodmead offering a cost to company salary negotiable on experience and ability. Contact Dudley on dudleyz@e-merge.co.za or call him on 011 463 3633 to discuss this and other opportunities.

Are you ready for a change of scenery? The e-Merge IT recruitment is a specialist niche recruitment agency. We offer our candidates options so that we can successfully place the right developers with the right companies in the right roles. Do you have a friend who is a developer or technology specialist?

We pay cash for successful referrals Dudley Zengeza

A.2 Sample 2: Cyber Security Penetration Tester

URL: https://www.google.com/search?client=firefox-b-d&q=cyber+penetration+testing+jobs+south+africa&ibp=htl;jobs&sa=X&ved=2ahUKEwiL9LGyusbjAhWPKlAKHR77Af0Qp4wCMAB6BAgKEAE#htidocid=Qrnbo7bM1tsFXRkbAAAAAA%3D%3D E-Merge IT Recruitment

Cape Town

Apply on Bizcommunity.com

Over 1 month ago. R 395K a year. Full–time

A Cape Town-based Financial Institution that leverage technology to ensure they remain ahead of the competitions requires a Cyber Security Penetration Tester. You will be required to simulate cyber-attacks against the groups' computer system to check for exploitable vulnerabilities. Attempt to breach a number of application systems, (e.g., application protocol interfaces (APIs), front-end/back-end servers) to uncover vulnerabilities, such as unsensitised inputs that are susceptible to code injection attacks.

Requirements:

- Two+ years of Ethical Hacking experience
- Relevant certification (OSCP, CASS, CEPT, CPT, CCTHP, CRTOP, CISSP, CEH, GPEN, OSCE)
- Strong technical background and knowledge
- Exposure to red team testing
- Exposure to threat hunting
- Exposure to identifying and exploiting attack paths to critical assets

- Exposure to cyber attack frameworks (MITRE, Cyber Kill Chain)Technologies

Required:

- Knowledge of C++, C, C#, Python, Scripting
- Good coding ability
- Technical Cyber-attack frameworks

Nice to haves:

- Knowledge of CBEST, CREST and TIBER
- Banking experience
- Technical IT qualification at Bachelors/Masters Level
- Hobbies hacking things

Responsibilities:

- Reverse engineering, coding, finding bugs in software/hardware
- Help establish a red team in the bank
- Ethical person
- Have theoretical knowledge of hacking
- Have practical experience in hacking
- Deep technical understanding in Linux and Windows operating systems

Reference Number for this position is DZ50050 which is a permanent position based in Cape Town offering a cost to company salary R400,000 CTC negotiable on experience and ability.

Contact Dudley on [[dudleyz@e-merge.co.za]] or call him on 011 463 3633 to discuss this and other opportunities. Are you ready for a change of scenery? The e-Merge IT recruitment is a specialist niche recruitment agency. We offer our candidates options so that we can successfully place the right developers with the right companies in the right roles. Check out the e-Merge website www.e-merge.co.za for more great positions. Do you have a friend who is a developer or technology specialist?

We pay cash for successful referrals

E-Merge IT Recruitment

A.3 Sample 3: Penetration Tester

URL: https://www.google.com/search?source=hp&ei=uRIRYNqDH-Sy8gLb5YnQAw&q=cyber+security+vulnerability+testing+job+&ibp=htl;jobs&rciv=jb&chips=e
-
DjkQiJcCKAJ6BAgWEAs#htichips=employment_type:FULLTIME&htischips=job_family_1,city

BASHR Consulting
Pretoria (+1 other) Over 1 month ago
R 780K a yearFull–time
Successful incumbent will:

- Perform penetration testing and attack simulations on business critical infrastructure including internal servers, networks and applications to identify and resolve security flaws.
- Occasional experiments with various methods attackers could use to exploit information security vulnerabilities.
- Complete threat assessment reports that outline penetration test findings and presents findings to clients.
- Conduct physical security assessments of servers, systems and network devices.
- Collaborate with the SecOps team to maintain a client's information security policies and procedures.

