

Institute of Technology Tallaght,
Department of Computing

INDUSTRY PROJECT

‘A project report submitted in partial fulfilment of the requirements for ITT
Dublin’s Bachelor of Science Degree (Honors) in Computing with I.T.
Management’

Table of Contents

Disclaimer

Abstract.....

Chapter 1 - Host Company Background and Strategic Objectives

- 1.0 Introduction
- 1.1 The Structure of the Company
- 1.2 Business Objectives
- 1.3 Key Business Processes
- 1.4 Role of IT
- 1.5 Strategic Challenges

Chapter 2 - Critical Evaluation of Work Undertaken at the Host Company

- 2.0 Roles
- 2.1 Work Undertaken
- 2.2 Work and College
- 2.3 Critical Evaluation

Chapter 3 – Mini Project.....

- 3.0 Introduction
- 3.1 Penetration and/or (Ethical) Hacking Explained
- 3.2 Kali Linux – Installation & introduction
- 3.3 Kali Linux – Pen Testing & Hacking Tools
- 3.4 Kali Linux – Analysis
- 3.5 Kali Linux – Other Opinions & Reviews

Chapter 4 – Mini Project - Conclusions & Recommendations.....

- 4.0 Introduction
- 4.1 Conclusions
- 4.2 Recommendations

Bibliography.....

Appendices.....

- Appendix A
- Appendix B

Disclaimer

The material contained in this study is intended to provide general information and should not be relied upon as professional advice.

It is illegal to perform Penetration and/or Hacking on any company, software, website, network, institute, etc without the permission of the owner. **Do Not** attempt to implement or recreate any of the tests carried out in this study!

This paper represents the opinions of the authors. This paper is the result of the analysis carried out within 'All n One -Bxp Software'. However, it is not meant to represent the position or opinions of 'All n One -Bxp Software', nor the official position of any staff members. Interviews in this paper are the opinions of the individual in question and were conducted with the permission of the individual. Any errors are the fault of the authors.

Abstract

This project studies the theory that the high availability of free and open source Penetration and Hacking tools, is both an advantage and disadvantage to the host company.

In this project, to examine the theory stated above, a free and open source operating system named 'Kali' and the tools included, were tested in a live industry environment in order for any results found to be as accurate as possible.

This project should be of interest to anyone involved in the area of Information Security, Quality Assurance, Information Technology, Ethical Hacking and any business owner involved with or within I.T.

The Industry Project has provided me with practical experience of undertaking a relevant IT project in Information Security. It has also endeavoured to integrate the academic content and practical skills acquired throughout the program with the industry environment. Furthermore, it has aided in the development and enhancement of my problem solving, interpersonal and communication skills in the context of an organization.

Chapter 1 - Host Company Background and Strategic Objectives



(BXP, 2018)

1.0 Introduction

The host company I am doing my internship in is 'All N One – Bxp Software'. All N One is a software company that supplies a tool called Bxp that helps businesses run better. The internship position I have taken is a Junior Information Security Manager. My internship with All N One – Bxp Software is for six months.

All n One was founded in 2005 by Nick Wheeler, Chris Thomson and Philip Lacey. Philip presented to Nick and Chris an idea for software that could “largely improve contact centre operations and could be very profitable.”

From 2005 to 2008, All n One ran and operated a contact centre using Business Express (BeX) which has now become BXP software. The software completed its alpha and beta release cycles and was first sold externally to the Response Interaction Centre and Conduit in October 2008. In 2008, Business Express was entered in the Contact Centre Management Association awards and won "Best New Product or Service in the Contact Centre Industry" award.

“Since 2006, All n One have tried to give back to education and giving people opportunities in life to learn and grow. All n One has operated a successful internship program which has given great starts to people in education and continues to do so.” (Lacey, 2018)

1.1 The Structure of the Company

All N One, like their software Bxp, is modularized, which means, each department is responsible for different aspects of the company. 'All N One – Bxp' work with a number of partners and suppliers to help the business build and grow.

- C.T.O – Philip Lacey

Philip Lacey is the Chief Technical Officer at All N One – BXP Software. Philip's departments include Projects, Learning and Quality Assurance.

- C.E.O – Nick Wheeler

Nick Wheeler is the Chief Executive Officer at All N One – BXP Software. Nick's departments include Sales and Business Development.

- C.O.O – Chris Thomson

Chris Thomson is the Chief Operating Officer at All N One – BXP Software. Chris's departments include Sales, Business Development and Marketing.

- Key Accounts Director – Aiden Rice

Aiden Rice is the Key Accounts Director at All N One – BXP Software. Aiden's departments include Sales and Business Development.

- Ops Manager – Patrick Jenkins

Patrick Jenkins is the Technical Operations Coordinator and Senior Projects Developer at All N One – BXP Software. Patrick's departments include Projects, Development and Coordination.

- Development – Meabh Landers

Meabh Landers is the Senior Content Developer at All N One – BXP Software. Meabh's departments include Content and Development

