ITNPA3-B14 – Research Essay

Group number and name	Group 1
Group member details	8RQXMCKR1 – Bisseru, Shailen (leader) HZKKXSBX2 – Strauss; Werner HCTVL6G21 – Singh; Bhavish DSML3RL95 – van Heerden; Heinrich NB95MJFJ5 – Ramathibela, Ontlametse
Project title	Investigating Social Engineering Techniques to Generate a Comprehensive Risk Assessment Report for Eduvos
Submission date	2022/07/01
Signature of group leader	

Research topic is based on the final topic in the research proposal

Names of Group Participants:

Bisseru, Shailen (Leader)

Strauss; Werner

Singh; Bhavish

van Heerden; Heinrich

Ramathibela, Ontlametse

Supervisor:

Eric T. Chemhere

ABSTRACT

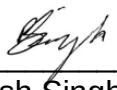
This research essay must address the problems and mitigates the effects of social engineering by developing methods and strategies to address vulnerabilities. The collection of information by generating scan trails to analyse potential vulnerabilities so that tools and techniques can be developed to assess the risks of social engineering and general cyber-attacks is therefore of vital importance. Practical penetration tests will allow for the identification of risks, and the results of the analysis and testing will lead to new, improved formulations of defensive strategies; focused within the boundaries of the research of deliberate attacks on Eduvos.

This research addresses a grey area in cybersecurity where there are no standard models, methodologies and techniques that underline the process of generating a scan trail and developing the measures to mitigate the risks of social engineering. This is accomplished through the implementation of botnet attacks and cryptocurrency mining, using infected computers, simple ways to gain access to data, mobile phone attacks, modern wireless network attacks, and ways to attack web applications.

DECLARATION OF ORIGINAL WORK

We, Werner Strauss, Bhavish Singh, Heinrich van Heerden, Ontlametse Ramathibela and Shailen Bisseru declare that this research report is our own, unaided work. It is submitted in partial fulfilment of the requirements of the BSc IT at Eduvos, Potchefstroom and Durban, South Africa. It has not been submitted before for any degree or examination at any other university or educational institution.

Werner Strauss



Bhavish Singh

Heinrich van Heerden

Ontlametse Ramathibela

Shailen Bisseru

On 04 July 2022

ACKNOWLEDGEMENTS

This research was supported by Eduvos. We thank our colleagues from Eduvos Midrand Campus who provided insight and expertise that greatly assisted the research.

We thank E.T. Chemhere for his guidance and assistance with the acquisition of the test server and with teaching all subjects related to the research paper, as well as all information system council members for their feedback which greatly improved the manuscript and overall content of the presentation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

Introduction

COVID-19 has had a devastating impact worldwide, affecting almost forty percent of the global economy, people's lives, and the way businesses operate resulting in a large proportion of the population having to migrate to performing their work or studies online. A survey conducted by Pandhya and Lodha (2021:2) of selected countries indicate a 50 to 70 percent increase in Internet use during the pandemic.

Software, data, and social engineering attacks have thrived in this environment where there is a lack of adequate countermeasures (Tam, et al., 2020: 2-3). Social engineering, which relies on the psychological manipulation of individuals to gain access to sensitive data have become more prevalent by establishing attacks such as pretexting, Business Email Compromise (BEC), diversion theft, phishing, whaling, tailgating, baiting, smishing, quid pro quo, and honey traps (Crowdstrike, 2021).

This research explores a technical grey area in the cyber security space where public and private sector organizations continuously fall victim to cyber threats due to the lack of a standardised model around the prevention and control of social engineering. The deployment of hybrid penetration testing tools and techniques into the Eduvos Potchefstroom campus network and systems are used to log the results and draft recommendations for standard guidelines of secure practices.

The tertiary sector is the primary focus of this research, as there has been a marked increase in the number of attacks, with 44 percent of institutions being affected (Kshetri, 2021). Similarly, institutions locally have also been afflicted by social engineering attacks, with the majority of attacks being initiated via e-mail. These attacks bring into question how effectively the institutions have secured their systems, as well as how knowledgeable the staff and students are regarding these threats (de Villiers, 2021).

Background of Research

Cybersecurity analysts and attackers have seen a shift in the norm of operations since the start of the COVID-19 pandemic. With the global occurrence of lockdowns, people were forced to stay indoors as much as possible, leading to a large proportion of the population working and studying from home. As a result of this migration from a physical working environment to a virtual one, approaches to safeguarding and exploiting systems have had to adapt (Venkatasha, et al., 2021:2).

Cybersecurity, and social engineering attacks in particular have since experienced an exponential surge during this period. This increase can be observed by comparing the patterns for 2019 (Figure 1) and 2020 (Figure 2) as illustrated below.

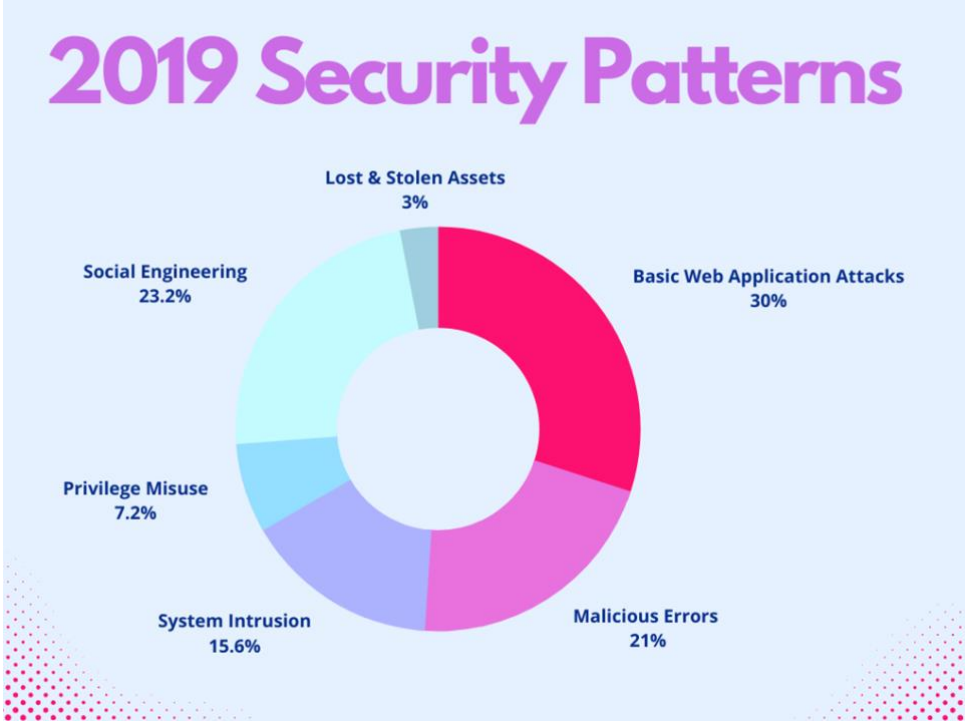


Figure 1: Security Patterns for 2019 (Verizon, 2021)

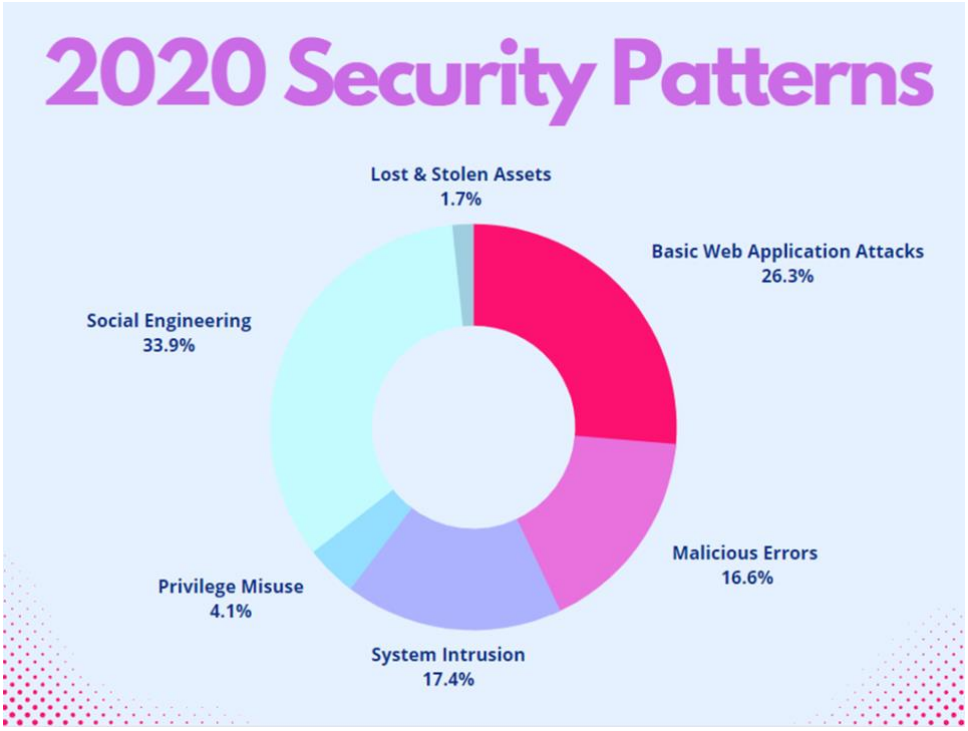


Figure 2: Security Patterns for 2020 (Verizon, 2021)

It is evident that attackers have been able to exploit the opportunity given to them where people were forced to work from their homes, usually where security is much more relaxed; and as such, a ten percent increase in security incidents and breaches can be seen by comparing the patterns as shown above.

Prior research has only yielded results to a theoretical extent, referenced in the articles by Nguyen and Bhatia (2020:1-8), where a model was created based on a theoretical scenario; or Alsulami, et al. (2021:1-13), where surveys were conducted to assess the awareness of social engineering in Saudi Arabia; or even Kyeremeh, et al. (2019), where the risks of social engineering were investigated in Ghana based on two focus groups, where one had formal training in information security, and one did not. This research explores the practical aspect of testing live systems and networks at Eduvos Potchefstroom, and covers the attacks that institutions face locally, in South Africa.

The chosen institution, Eduvos, was founded in 1979 as the Computer Technology Institute (CTI). It offers 21-degree programmes across 12 campuses throughout South

Africa, with many international students. Learning is facilitated through a blended mode, where classes are held online or face to face (Eduvos, n.d.).

Aim of Research

The primary aim of this research project is to identify and analyse various social engineering techniques to generate a comprehensive and detailed risk assessment report for Eduvos. This will allow the authors to identify any security threats, risks, and vulnerabilities, as well as to develop solutions or recommendations to address the prior mentioned security issues.

Research Objectives

In order to successfully investigate social engineering techniques and generate a risk assessment report for Eduvos, the objectives of the research project are as follows:

- Identifying and documenting the various possible attack vectors that may potentially affect Eduvos
- Compiling and reviewing all open-source intelligence pertaining to Eduvos
- Implementing Google dorking to identify security flaws within Eduvos.
- Tracing and spoofing Eduvos' emails.
- Utilising Maltego to collect and visualise data, relevant to Eduvos.
- Executing an approved simulated phishing attack within Eduvos.
- Conducting approved hacks on Eduvos' Facebook, Twitter and Gmail accounts.

Problem Statement

Research and investigations conducted by Security Boulevard (2021) has highlighted that from 2016 through to 2020, the average amount of money stolen from various school districts, as a result of social engineering-based attacks, has accumulated to $2 million. In addition to the prior mentioned, TechRepublic (2020) has stated that 3.5 million spear phishing attacks were seen from June through September 2020 and Barracuda had found that more than a staggering 1,000 educational institutions that were targeted within this four-month period. This indicates that Eduvos, being a successfully established higher

educational institute with 12 institutes throughout South Africa, may be seen as a potential target to a form of social engineering-based attack. It is due to the lack of awareness around social engineering that has necessitated this research project and thus the authors have decided to implement the prior mentioned techniques and strategies, in addition to others, within the Eduvos environment to shed some light on this area of cybersecurity and highlight the threats and risks associated with social engineering.

According to PurpleSec (2021), 98 percent of all attacks rely on some form of social engineering exploitation and 43 percent of interviewed IT professionals have admitted to being targets of social engineering schemes, within the year 2020 alone. This indicates that cyber attackers are shifting their focus onto the human element of the organisation's system, as the human element of a system will always be the weakest link, as stated by Mouton, et al. (2014).

Therefore, social engineering exploitation is a problem that poses a threat and security risk to individuals, companies, and organisation, including Eduvos. The authors address this problem by identifying and mitigating any existing and potential security threats to Eduvos. This will prevent any future social engineering exploits and allow for security protocols and procedures to be in place.

In order to reduce and mitigate the security threats and risks, the authors utilise a risk assessment report, compiled specifically for Eduvos, to devise and implement solutions for the identified security threats and issues.

Threat	Definition	Property	Scenario	Possible Mitigation
Spoof Identity	Impersonating a target individual.	Authentication	Hacking Eduvos' email and sending emails under a false pretence.	Implementing the use of multifactor authentication and digital signatures.
Data Tampering	Altering existing data, and code.	Integrity	Alter any Eduvos' existing data, or code.	Assigning permissions, according to a developed access control list.
Repudiation	Deniability of a situation.	Non-repudiation	An employee or member of Eduvos denying an allegation, such as sending an email.	Implementing secure auditing and logging.
Information Disclosure	Disclosing sensitive information.	Confidentiality	Disclosing Eduvos' sensitive or personal information.	Implementing more advanced data encryption methods and assigning permissions, according to a developed access control list.

Threat	Definition	Property	Scenario	Possible Mitigation
Denial of Service (DoS)	Non-availability of a service.	Availability	The institute's online platforms do not respond to the client base's requests.	Assigning permissions, according to a developed access control list and the organisation's data analytics as a service.
Elevation of Privilege	Conduct unauthorised actions.	Authorisation	Hackers or potential threat actors are able to tamper with other accounts and access restricted data of Eduvos.	Implement input validation, within the organisation.

Table 1: Threat Model

Sub-Problems

Social Engineering Exploitation

The authors have identified that Eduvos does not have any strategies or procedures in place that may mitigate the effects of social engineering exploitation on the human element of their system. Thus, a scan trail of social engineering exploitations is generated, to identify the social engineering security threats and risks within Eduvos' system.

What is the problem?	Identifying social engineering exploits of the human element, within Eduvos' system.
Who may be affected and how?	Eduvos is adversely affected, as this problem hinders, if not halts, the day-to-day functioning of the organisation. This may result in potentially greater security threats and possible cyberattacks.

What is being done to control the risks?	Eduvos has basic security procedures and staff awareness programmes, regarding to social engineering, in place.
What further actions need to be taken?	A scan trail of social engineering exploitation is generated for Eduvos.
Who needs to carry out the action?	The authors will carry out this action.
When is the action needed by?	08/07/2022

Table 2: Risk Assessment of Social Engineering Exploitation

Eduvos' Level of Vulnerability

Due to the exponential growth in social engineering attacks to obtain personal and confidential data, Eduvos is an ideal target due to its level of vulnerability. Thus, efficient and effective tactics that may be employed to reduce the overall vulnerability of Eduvos are identified and implemented. The data obtained from the authors implemented techniques and strategies will provide enough data and information regarding Eduvos' unknown vulnerabilities.

What is the problem?	How to mitigate the identified exploits and potential security threats of Eduvos.
Who may be affected and how?	Eduvos' vulnerabilities will be identified and utilised by potential threat actors to gain access their system and obtain sensitive information, which can be sold to Eduvos' competitors, held for ransom, and even allow the attacker to launch potential future attacks
What is being done to control the risks?	Eduvos will have basic security procedures in place to mitigate any known security threats.

What further actions need to be taken?	The data collected from the generated scan trail must be used to identify solutions, and recommendations, that will address the problem at hand.
Who needs to carry out the action?	The authors will carry out this action.
When is the action needed by?	08/07/2022

Table 3: Risk Assessment of Eduvos' Level of Vulnerability

Benefits of Study

The goal of this research project is the development and implementation of frameworks and strategies that enhance cybersecurity protocols and procedures regarding social engineering based cyberattacks, within Eduvos' educational environment. Throughout this study the authors gather and compile information on how to subsequently utilise social engineering techniques, as well as demonstrate how a social engineering-based attack occurs in a real-life situation. This is because cybersecurity specialists are able to find and shut holes before they are attacked, says Hummingbird networks. General benefits include revealing vulnerabilities, showing real risks, testing cyber-defence capabilities, ensuring business continuity, and maintaining trust (Wierckx, 2021).

Various institutions spend a great deal of their time protecting their external network perimeter, but the authors will focus on dividing resources amongst both the external and internal network perimeters to reduce the chance of a successful breach. Having a social engineering evaluation at-hand could help institutions with a selection of security solutions that are specific to their needs. Clients, employees, suppliers, students, and other stakeholders would be more likely to conduct business if the recommended social engineering assessments are implemented. Some incentives the authors look at include post-exploitation terminologies (JavaTpoint, 2021), installing backdoors (Najera-Gutierrez, et al., 2019), and creating a simple ransomware (Checkpoint, 2021).

In addition to the above stated, the authors conduct approved penetration tests to gauge the current vulnerabilities of Eduvos to cyber threats and potential risks. There are five

steps to plan a successful penetration test all made possible by the penetration test lifecycle, planning and reconnaissance, scanning, gaining access, and analysis and reporting. The authors crack WEP's, WPA, WPA2 and WPA3's as well as WPS's. Performing a full, limited, or focused penetration test determines the regression, or degradation of the system's capabilities, from one version to the next. The different approaches to penetration testing according to Firch (2021) include Black Box, White Box and Grey Box.

Delimitation of Study

The authors analyse and examine the risks to user data and privacy associated with the use of social media. A test machine is created at Eduvos in Potchefstroom to perform the penetration test. The authors go through the process of reconnaissance and examining whether it is possible to lure a user into clicking a link that will manipulate them into being redirected to a cloned website. The listener spyware program is activated to ensure that whatever is typed by the user is captured.

The user's credentials will be replicated and unauthorized access to the portal is gained where the system is infected with a botnet that will mine crypto currency and send it to the host machine. The authors then establish solutions and improvements to current regulations regarding cyber security and cyber-attacks and discuss measures on how to solve network security vulnerabilities in Eduvos.

The authors identify and gather useful malware to create a rootkit that allow to test vulnerabilities on Eduvos' systems. The built-in features of Kali Linux and Ubuntu are also used. With the use of the penetration testing rootkit, data is produced, in a clear and a concise manner, that is used to categorise and determine the possible threats associated with Eduvos' websites and student platform.

The authors are limited to the Eduvos Potchefstroom campus environment, and only a controlled portion of the networks and systems are available for testing. This is in line with the ethical guidelines the authors adhere to, to protect critical information and data.

CHAPTER 2: LITERATURE REVIEW

Introduction

The early stages of the 4th Industrial Revolution have seen rapid and exponential growth in terms of the technology used and implemented in our day to day lives, but the rate of technological growth and implementation had seen a tremendous spike during the COVID-19 pandemic.