Must have

- Relevant tertiary qualification
- Security related certifications such as OSCP, OSCE or CREST are desirable
- Extensive penetration testing experience in a similar role.
- Experience with both commercial and open source security tools and scripting languages
- Exposure to security testing scenarios e.g. Capture the Flag / Red Team / Blue Team is desirable
- Experience with various testing platforms is desirable
- 10 years + working experience

A.4 Red Team Penetration Tester

https://www.google.com/search?source=hp&ei=uRIRYNqDH-Sy8gLb5YnQAw&q=cyber+securit
-DjkQiJcCKAJ6BAgWEAs#htichips=employment_type:FULLTIME&htischips=job_family_1,cit

Banking Johannesburg CBD

Salary: R66 667.00 - R83 333.00 Per Month

Job Type: Permanent

Sectors: Banking IT

Reference: STJan21

Employment Equity Position

Are you a Treat Hunter? And proffiecient in Cyber Security | Threat Analysis | Incident Management | Threat Modelling | Planning and Management | Technical Delivery | Cloud Security

Make sure you dont miss opportunity to join my client, a large multi national giant in Financial Services in the Red or BlueTeam... Red Teaming is a full-scope, multi-layered attack simulation

designed to measure how well a company's people and networks, applications and physical security controls can withstand an attack from a real-life adversary. Say what? To put red teaming

in layman's terms, it's "ethical hacking"—a way for independent security teams to test how well an organization would fare in the face of a real attack. 6% to 28% of the attacks are conducted

with the help of current or former employees of the infected organizations — InfoSec Institute We estimate that each of our projects averages about 20% automated and about 80% manual,

deep-dive, advanced penetration.

Duties & Responsibilities

- Threat Intelligence, Threat Analysis, Incident Response, Security Operations, Technical Delivery
- Responsible for technical design, delivery, and implementation management of cyber security offerings.
- Provide technical support on client cyber infrastructure deployments.
- Review and Presentation of reports at client meetings
- Research on Security Intelligence and provide insight into current cyber security threats.
- Analyse threats observed in client enterprise environments and provide recommendations.

- Implement and optimize SIEM platform detection capabilities.
- Implement and support Security Incident Response Platforms (IRP).
- Integrate Threat Intelligence feeds into SIEM solutions.
- Assess security risks and advise on mitigating controls.
- Report and alert on cyber security threats.
- SIEM experience includes IBM QRadar, HP ArcSight and McAfee Nitro.

Desired Experience & Qualification

Required Skills

- Cyber security : 2 to 3 years
- Offensive : 2 to 3 years

Candidate Requirements

- Red Team (Offensive engagement)
- Custom Web and Application Exploitation
- Vulnerability Management
- Penetration Testing
- Manipulating System Misconfigurations
- External and internal Penetration Testing
- Cyber Security Awareness Campaigns

A.5 Senior Penetration Tester

URL: https://www.cybersecurityjobs.net/job/ignata-tech-london-79-penetration-tester/

Ignata Tech

Our consultants are all specialists within their discipline and are passionate about delivering exceptional service. Focused entirely on results, we work closely with our clients and candidates to deliver the right outcome for every requirement.Whether you are looking for highly skilled professionals, a team move or an end to end solution for all your recruitment needs, Ignata has an expert who will support you every step of the way.

Job Summary

- Location: London
- Salary: £85.000-£85,000

Job Details

About the Job Ignata Technology is partnering with an innovative Cyber Security Consultancy as they look to appoint a Penetration Tester to join their expanding operation. If you're the kind of person that loves to help clients solve real-world security challenges by breaking stuff and securing things then we would like to hear from you.

The organisation in question seeks experienced individuals to join our security consultancy based in London to lead and deliver projects that include application security assessments, red teaming, hardware and software configuration reviews, infrastructure security assessments and code reviews.