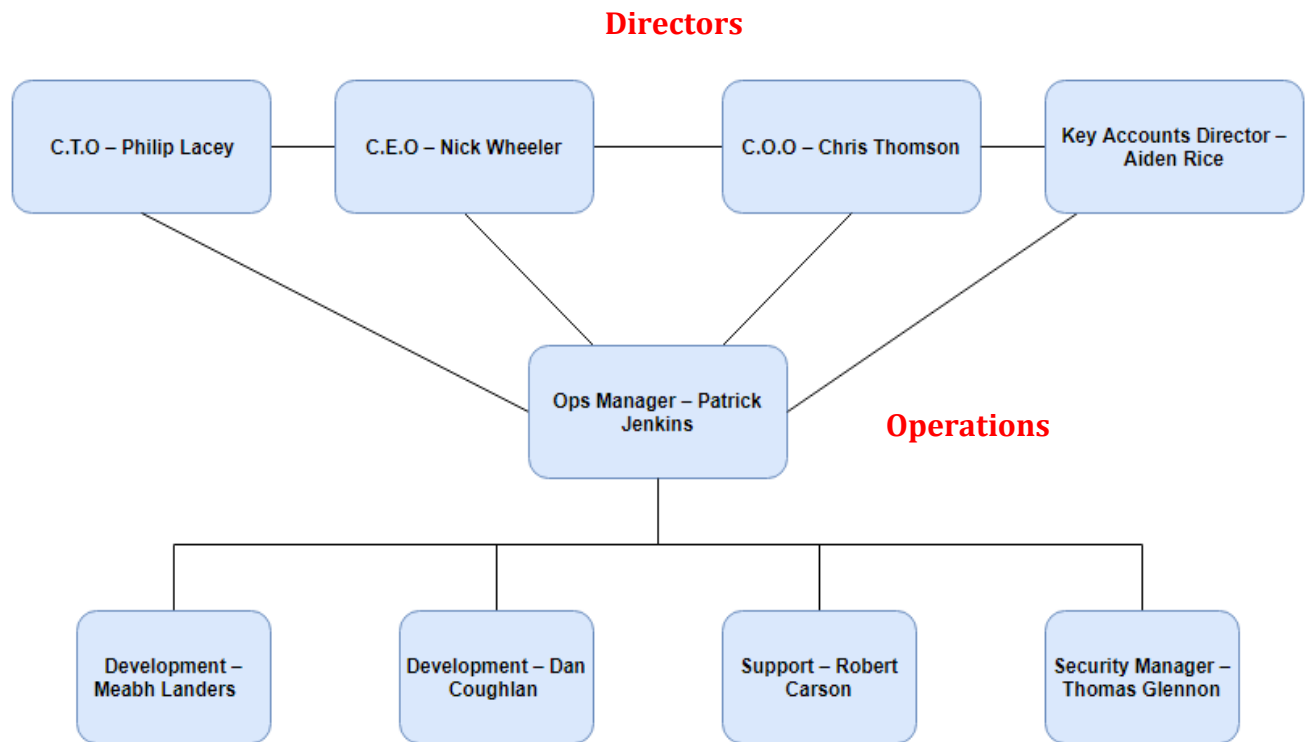
- Development – Dan Coughlan

Dan Coughlan is the Senior Framework and Full Stack Developer at ALL N One – BXP Software. Daniel's departments include Framework and Development.

- Support – Robert Carson

Robert Carson is the Jr. System Architect All N One – BXP Software. Robert's departments include Contact, Support and Quality Assurance.

- Chief Information Security Officer (CISO) – Thomas Glennon
Thomas Glennon is the IT Security and Infrastructure Manager at All N One – BXP Software.
Thomas's departments include Security and Infrastructure.



(Cooke, 2018)

Staff

1.2 Business Objectives

“All N One – BXP own and distribute and develop Business Express (BXP), a specialist software solution providing a range of award-winning CRM, Contact Centre Management, eLearning and Quality Assurance tools aimed at maximizing efficiency and profitability.” (Jenkins, n.d.)

“They tailor-make web-based software for a range of blue-chip clients in the areas of BPO’s leisure & gaming, telecoms, utilities and financial services and will have a relevant and profitable solution for your challenge.” (Jenkins, n.d.)

All N One – BXP has two primary business objectives.

- Bxp the Software
- All N One the consultancy arm

Bxp the software is an engine on which business processes can be tailor-made. Bxp enables staff with no technical abilities to design, build, operate and refine processes without the need to have dedicated technical skills such as computer programming.

With the experience and technical knowledge gathered over a decade, All n One can provide support in all areas and are there to help and consult.

1.3 Key Business Processes

As Bxp is a modular software solution, every process offers tools of related functionality. These processes are grouped into pillars for ease of concept. Each Process and pillar can run isolated or integrated of each other.



(Lacey, 2016)

- **Contact Management**

Customers will communicate with a business through a number of different ways such as email, phone fax, SMS, MMS, website, social media or post. Bxp has a tool that I developed to be able to handle all forms of communication and provide a unified display of the communications.

“Contact management is an application that allows users to easily locate and save contact information, including names, telephone numbers and addresses.” (techopedia, 2018)

- **Customer Relationship Management**

Bxp has tools to help with Customer Relationship Management. Once incoming contacts have been managed, a company then wants to proactively keep in touch with clients and customers.

“Customer Relationship Management (CRM) is a strategy for a business to manage its interactions with its customers. A CRM system is an essential tool for business that helps you manage your customers, sales and marketing.” (Systems, 2018)

- **ELearning**

It is important for a running business to make sure that staff is trained and familiar with processes and procedures. This training and documentation can be provided with a suite of tools in Bxp.

“eLearning is a learning system based on formalized teaching but with the help of electronic resources. The use of computers and the Internet forms the major component of E-learning. E-learning can also be termed as a network-enabled transfer of skills and knowledge, and the delivery of education is made to a large number of recipients at the same or different times.” (times, n.d.)

- **Quality Assurance**

Quality Assurance is provided by tools in Bxp for any process, computer or real-world based operational improvement.

“Quality assurance (QA) is any systematic process of determining whether a product or service meets specified requirements. QA establishes and maintains set requirements for developing or manufacturing reliable products. A quality assurance system is meant to increase customer confidence and a company's credibility, while also improving work processes and efficiency, and it enables a company to better compete with others.”

1.4 The Role of IT

The department I work in is Information Security and Administration. The objectives of my placement in the organization is to assist in day to day running of the business, learn new skills and get to experience what it is like to work in the IT/ Information Security & Administration Industry.

The role of IT in IT Security is responsible for protecting networks, infrastructure and systems for a business or company. IT enables Security to protect computer systems by creating barriers deterring external access to them, locate problems within systems by identifying uncharacteristic activity, monitor current situations with the network security and carry out audits and reports and develop improvements where needed and keep the users informed by completing performance reports regularly to communicate the status of the system security.

Administration provides the ability for the business and products provided to run both internally and externally. As an IT Administrator, you are responsible for making sure networks, security systems and servers are constantly maintained. The administration is essential for a company to ensure business continuity. For example, if a network was to fail the impact could be catastrophic for the running of the business.

My role supports both directly and indirectly with the objectives of the business. Although I am not programming, creating or selling the software, I am assisting in providing the security and Administration for the businesses integrity as well as the software's integrity. The role of the Security and Administration team allows the business to stay safe, secure and meet standards which then provides evidence for customers to see that the company has all the necessary requirements to be trusted, (Quality Assurance). However good the physical software may be, the security aspect provides assurance in areas such as data protection and data integrity which is extremely valuable to clients.

In my role, I have performed tasks such as penetration testing, system and server maintenance, reporting, scripting/ coding and network troubleshooting. These tasks have been both direct and indirect in supporting the objectives of the business.

Penetration testing is a procedure which aims to discover security vulnerabilities, flaws and unsafe environments. Penetration testing is or can be seen as a successful but not harmful way to hack a specific system. Penetration testing recreates activities and steps cybercriminals would take in an attempt to compromise said systems.