Every sector, if not all, has adopted and implemented technological based strategies to combat the limitations set as a result of the pandemic. One of the leading sectors in the implementation of technology and digitisation in day-to-day functioning being the education sector. However, the education sector's high dependency on technology and online platforms for daily operations has left many institutions vulnerable to social engineering-based attacks. This vulnerability was highlighted by Lance Whitney's article titled "Attackers are exploiting the need for schools to receive critical updates from teachers, principals, and department heads", says Barracuda (2020) in which he states that out of 3.5 million attacks, seen from June to September of 2020, over 1000 of the targets were educational institutions.

Muncaster (2020) implies that social engineering is a set of techniques that are implemented by potential threat actors to obtain an organisation or institution's confidential data by manipulating and taking advantage of the human element of the organisation or institution's system.

The human element in this case being Eduvos' employees as well as the students at the institution, as attackers intend to gain their credentials and any other confidential data that may prove useful for a future attack. The main method of implementing social engineering-based attacks within the educational environment are via emails as stated by de Villiers (2021), thus, raising the questions as to whether the staff and students of these educational institutions have any knowledge of social engineering-based attacks and how it may affect them.

Therefore, based on the above stated, it is evident that social engineering exploitation is a problem that poses a threat and security risk to individuals, companies, and organisations, including Eduvos' campuses throughout South Africa. Thus, the main focus of this research project is to shed light on this grey area of social engineering-based attacks within tertiary educational institutions, at Eduvos Potchefstroom Campus. In addition to the prior stated, any potential or existing cyber security threats to Eduvos' Potchefstroom campus will be identified and mitigated, thus preventing any future social engineering exploits; and it will also allow for security protocols, and procedures, to be put in place.

Related Work

Cyber Security Analysis

The penetration test lifecycle outlines the steps required to perform a penetration test. Three generalised phases as discussed by Sahri et al. (2014) are the Pre-attack Phase, where the target is investigated; the Attack Phase, where the actual attack is performed; and the Post-attack Phase, where the systems are returned to the prior state, is shown in Figure 3; with more detailed processes listed under these phases as Planning and Preparation, Information Gathering and Analysis, Vulnerability Detection, Exploitation, Analysis and Reporting, and Resolution, shown in Figure 4.

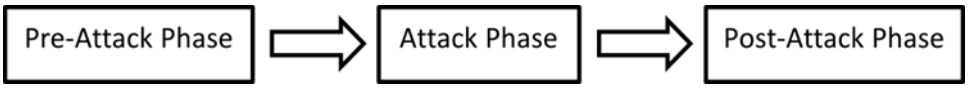


Figure 3: General Penetration Test Life Cycle (Wang & Kou, 2012)

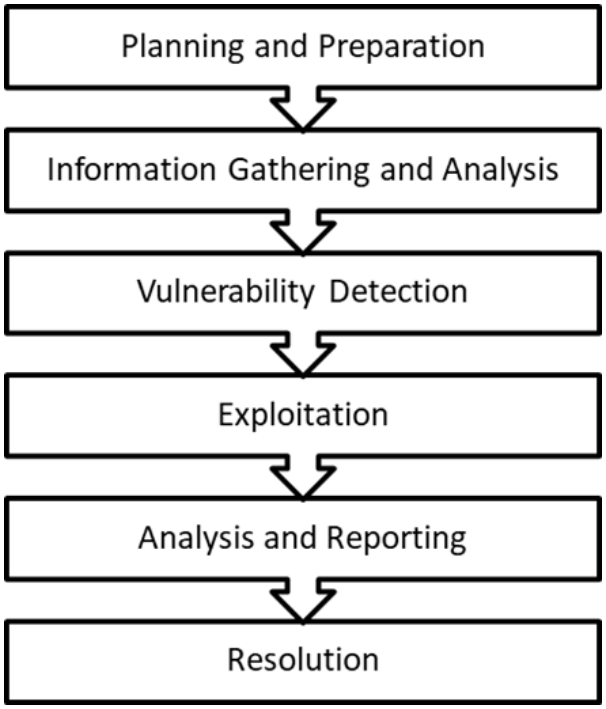


Figure 4: Penetration Testing Process (Wai, 2001)

To speed up the process, security professionals and industry enthusiasts are looking for ways to automate key steps of manual penetration testing. There are a number of tools that are known to make automated penetration testing possible. To plan and command cyber-attacks by ethical and skilled hackers, a portfolio of multiple automated security systems is required. The popularity of automated technologies has increased the utility of cyber-attacks, as they aid in automating anything from manual testing to remote password brute force. Security professionals who employ the correct blend of machine learning and artificial intelligence to recognise various details, such as the location of the pen, the type of computer utilised, and so on.

The use of machine learning to scan findings will rely on manual effort to determine whether or not a certain issue is still present. Machine learning and artificial intelligence are considered essential components of penetration testing. It has the necessary processing power, which aids in improving the software's performance. It allows various tools and software to learn from past experiences and current market trends, make better-informed judgments, and pass the time. Artificial intelligence (AI) and machine learning capabilities in penetration testing tools aid in better planning. It aids in the faster detection

of vulnerabilities and faults. As a result, you will be more successful in resolving a variety of tools than you would with standard tools (TekhiToday, 2021).

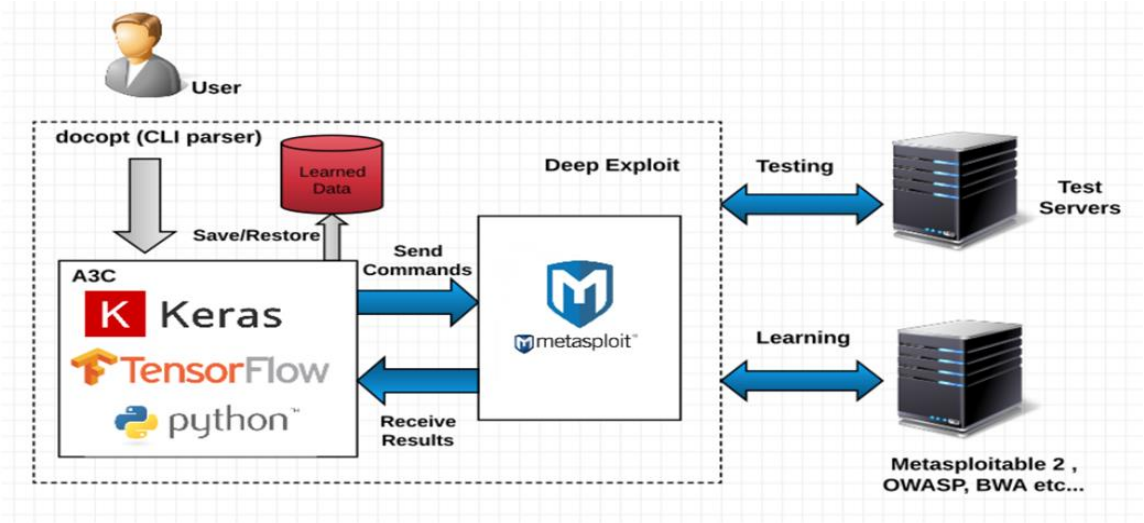


Figure 5: Penetration testing tools

Keras: Keras is an open-source software library that provides a Python interface for artificial neural networks. Keras acts as an interface for the TensorFlow library.

TensorFlow: Tensorflow is an open-source library for numerical computation and large-scale machine learning that ease Google Brain TensorFlow, the process of acquiring data, training models, serving predictions, and refining future results.

Python: Python is an interpreted, object-oriented, high-level programming language with dynamic semantics.

Metasploit: Metasploit is a penetration testing framework that makes hacking simple. It's an essential tool for many attackers and defenders. Point Metasploit at your target, pick an exploit, what payload to drop, and hit Enter.

Test Server: A test machine will be provided at Eduvos so that we do not cause chaos on the real system.

Related Work on Penetration Testing and Cybersecurity.

There was ground-breaking research about the human element being the weakest link in regard to system security, and as such, form the basis of social engineering attacks. Attackers, attempting to gain access to information, manipulate individuals into divulging information or granting them access (Duarte, et al., 2021:2). Recent studies have focused on the development of models and measuring awareness of social engineering at educational institutions. However, few researchers have considered testing, recording, and developing models in a live environment and contrarily, the majority are based on theoretical scenarios. While it may not be feasible to perform all social engineering attacks in a live environment, important information can be garnered from such tests.

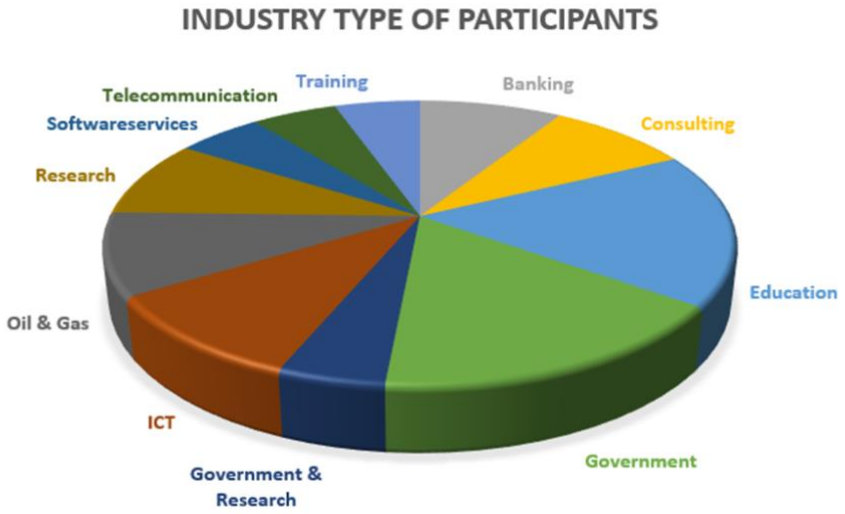


Figure 6: Industry type of participants (Aldawood, 2017)

In order to assess the awareness of social engineering amongst individuals in the educational environment, a survey was conducted by Kyeremeh, et al. (2019:22-23), in which 50 respondents were questioned. He found that, of those questioned, those in an environment where security policies and training were implemented tended to have a better understanding of attack techniques and methods to safeguard against them, in contrast to those where no security policies were in place. These findings are substantiated by Alsulami, et al. (2021:10) in a survey of 465 respondents. He established that only 34 percent of the respondents had any prior knowledge of social engineering, further

highlighting the need to develop standardised models, methodologies and techniques against such attacks.

According to an interview, attacking human knowledge would continue to be a big danger in the coming years. The most serious cyber security concerns will be the trafficking of personal data on the dark web and consequent data breaches (Thomas, 2017). Some participants were unsure if social engineering would remain to be the most important factor as people become more aware of such attempts. It's safe to assume that the attackers will use a combination of approaches to get entry to personal information.

New assaults that sectors should be wary of include blockchain hacking, cryptocurrency hacking, machine learning attacks, and AI-based attacks, with social engineering playing a big part at the moment. As a result, there is a necessity to offer personnel with training so that they can better spot these types of assaults. (Reddy, 2014). Other respondents stated that phishing emails might be the next emerging issue since victims are unable to recognize well-designed social engineering assaults. In addition to manage private data and guarantee that it is secured, social engineering must tackle a number of tasks.

Nevertheless, the interview revealed that risks like as ransomware, impersonation or pretexting, phishing, data leakage, hacking, and insider threats continue to be big concerns for businesses (Gupta, 2017). The process of a cyber security expert, that acts as an external threat actor and or cyber terrorist, performing a simulated cyber-attack against a computer system in order to identify any vulnerabilities that are present within the system in question is referred to as penetration testing, also known as ethical hacking or a pen test (Campbell, 2021).

This research project focuses on identifying security weaknesses within the Eduvos Potchefstroom Campus and mitigation methods that may be implemented. Thus, the research will be based on the penetration testing cycle, in addition to identifying social engineering techniques. Penetration testing may be divided into two categories, internal and external network penetration testing. Moulder, et al. (2021) describes internal network penetration testing as an internal test, in which the tester is able to perform simulated

attacks from within the firewall, and an external network penetration test is defined as test that targets assets of an institute or company that are visible to the public. All penetration tests follow a basic cycle that consists of five stages, as seen in Figure 7.

Figure 7: What is Penetration Testing (Imperva, 2022)

According to various articles and courses (tutorialspoint, n.d.), the five stages of a successful penetration test may be defined as follows. The first stage, Reconnaissance, is the information gathering stage in which data and information, relating to the targeted network or system, is obtained. The second stage, Scanning, implements the use of tools such as Nmap, ICMP scanners, vulnerability scanners and SNMP sweepers to determine open ports, available access points, operating systems utilised and uncover any services available to exploitation. This allows for a profile of the intended target to be created (enumerating). The third stage, Exploitation, is the stage in which the actual penetration test takes place, by utilising the Kali Linux tools and services. The fourth stage, Maintaining Access, is a stage in which techniques must be employed to maintain access to the intended target. These techniques include the implementation of backdoor tools, Netcat, ransomware and tunnelling data and commands via DNS. The final stage of a successful

penetration test is to develop an overview of the performed penetration test and recording all the data and results obtained from the penetration test.

These five stages will be utilised and implemented in the research project and will allow any existing or potential cyber security vulnerabilities, within the Eduvos environment, to be identified. In addition to the prior stated, the report developed in the final stage of the penetration test will be used to create strategies and procedures to address any found cyber security vulnerabilities. The proliferation of digital devices and the evolution of technology have heightened the demand for cyber security.

Frumento (2016) provided data on social engineering assaults, estimating the number of cyber-attacks on corporate and government entities. He emphasized that hackers are more likely to target human weaknesses to get access to organizational systems rather than hardware or software flaws. He further claimed that just 3% of attacks are directed at corporations' technological infrastructures. On the other hand, social engineering hacking attempts were used in 97% of malware infections.

Professional expertise, clearly identifiable contemporary difficulties in the research topic, and a strong personal interest in the field all contributed to the inspiration for this study. The motivation for the study stems from a major issue faced by many firms throughout the world and employees' lack of understanding about cyber security social engineering risks.

Furthermore, numerous strategies of social engineering have been verified in the literature to produce cyber security concerns in a variety of situations (Aldawood, et al., 2020). This research is crucial in revealing social engineering dangers to companies, since social engineering manipulation tactics evolve with the advancement of cyber technology (Alazri, 2015). Those threats are becoming the most common way to target specialized corporate cyber systems all across the world.

This research is important because it reveals hackers' abilities to target corporate security architecture at varying degrees of complexity by abusing their human layer of protection. This research will also result to an investigation of techniques and solutions that can assist

firms to combat cyber-attacks and identify vulnerable patches that need to be addressed at the human resource level (Loukas, 2017).

The qualitative study method was utilized to collect subjective perspectives on human behaviour in relation to cyber security, especially social engineering awareness. In the framework of social engineering awareness, this study conducts a qualitative examination of replies from acknowledged cyber security specialists to specified interview questions. Aside from awareness initiatives, the goal of this research is to uncover the best working tools to eliminate social engineering dangers and then supply dependable solutions to build such a secure work environment.

Significant Findings in the Related Work

This research fills the gap where no tests on live systems have been performed, and subsequent models and recommendations developed. As stated by de Villiers (2021), “the main method whereby social engineering-based attacks are implemented is via email”, thus it is not known if the staff and students of these educational institutions have any knowledge of social engineering-based attacks and how it may affect them. If any current risks to the Eduvos campus were uncovered, they will be identified and addressed so that security standards and procedures may be implemented.

The use of the penetration life cycle and the three step generalized phases as discussed by Sahri et al (2014), will be utilized to perform the penetration test on the servers. Security experts and industry enthusiasts are seeking solutions to automate essential manual testing tasks, which means the procedure of identifying weaknesses will be carried out using penetration testing software rather than having competent security researchers perform a complete examination of a security architecture. Machine learning will be used to scan findings, but manual work will be required to identify whether or not a specific issue is still there. Resolving a variety of tools will be more successful than standard tools in the detection of vulnerabilities and faults.

There are findings of a research that was done describing the human factor in being the weakest link in system security, hence forming the basis of social engineering assaults. Only a few studies have investigated testing, recording, and building models in a real-world setting, while the vast majority are based on hypothetical circumstances. It's revealed that the development of a variety of models and grading social engineering awareness at educational institutions has been the focus point in resent studies.

In the survey conducted by Kyeremeh, et al. (2019), the questioned respondents provided evidence that those who were in an environment where security policies and training were implemented tended to have a better understanding of attack techniques and methods, whereas those who were not in the same environment were less likely to react in a similar matter.

CHAPTER 3: RESEARCH METHODOLOGY

Introduction

One of our main goals is to create awareness of social engineering. "One of the dangers of social engineering attacks is their harmless and legitimate appearance so that targets (i.e., a person and not the goal of the attack) are unaware of being victimized" (Hadnagy & Wilson, 2020). Social engineering can only be stopped only by promoting awareness. It is not just organizations that are the potential targets, but normal people as well. This is because we are not aware and are not careful about our personal information as we don't understand its significance. Social engineers study the victim and get to understand their strengths and weaknesses.

Our team has discovered evidence regarding the lack of awareness of the target industry. "Cybersecurity incidents are more often caused by human failure (Chan Ethan, 2021) than by technology failure (Schneier 2019)". Consequentially, humans are the weakest link in information security (Happ Nathan, 2019). To put it bluntly: "only amateurs attack machines, professionals attack humans" (Schneier 2018).

There is currently a lack of awareness amongst students, professors, and higher education IT staff due to the absence of education that is readily available to them, according to Verizon's "2018 Data Breach Investigations Report". In 2018, the education industry was ranked the worst in cybersecurity out of 17 major industries (Verizon, 2019).

In its 2018 Education Cybersecurity Report, the company found that the education industry is not taking many of the necessary steps to protect students from cyber-vulnerabilities. According to the study, the main areas of cybersecurity weaknesses in education are application security, endpoint security, patching cadence, and network security. Students often use more than one device on campus and in-class, such as computers, phones, tablets or other "internet of things" devices, and that while beneficial, creates "a heterogeneous environment, where all of the devices are not secured equally" (Foresman, 2018).

Figure 8 contains a road map of common questions that should be asked regarding a business's cyber security.