Personal attributes

- Motivated self-starter with high capacity for rapid learning
- Positive can-do attitude to thrive in a fast-paced, high-performance team
- Ability to direct, lead and work well with other team members
- Strong communication skills both in written and verbal English
- Excellent time management skill with ability to work under pressure

Required Qualifications

- Crest (CCT), Tigerscheme (SST) or Cyber Scheme (CSTL) Qualification
- UK Security Clearance or ability and willingness to obtain UK Security Clearance

Preferred Experience

- Minimum of 5 years IT Security experience
- Penetration testing, application security assessments, security code reviews
- Experience in software development •
- Strong UNIX, Linux, Windows, iOS, Android and/or networking security skills

A.6 Penetration Tester Brentford

URL: https://www.cybersecurityjobs.net/job/vodafone-brentford-79-penetration-tester-brentford/

Vodafone

As we evolve into a truly digital company, Vodafone Group Technology spans across the entire Vodafone footprint and drives our technology advancements, to enable us to be the best and most secure in unified communications. We empower our consumer and enterprise customers to be confidently and securely connected. Our unique capabilities create the best voice and data to our customers and continue our advancement in the Internet of Things (IOT), BIG Data, Cybersecurity, Cloud & Hosting, TV and Video. We're heading to an exciting future – fancy being part of our Vodafone Gigabit growth?

Job Summary

- Location: Brentford
- Title: Penetration Tester

Job Details

Role Profile

At Vodafone Group Cybersecurity operations, we help our customers remain secure and resilient in a world of increasingly sophisticated cyber-attacks. We offer a unique combination of highly resilient networks, enterprise-class cloud platforms, advanced security systems and expert advice, helping limit the risks of a mobile workforce, such as commercial losses, regulatory breaches or threats to individuals, whilst enabling productivity and employee satisfaction.

Joining as our Cyber Defence Problem Manager now has never been a better time to be part of our success. As a specialist in Vodafone Group Technology Security you will be responsible for operating security service for ethical hacking and penetration testing.

Key Accountabilities

- Execute security assessments and penetration tests to highlight and clearly articulate risk to the business in terms they understand
- Create detailed technical reports of security tests
- Participate in the scope definition of security tests
- Maintain and operate the tools, devices and lab environment needed for security tests

- Contribute to the creation and maintenance of Group level policies and guidelines concerning security assessment and testing
- Accountable for the overall test execution, quality of work and deliverables of assigned security test engagements
- Hold regular presentations and workshops on new techniques and methods both within and outside of the team

Your Profile

- You will have a proven track record of penetration testing

Essential

- Manual and automated penetration testing experience
- Experience in compiling penetration testing portfolio/images/test environments, change management
- Experience in a multi-national, shared services environment,
- IT infrastructure knowledge, including clear customer service and resolution of escalated issues,
- Cross cultural sensitivity, risk assessment experience

Desirable

- CHECK Team Member or OSCP
- What is the key to our success? It's simple – our people. Across a Global footprint, we believe we're at our best when you're at yours. From our diverse workforce, our flexible working policies to our creative work spaces, we embrace a culture of learning and sharing to develop our next stage growth. It's in our hearts to push forward, to create a better future, to never rest and find new ways that help people communicate.
- We are committed to developing the very best people by offering a flexible, motivating and inclusive workplace in which talent is truly recognised and rewarded. We respect, value and celebrate our people's individual differences – we are not only multinational but multicultural too. Our excellent flexible benefits programme allows you to choose what's right for you. Our Vodafone Foundation gives the ability for our people to give something back. We embrace empowering our people to shape their world. That's what we mean when we say Power to you.