Penetration testing allowed me to create a report of my results. This report can be used to provide assurance that the companies systems are reliable. A company with proof of

reliable systems is more likely to be chosen for business. Penetration testing is an indirect task in supporting the objectives of the business.

System and server maintenance is a procedure which aims to monitor systems and servers in a company. This can be done both remotely and locally. System and server maintenance ensures that all computer systems, information systems and servers are running and up to date. This is important for business integrity.

System and server maintenance support directly with the business objectives as it allows the Bxp software to be available 24/7.

Reporting can benefit businesses to increase understanding of risks and opportunities by highlighting the links between non-financial and financial performance in all areas of a company including IT.

Some of the reports I had to do link with my other tasks including penetration testing and administration. These reports allowed for creating long-term management strategies, reducing costs, preventing failures and streamlining processes.

Reporting in my department supported indirectly with the business objectives.

Scripting is a programming method in which a list of commands is written to be executed without user interaction.

The scripts I wrote supported directly with business objectives as it was designed to retrieve information for monitoring purposes.

1.5 Strategic Challenges

Strategic Challenges is the term that refers to pressures that an organization faces in relation to future success. These challenges can be both internal and external. External Challenges may relate to the current market need, expectations or customer need.

New strategic challenges are always developing in the Information Technology sector due to technological advancements and rapid growth of the industry.

Strategic challenges are faced by all companies, during my internship I have seen and experience challenges and ways my host company has tried to deal with them.

Due to NDA, there are some challenges I cannot discuss in this document.

Here is an example of some more general strategic challenges I have seen in the Information Technology industry.

1.0 GDPR – General Data Protection Regulation

Companies need to make sure they are GDPR compliant as legislation becomes more strict and wide-ranging.

2.0 Agility

Companies need to keep up to date with the ever growing and changing IT industry and stay agile to compete.

Chapter 2 - Critical Evaluation of Work Undertaken at the Host Company

2.0 Roles

My role in my internship was an IT/ Information security intern. In this internship position, I was working alongside the Senior Information Security Officer/ Chief information security officer (CISO).

A chief information security officer (CISO) is the head of IT security within an organization. The chief information security officer aims to enforce the IT security strategy and implementation in order to protect the business from potential threats such as cyber-crime. A chief information security officer must ensure compliance is met to all ISO and other standards and regulations.

Some of my responsibilities as an information security officer including:

- Running security audits and risk assessments.
- Managing the daily operation and implementation of the IT security strategy.
- Ensuring compliance and governance is met.
- Protecting the intellectual property of the organization at all times.
- Devising strategies and implementing IT solutions to minimize the risk of cyber-attacks.
- Reporting to the board and being an active member working with the senior management team.
- Conducting a continuous assessment of current IT security practices and systems and identifying areas for improvement.
- Monitoring security vulnerabilities and hacking threats in network and host systems.
- Managing the IT security team.
- Tracking latest IT security innovations and keeping abreast of latest cybersecurity technologies and threats.

In my internship, I was also working in some infrastructure roles as these coincided with the information security position. The responsibilities included:


- Install and configure software and hardware
- Manage network servers and technology tools
- Set up accounts and workstations
- Monitor performance and maintain systems according to requirements
- Troubleshoot issues and outages
- Upgrade systems with new releases and models
- Build an internal wiki with technical documentation, manuals and IT policies.

2.1 Work Undertaken

In my role in my internship the work that I have undertaken has included tasks such as Penetration Testing/ Ethical Hacking, installing SSL Certificates, setting up Squid Proxy Servers/ Ubuntu LAMP Servers, Server Administration, maintenance, reporting, encrypting drives, working with Active Directory/ Windows Server Manager, working with Kali Linux and Scripting.

The Penetration Testing and Ethical Hacking I performed was designed to test the host companies infrastructure, ie. How vulnerable that they would be to different forms of cyber-attacks.

I tested the companies Infrastructure using Kali Linux to show potential areas of vulnerabilities. I then created a report with the information I had obtained. Once this report was reviewed, I discussed with the security team how and why these vulnerabilities were found and what we could do to improve security. This information and reports can be also used to show clients the methods and strength of the company's security and this can provide guaranteed assurance.

An SSL Certificate is a small data file that binds a crypto key to the details of an organization when it is installed on a web server. When a web page is searched on Google, a site using SSL certificates will look like this:  Secure |

To install these SSL certificates on my host companies web servers I used command line software called Win Simple to obtain a certificate from a Certificate Authority (CA) called Lets Encrypt.

In my placement, I had been assigned tasks to set up a Squid Proxy Server and an Ubuntu Server with LAMP.

“Squid is a type of caching and forwarding HTTP web proxy.” (Squid, 2013) A proxy server is a server that acts as an intermediary between a user and the internet, thus allowing a user to make an indirect connection to outside networks. This can be used for people such as admins to connect to sites other general users are blocked from using. The LAMP is a web development platform that uses Linux as its OS (Ubuntu), Apache Web Server, MySQL as the Database Management System (DBMS) and PHP as its Object-Oriented Scripting Language.

I performed some administration tasks while working with my host company. These tasks included monitoring the Databases and Web servers, encrypting new drives using BitLocker, working with Active Directory and Server Manager to manage the domain and networks and I also performed some scripting in Python and PowerShell to do some administration tasks. I also had the opportunity to work with and learn VBScript.

2.2 Work and College

Before I started my placement with my host company I felt that work and college wouldn't have much of a relationship and if any, only small connections. But as the weeks went on and even from my very first day I began to see there were more connections than I had expected.

There were a lot of things I came across in the placement that triggered my mind to something I had learned while in my college modules but not really thought of or understood in much detail.

Most of the modules I have done in college have really helped me with my placement. From Networking to Databases, to Information Security. All of the modules really helped me understand aspects of tasks and difficulties I faced or witnessed in the placement.

I feel that my work placement has helped me to learn better and get a better understanding of things that I am learning in college. Because of the hands-on approach and because I am seeing real-world examples it makes complicated aspects easier to grasp, whereas in college sometimes even if you try to study complicated things it does not clear them up entirely.

Some modules I think were key or related most to my position:

- Information Security
- Networking
- Advanced Databases
- Database Administration
- Scripting & Automation
- CS&DC
- Operating Systems

2.3 Critical Evaluation

In conclusion, I think that the internship was a very important part of my college learning experience. It has given me the opportunity to get a better grasp on the modules I am learning and the skills I am trying to develop.

The internship has also given me further insight into the area I would like to work in when I am finished college. This area would be preferably Information security.

I have learned a lot of new skills as well as improving and bettering the skills I currently have.