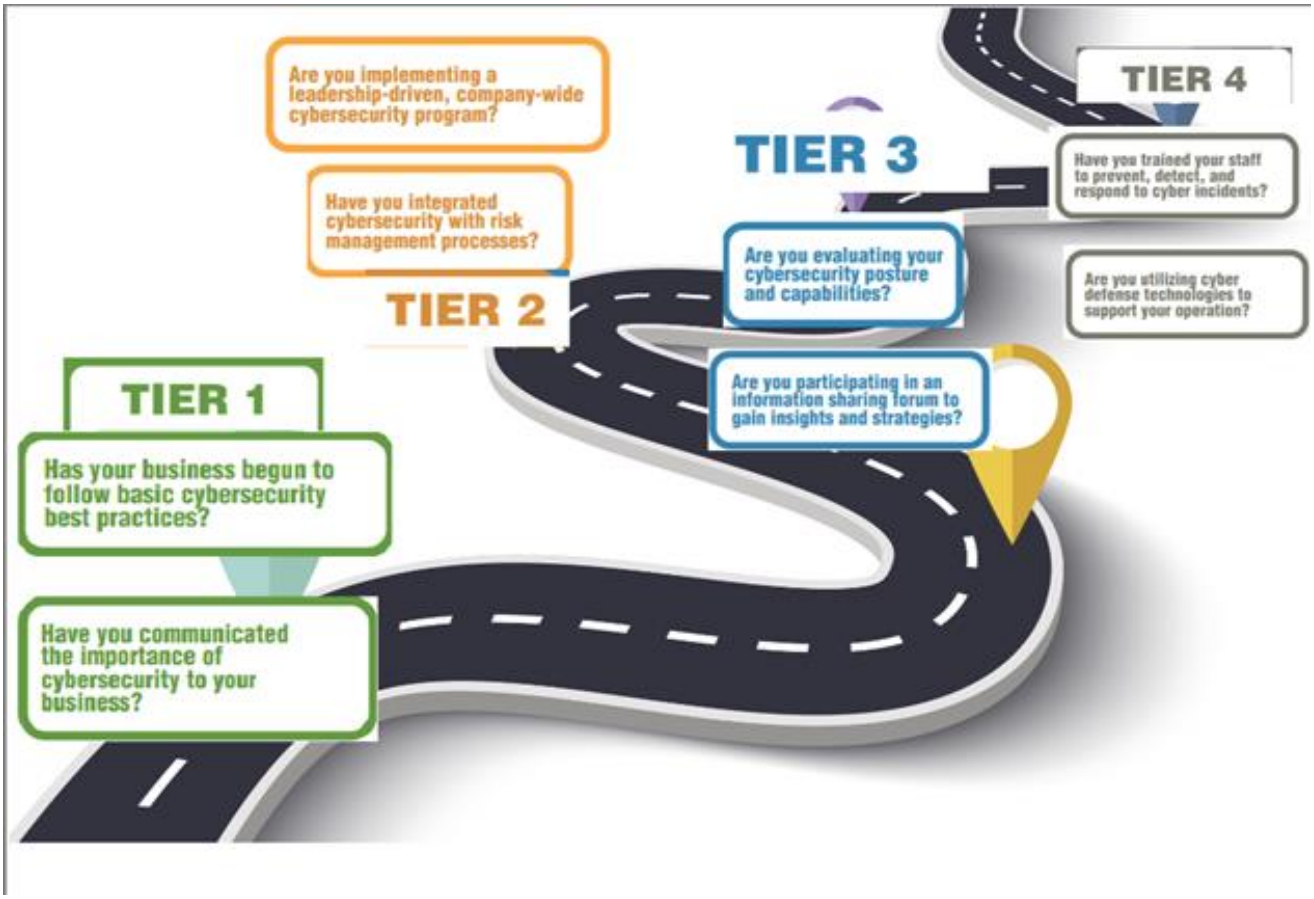


Figure 8: Roadmap of research

Level of awareness or lack thereof in the public. “Deception and manipulation are used by offenders to make targets assist in their victimization (Bosworth Copper. 2020)”. “The social engineering attack vector is considered the biggest threat to information systems” (Rouse, 2006). Never share personally identifiable information over the phone, if the callers insist ask for a call back number, inform managers about it. Limit the amount of personally identifiable information they carry physically, and in case of theft, immediately inform parents and register a complaint with the police. This kind of awareness will help users realize that social engineering is a serious risk and to be serious about how they deal with it.

This research topic emanated from an area that requires more urgent attention. Due to the lack of resources the team couldn’t reach other industries. The lack of knowledge regarding the above topics makes the education sector a prime target for social

engineering. Lack of awareness is demonstrated by stakeholders using common passwords, stakeholders writing down their passwords and stakeholders using the same password for all their accounts.

Research is about identifying targeted devices. Security camera systems which are the most hacked IoT devices. Many of these attacks can bypass the security of cheap models of IP camera – with many of these low-cost devices based on a similar blueprint, meaning that if a vulnerability is found in one, it may also work against other models. Smart hubs and network-attached storage devices are the next most vulnerable devices, claims the research, accounting for 15% and 12% of the most-hacked devices respectively. Printers, smart TVs and IP Phones are also common attack vectors for successful hacks.

Attack Types	Attack Complexity	Attack Time	Attack Result
Phishing: These attacks are often low effort but widely spread; for instance, a phisher might send out thousands of identical emails, hoping someone will be gullible enough to click on the attachment.	Skilful social human interaction is needed to successfully pull of this attack.	Need to gain the trust of the victim.	Stealing login credentials or trick users into clicking a link that leads to deploying a payload of malware.
Botnets: Botnets are often used to launch Distributed Denial-of-Service (DDoS) attacks against networks, websites, and online services.	Consisted of simple spamming operations but have evolved to be more complex in nature, intended to defraud or manipulate users.	Open source botkits are available that can easily and quickly create botnets for various needs and applications.	Taking over a victim's pc and installing malware to steal information and installing bitcoin miners.

Spoofed website: Fraudulent websites that masquerade as legitimate sites by copying the design of the website as well as in some cases utilizing a URL like the real site.	Registering a domain name that is nearly identical to the intended landing page and create a website nearly identical to the original.	Need to create an accurate copy of a website which takes a lot of time. Registering a domain name is easy.	Steal login credentials and redirect user to original site.

Table 4: Attack types

December 2020, the Federal Trade Commission (FTC) and 46 states sued Facebook, accusing the firm of buying up competitors, chiefly WhatsApp and Instagram, to liquidate competition in the social media industry. The FTC antitrust lawsuit aimed to force Facebook to unwind these two major acquisitions. Antitrust laws were created by Congress to preserve competition among businesses and prevent any one business from dominating a single industry and building a monopoly. When businesses compete and monopolies are restricted, companies have strong incentives to “operate efficiently, keep prices down and keep quality up,” according to the Federal Trade Commission (n.d.).

The research aims to use all these techniques to collect data and to analysing the data and come up with a framework to guard organizations against social engineering. The education sector will be targeted in this project to test their susceptibility to social engineering attacks. Eduvos is an educational institution that has allowed us to test their security.

Research Strategy

“Mixed methods research requires a purposeful mixing of methods in data collection, data analysis and interpretation of the evidence. The key word is ‘mixed’, as an essential step in the mixed methods approach is data linkage, or integration at an appropriate stage in the research process” (Ivankova, et al., 2006).

By using the mixed methods research we draw on potential strengths of both qualitative and quantitative methods, allowing us to explore diverse perspectives and uncover relationships that exist between the intricate layers of our multifaceted research questions. Primary data collection is the process of gathering data through surveys, interviews, or experiments. Our teams research focuses on primary data collections. Are team is not interested in the data itself. But what can be achieved with said data. Field surveys are one of the most effective medium for primary data collection. Regarding our research question, these interviews may take the form of household surveys or business (firm) surveys. The research team must plan and prepare for primary data collection in advance.

As with any ambitious endeavour, a successful cyberattack requires careful planning and precise execution. One thing that effective cyberattack have in common is the ability to remain covert – right up until the moment that the time is right to attack the system. While the precise methods of attacks vary, they usually follow a series of similar steps, referred to as the cyberattack chain.

Creating guidelines to breaking into user accounts. Phishing attacks will be the first step. This will occur through emails that either contain fraudulent links to cloned websites or a malicious attachment. Somewhere along the chain of events that begins with the user taking the bait, the fraudsters will present a fake login form to steal the user's login name and password. Fraudsters will also use some form of interception between a user and a genuine sign-in page, such as a man-in-the-middle attack to steal credentials.

We shall use a form of password spraying. This will take a list of user accounts and test them against a list of passwords. The passwords are all known passwords for users. Password spraying is blunter. The fraudster has a list of usernames, but no idea of the actual password. Instead, each username is tested against a list of the most used passwords. That said, there are lots of publicly available post-exploitation kits that offer attackers off-the-shelf keyloggers, as well as commercial spyware tools supposedly for parental or employee monitoring.

The Model

Use Case Diagram

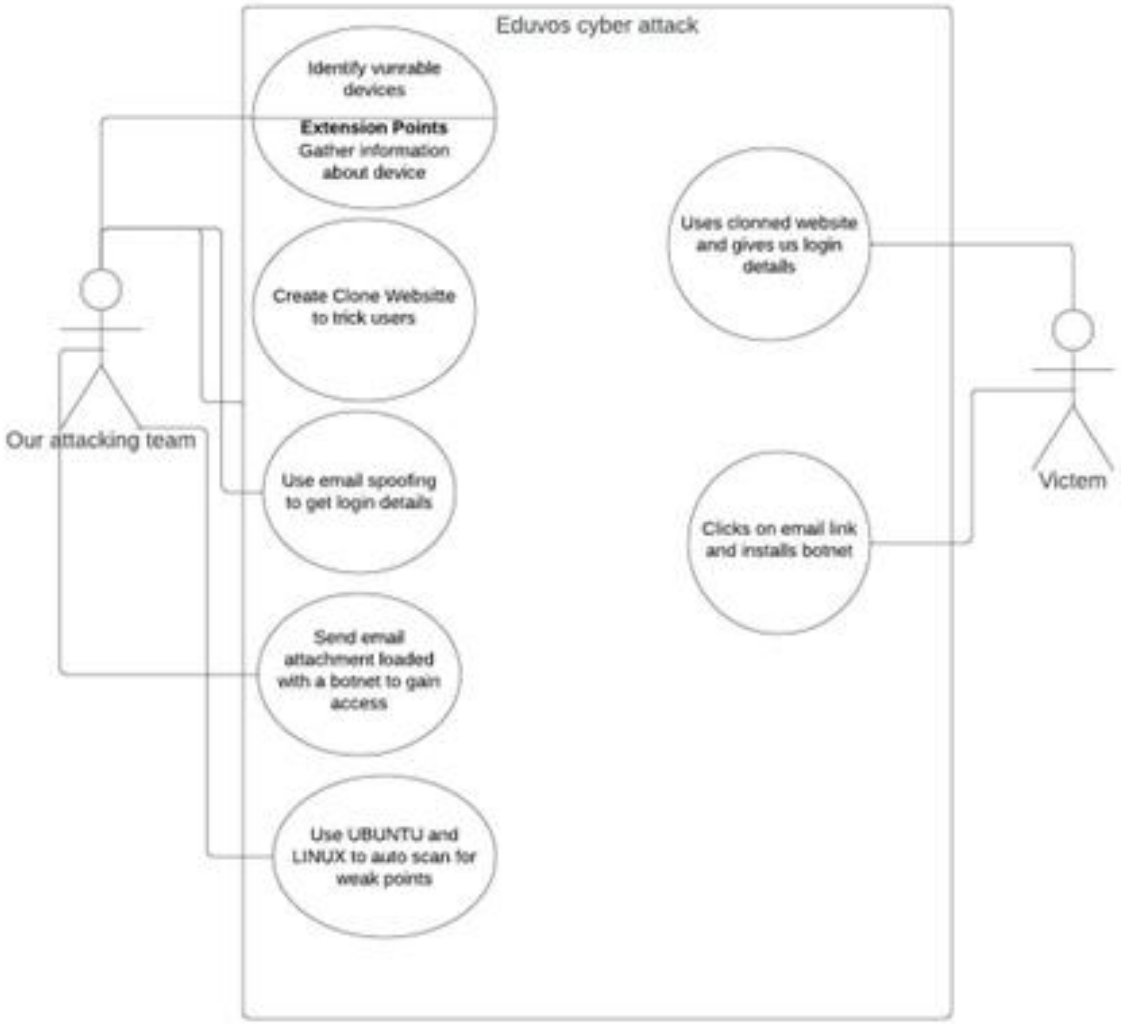


Figure 9: Use case diagram

Context Diagram

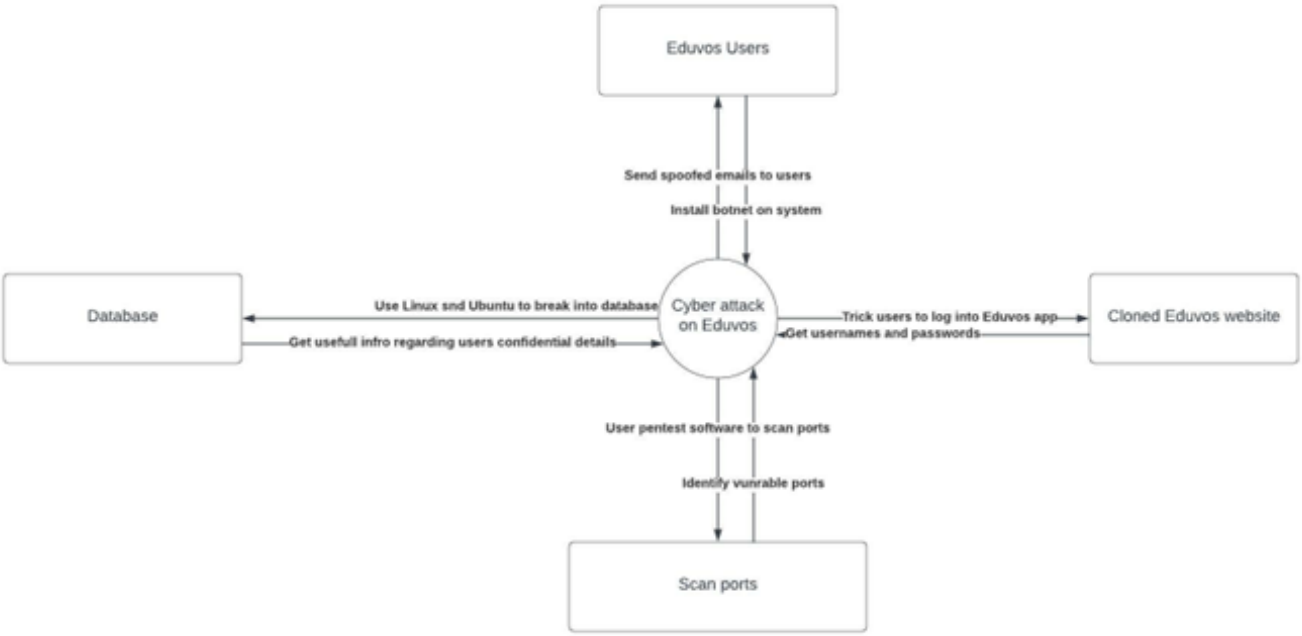


Figure 10: Context Diagram

Data Flow Diagram (DFD)

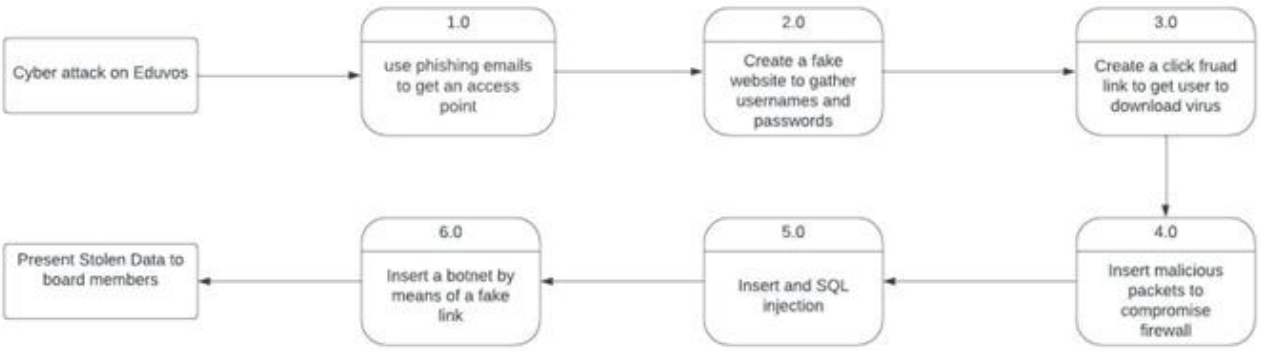


Figure 11: Data Flow Diagram (DFD)

Entity Relationship Diagram (ERD)

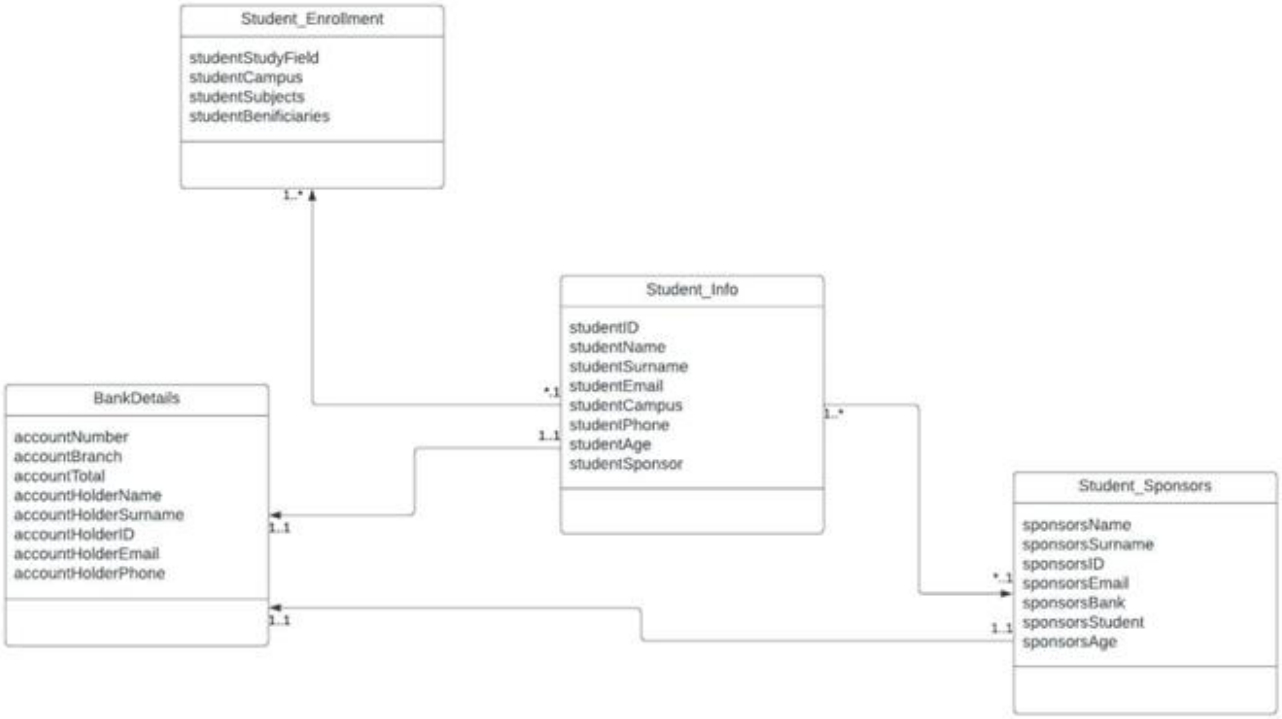


Figure 12: Entity Relationship Diagram (ERD)