A.7 Penetration Tester Leeds, UK

URL: https://www.cybersecurityjobs.net/job/evolution-recruitment-solutions-leeds-79-penetration-tester-leeds-uk-or-home-based/

Job Summary

- Location: Leeds
- Ref: MSTR/D1L/637792/152525
- Salary: £65000

Job Details

The penetration tester will report into the Technical Vulnerability Manager and play a crucial role in supporting and developing red team activities within the vulnerability management regime. You will provide infrastructure and application layer testing, working across a variety of projects.

You will be responsible for

- Establishing in-house penetration testing methodology and framework, templated for reporting and scoping document templates.
- Working with stakeholders to define, scope and execute red team threat simulations and penetration tests against business units and services.
- Performing Cross Tribe, post-finding reviews and agreeing remediation actions with stakeholders.
- Provide technical findings and executive reports.
- Producing weekly report packs and metrics for stakeholders.
- Tracking and verifying remediation activities through re-testing and ad-hoc reporting.

Key Skills

- Commercial exposure performing pen tests
- Clear understanding of the law as it relates to computer security
- Offensive Security (OSCP, CTP, OSWE), GIAC (GWAPT, GPEN), CREST Certifications all advantageous
- Please note that no terminology in this advert is intended to discriminate on the grounds of age, and we confirm that we will gladly accept applications from persons of any age for this role.

A.8 Cybersecurity Penetration Tester

URL: https://www.indeed.com/q-Cyber-Security-Penetration-Tester-jobs.html?vjk=83aa79a505e

Livermore, CA 94550

Company Description

Join us and make YOUR mark on the World! Are you interested in joining some of the brightest talent in the world to strengthen the United States' security? Come join Lawrence Livermore National Laboratory (LLNL) where our employees apply their expertise to create solutions for BIG ideas that make our world a better place. We are looking for individuals that demonstrate an understanding of working in partnership with team peers, who engage, advocate, and contribute to building an inclusive culture, and provide expertise to solve challenging problems.

Job Description

We have openings for Cybersecurity Penetration Testers to conduct comprehensive penetration testing of LLNL networks, devices, computers, web applications and cloud-delivered services. This position is within the Information Technology Solutions Division (ITSD) of the Computing Directorate and matrixed to the Cyber Security Program (CSP), in support of the Livermore Information Technology (LivIT) Program. This position will be filled at either level depending on your qualifications. Additional job responsibilities (outlined below) will be assigned if you are selected at the higher level. In this role, you will

- Develop processes, techniques, and procedures for performing penetration assessments.
- Perform network, system, web application, client application and cloud application penetration tests on internal and external systems as well as systems on air-gapped networks.
- Provide penetration testing support including troubleshooting and resolution of issues.
- Create and manage processes, systems, and tools exercising a high degree of responsibility.
- Serve as a penetration testing technical point of contact and interact with internal and external personnel.
- Perform technical assessments, document actions, findings, and make remediation recommendations.
- Perform other duties as assigned. Additional job responsibilities, at the SES.3 Level

- Manage multiple complex parallel tasks and priorities of customers and stakeholders, ensuring deadlines are met, while leveraging team member skills.
- Develop advanced methods, tools and procedures to improve penetration testing capabilities and automate various complex tasks.
- Mentor and provide technical guidance to team members in penetration testing best practices and procedures.

Qualifications

- Ability to obtain and maintain a U.S. DOE Q-level security clearance which requires U.S. Citizenship.
- Bachelor's degree in Computer Science, Computer Engineering or related field, or the equivalent combination of education and related experience.
- Comprehensive knowledge of computer and network technologies and Windows, Linux/UNIX and/or Apple hardware and operating systems, cloud service technologies and security requirements.
- Experience with programming or scripting languages such as C, C#, Python, Java, PowerShell and PHP.
- Experience with NMAP, Wireshark, and Burp Suite Pen Tester or other cybersecurity tools.
- Proficient written and verbal communication, strong interpersonal skills, ability to collaborate in a multi-disciplinary team environment and to interact with all levels of management and staff.
- Ability to effectively manage concurrent technical tasks with conflicting priorities, to approach difficult problems with enthusiasm and creativity and to change focus when necessary, with experience working independently.
- Current penetration testing certification such as GIAC Certified Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), GIAC Exploit Researcher and Advanced Penetration Tester (GXPN).
- Ability to work off-hours and on-call to respond to incidents (intermittently, either as-needed or as part of a rotation). Additional qualifications at the SES.3 Level
- Significant penetration testing and technical experience with Linux or Windows operating systems, networks, and/or related hardware.