Some skills & competencies I learned or developed in my placement:

- Penetration Testing/ Ethical Hacking
- System Administration
- Team Leadership & Team Work
- Implement and support professional and legal aspects of IT management
- Quality Assurance
- Select, implement and manage local and wide-area networks
- Install and administer a server
- Scripting
- Networking
- Write Reports
- Communicate effectively with professionals in the field of computing management and information systems
- Work independently on projects with clearly defined objectives
- Operate in a professionally responsible and ethical way
- Take responsibility for work and presentation of results

Chapter 3 – Mini Project

“A Study of the Benefits and Downsides of the Availability and Ease of Use of Penetration and (Ethical) Hacking Tools to the Host Company.”

3.0 Introduction

This project will look at the positive and negative factors in relation to the highly available and easily used Penetration and (Ethical) Hacking tools that currently exist. In this study, I will look at a ‘Linux’ Distribution for Pen testing and hacking called ‘Kali’.

In this study, I will look at how easy it is to access and install ‘Kali’. I will study and review some tools within ‘Kali’ that I have used in my current work placement in Information Security and tools that could be of relevant use or danger to my host company. I will also look at what sort of information can be revealed using these tools and how this information and these tools can be useful or harmful to my host company or other organizations.

I have chosen to do this study as my project as IT Security is an area I am highly interested in and am currently participating in an internship in this area. I first came across Penetration and (Ethical) Hacking tools in my Information Security module in college. Although we had only tried some basic network scans and computer access on a virtually simulated network, I obtained a sense how easy these tools were to use to get a broad range of potentially dangerous information. After this experience, I decided to do my own research outside of college. This is where I gained more of an interest and understanding of what could be possibly done, both for ethical hacking and non-ethical hacking reasons.

Now that I am in an internship I have decided to take my interests and investigate further. By completing this study I hope to outline to and educate companies such as my host company that these tools exist and can be both dangerous and beneficial to security and also can provide a cheaper or even free solution to Security Auditing, thus lowering the need to outsource these tasks which can be very costly.

I would like to thank Thomas Glennon for his participation in this study. I would also like to thank ‘All n One -Bxp Software’ for allowing me to complete this study within the company.

3.1 Penetration and/or (Ethical) Hacking Explained.

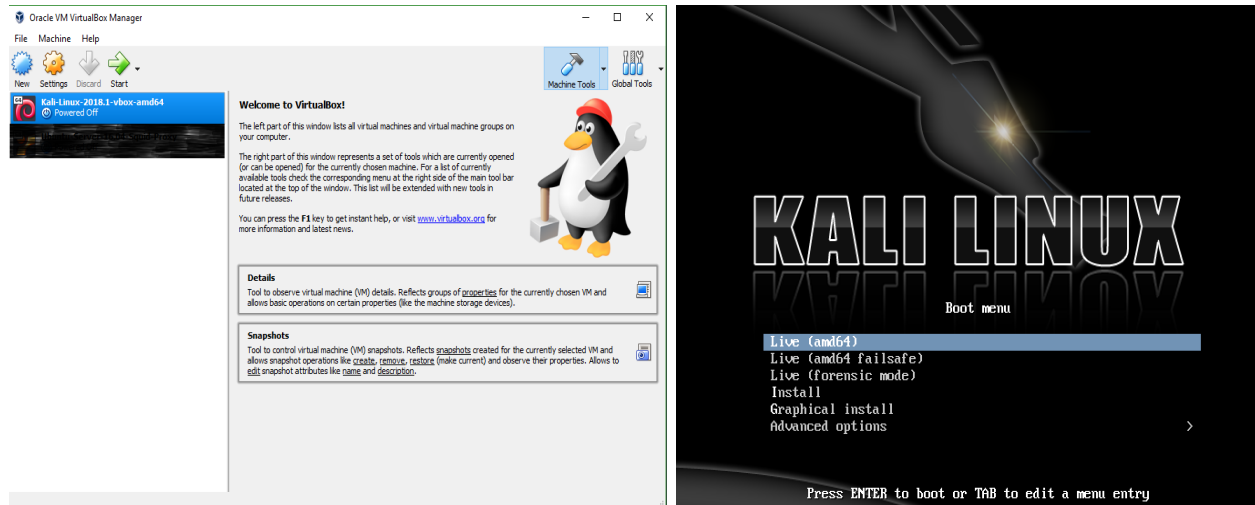
“Penetration testing is a formal procedure aiming at discovering security vulnerabilities, flaws risks, and unreliable environments. In other words, penetration testing can be seen as a successful but not damaging attempt to penetrate a specific information system; mimicking activities cybercriminals would engage in with the intention to compromise this system.” (Kostadinov, 2016)

“Ethical hacking is an all-embracing term that includes all hacking methods, and other related cyber-attack methods. Some people disagree with hacking being considered “ethical” in any way. They deem that the word “hacker” in the term “ethical hacker” is added to attract more people to training programs and courses. For that reason, among other things, these people would prefer not to associate this term with them.” (Kostadinov, 2016)

3.2 Kali Linux – Installation & introduction

‘Kali Linux’ comes with everything installed such as packages that can be updated. ‘Kali’ is designed based on ‘Debian’ and is a complete operating system in itself. ‘Debian’ is a free operating system that uses the Linux kernel.

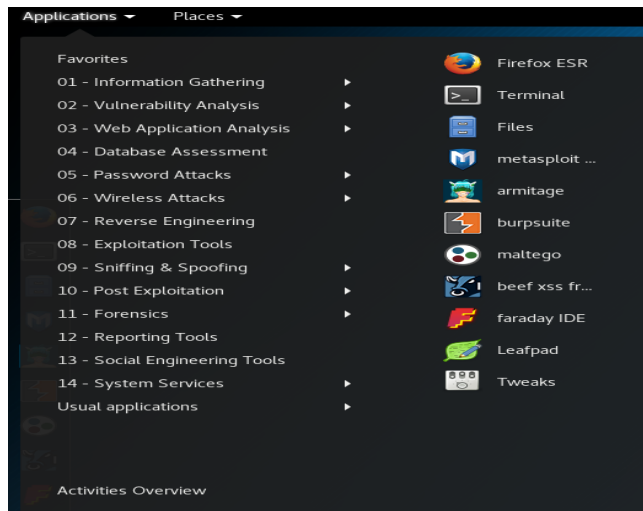
‘Kali’ is easy to install. In my case, it was installed inside a virtual machine using ‘Virtualbox’. ‘Kali’ provides a boot menu with the options for a graphical or text-based installer. The graphical installer is easier for inexperienced users.