Data Driven Models

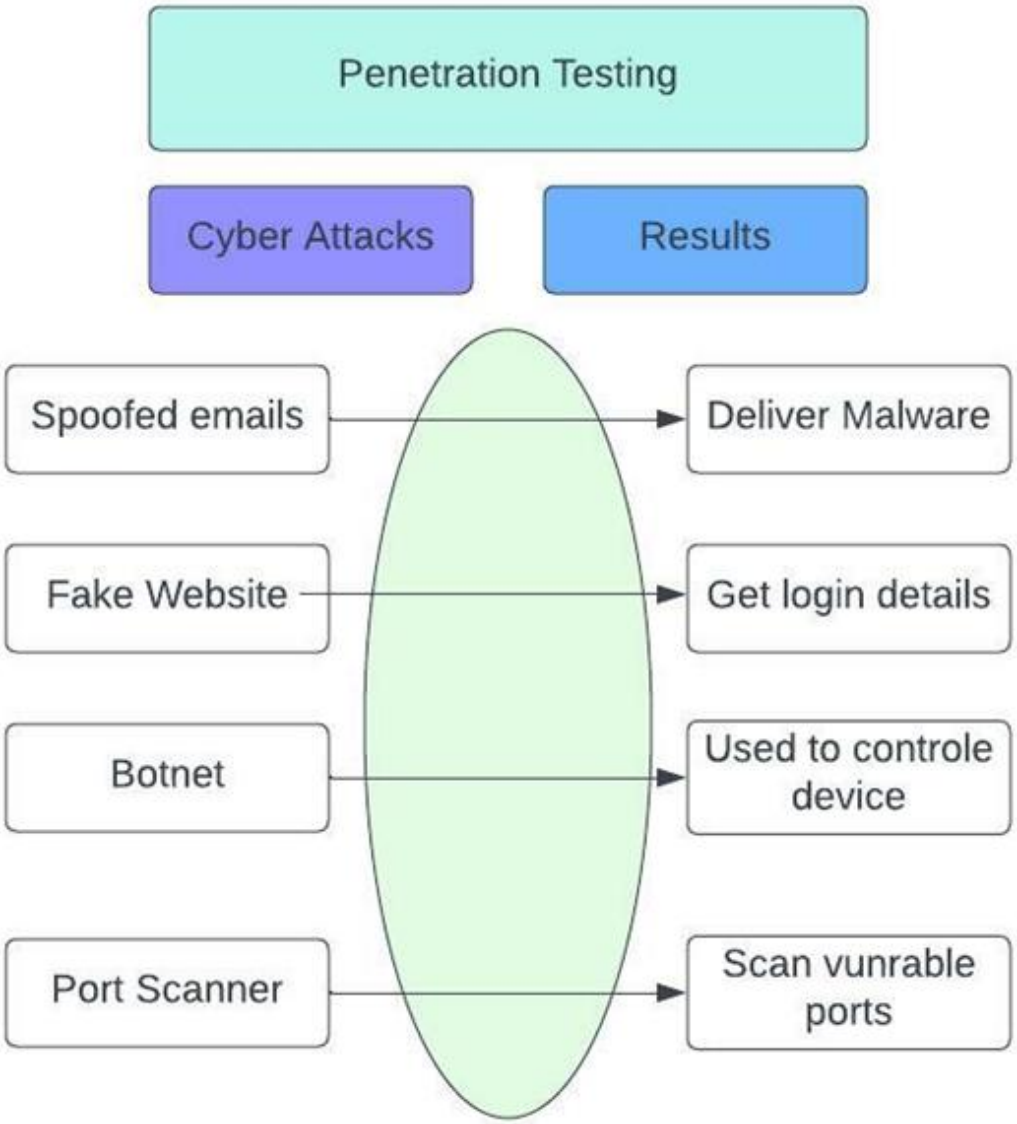


Figure 13: Data Driven Model

Cyber Security Incidents

In an RSA Security LLC breach in March 2011, a group of offenders used social engineering techniques to hack into RSA Security. The company, named after the initials of co-founders Ron Rivest, Adi Shamir, and Leonard Adleman, is known for the RSA two-factor authentication tokens. “By using social engineering via email (i.e., email phishing),

the offender persuaded an employee to open an attached malware-containing spreadsheet file". The malware installed a backdoor that allowed the offender access to the machine. "From there the offender was able to browse the network (Richmond, 2011)".

Phishing is defined as "a scalable act of deception whereby impersonation is used to obtain information from a target" (Lastdrager, 2014). The first part of the definition ("scalable act") relates to the bulk distribution of messages. The second part ("deception whereby impersonation is used") is required to make it fraudulent.

"In one account, the target receives a message via WhatsApp from one of its contacts that encourage to click and receive a £100 worth of vouchers for the supermarket. Clicking the link allows the offender to install malicious software on the phone (McGoogan, 2016)".

"An attack scenario, using WhatsApp, aims to steal money by impersonating a family member. The following MO is used: The offender informs the target of having a new phone number. This includes a matching profile picture of the person who is impersonated. The picture is harvested from social media, as well as family relations and how people interact with each other (Fraudehelpdesk, 2018)".

Impacts

Social engineering has a massive impact on the business sector (ostec, 2018). Every year, many businesses fall prey to some type of social engineering. The reputational impact of social engineering on a company is the first step. While losing commercial information can be disastrous, few factors are more challenging to regain than client trust. For instance, why are hackers able to have such a profound impact on customer perception?

The impact of getting hit by Ransomware

Malware is frequently the source of social engineering's business impact. Especially software that makes money for criminals, including such ransomware. This type of malware is designed with one objective in mind: infecting, encrypting, and holding files for ransom. When it's revealed that a firm has succumbed to ransomware, it loses the hard-

won trust of present and future customers (EASYDMARC, 2022). Certainly, incidents like these tend to motivate further security measures, however the harm has already been committed, and rebounding back requires more than restoring stolen data.

The impact of falling prey to watering hole attacks

This assault effectively hacks a company's most-visited websites and uses them as a breeding ground for infection (Velusamy, 2018). Whether a company's own website is included on the blacklist, the consequences are felt well beyond the firm, affecting current and future customers.

The impact of cost on business productivity

Many attacks, if serious enough, render going about your daily routine difficult. Some amount of management and clean-up will be required. Certain assaults, particularly ones that need extensive investigation, might, nevertheless, wreak havoc on a company's productivity (Ugoani, 2019).

The impact of financial losses

While reputation and productivity are crucial, businesses exist to make money. One of the most dangerous impacts of social engineering on company is the loss of money. Whatever social engineering assault might result in financial consequences for a firm. This is due to the illegal sale of sensitive information on black markets, as well as the consequences of losing public trust. Business will be lost should clients lose trust as a result of a security breach and data loss.

The impact of disruption in operations

The impacts of social engineering on companies extend beyond job performance. It's typical for operations to be disrupted, and it may get a lot worse. Almost every assault has some impact on a company's operations (Essuman, et al., 2020). Those who compromise

systems and websites, on the other hand, are the ones that frequently create the greatest disruption and havoc.

Social engineering may have far-reaching impacts that go beyond lost files and stolen information. Different attack methods can affect a company's operations to be disrupted, as well as financial loss and a negative reputation. That's why it's critical that you and your team know how to prepare for, recognize, avoid, and respond to social engineering assaults.

Risk Factors

“Research has been done to investigate the degree to which users are prepared to disclose personal information online and the context in which disclosure increases or decreases". Information online and the context in which disclosure increases or decreases (Security Intelligence, 2019).

Social engineering, a technique that utilises the vulnerability and manipulations of human interactions and emotions to obtain data or information, leaves Eduvos open to a vast number of risks and potential social engineering-based attacks. Threat actors may pose as sponsors or students and utilise phishing and spear-phishing to send emails, to staff and faculty of Eduvos, to obtain student data. The attacker may also do the reverse and pose as Eduvos and target the students with phishing attacks. This data may be incorporated into future potential attacks and social engineering tactics.

Scenario Models Simulations

The scenario is modelled on Eduvos’ systems and is executed by utilising two desktops. These desktops utilise the Windows Server and Ubuntu operating systems as the entry point for the penetration testing. Exploitation of the server is performed using Kali Linux, utilising Wireshark, Nmap, Social-Engineer Toolkit (SET), Nessus, Maltego, GetNotify, and Emkei’s Mailer as the primary tools.

Kali Linux, formerly known as BackTrack Linux, is a Debian-based Linux platform used to perform advanced penetration testing. It is open-source and includes over 600 tools for penetration testing tasks (g0tmi1k, 2022).

Wireshark is a packet sniffer, or network protocol analyser that captures packets from a network connection. In addition to packet capture, Wireshark is also able to apply filters to only obtain specific information and visualise conversations and network streams in a packet. It is used to troubleshoot networks, trace connections, view transactions of suspect networks, and identify bursts of network traffic (Wireshark, n.d.; CompTIA, n.d.).

Nmap is a tool used to scan and discover networks and ports. The information gathered from the IP packets include the available hosts on the network, the operating systems and services they are running, and the firewalls or packet filters in use, in addition to many other features (Nmap, n.d.).

The Social-Engineering Toolkit (SET) is an open-source Python based tool used for penetration testing and is comprised of features such as instant cloning of a website to create a phishing page, sending SMSs, and faking phone numbers. Phishing, web and mass mailer attacks can also be launched with this toolkit (Borges, 2020).

The Nessus vulnerability scanner allows a penetration tester to perform malware detection, asset discovery, target profiling, and sensitive data discovery. It is used for penetration testing and vulnerability assessments and is free to use for non-enterprise purposes (Obbayi, 2019).

Maltego is a data visualisation tool for real-time data mining and information gathering. The collected data is represented graphically with nodes on a graph, where they can be grouped together (Maltego, n.d.).

GetNotify is an email tracking service that attaches an invisible tracking image to outgoing emails that notifies the sender of the exact time the recipient email was opened (GetNotify, n.d.). Emkei’s Anonymous Mailer can be used to spoof email addresses to launch phishing

attacks. The recipient receives an email from the spoof email address, through which malicious attachments can be sent as well (Husein, 2020).

Scenario Models Outlines

This time-honoured model has been around the longest, and cybersecurity pros and software applications refer to it often. Originally published in 2011, the Cyber Kill Chain, shown in Figure 14, outlines the following seven steps that an attacker takes during an intrusion:

Reconnaissance: Ports will be scanned, and weak security and weak password will be exploited. Weaponization: Will user phishing attacks to gather useful user credentials.

Delivery: The malware will be delivered on a link.

Exploitation: Will use a password obtained by phishing to get admin access.

Installation: Will install a Botnet to give us full control over the system.

Command and Control: Will use the botnet to install a crypto currency miner.

Actions on Objectives: Break into Eduvos' computer network and get user credentials and convince counsel of the threat of social engineering.

It is an effective model because it authoritatively lays out the typical steps an attacker takes. Furthermore, this model took the anecdotal wisdom of thousands of subject-matter experts and standardized a great deal of the vocabulary used in the industry.

Attack Scenarios

- Weak antivirus or default antivirus installed on a computer system makes exploiting them with a low-level attack much easier. Free antivirus programs are much easier to exploit.

- Use social engineering tactics to simulate password requests from familiar sources such as the help desk or even executives from Eduvos and try to get login details.

- Create a spoofed website to trick Eduvos students and staff to enter their login credentials. Apps without stringent password policies for business accounts, weak passwords, and no multi-factor authentication are prime targets for the attack.