- Significant knowledge and experience with programming or scripting languages such as C, C#, Python, Java, PowerShell and PHP.
- Advanced ability to provide innovative approaches and apply new technologies to tasks and projects that may not be well defined.

Qualifications We Desire

- Master's degree in Computer Science, Computer Engineering, or a related field, or equivalent level of knowledge.
- Significant penetration testing experience, including cloud services such as AWS/Azure.
- Knowledge of LLNL's Cyber Security policies, processes and requirements.

Additional Information

- Why Lawrence Livermore National Laboratory?
- Included in 2020 Best Places to Work by Glassdoor!
- Work for a premier innovative national Laboratory
- Comprehensive Benefits Package
- Flexible schedules (*depending on project needs)
- Collaborative, creative, inclusive, and fun team environment
- Learn more about our company, selection process, position types and security clearances by visiting our Career site.

Security Clearance

LLNL is a Department of Energy (DOE) and National Nuclear Security Administration (NNSA) Laboratory. Most positions will require a DOE L or Q clearance (please reference Security Clearance requirement). If you are selected, we will initiate a Federal background investigation to determine if you meet eligibility requirements for access to classified information or matter. In addition, all L or Q cleared employees are subject to random drug testing. An L or Q clearance requires U.S. citizenship. If you hold multiple citizenships (U.S. and another country), you may be required to renounce your non-U.S. citizenship before a DOE L or Q clearance will be processed/granted. For additional information please see DOE Order 472.2.

Equal Employment Opportunity

LLNL is an affirmative action and equal opportunity employer that values and hires a diverse workforce. All qualified applicants will receive consideration for employment without regard to race, color, religion, marital status, national origin, ancestry, sex, sexual orientation, gender identity, disability, medical condition, pregnancy, protected veteran status, age, citizenship, or any other characteristic protected by applicable laws. If you need assistance and/or a reasonable accommodation during the application or the recruiting process, please submit a request via our online form.

California Privacy Notice

The California Consumer Privacy Act (CCPA) grants privacy rights to all California residents. The law also entitles job applicants, employees, and non-employee workers to be notified of what personal information LLNL collects and for what purpose. The Employee Privacy Notice can be accessed here.

A.9 Penetration Tester

URL: https://www.indeed.com/q-Cyber-Security-Penetration-Tester-jobs.html?vjk=a588ceaa8cc5

Washington, DC

On Company Site

SIXGEN is a mission-focused company. Our success is predicated on our experienced cadre of technical Subject Matter Experts who provide solutions to the Nation's toughest challenges in cyberspace. We conduct intelligence operations, mitigate threats to critical infrastructure and key resources, and develop the capabilities necessary for providing enhanced situational awareness to war fighters and decision makers through rapid data solutions backed by security best practice. Currently, both commercial and government organizations are facing obstacles in today's rapidly changing net-centric landscape, making cybersecurity a chief necessity.

SIXGEN would like to add an ambitious, dedicated, and self-motivated Penetration Tester to our team.

Job Location: Arlington, VA Relocation may be offered.

Required:

- Must have at least 5 years experience in 3 or more of the following areas:
  - Penetration testing
  - Wireless penetration testing (WPA2 handshake attacks, PMKID attacks, WPS attacks)
  - Phishing

  - Reverse engineering exploits Log analysis
  - Operation of assessment tools
  - Script Writing
- Minimum 2 years in a leadership role
- Ability to obtain a Public Trust Clearance
- At least one of the following industry certifications: GPEN, GXPN, OSCP, OSCE, CEPT, eCPPT, or equivalent.