The install is just a case of following the instructions and it should work without any problems.

In the event a user was experiencing problems or had never worked with ‘Linux’ before there are large amounts of resources available on the internet, such as YouTube, forums, blogs etc., to show you how to install and set up ‘Kali’ or fix any problems you may have.

By default, 'Kali' comes with an abundance of security tools, all of which are easily located in the GUI (Graphical User Interface). Any tool can be run from the command line terminal.



'Kali' categorizes its tools according to relevance. For example, categories include; Database Assessment, Vulnerability Analysis and Reporting tools. There is also a separate list of the top 10 tools.

The top 10 tools list is the most popular, most useful and most featureful tools on 'Kali Linux' that are related to hacking, penetration testing and security.

3.3 Kali Linux – Pen Testing & Hacking Tools

In this section, I will list, describe and give my review of some of the tools within kali that I believe could be an advantage and/ or disadvantage to my host company.

I have studied and tested the tools in this section with the permission of my host company.

- **Maltego – Information Gathering**

Maltego is an open source application used for intelligence and forensics. Maltego offers you in-depth mining and gathering of information as well as the representation of this information in a format that is easy to understand.

Essentially, Maltego is an information gathering tool that uses the internet to search for publicly available information about any given site or organization.

I chose this tool to test since information and data is quite a topical area in information security at the moment due to the new General Data Protection Regulations (GDPR) coming into place.

Maltego is very easy to use. There is also an abundance of tutorials on the internet available that even the most inexperienced user could follow.

On testing it, without the initial help of tutorials, it was quite easy to use, to begin with.

For example, if an attacker was to use this software to find potential company information like something as basic as a person's name, Maltego can enable them to mine information based off that. This could reveal email addresses to start, leaving people vulnerable to phishing emails.

For my host company or other businesses, tools like Maltego can be used to identify loopholes or vulnerabilities in their security, storage or processing of data. This could also save them from facing huge fines from the Data Protection Commissioner and loss of clients and customers.

Maltego was not the most dangerous tool available in 'Kali' but I definitely would recommend it as an advantageous tool to someone working in the area of Information Security and currently trying to deal with the pressure of being GDPR compliant.

- **Nmap – Port Scanner**

Nmap is one of the oldest and the most powerful port scanning tool there is. Although it started out as a port scanner, it is capable of doing much more than that. Nmap can scan large network areas for live hosts, port scan the discovered hosts, get the daemon banners and get detailed information about the host including operating system etc.

Nmap now includes a new feature called Nmap scripts which allows developers to write scripts that can be used along with Nmap to automate specific types of scanning tasks.

Nmap has a GUI (graphical user interface) called Zenmap. Zenmap can be used to save previous scan settings as profiles and use them again. Nmap also includes a Netcat type utility called Ncat which is a very featureful tool that is available for both Windows and Linux.

I chose this tool to test as in my role in my internship I worked around a lot of servers and other network equipment.

Nmap was another tool that was easy to use, especially due to the Zenmap GUI, with a huge availability of tutorials and resources to help you learn and use Nmap to its full potential.

I was able to run some basic network scans that would show me open ports on any specific network. I was able to run these scans and have the output saved in a notepad document that was easy to read and implement into reports if necessary.

This tool is useful when trying to locate potential vulnerabilities in new servers I had set up for tasks like SFTP forwarding (Secure File Transfer Protocol) on specific ports.

One dangerous aspect was my ability to network sniff and run scans that would allow me to go undetected or to spoof addresses on the same network. This could be used for “man in the middle” attacks. But again discovering vulnerabilities for a business is extremely important as it allows you to be as secure as possible.

- **Owasp Zap – Web Application Testing**

The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

The Zed Attack Proxy can be used to ping/poke/attack web applications in a number of ways to discover security flaws like SQL injection, XSS (Cross-Site Scripting), CSRF (Cross-site request forgery) etc in them.

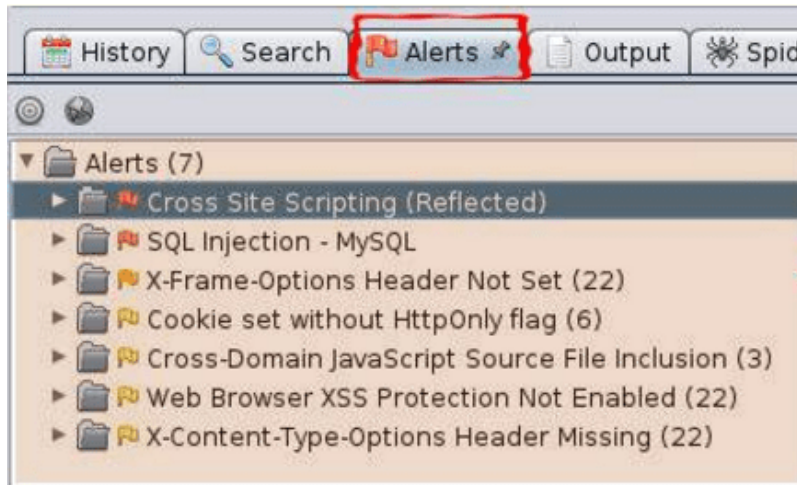
Owasp ZAP is a free and open source and led by Owasp.

I chose to test Owasp ZAP as the host company where I am working, develops cloud-based software.

ZAP was easy to use and had a user-friendly GUI. As with all tools in ‘kali’, you will find a tutorial or answer any question or problem you have.

By telling Zap the address of the target site, ZAP will limit the scope of the scan and only scan the target site for its vulnerabilities. ZAP will also allow you to generate and save a report.

Zap will give you a list of vulnerabilities in an alerts tab.



(Picture for example only. Does not reflect the vulnerabilities of any specific application)

This is extremely advantageous to businesses. You can easily find vulnerabilities in your web applications before they go live.

ZAP is also very dangerous. It is easy to access and easy to use. The least experienced user with intent to attack could easily perform some very dangerous attacks. **It is illegal to perform such scans or attacks without the consent of the site owner.**

I could not see any reason that developers, functional testers or security experts would not use Zed Attack Proxy. It is a great tool backed and provided by a highly commendable organization.

- **Sqlmap – Automatic SQL Injection**

Sqlmap is an open source penetration testing tool. Sqlmap automates the process of detecting and exploiting SQL injection flaws and taking over database servers. Sqlmap comes with a powerful detection engine, many features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system.