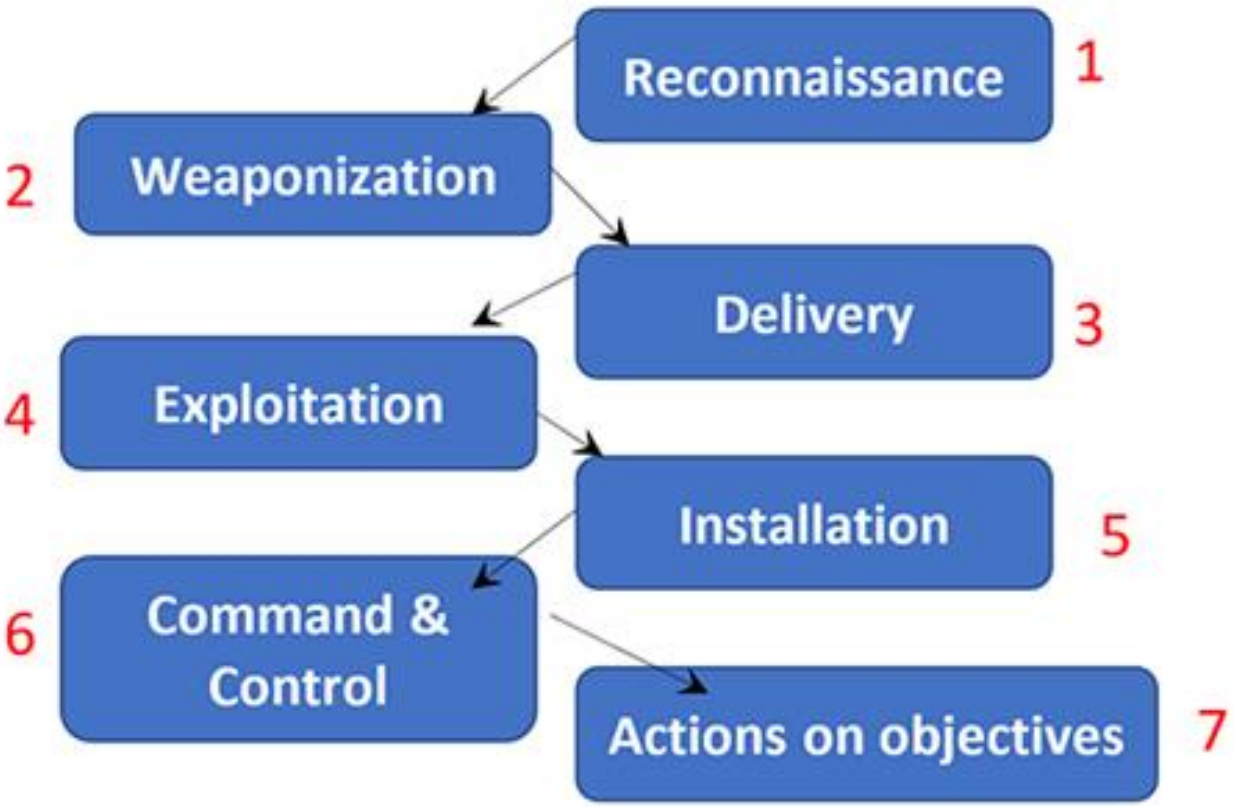


Figure 14: Cyber Kill Chain

Simulation results and analysis

Simulation Labs
SQL injection using Burp Suite tool

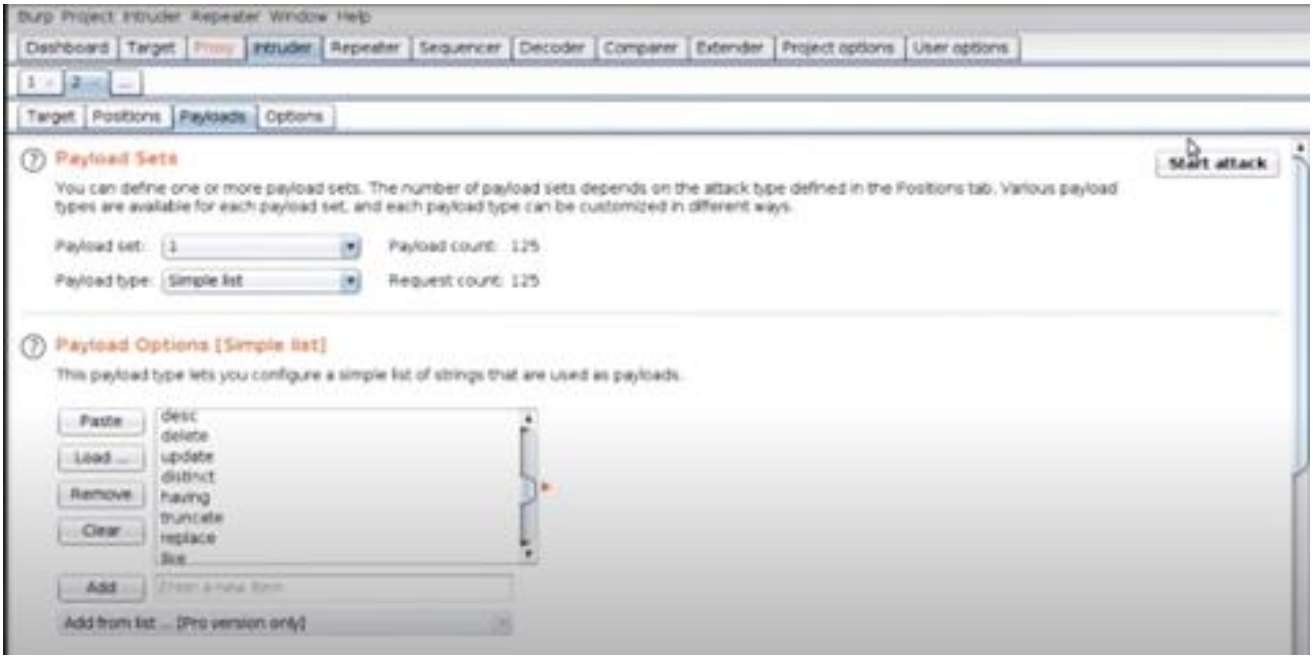


Figure 15: SQL injection (SQLi) Payload

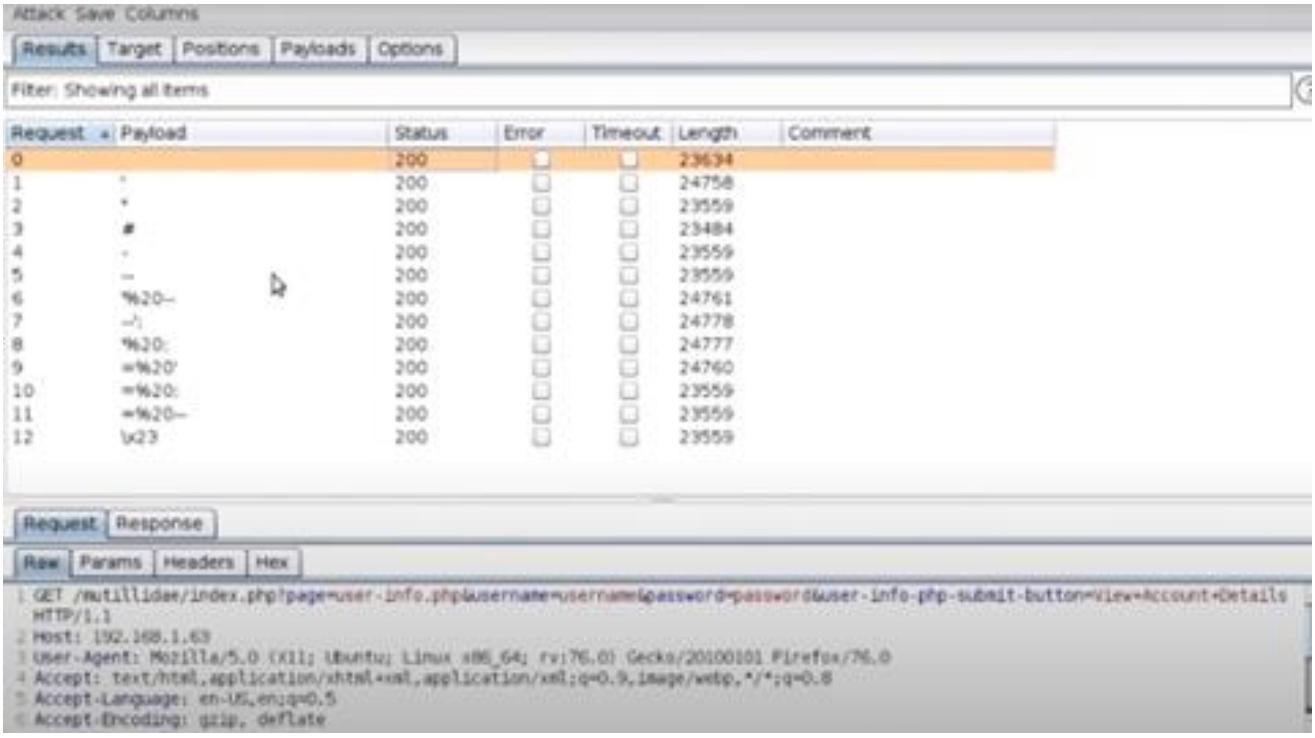


Figure 16: SQL injection (SQLi) Result

Portscanning using ZenMap on ParrotOS

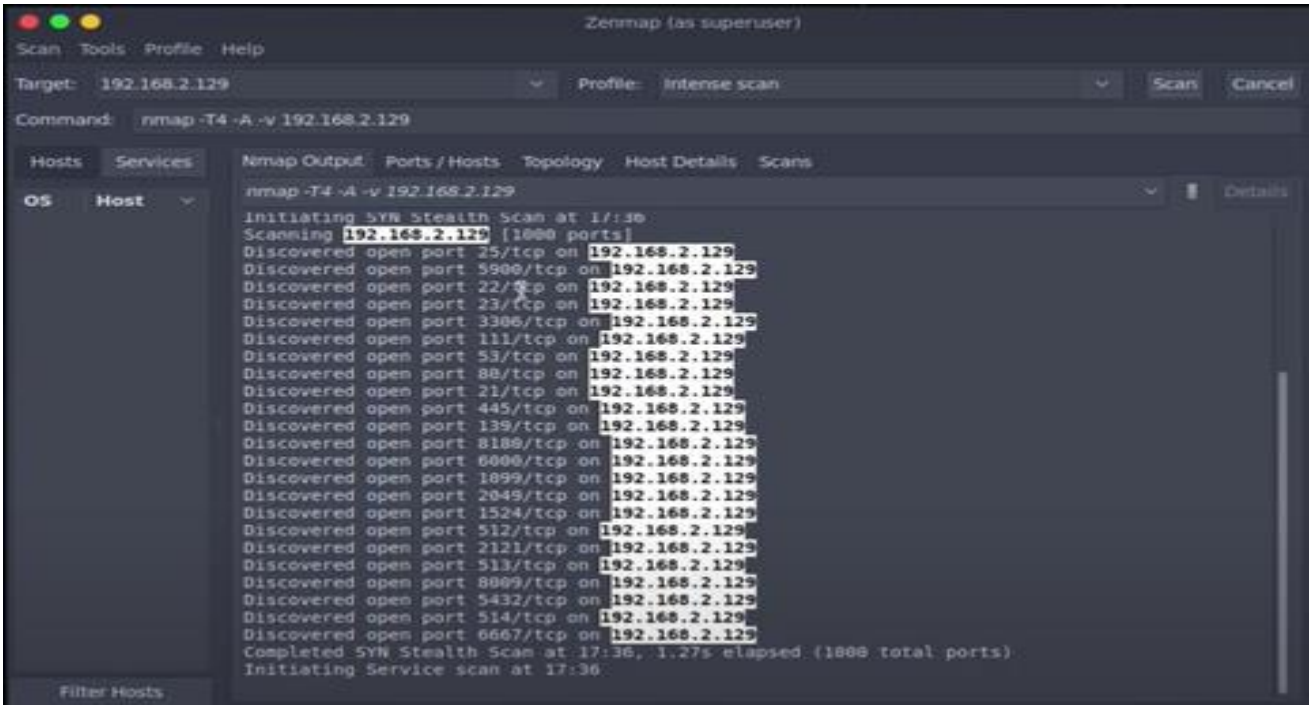


Figure 17: Port Scan Output

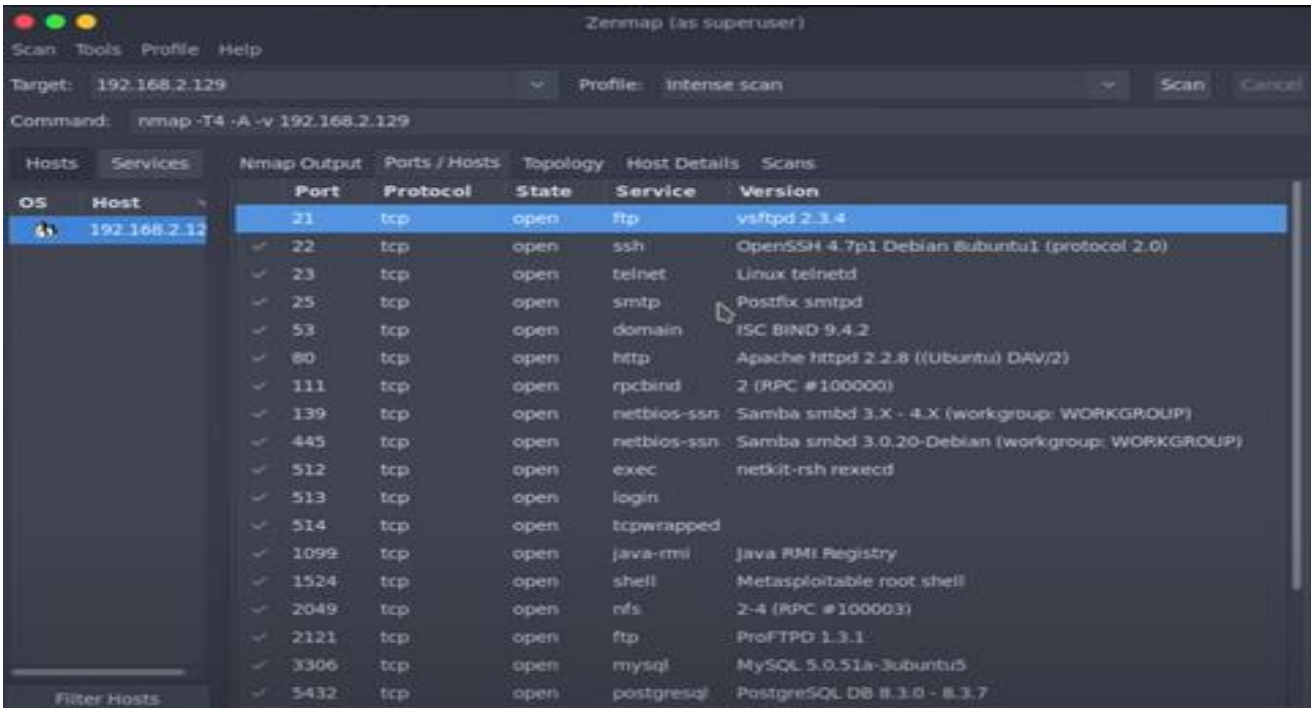


Figure 18: Port Scan Ports

Simple Python Port scanner:

portscanner.py

```python
import socket
import sys


def scanHost(ip, startPort, endPort):
    """ Starts a TCP scan on a given IP address """

    print('[*] Starting TCP port scan on host %s' % ip)

    # Begin TCP scan on host
    tcp_scan(ip, startPort, endPort)

    print('[+] TCP scan on host %s complete' % ip)


def scanRange(network, startPort, endPort):
    """ Starts a TCP scan on a given IP address range """

    print('[*] Starting TCP port scan on network %s.0' % network)

    # Iterate over a range of host IP addresses and scan each target
    for host in range(1, 255):
        ip = network + '.' + str(host)
        tcp_scan(ip, startPort, endPort)

    print('[+] TCP scan on network %s.0 complete' % network)
```

Figure 19: Python Port scan 1

portscanner.py

```python
def tcp_scan(ip, startPort, endPort):
    """ Creates a TCP socket and attempts to connect via supplied ports """

    for port in range(startPort, endPort + 1):
        try:
            # Create a new socket
            tcp = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

            # Print if the port is open
            if not tcp.connect_ex((ip, port)):
                print('[+] %s:%d/TCP Open' % (ip, port))
                tcp.close()

        except Exception:
            pass


if __name__ == '__main__':
    # Timeout in seconds
    socket.setdefaulttimeout(0.01)

    if len(sys.argv) < 4:
        print('Usage: ./portscanner.py <IP address> <start port> <end port>')
        print('Example: ./portscanner.py 192.168.1.10 1 65535\n')
        print('Usage: ./portscanner.py <network> <start port> <end port> -n')
        print('Example: ./portscanner.py 192.168.1 1 65535 -n')
```

Figure 20: Python Port scan 2

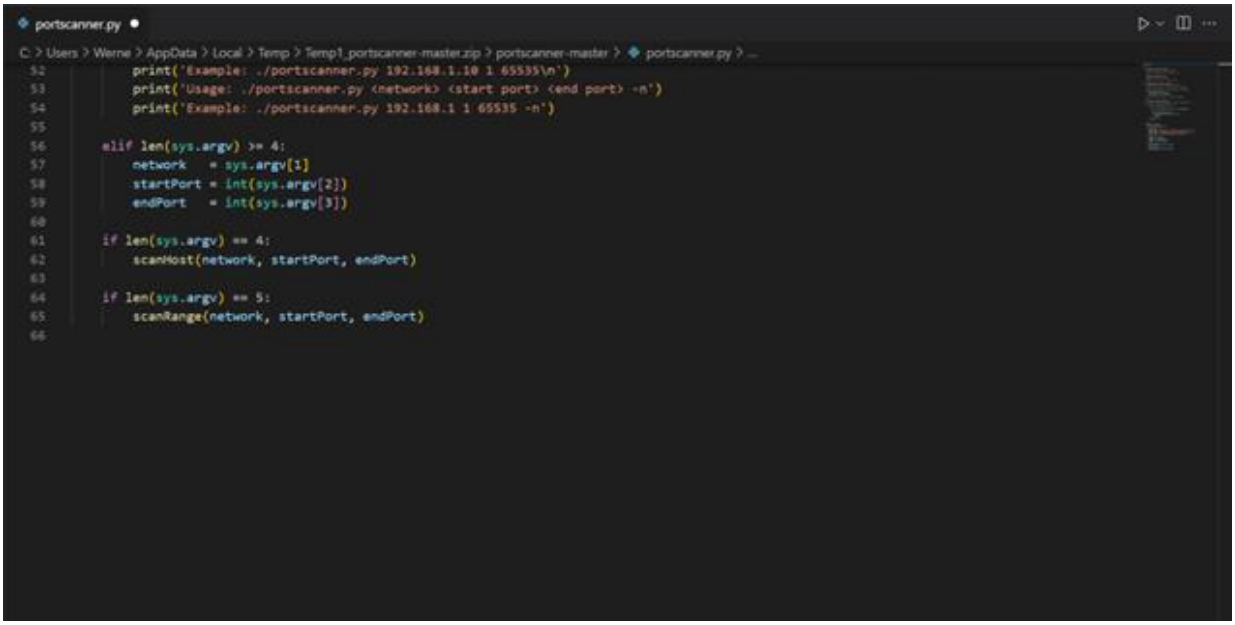


Figure 21: Python Port scan 3

Kali Linux Nmap port scan

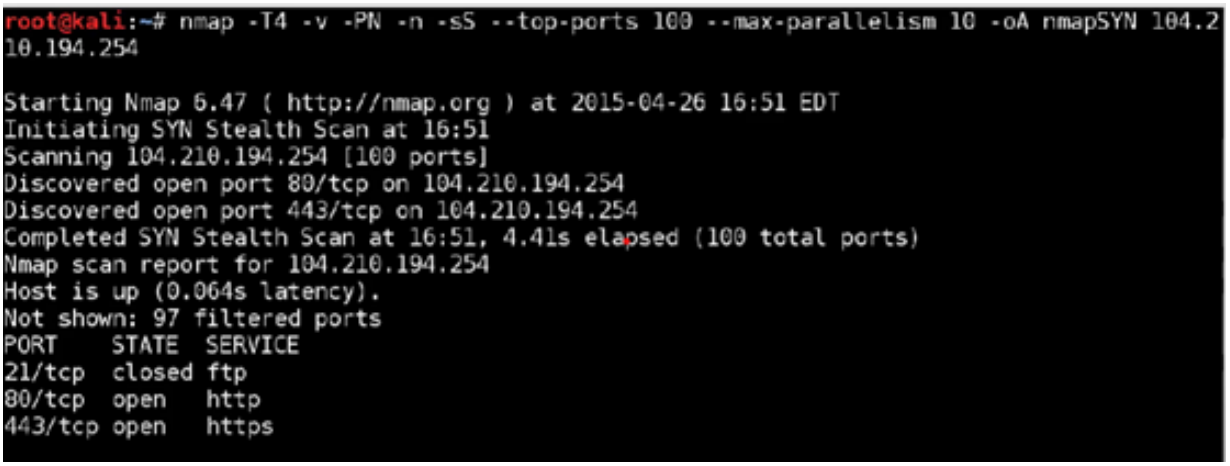


Figure 22: Nmap Port scan

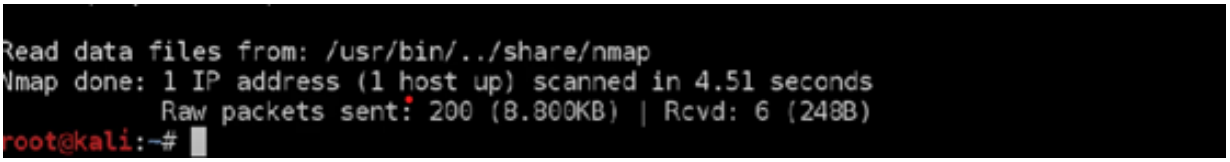


Figure 23: Nmap Port scan result

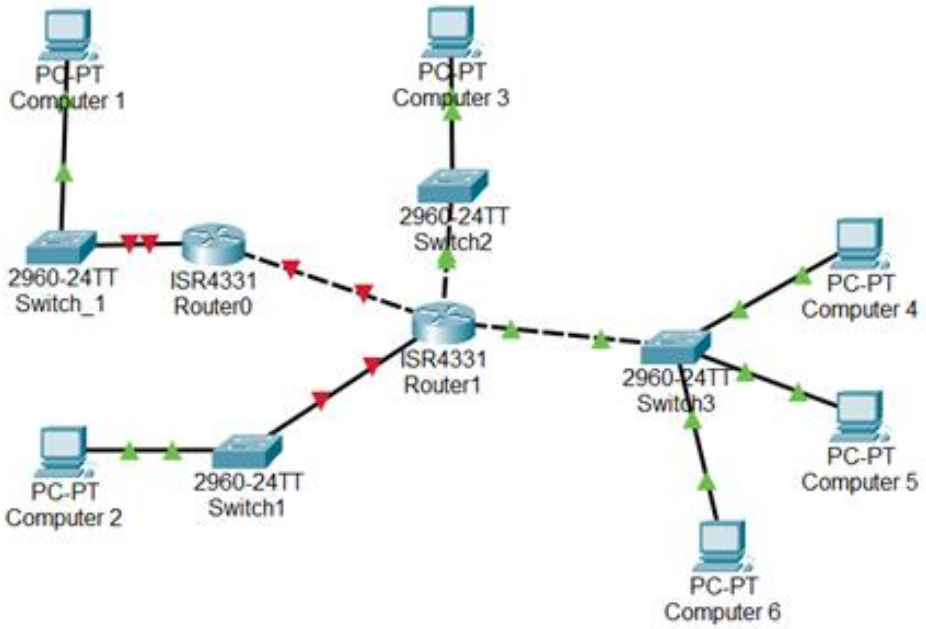


Figure 24: Packet Tracer Network Simulation

Running Nessus and Nmap in Kali Linux

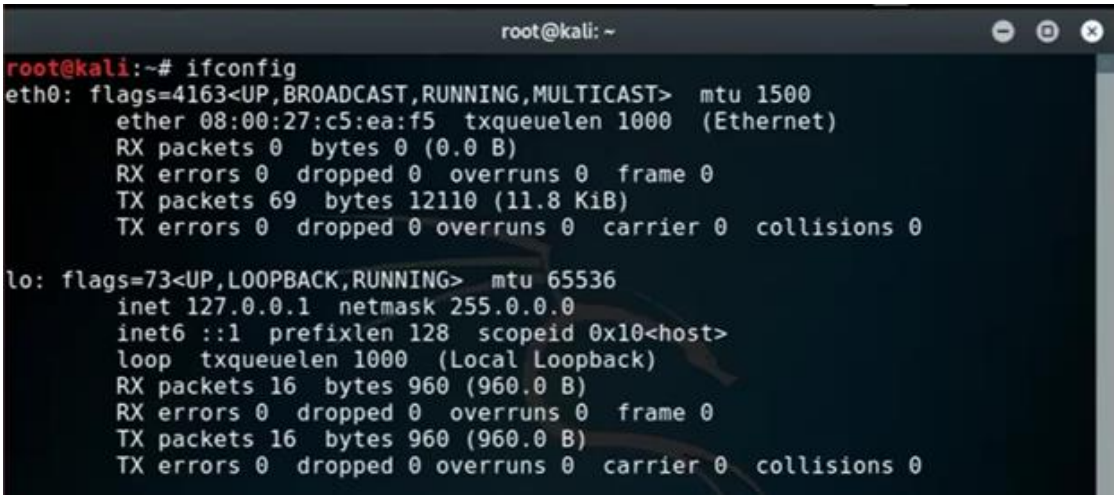


Figure 25: Nessus Scan

Configuring IP address and pinging default gateway.

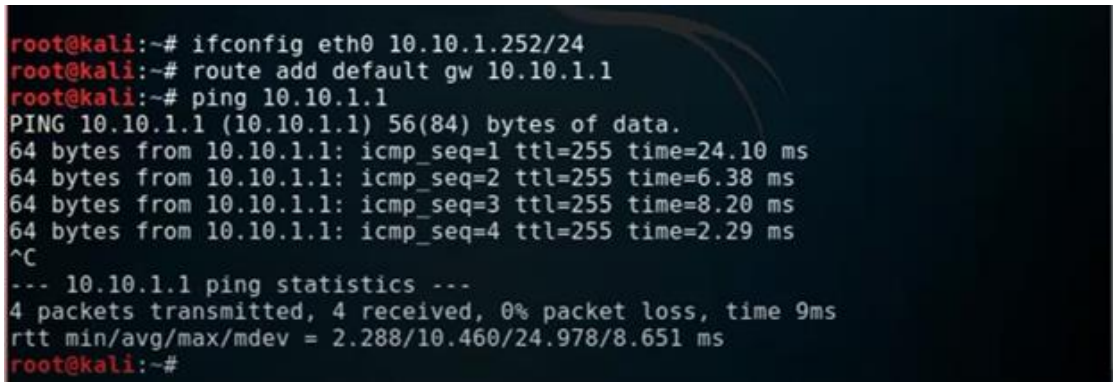


Figure 26: Ping Default Gateway

Test plan

According to Rubin and Chisnell (2018), the “test plan is the foundation for the entire test. It addresses the how, when, where, who, why and what of your usability test.” The test plan follows the process of obtaining an entry point into the system, performing techniques and exploits, and finally recording the results. Details of the methodical procedure of testing performed are outlined in Table 5.