Highly Desired:

- Active TS/SCI Clearance
- Bachelor's degree in Computer Science or related discipline Travel up to 30%
- Remote work may be offered

Benefits:

- SIXGEN pays 100% of health benefits - Medical, Vision, Dental
- 401K with 3.5% matching offered
- Some training and education may be covered by SixGen
- Relocation offered if necessary
- The salary range is dependent on skills, experience and is negotiable (SIXGEN typically pays above average)

A.10 Junior Penetration Tester

URL: https://www.indeed.com/q-Cyber-Security-Penetration-Tester-jobs.html?vjk=f62a02f5ae2f

SixGen, Inc.

Arlington, VA

SIXGEN is a mission-focused company. Our success is predicated on our experienced cadre of technical Subject Matter Experts who provide solutions to the Nation's toughest challenges in cyberspace. We conduct intelligence operations, mitigate threats to critical infrastructure and key resources, and develop the capabilities necessary for providing enhanced situational awareness to warfighters and decision makers through rapid data solutions backed by security best practice. Currently, both commercial and government organizations are facing obstacles in

today's rapidly changing net-centric landscape, making cybersecurity a chief necessity. SIXGEN would like to add an ambitious, dedicated, and self-motivated Junior Penetration Tester to our team.

Required:

- Must have at least 2 years experience in 3 or more of the following areas:
  - Penetration testing Wireless penetration testing (WPA2 handshake attacks, PMKID attacks, WPS attacks)
  - Phishing
  - Reverse engineering exploits
  - Log analysis
  - Operation of assessment tools
  - Script Writing
- Ability to obtain a Public Trust Clearance
- At least one of the following industry certifications: GPEN, GXPN, OSCP, OSCE, CEPT, eCPPT, or equivalent.

Highly Desired:

- Active TS/SCI Clearance Bachelor's degree in Computer Science or related discipline

Travel up to 30%

- Remote work may be offered

Benefits:

SIXGEN pays 100% of health benefits - Medical, Vision, Dental 401K with 3.5% matching offered

Some training and education may be covered by SIXGEN

Relocation offered if necessary

The salary range is dependent on skills, experience and is negotiable (SIXGEN typically pays above average)

A.11 Cyber Security Specialist

URL: https://www.careers24.com/jobs/adverts/1732454-cyber-security-specialist-cape-town/?jobindex=3

Cape Town

Salary: Market Related
Job Type: Permanent
Sectors: IT
Reference: 20583
Vacancy Details
Employer: DatafinRecruitment
Environment

A rapidly growing UK-based tech company seeks a forward-thinking Cyber Security Specialist to serve as the technical lead of their Cyber Security Operations Centre (CSOC), managing and improving all SIEM and security platforms. You are expected to think beyond a conventional SIEM approach and seek to enhance the security suite to a comprehensive automation and orchestration capability. You will require experience with a variety of SIEM platforms & monitoring tools, EDR, DLP, AV, Snort, Wireshark, TCPdump, working knowledge & experience of core security and infrastructure tech including firewall logs, network security tools, malware detonation devices, proxies, IPS/IDS, a strong awareness of Cyber-Attack techniques & in-depth knowledge of log formats, log transports and log analysis as well as automating log ingestion and normalisation in a SOC environment.

Duties:

- Be a technical lead / SME for the CSOC and SIEM service offering by managing and improving the platforms to meet the requirements of the business and/or client.

- Configure and develop SIEM tooling, and associated tool sets, to deliver effective and efficient SOC services through automation and orchestration, and to improve MTTD and MTTR whilst reducing false positives and negatives.

- Ensure all security platforms are optimised to detect and prevent security threats across all onprem and cloud environments to meet business objectives and regulatory requirements.