Sqlmap is one of the most infamous hacking tools of the century. Sqlmap allows anyone to hack and destroy any website that forgot to escape its SQL queries properly. It's a completely automated exploitation tool for SQL injection vulnerabilities. Most of the

websites being hacked today have this tool behind the scene. It puts the hacker in complete control of the entire database of any web application.

I chose to test Sqlmap because it is one of the most powerful and most popular SQL injection automation tool available. It can also be used alongside some of the other tools I have tested such as Owasp ZAP.

Sqlmap was one of the more advanced tools that I used. Although it is very easy to learn how to use it if you are familiar with using the command line. Again there is more than plenty of tutorials and information online that could help you with any problems or specific tasks you would like to undertake.

Sqlmap is both advantageous and disadvantageous to businesses. It is a tool that is crucial to have for any company task has any web applications or is developing for the cloud.

The disadvantage is the danger that this tools can provoke with very little effort or knowledge.

- **Metasploit - Develop, maintain and launch exploits**

Metasploit allows you to safely simulate attacks on your network that may be used to uncover vulnerabilities in security, test security controls, verify defences in place, monitor mitigation implementations, audit web applications and control exposure to fishing.

Metasploit can be run on the command line or on its GUI named Armitage. This makes it usable for any experience level user.

I have chosen Metasploit as another test vector as it is a very professional tool. In industry, Metasploit would be ideal for testing exploits in a safer less aggressive environment than most other tools that I examined.

Metasploit also contains a huge library of exploits and you can even create your own. This can be an advantage and disadvantage to both businesses and Hackers.

3.4 Kali Linux – Analysis

In this section, I will discuss the results of this study of the “Benefits and Downsides of the Availability and Ease of Use of Penetration and (Ethical) Hacking Tools to the Host Company” and analyze the results.

In this study, I tested the tools available within the free and open source ‘Linux’ operating system called ‘Kali’.

The tools used were chosen as most relevant to my host company in terms of both Penetration testing they may want to carry out or potential hacking threats to my host company.

The specific tools chosen were:

- Maltego.
- Nmap.
- Zenmap
- OWASP ZAP
- Sqlmap
- Metasploit
- Armitage

In the case of each of these tools, I was able to use each one of them and get some information from test environment scenarios.

I would consider myself to be an advanced computer user and have experience using Linux and the command line. Even so with the number of resources available online and the user-friendly Graphical User Interfaces (GUI), it would not take long to figure out how to use these tools for Pen Testing in industry or hacking for the criminal benefit.

So here’s what I found.

- Maltego – Information Gathering

When using Maltego, I created a test target. By giving the name of this test target I was able to reveal multiple email addresses that could be potentially linked to this test name. I did not go any further as I know only one of the emails belonged to my test case. I cannot show results of this due to privacy and security issues.

This result shows that private data can become very accessible with very little effort. It also can allow companies to become aware that they may be subject to fishing or other scam emails and therefore can put filters and restrictions in place to limit these sorts of attacks.

I also believe that Maltego can highlight major GDPR issues.

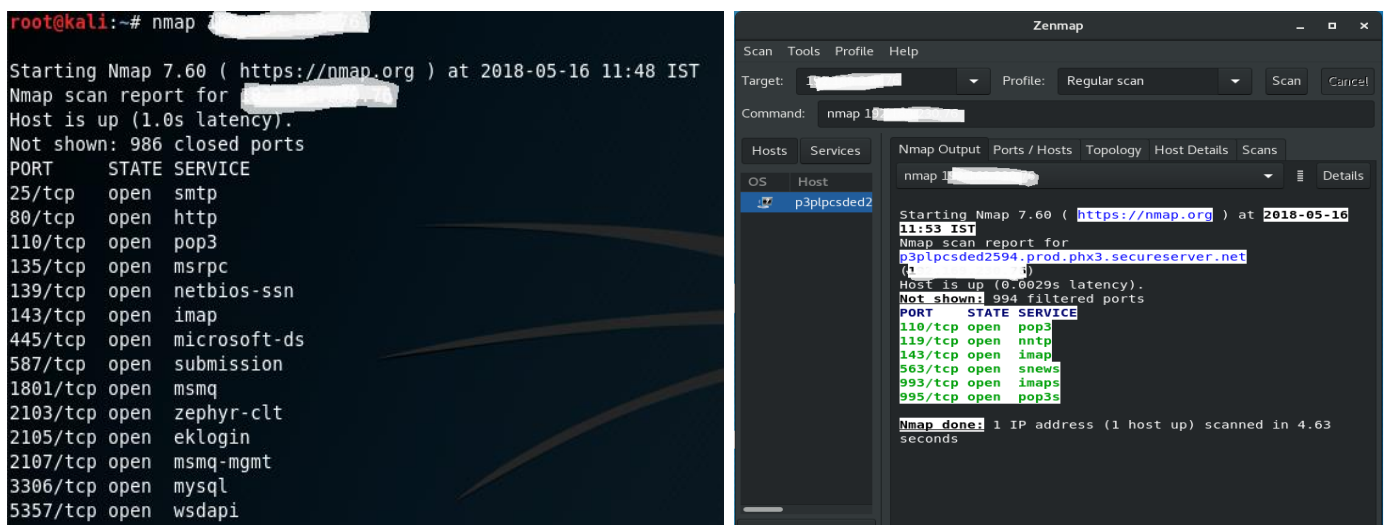
- Nmap – Port Scanner

When using Nmap and Zenmap I found that it was a great tool for examining port security. From the perspective of an Information Security position or even Infrastructure this tool is great for network security with its thorough scanning capabilities and reporting features.

It is most definitely a dangerous tool for hacking as it can help “Hackers” just as much as it can help companies.

In this test case, I targeted a test server with multiple different scans and recorded my results with the reporting feature.

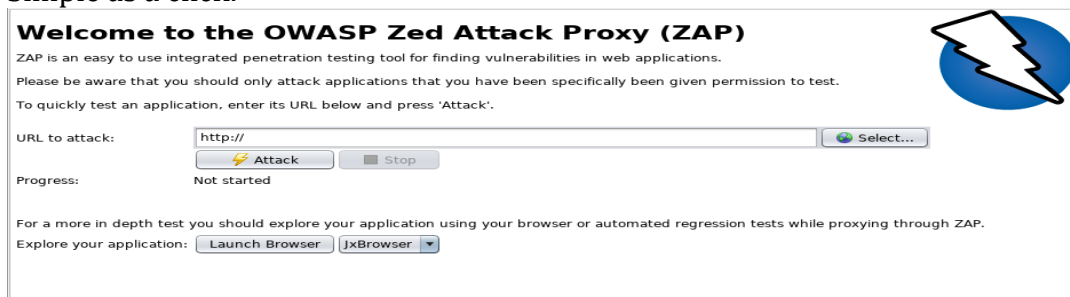
These images below were for example purposes only and were not in any way intense scans or revealing too much but it is revealing information that could be useful to both companies and ‘hackers’.