Test plan for Attack Eduvos computer network in a controlled environment.				
Increment	**Test type**	**Test date**	**Team members**	**Successful YES/NO**
Use phishing email to obtain a system entry point	Ethical Hacking	13/06/2022	Werner Heinrich	Yes
Create a phishing website to log and extract usernames and passwords	Risk assessment	14/06/2022	Werner Shailen	Yes

Increment	Test type	Test date	Team members	Successful YES/NO
Generate links embedded with malware to infect host PC's	Ethical hacking	15/06/2022	Ontlametse Bhavish	Yes
Insert malicious packets to compromise firewalls	Infrastructure Penetration testing	16/06/2022	Bhavish Werner Heinrich	Yes
Insert and execute SQL injection	Vulnerability Scanning	16/06/2022	Ontlametse Werner Shailen	Yes
Generate links to deploy botnets	Security auditing	15/06/2022	Shailen	Yes
Record findings	Risk assessment	17/06/2022	Heinrich	Yes

Table 5: Attack types

Ethical considerations

As a result of the nature of this research project, many ethical issues and considerations must be addressed. These ethical issues and considerations need to be addressed, in order to prevent the group from breaching and or violating any existing laws and regulations pertaining to accessing, altering, or damaging a computer system without permission. According to Pike (2013), students should not be practicing ethical hacking as it encourages the students to conduct illegal activities, but ethical hacking in this case is used to identify vulnerabilities and mitigate them before an attack. Thus, the group has submitted the proper documentation to Eduvos (See Appendices 1, 2 and 3), thus giving us the required clearance to conduct our research within the Eduvos environment.

Another large potential ethical issue that has become apparent is the safety and security of the personal, and or privileged, data of Eduvos. Ethical issues will always arise when conducting a penetration test. When penetration testing, evaluating a security feature of a computer system may result in the disclosure of personal or confidential information to the penetration tester and organization management (Faily, et al., 2015). In order to prevent any privileged information from being disclosed, the group has opted to create a virtual and mock server to mimic Eduvos Potchefstroom's Servers. Therefore, allowing the group to not only test the possibility of gaining access to the server but to also identify existing vulnerabilities within the Eduvos Potchefstroom servers.

Summary

A Mixed method approach to our research has been a great approach thus far, as it enables us to gather more information than we have predicted. Our mixed approach is inclusive of field surveys, questionnaires, penetration testing tools such as Kali Linux, Ubuntu, Parrot. These tools assisted us in enumerating data, and we were able to scan ports using Nmap, Wireshark and Python using TCP scans using sockets in the python library. Using the root terminal in Kali Linux, after running a few commands were able to get the IP address and information of the virtual machine.

Information gathering is a crucial step or phase in ensuring successful execution of the testing. Chapple and Seidl (2018) stated that successful penetration testers need to build a solid information-gathering plan that showcases each tools capabilities and where each tool can be used accordingly. Based on the figures present earlier, a solid foundation of information gathering is formed and has opened the door to the next phase of the penetration life cycle, which is known as the Attacking and Exploiting phase.

CHAPTER 4: PRESENTATION OF RESULTS/FINDINGS

Introduction

The main goal of this study is to investigating Social Engineering Techniques to generate a comprehensive risk assessment report for Eduvos. However, to obtain the results, we desire, the group must now take on the role of the “attacker” and perform penetration testing techniques, within a controlled environment that will simulate that of the Eduvos environment and document our findings. The mixture of the proposed penetration techniques requires a suitable methodology; thus, we have opted to utilise a mixed methodology, consisting of quantitative and qualitative techniques, allowing us more flexibility within the study. As stated before “Mixed methods research requires a purposeful mixing of methods in data collection, data analysis and interpretation of the evidence” (Nataliya, et al., 2022).

The group members will each carry out a proposed field within penetration testing. These fields include mobile phone attacks, botnet attacks, simple ways to gain access and modern wireless network attacks. Each will be conducted in an Eduvos simulated environment, in a manner that will ty and mimic the real-world environment as much as possible.

Developing a system architecture

The system architecture, as seen in Figure 27 below, illustrates various phases that will be implemented during the practical portion of the research project. The phases may be divided into three main stages, the first stage being the planning and reconnaissance stage. This stage simply consists of each group member planning out how to execute their own proposed attack, these attacks include mobile phone attacks, botnet attacks, simple ways to gain access and modern wireless network attacks, in addition to using social engineering techniques to obtain as much information as possible, regarding the target system. The second stage of the research is the attacking stage, in which we will utilise our proposed attacks to try and obtain access to the respective targets. The third, and final stage, is to obtain, document and compile a report on our findings during our research.

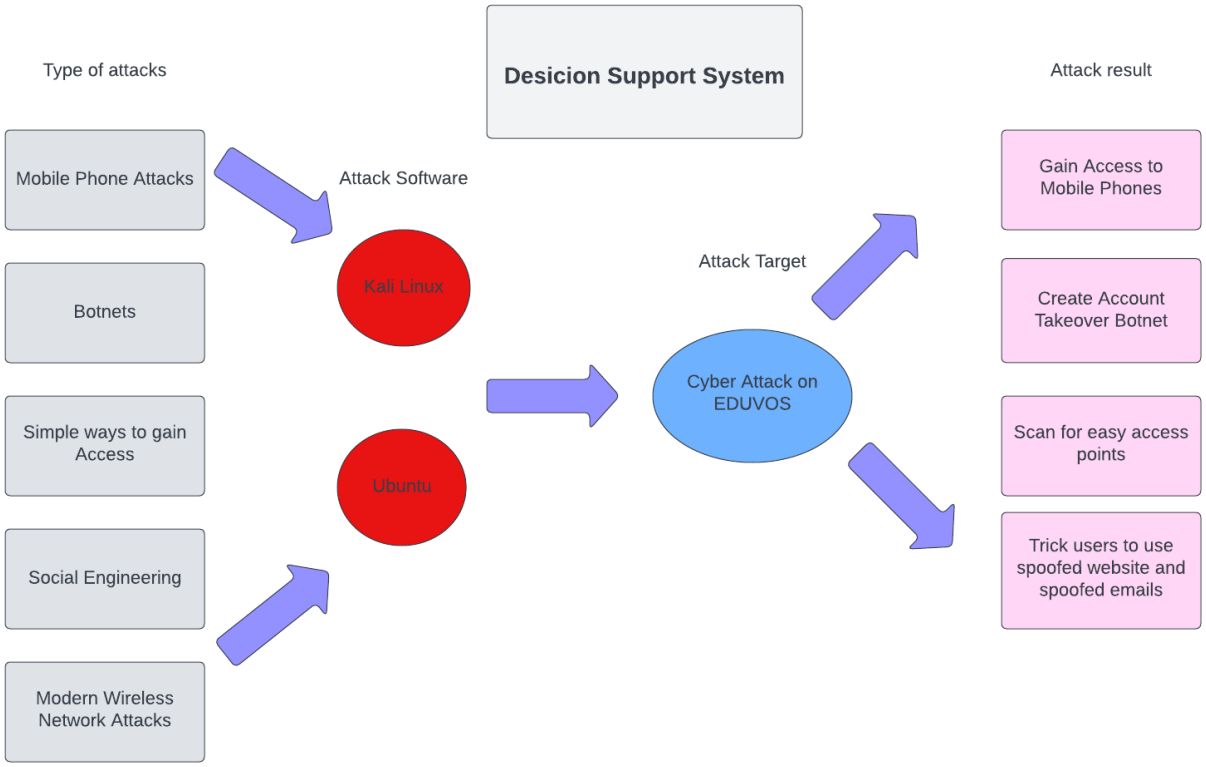


Figure 27: Decision Support System (DSS)

Analyse and design the system

Our team will use action-orientated research to strengthen our case. We will show practical uses of penetration testing principles and tools to try and show that Eduvos is vulnerable to a social engineering attack, as well as a cyber-attack. We will look at previous attempts of social engineering attacks on the education sector, by conducting our research on a test machine will ensure that we do not disturb the everyday workings of the institute. Our team will document every step that will be taken in this simulated attack and after we have completed our test, we will present our findings.

We first need to define the goal of what we want to get out of the experiment. Our team will be contributing to the project by designing and creating their own type of attack framework. These frameworks will later be combined into the final attack framework. The target has already been identified as the educational institute Eduvos and the target system is a test machine stationed at Eduvos.

Implemented Frameworks:	Description:
Botnets	• Setting up and configuring a Botnet. • Utilising the configured Botnet to execute an account takeover within the mock Eduvos Environment.
Simple Ways to Gain Access	• Execute and implement password cracking and or hacking techniques on the mock Eduvos server. • These techniques are as follows: - Brute force, Dictionary, and Wordlist password hacking. - Password Hashing. - NMAPing
Mobile Phone Attacks	• Exploiting data storage vulnerabilities in a physical device, from the Eduvos environment, to gain access.
Modern Wireless Network Attacks	• Executing an attack on a mock Eduvos network to gain a better understanding of current wireless network attacks and what countermeasures may be taken to mitigate them. • These wireless network attacks include: - MitM - DDoS (Distributed Denial of Service) - Packet Sniffing - WEP, WPS, and WPA, WPA2 assaults
Social Engineering	• We shall conduct social engineering-based attack within a controlled Eduvos environment. • These social engineering attacks include: - Phishing - Spoofing - Spear phishing

Table 6: Implementing Frameworks

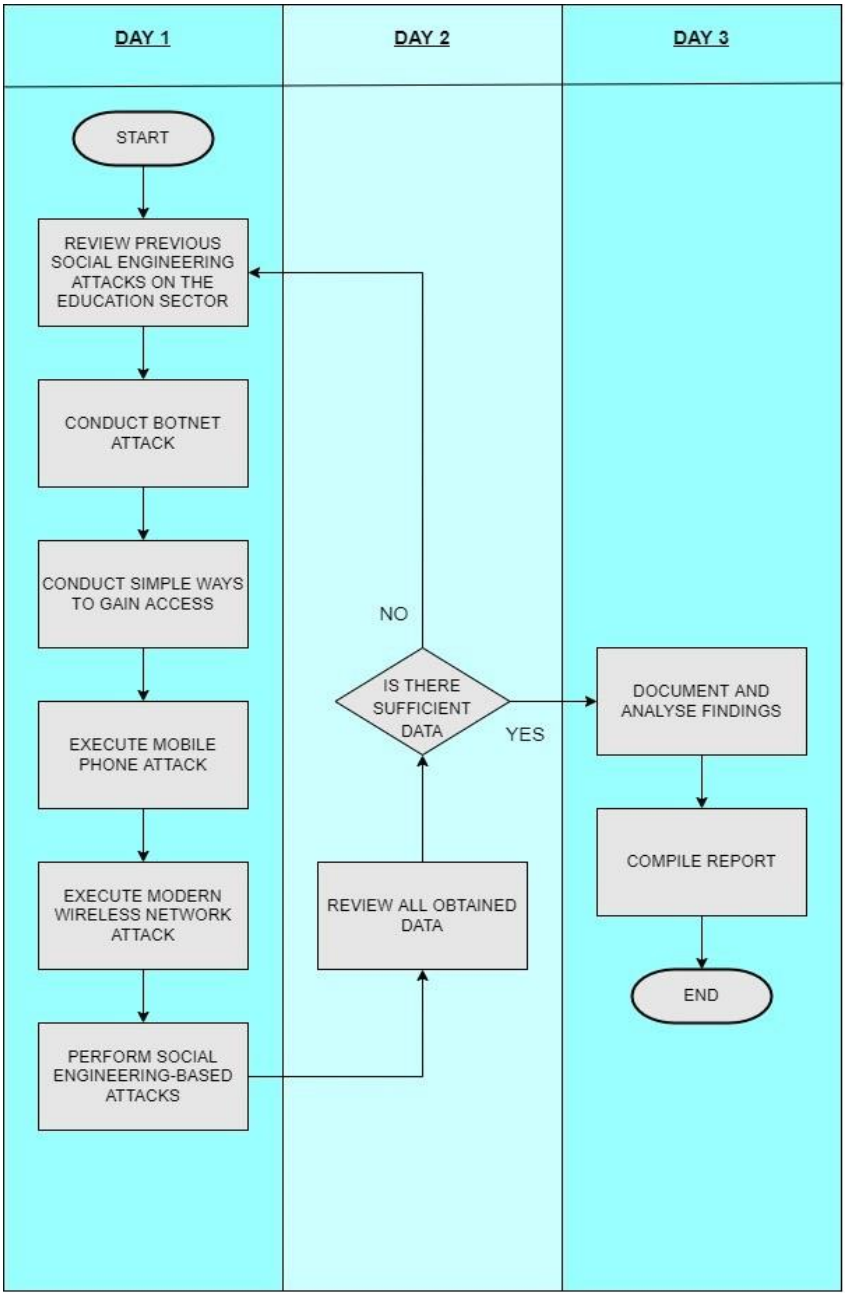


Table 7: Attack Data Flow

Botnet Attack

“Account takeovers botnets are one of the most common ways for businesses and individuals to lose money today. Businesses, in practise, rely on limited detection methods such as static security rules, rate limits, and basic bot protection. These techniques are effective against technical threats such as SQL injection and cross-site scripting. They can

also provide defence-in-depth by slowing the momentum of a wide range of attacks when used as part of a multi-layered strategy.” (Yury & Nadav, 2019). Our team will focus mostly on the use of an account takeover botnet for the project. This botnet is specially designed to harvest user accounts login information.

The account takeover botnet will be used in conjunction with the other attack projects to give the desired result. The botnet will be loaded onto a trojan virus. The virus will be used as a payload to send out to compromised computers and mobile devices. These devices will be compromised using social engineering attacks and spoofed websites and email.

The team will use Nmap to scan the targeted network and search for entry points. Nmap will show by means of IP packets what services the targeted system is running and show what filters and firewalls are in use. This will give our team a good starting point for the rest of the attack.

Nessus will be used by the team to remotely scan and check the targeted system for security vulnerabilities. Nessus will give alerts to the team of any potential security flaws. When security flaws are detected, the team will have a clear understanding of the weak points of the system. Wireshark is another tool that will prove useful in this attack.

Kali Linux has numerous low skill attacks regarding password cracking. These attacks include crowbar, crunch, Medusa, findmyhash, gpp-decrypt etc. These tools range in function from cracking hashes in encryptions to brute forcing passwords and many more. These attacks are commonly used in penetration testing and if they are successful will prove that Eduvos is vulnerable to cyber-attacks and social engineering.

Wireshark will be used to analyse the packets of the network and provide a detailed report regarding the state of the packets. A botnet will be created to infect other computers on the network an install automatic crypto-currency miner on them. Build Your Own Botnet (BYOB) is a very well know open-source botnet builder that has many builds in modules that will be useful in the attack scenario. The BYOB botnet builder is run through the cmd of Kali Linux. Docker, opencv-python, and Flask will be installed into the botnet file as well.

A spoofed website will be created to mimic the login page of MyLMS to trick users to giving up their login credentials. Burp Suite will be used to for security testing of the current MyLMS website to search for potential weak points. The spoofed website will upon completion redirect the user to the legitimate website.

A phishing attack will be launched to try and get potential victims to download our rootkit to infect their computers. The rootkit will have a botnet as its payload that will infect other computers and install crypto-currency miners on them.

Botnet installation process

- Setting up the botnet by first downloading the Byob project then running all necessary commands then installing all file dependencies.
- Installing docker because it has many of the needed file dependencies.
- Running the **sudo ./startup.sh** script will begin to create the botnet by downloading all the required file libraries.
- Error was fixed by reinstalling docker.
- Additional libraries and dependencies being installed.

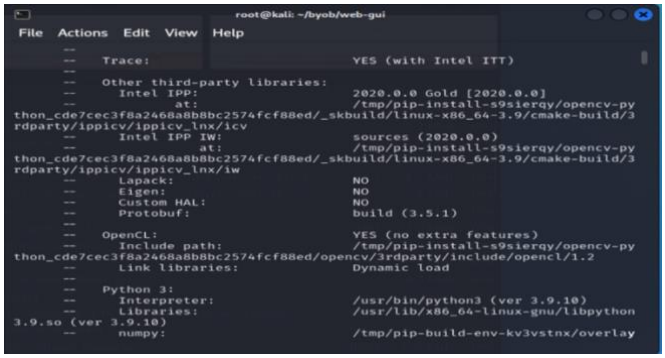


Figure 28: Build Your Own Botnet (BYOB) Installation

- Installing pip
- This botnet uses extensive C++ libraries.
- Ubuntu packages being installed.

- Botnet installation
- Installing crypto currency miners.

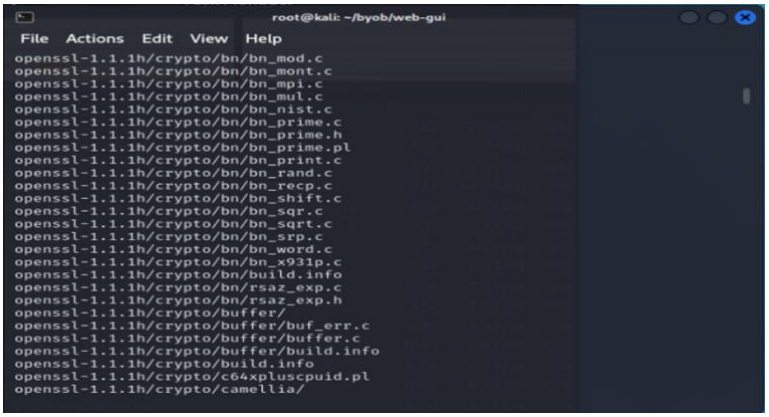


Figure 29: Install Crypto Miners

Other Types of Botnets

- Updating the required python packages.
- Installing the python setup file.
- Running ufonet
- Types of botnets.

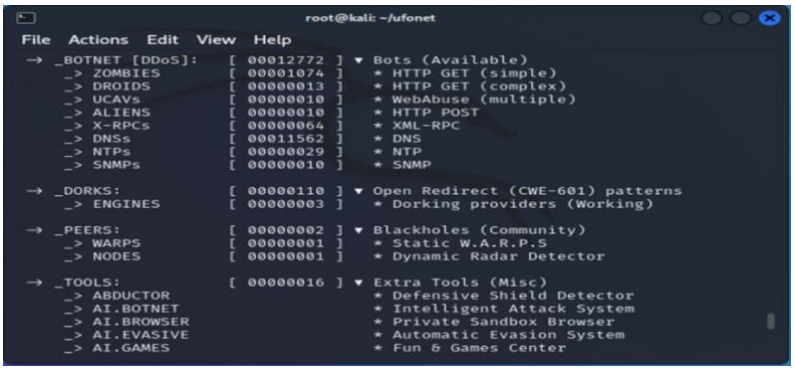


Figure 30: Available Botnet Units

Simple Ways to Gain Access

This attack framework focuses on gaining access to the targeted system by exploiting the targeted system's existing vulnerabilities and utilising tools, available on a Kali Linux Operating System. These tools include Nmap, Hashcat, HYDRA, Burp Suite, and

Metasploit Framework. In order to prevent disruption in the Eduvos's day-to-day functioning, a virtual machine was setup up and utilised to mimic a system within the Eduvos environment, as seen in Figure 31 below. Thus, all intended attacks had targeted this "Eduvos" virtual machine. The following figures and descriptions the setting up stages are of the planned attack on the Eduvos virtual machine.