- Provide technical oversight and support for the identification, triage and response to events or incidents of a suspicious or malicious nature, and apparent security breaches.

- Work collaboratively with infrastructure teams and key stakeholders inside and out of the business ensuring security and monitoring requirements are determined and implemented through onboarding or continuous improvement activities.

- Actively support the onboarding of new clients throughout the transition to service delivery lifecycle.
- Conduct project activities including planning and execution of changes, documentation, training / skills / knowledge transfer to the team and clients.
- Maintain a continuous understanding of the threat landscape with in-depth knowledge around threat actors, TTPs and vulnerabilities.
- Be a technical mentor to the CSOC Specialists and Analysts, providing technical knowledge and training to the team.

Requirements:

Essential:

- Experience with a variety of SIEM platforms and monitoring tools, configuration management tools, host virtualisation, containerisation, vulnerability scanners, proxies, WAFs.
- Significant experience with intrusion analysis and investigation.
- Demonstrable technical knowledge, skills and/or experience in intrusion analysis, and network and security investigation using a variety of security tools (EDR, DLP, AV, Snort, Wireshark, TCPdump etc.).
- Working knowledge and experience of core security and infrastructure technologies (e.g., firewall logs, network security tools, malware detonation devices, proxies, IPS/IDS).
- Technical experience in a Security Operations Centre, Incident Response Team or similar environment.
- An in-depth knowledge of log formats, log transports and log analysis as well as automating log ingestion and normalisation in a SOC environment.
- Strong awareness of cyber-attack techniques and how protective monitoring systems can be used for detection, mitigation, remediation and protection.
- Awareness of risk management and the ability to contextualise technical issues into business risk relevant to the business and clients.

Desirable:

- Having achieved at least a BSc or MSc in Cyber Security incorporating Ethical Hacking, Digital Forensics or Information Security; OR One or more of the following industry certifications: CEH, GCIA, GCIH, GSEC, Security+, GCTI.

- Experience in secured cloud architectures (Azure, AWS) and engineering solutions.
- Formal experience in Digital Forensics or experience using EnCase, FTK Imager or similar.
- An understanding of multiple operating systems and their programming interfaces such as UNIX Shell and PowerShell.
- An awareness of Cyber Security-related standards and regulations, for example, NIST, CIS, ISO 27001 and PCI DSS.

Attributes:

- Team player.
- Problem-solving.
- Strong communication skills.
- Self-starter who is able to demonstrate excellent customer service and can collaborate effectively.

While we would really like to respond to every application, should you not be contacted for this position within 10 working days please consider your application unsuccessful.

B

Penetration Testing report writing framework

Report writing is an important part of the penetration testing process. After each step of the penetration testing process all findings need to be documented to be able to compile a full report after completion of the penetration test. Penetration testing report writing is discussed in Chapter 2 paragraph 2.3.13.

Penetration testing report writing framework layout

1. Cover page.
2. Table of Content.
3. Executive Summary.
    - Scope of work.
    - Project objectives.
    - Assumption.
    - Timeline.
    - Summary and findings.

    - Summary and recommendations.
4. Methodology.
    - Planning.
    - Exploitation.
    - Reporting.
5. Detail Findings.
    - Detailed system information.
    - Windows server information.
6. References.
    - Appendix.

C

Most used Penetration Testing Tools

Table D1: Most used Penetration Testing Tools.

Tool	Use	URL	Description
Nmap	Network discovery and Security Auditing	https://www.nmap.org	Nmap is a utility for network discovery and security auditing. Can also be used for network inventory, management of service upgrade schedules and monitoring host or service uptime. Nmap was designed to rapidly scan all sizes of networks, giving results such as what hosts are available on a network, what services are active on the host, which operating system the host runs, which packet filters and firewalls are in use (Ferranti, 2018).