- Owasp Zap – Web Application Testing

When testing OWASP ZAP, I used a test instance of a web application. As this web application was for demo purposes it had previously been tested and debugged so I did not find any vulnerability in my results. Although there are websites available publicly, which are designed to be vulnerable to learn how to use this software.

Simple as a click:



- Sqlmap – Automatic SQL Injection

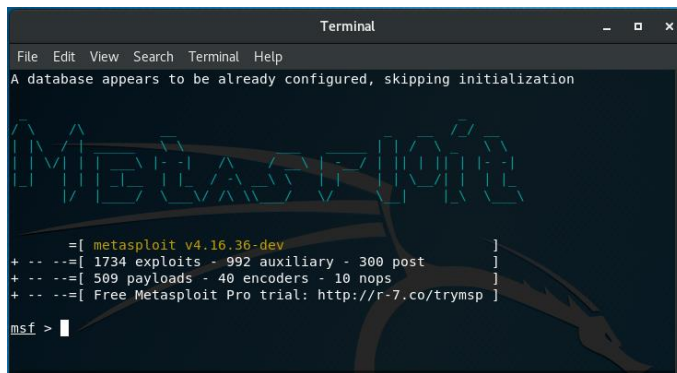
Like OWASP ZAP, testing Sqlmap was difficult due to the severity of its abilities. Again for this test case, a test environment was used.

A simple command “sqlmap -r example-sqlmap-example.req --threads=10 -b”, displays the web server, backend database web technology and the system OS.

- Metasploit - Develop, maintain and launch exploits

Metasploit itself was essentially a test environment in itself. It was highly useful for learning penetration testing and hacking.

The tests that I performed for Metasploit were based on those of which Information Security or Quality Assurance in my host company would perform.



I was able to use Metasploit to look for possible exploitable issues in a testing environment. I was able to also search Through Armitage for recently found or existing exploits in their library of exploits.

3.5 Kali Linux – Other Opinions & Reviews

For this section, I have interviewed and asked the opinion of an Information security expert on the topic of this study.

Thomas Glennon is the Infrastructure and Security Manager at 'All n One -Bxp Software'.

The interview questions and answers were as follows:

What is your opinion on the availability and 'Ease of Use' of Pen testing and hacking tools?

Have you used them?

"Yes, obtaining these tools can be done through a quick google search of hacking tools. I used Kali Linux as a base to understand and utilize hacking tools. There is defiantly an initial fear of unfamiliarity for the tools due to jargon and code requirements, But I stuck with it. At the start, YouTube became my education. This was because you could follow step by step a process and see how it's actioned. It provides a greater understanding of what a tool can do. It also breaks the unfamiliarity with the tool as you can in most cases follow the steps and action the attack yourself." (Glennon, 2018)

What are the pros and/or cons or these tools?

Pros:

"Learning a using these tools allow you to see how insecure certain systems are. This only leads to the promotion of increased security. " (Glennon, 2018)

Cons:

"A company who does not take IT security seriously can be exposed by simple hacks that anyone with interest could do." (Glennon, 2018)

Do you think they are useful in the industry?

"Although it's hard for people to grasp the gravitas of how important IT Security is, New legislation like GDPR is causing a stir with the upper management tiers of businesses who wouldn't have considered data security as a priority." (Glennon, 2018)

"This creates a push for vulnerability scans and data protection officers. The tools are just as good for hacking as they are to protect a company from various vulnerabilities they would have been unaware of." (Glennon, 2018)

Do you think they present a danger to businesses?

“No. I think they present an opportunity for a business to find and solve a flaw they may have. It can present danger if a business does not take IT security seriously.” (Glennon, 2018)

Would you recommend using them?

“Of course! The education value it can provide to you is paramount. Even for the tools I still do not fully understand today. I intend on learning their functionality and thus will allow me to secure ‘All n One’s’ software further!” (Glennon, 2018)

Chapter 4 – Mini Project - Conclusions & Recommendations

4.0 Introduction

This chapter will outline and discuss the conclusions and recommendations found when carrying out this project.

The Industry Project has provided me with practical experience of undertaking a relevant IT project in Information Security. It has also endeavoured to integrate the academic content and practical skills acquired throughout the program with the industry environment. Furthermore, it has aided in the development and enhancement of my problem solving, interpersonal and communication skills in the context of an organization. This project looked at the positive and negative factors in relation to the highly available and easily used Penetration and (Ethical) Hacking tools that currently exist. In this study, I will look at a 'Linux' Distribution for Pen testing and hacking called 'Kali'.

In this study, I looked at how easy it is to access and install 'Kali'. I studied and reviewed some tools within 'Kali' that I have used in my current work placement in Information Security and tools that could be of relevant use or danger to my host company. I also looked at what sort of information can be revealed using these tools and how this information and these tools can be useful or harmful to my host company or other organizations.

4.1 Conclusions

In this section, I will discuss the conclusions that I have gathered from the results of the study of the "Benefits and Downsides of the Availability and Ease of Use of Penetration and (Ethical) Hacking Tools to the Host Company".

Installation & introduction

My conclusion of the installation of 'Kali' was that it was quite an easy and accessible process. Whether you have no experience at all or are an IT professional, installing 'Kali' is not very challenging or difficult to get running and I believe this makes it an ideal user-friendly software. You can also find an abundance of guides and materials to set up 'Kali' and have it running in no time regardless of if you're installing it on a VM or a standalone workstation.

By default, 'Kali' comes with an abundance of security tools, all of which are easily located in the GUI (Graphical User Interface). Any tool can be run from the command line terminal or can be run by clicking on the application as you would on your regular windows machine.

'Kali' is laid out and designed in a way that you will find exactly what you want to work on, as 'Kali' categorizes its tools according to relevance. For example, categories include; Database Assessment, Vulnerability Analysis and Reporting tools. There is also a separate list of the top 10 tools.

Pen Testing & Hacking Tools

The tools tested were chosen as most relevant to my host company in terms of both Penetration testing they may want to carry out or potential hacking threats to my host company.