Setting up the KALI Linux virtual machine and the targeted Eduvos virtual machine and ensuring it is on the correct network. The setup includes the Mr Robot virtual machine, that will mimic an Eduvos system. This Virtual machine has a login and password that is unknown to the group, to enhance the validity of the results, as we would not know the login credentials of the real world Eduvos system.

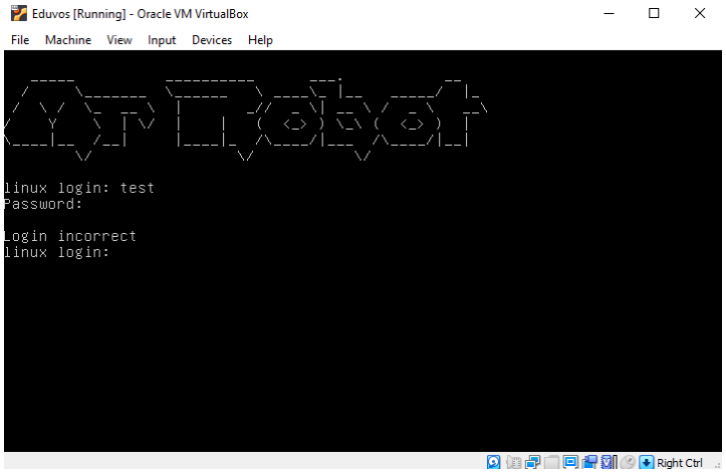


Figure 31: Mr Robot Setup

Attack Modern Wireless Networks

This attack framework focuses on a series of threats that lead the establishment of a variety of rules aimed at protecting users from assaults. Man-in-the-Middle (MitM), Distributed Denial of Service (DDoS), Packet Sniffing, and WEP, WPS, WPA, WPA2, and WPA3 attacks are just a few of the emerging wireless network threats. To avoid disruptions in Eduvos' daily operations, a virtual machine was built up and used to simulate a system within the Eduvos environment. These and other methods help to reduce wireless network attacks, allowing customers to continue to enjoy the numerous benefits of wireless

networks. As a result, all planned attacks were directed towards the "Eduvos" virtual computer. The proposed attack on the Eduvos virtual machine is depicted in the accompanying figures and explanations of the setup steps.

Mobile phones, tablets, and laptops automatically memorize the names of the networks to which they join (this is referred to as the network's SSID in technical terms). Users frequently allow the unsafe setting to link to familiar Wi-Fi networks automatically. The issue is that this choice is dependent on the SSID. The device will attempt to join whenever it is inside the coverage area of another Wi-Fi network with the same SSID.

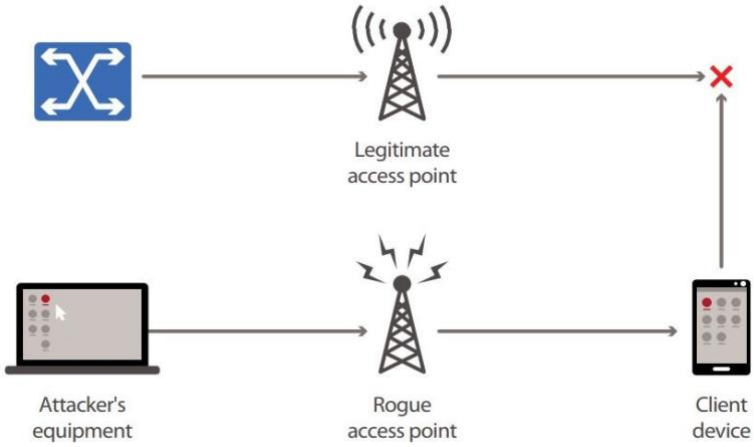


Figure 32: Access Point Spoofing

Employee devices near the rogue access point will automatically make requests for authentication, allowing hackers to construct a rogue access point with the identical SSID. Attackers can get the Challenge–Response values utilized in authentication by using the PEAPv0/EAPMsCHAPv2 protocol in conjunction to non-existent or incorrect certificate verification of the access point. The attacker may then brute force the password hash for the legal network with the same SSID using this information. Consumers might have no idea they have been targeted.

Attacking A Web Application

In this web application attack, we are preparing to launch a SQLmap SQL injection. Fundamentally, this is an open-source penetration testing tool that automates the process the exploitation of SQL flaws and then penetrates the database servers.

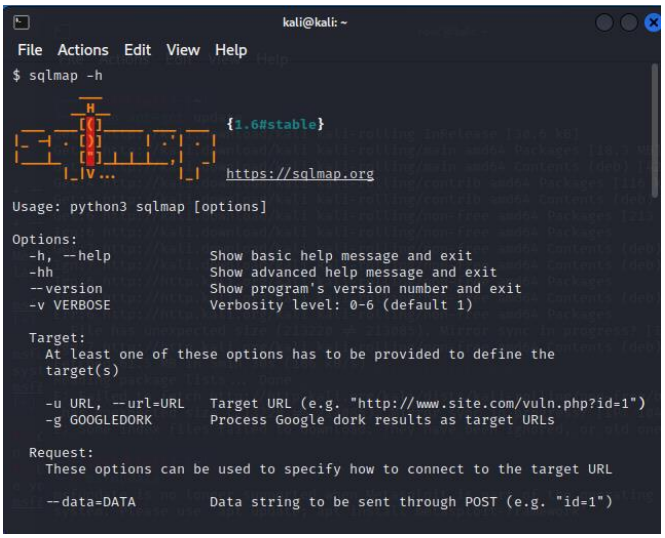


Figure 33: sqlmap Setup

Now we are testing the vulnerability of the website. As shown below the connection to the URL is being tested on whether it is protected by any security protocols.

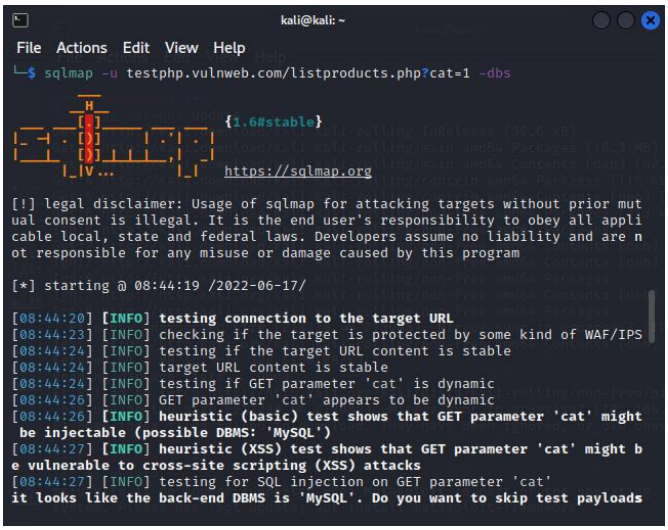


Figure 34: Testing URL

Mobile Phone Attacks

Mobile devices can be exploited in many ways, with some exploitation techniques explored including decrypting an SSL session, reverse engineering an Android application, and hacking into a mobile device.

Decrypting SSL Session

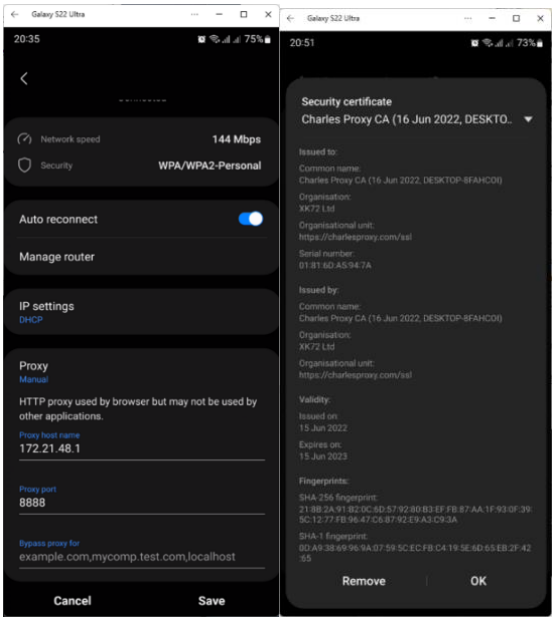


Figure 35: Installed CA Certificate

By using Charles proxy and installing its signed certificate on an Android mobile device, the usage of applications is generated in real-time. Details generated according to how the application is used include information on server hierarchy structure, cookie information, and in some instances, user credentials.

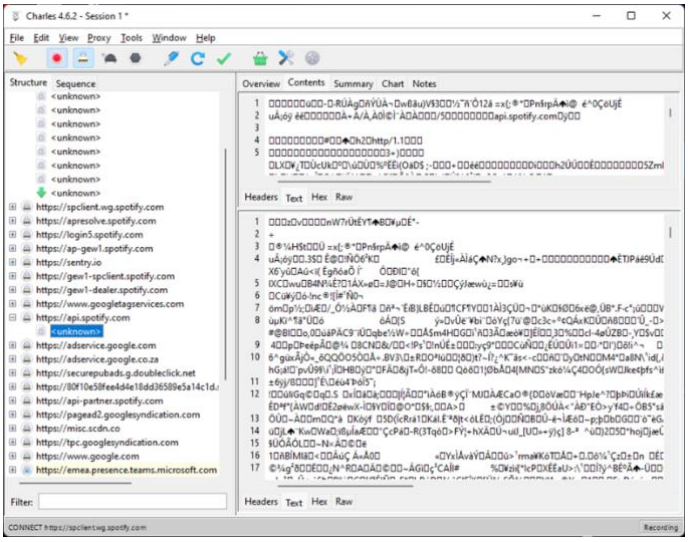


Figure 36: Encrypted contents of the application

By enabling SSL Proxying in Charles Proxy, the contents of the application are presented in cleartext.

Observe and evaluate the system

Botnet Attacks

Available botnets and opening the web GUI

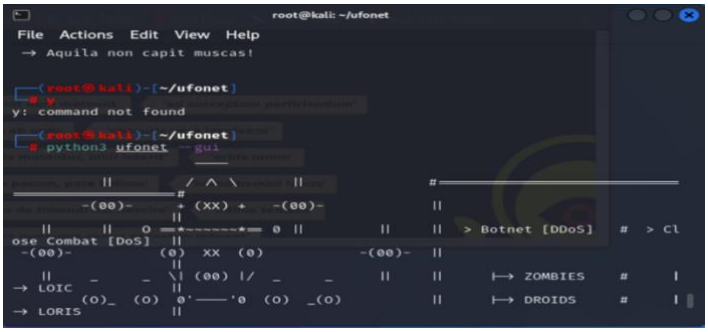


Figure 37: Opening Botnet GUI

The web GUI of UFONet

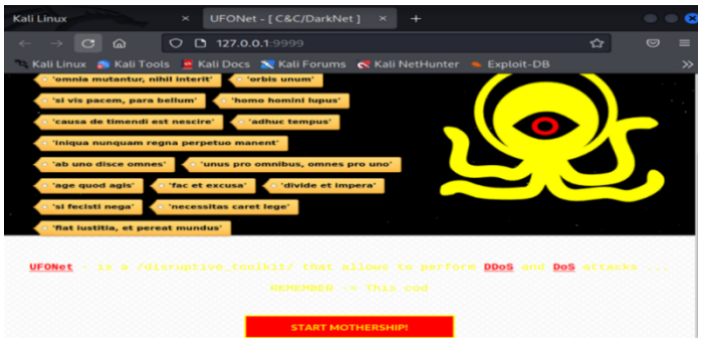


Figure 38: UFONet Interface

Botnet configuration screen with map of botnets

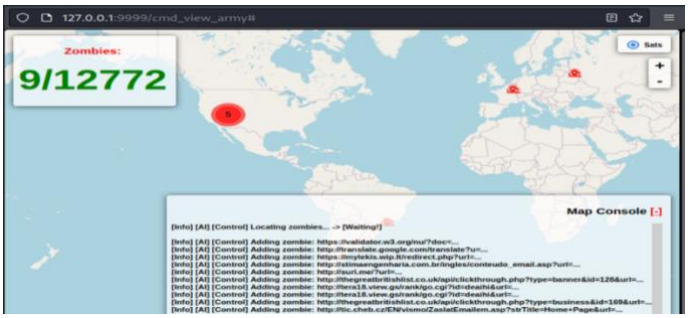


Figure 39: Map of Botnets

How to combat botnets

“Botnets are usually disguised in Trojan-type malware that can be found in a variety of mediums including: An email attachment that appears harmless, such as a nice image or a document that is significant like invoices and exclusive offer promotions, and so on.” (Engel, 2019)

Tricking users to download and install the infected file attachment is the most common attack users fall for. Users that download software from an untrustworthy source, can be at risk of being infected by a botnet. Attackers also use advertisement or notification in the form of pop-up windows to trick the victim to download an executable a file containing the botnet.

Many botnet assaults target vulnerabilities in apps or software, and many of these flaws could have been addressed in the form of security updates or patches. Out of date software is a prime target for botnet attacks.” Keeping software up to date is essential in stopping botnet attacks. 24-hour monitoring of the network should be the policy, if possible, by using analytics and data-collection solutions that can automatically detect anomalous behaviour, such as botnet attacks. The network monitoring software Nessus is a notable example of an automated network vulnerability scanner.” (Bort, 2020).

Botnets are frequently used to test many stolen username and password combinations in attempt to obtain illegal access to users' accounts. These are revered to as account takeover botnets. “Monitoring your typical rate of failed login attempts will help you establish a baseline, allowing you to set up alerts to notify you of any unusually high rates of failed logins, which could indicate a botnet assault. These botnet attack notifications may not be triggered by "low and slow" attacks coming from many distinct IP addresses.” (Whitney, 2020).

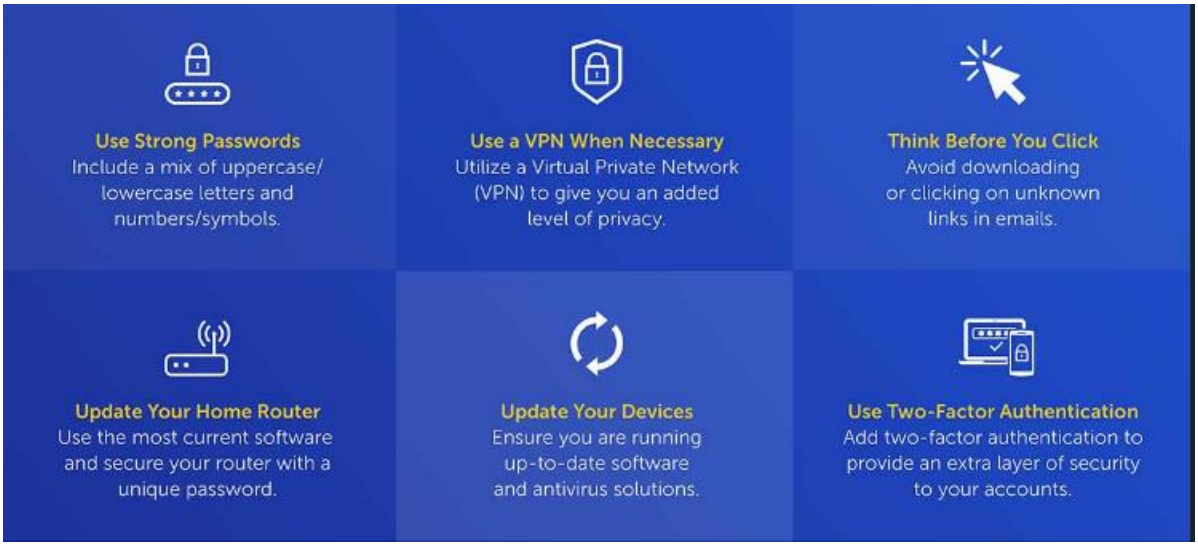


Figure 40: Tips to stop botnets

Notable Botnet attacks on the education sector

“In the education sector, BitSight found that Jadtre and Flashback were the most prevalent botnets. Flashback is malware that targets Apple computers by taking advantage of a Java vulnerability," the report notes. Mac computers are popular among younger generations and educational institutions, intensifying the proliferation of this malware in education” (Prince, 2015).

A peer-to-peer The Golang botnet reappeared after more than a year to jeopardise servers affiliated to entities as in healthcare, education, and government sectors within a month, infecting 1,500 hosts. FritzFrog is a “decentralised botnet that attacks any gadget that reveals an SSH server with cloud instances, data centre servers, routers, etc., and is able to run any arbitrary code on infected nodes.” (Lakshmanan, 2020).

Botnet Statistics

According to Spamhaus (2022), the Latin American area had 60% of active botnet C&C postings in Q4 2021. In the fourth quarter of 2021. The hosts, according to Spamhaus (2022), either have an abuse problem or do not take the necessary action when abuse reports are received.

Simple Ways to Gain Access

An Nmap was executed on an IP range of 10.38.1.110 to 10.38.1.120, in which the Eduvos virtual machine was found (IP 10.38.1.111). We found that the targeted system is hosting a website, with open ports 80 and 443. By opening the IP in the web browser, we are taken to the hosted website.

NIKTO was used to analyse the targets IP address, we can see that WordPress is present on the website.

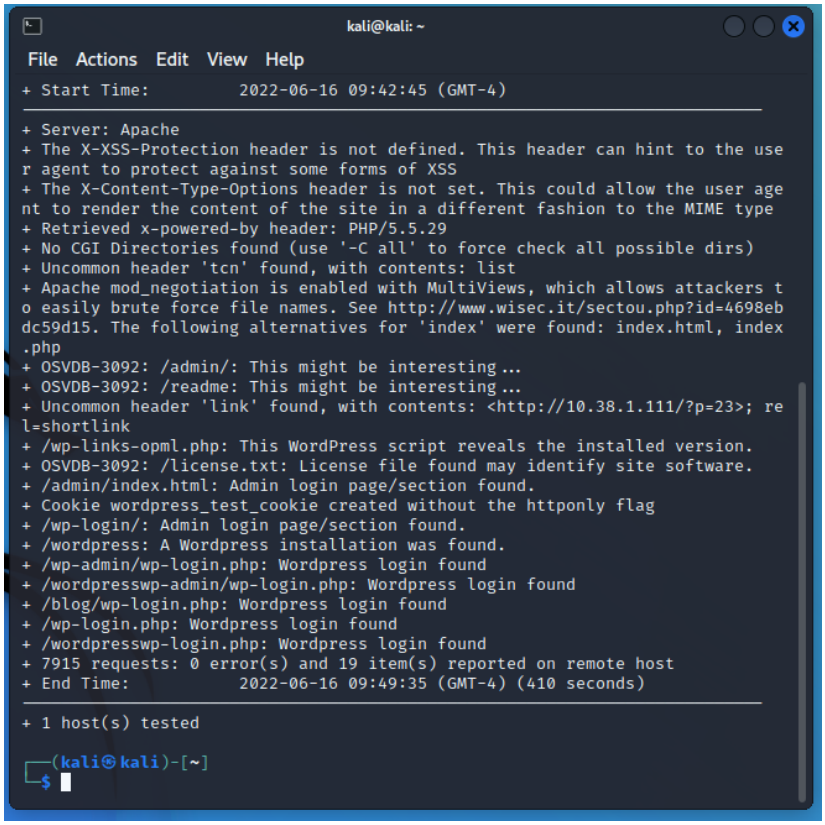


Figure 41: NIKTO Setup

In addition to the IP address “/login” was added to confirm if the WordPress login interface. Upon adding an extension to the found website, we may take note of the present files.