Tool	Use	URL	Description
Metasploit/ Armitage	Penetration Testing	https://www. Fastandeasy-hacking .com, https://www. resources. in-fosecinstitute .com	Armitage is a GUI for Metasploit. It has advanced post exploitation features and gives visualization of targets. Can scan specific targets or import data from other security scanners to be used in further attacks. Armitage recommends exploits when executing a Penetration Test and indicates which exploits will work. When a target is compromised actions such as privilege escalation, browsing of files and dumping of hashes (Krishnan, 2012) take place.
John the Ripper	Password Cracking	https://www. openwall .com /john	John the Ripper is a password cracker available for Windows, Unix, macOS, DOS, OpenVMS and BeOS operating systems. Primary purpose is to detect weak Unix passwords but the Pro versions of the software support additional hashes and passwords (Puha, 2019).
THC Hydra	Password Cracking	Due to the THC Hydra url www.htc.org not working any more the tool is still available on https://sectools .org/ tool/ hydra/	Hydra is a remote brute force password cracker. Hydra can perform rapid dictionary and wordlist attacks against multiple protocols including ftp, https, http, telnet, smb and databases. This tool is very flexible with fast performance (Shaheer, 2019).
OWASP Zed	Web vulnerability scanner	https://www. owasp.org/ index.php /OWASP_ Zed _Attack _Proxy_Project	OWASP Zed helps with automatically finding security vulnerabilities in web applications during development and testing. Experienced Penetration Testers use the tool for manual security testing (OWASP, 2019).

Tool	Use	URL	Description
Wireshark	Web vulnerability scanner	https://www. wireshark .org	Wireshark is a network protocol analyzer that enables you to see what is happening on a network at a microscopic level. Wireshark analyze network traffic in real time and is also used for troubleshooting issues on a network (Porup, 2018).
Aircrack -ng	Wireless tools to access WiFi networks	https://www. aircrack-ng.org	Aircrack-ng is a complete suite of wireless tools used to access WiFi network security. Aircrack-ng is used to monitor and export packet data, attack WIFI access points and clients, and to crack WEP and WPA keys (McCauley, 2018).
Maltego	Digital forensic	https://www. paterva .com /web7/	Maltego is an interactive visual data mining tool that renders directed graphs for link analysis. It is used in online investigations to find relationships between pieces of information from various sources located on the Internet. It makes use of a library of plug ins called “transforms” (Sanchez, 2017).
Cain and Able	Password Cracking	https://www. oxid.it /cain.html	Cain and Able is a password recovering tool for Microsoft operating systems. It easily recovers various kinds of passwords by sniffing networks, cracking encrypted passwords making use of Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled password, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols (Mohamed, 2018).

Tool	Use	URL	Description
Nikto	Website vulnerability	https://cirt.net /Nikto2	Nikto is an Open Source web server scanner used to identify security issues on web applications such as potentially dangerous files and programs, outdated versions of servers, version specific problems on servers and server configuration issues (Obbayi, 2018b).
Nessus	Vulnerability scanner	https://www. tenable .com	Nessus is an open source network vulnerability and remote security scanning tool, and uses the common vulnerabilities and exposures architecture when identifying vulnerabilities (Obbayi, 2018a).
Acunetix WVS	Web vulnerability scanner	https://www. acunetix.com / Vulnerability -scanner/	Acunetix Web Vulnerability Scanner crawls your website, automatically analyze web applications and finds dangerous SQL injections, cross site scripting and vulnerabilities exposing you online (Ortega, 2014).
oclHashcat	Password Cracking	https://hashcat .net/ hashcat/	oclHashcat is an open source password recovering and password hacking tool (Balabanov, 2016). According to Balabanov (2016) it is the fastest password cracking tool.
Social Engineering Toolkit	Social Engineering	https://www. trustedsec .com/social- engineer -toolkit-set/	Social Engineering Toolkit (SET) was specifically designed to perform advanced attacks against the human element. The attacks built into the toolkit are used during a penetration test, and are designed to be focused attacks against a person or organization (Son, 2018).