The specific tools chosen were:

- Maltego.
- Nmap.
- Zenmap
- OWASP ZAP
- Sqlmap
- Metasploit
- Armitage

In Conclusion, Again just like the 'Kali' OS, I found that each of these tools was very easy to use with little knowledge, had plenty of resources available for instruction and also with some learning and research you could create validly and in-depth Penetration Tests or simulate cyber-attacks.

From the findings of this study, my belief that there is both "Benefits and Downsides of the Availability and Ease of Use of Penetration and (Ethical) Hacking Tools" has been confirmed.

The benefits of these tools include, they are free, they are easy to configure and use, they are easy to learn, they reduce the need for outsourcing expensive security reports and testing and they can actually allow you to get an understanding of how possible attacks can happen, as cybercriminals will most likely use similar if not the same software, which can allow you to further eliminate vulnerabilities that industry testing may not detect.

The disadvantage of these tools is almost in cohesion with the advantages of the tools. Yes, they are easy to learn and understand with little knowledge. This multiplies the possibilities of cybercriminals, or even someone just interested in hacking for fun, launching a dangerous attack.

Although this might seem like a reason for such tools not to be publically available, it is actually a better solution to security problems. This is because, if a free tool, such as 'Kali', becomes the number one choice for hacking, it allows companies to narrow down and eliminate the range of possible bugs or attacks that they do not know how to test for or defend against.

4.2 Recommendations

In this section, I will list any recommendations I have now based the findings of my study, on both my Host Company and similar companies. I will also list any recommendations I have for doing this study or a similar investigation.

I would recommend the use of free and open source Penetration and or Ethical Hacking tools in the industry. I believe it is the way forward in Information Security for companies to become self-reliant and lower costs overall. These tools could also help with providing assurance to clients and also assist in dealing with GDPR (General Data Protection Regulation) issues.

I also believe it is the best way to rule out the majority if not all possible vulnerabilities in a companies Infrastructure and Security regardless of what they are providing or selling.

“A company who does not take IT security seriously can be exposed by simple hacks that anyone with interest could do.” (Glennon, 2018)

If I was to do this study again or research something similar would like to broaden the range of tools. Maybe some tools outside of ‘Kali’, possibly some paid software tools or torrents of such (*See appendix*). I would like to do this as a more advanced study as this study that I have done was to prove how easy it is to access and use these tools and how that can provide a benefit or threat to my host company.

I would recommend looking further into this topic for your own business. Research and testing should be carried out in other scenarios. The environment for this study was carried out within and for an SME, Small to Medium Enterprise, that develops and supplies cloud-based software solutions. Results and tests may vary based on the size and infrastructure of the company.

Like all testing, the tests were carried out multiple times to make it a fair test. If I was testing again I would base my results on success and data found. For this study, successful outcomes were based on how easy it was to use the tools in question and how easy it was to replicate a possible real-world cyber attack.

Bibliography

BXP, 2018. *BXP Software Logo*. s.l.:s.n.

Cooke, C., 2018. *Structure Diagram*. Dublin: s.n.

Enaqx, 2018. *Github.com/enaqx/awesome-pentest*. [Online]

Available at: <https://github.com/enaqx/awesome-pentest>

[Accessed June 2018].

Glennon, T., 2018. *The opinion of Pen & Hacking tools* [Interview] (1 May 2018).

Jenkins, P., n.d. *LinkedIn*. [Online]

Available at: <https://ie.linkedin.com/in/patrick-jenkins-ba822653>

[Accessed Monday, March 2018].

Kostadinov, D., 2016. *Infosec Institute*. [Online]

Available at: <http://resources.infosecinstitute.com/ethical-hacking-vs-penetration-testing/#gref>

[Accessed 08 February 2018].

Lacey, P., 2016. *The Pillars of bxp*. s.l.: Bxp Software.

Lacey, P., 2018. *About All n One*. [Online]

Available at: https://www.bxpsoftware.com/wixi/index.php/About_All_n_One

[Accessed Wednesday, March 2018].

Systems, R. S., 2018. *Really Simple Systems*. [Online]

Available at: <https://www.reallysimplesystems.com/faq/customer-relationship-management/>

[Accessed Tuesday, March 2018].

techopedia, 2018. *techopedia*. [Online]

Available at: <https://www.techopedia.com/definition/170/contact-manager>

[Accessed Tuesday, March 2018].

times, E., n.d. *The Economic Times*. [Online]

Available at: <https://economictimes.indiatimes.com/definition/e-learning>

[Accessed Tuesday, March 2018].

Appendices

Appendix A

This Appendix contains a list of links to tools relating to the topic contained in this study and could be used for further or future studies.

All Links can be found at <https://github.com/enaqx/awesome-pentest> (Enaqx, 2018)

- [Tools](#)
 - [Penetration Testing Distributions](#)
 - [Docker for Penetration Testing](#)
 - [Multi-paradigm Frameworks](#)
 - [Network Vulnerability scanners](#)
 - [Static Analyzers](#)
 - [Web Vulnerability Scanners](#)
 - [Network Tools](#)
 - [Exfiltration Tools](#)
 - [Network Reconnaissance Tools](#)
 - [Protocol Analyzers and Sniffers](#)
 - [Proxies and MITM Tools](#)
 - [Wireless Network Tools](#)
 - [Transport Layer Security Tools](#)
 - [Web Exploitation](#)
 - [Hex Editors](#)
 - [File Format Analysis Tools](#)
 - [Anti-virus Evasion Tools](#)
 - [Hash Cracking Tools](#)
 - [Windows Utilities](#)
 - [GNU/Linux Utilities](#)
 - [macOS Utilities](#)
 - [DDoS Tools](#)
 - [Social Engineering Tools](#)
 - [OSINT Tools](#)
 - [Anonymity Tools](#)
 - [Reverse Engineering Tools](#)
 - [Physical Access Tools](#)
 - [Side-channel Tools](#)
 - [CTF Tools](#)
 - [Penetration Testing Report Templates](#)

Appendix B

This Appendix contains a list of links to books relating to the topic contained within this study and could be used for further or future studies.

- [Books](#)
 - [Penetration Testing Books](#)
 - [Hackers Handbook Series](#)
 - [Defensive Development](#)
 - [Network Analysis Books](#)
 - [Reverse Engineering Books](#)
 - [Malware Analysis Books](#)
 - [Windows Books](#)
 - [Social Engineering Books](#)
 - [Lock Picking Books](#)
 - [Defcon Suggested Reading](#)
- [Vulnerability Databases](#)
- [Security Courses](#)
- [Information Security Conferences](#)
- [Information Security Magazines](#)
- [Awesome Lists](#)