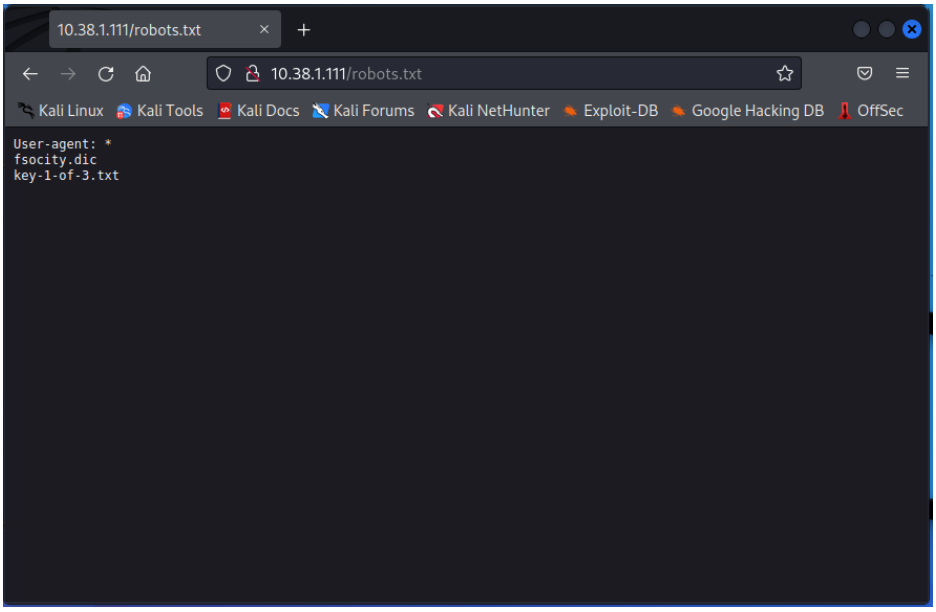


Figure 42: robot.txt Contents

The directory "./mrrobot" (a directory for the target system) had been removed and remade. After which the directory on the Kali Linux system was changed to access files in the "mrrobot" directory. This target virtual machine has a wordlist, fsocity.dic, which will reduce the time for a dictionary attack. As we will be able to use this dictionary, as opposed to a larger one such as the rockyou password list on Kali Linux.

The list was then opened and all repeated words and characters were removed and added to a new list. This resulted in the list decreasing from 858160 words to 11451 words, thus reducing the runtime of the dictionary attack.

A random username and password is entered and Burp Suite was then used to intercept any requests and responses from the website. In order to find a username, we had utilised the obtained dictionary and the HYDRA tool to look for valid usernames. The username "elliot" had been identified as a valid user by the HYDRA tool.

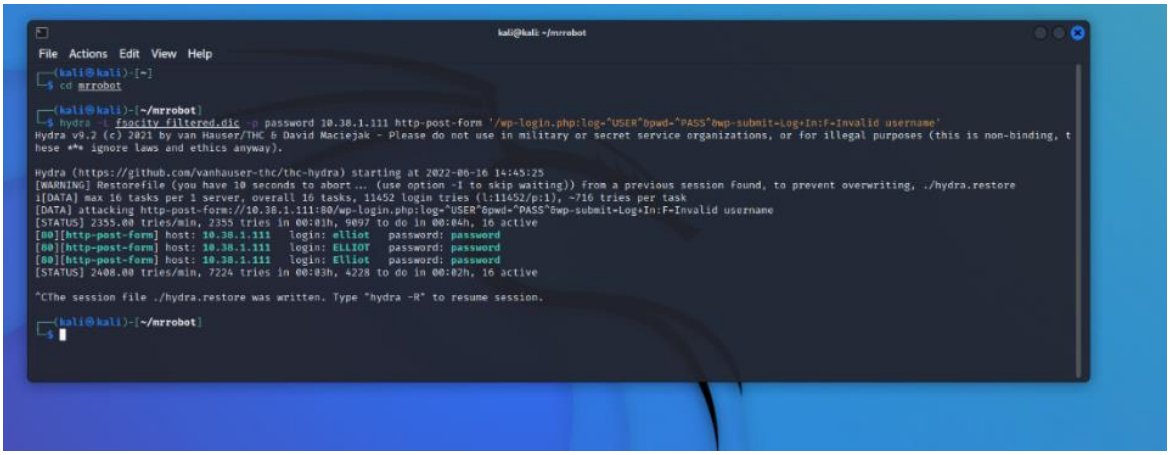


Figure 43: Using HYDRA

The username was entered into the WordPress login, and at this point a brute force attack may be initiated to obtain the password. However, the obtained dictionary and the HYDRA tool may also be utilised again, to reduce the attack duration.

Similar commands are used to the previous implementation of HYDRA, but the username “elliot” is entered into the USERNAME field. Thus, HYDRA will look for valid passwords for the specific user “elliot” and we can see that the password “ER28-0652” has been obtained.

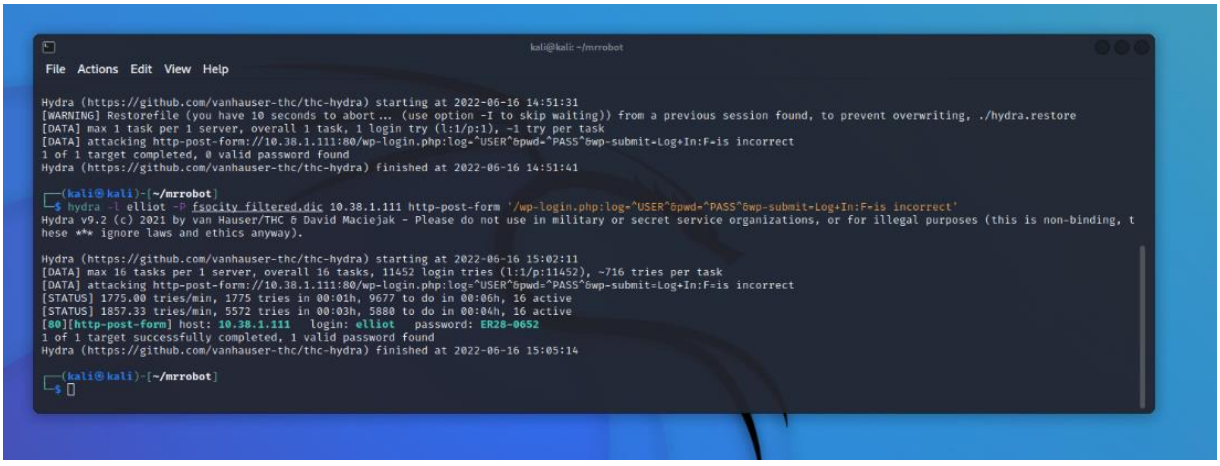


Figure 44: Obtaining Passwords

We are now able to access the WordPress login, but we wish to continue until we gain access to the system hosting this website. Metasploit was utilised to open a shell and exploit the fact that Nmap, on the target system, runs on the root user. Thus, this exploit will be used to gain access to the targeted virtual machine. We then finally have access to the systems root user, thus indicating we have successfully gained access to the virtual machine.

Attack Modern Wireless Networks

A technique called the “watering hole” was performed to attack the targeting places where staff of the target company were likely to congregate. A student’s device will try to connect to an attacker’s network as soon as it encounters a recognized SSID, which may be the entrance of an Eduvos campus, or the next taxi stop. This is easy and effective since an attacker may collect authentication data from many devices with minimal effort without ever having to step foot on campus.

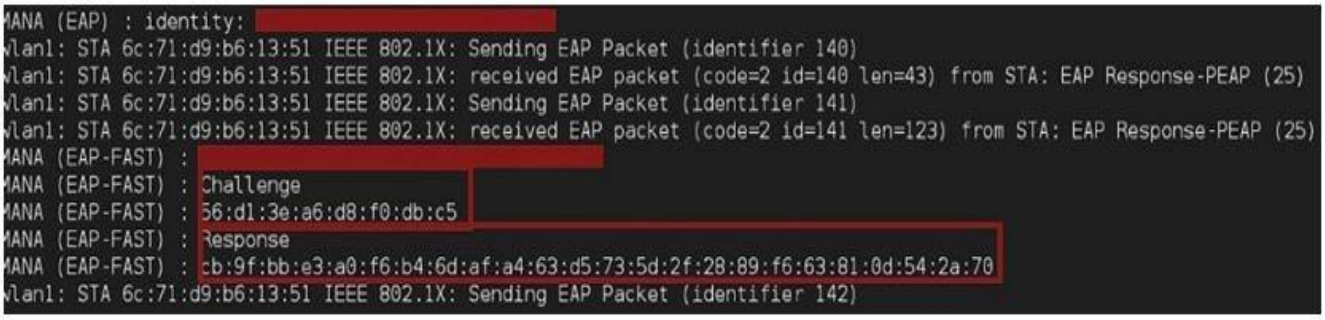


Figure 45: Interception of the challenge-response pair

An attacker can utilize a supercomputer to brute force 256 keys depending on the DES and SHA1 algorithms and obtain a hash of the password upon capturing the Challenge–Response pair (which is enough for logging in to the wireless network). This approach of physical force has a 100% probability of succeeding.

From A Guest Network to Corporate

Furthermore, students may utilize the guest network on a regular basis. Guest networks, on the other hand, are not necessarily encrypted. As a result, if the access point does not segregate users from one another, an attacker with access to an unencrypted guest network can target corporate personnel, listen in on their traffic, and steal valuable information such as access passwords. Attackers can utilize this weakness in conjunction with the above-mentioned rogue access point.

Unauthorised Access Points

For personal reasons, many students use the Internet. However, some institutes impose restrictions or outright bans on the usage of the Internet.

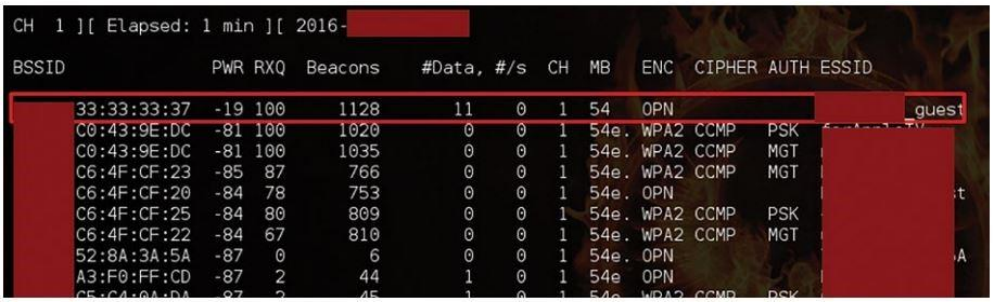


Figure 46: Unauthorised Access Points

Web application attack

Now that we have noticed that website is vulnerable, we can now scan for available database tables that have stored all the sensitive data.

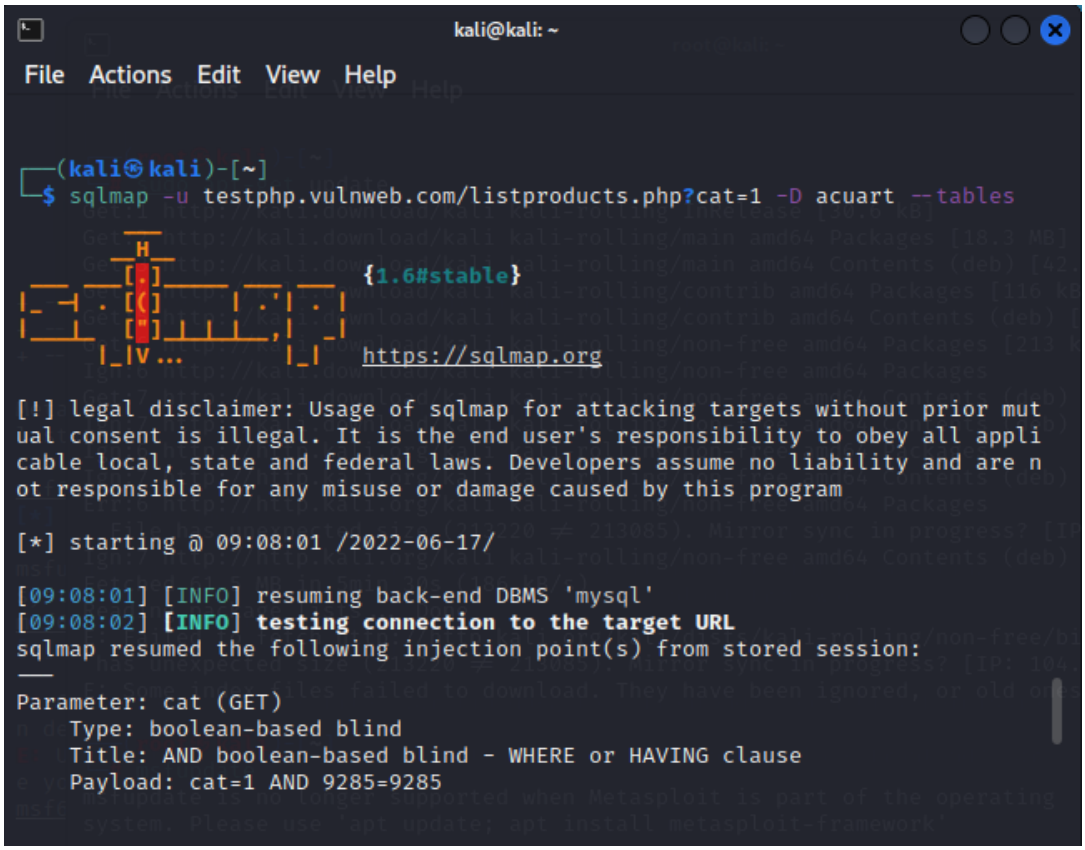


Figure 47: sqlmap query to retrieve database

We were able to retrieve the database using the above sqlmap command.

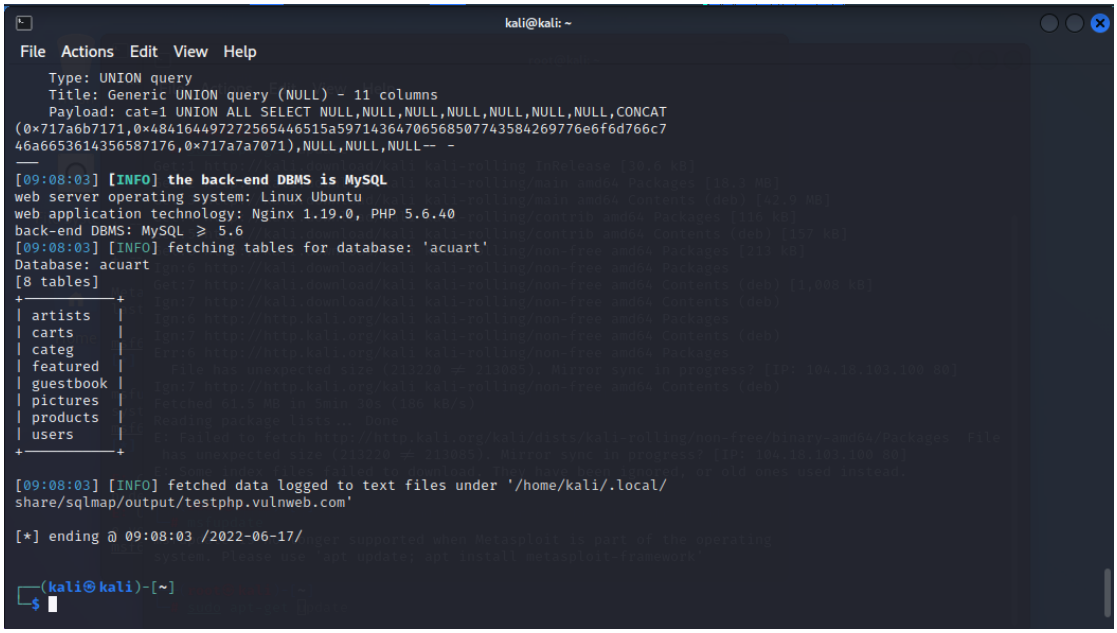


Figure 48: Retrieval of 'acuart' database

Now that we have fetched the tables for the database, we are able to access any specific table and gain unauthorized access to the database. This technique is crucial as it leads to the enumeration of the most sensitive part of an organization.

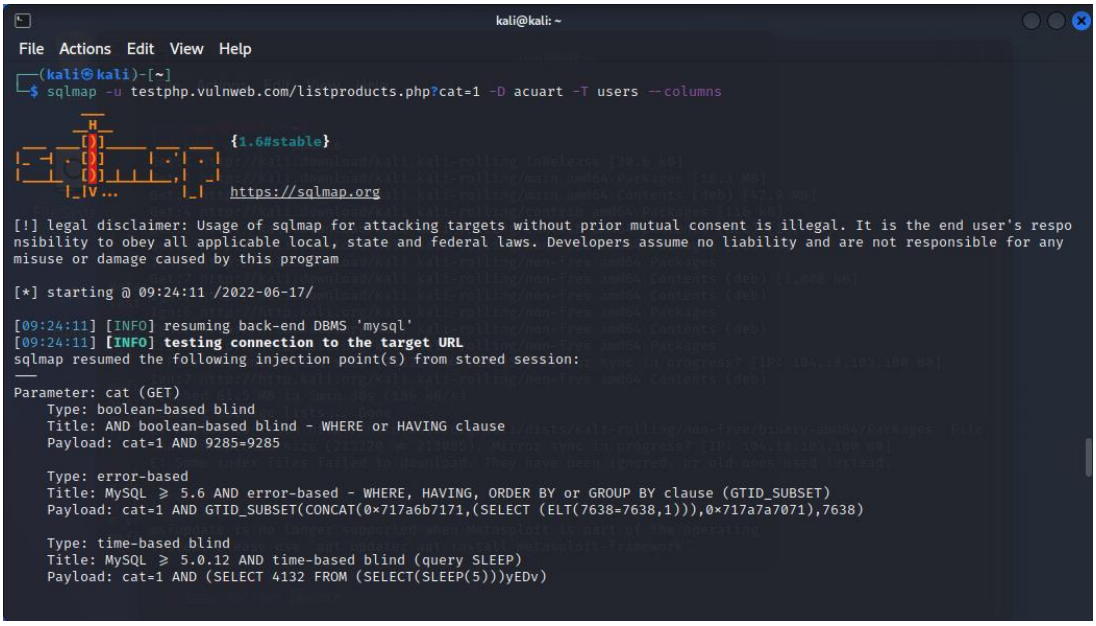


Figure 49: Accessing the database

Mobile Phone Attacks

Reverse Engineering an Android Application

This technique allows for the extraction and manipulation of Android APK files, to compromise a user's mobile device. Running the apktool extracts the files and file structure of the APK file. The APK file is then extracted and stored on the device, where it is then copied onto the Kali Linux machine. After making changes to the code in the source smali files, the application can be rebuilt using apktool once again. Once the APK file has been rebuilt, it can be deployed using various social engineering techniques, such as including it in a download link via a phishing attack.

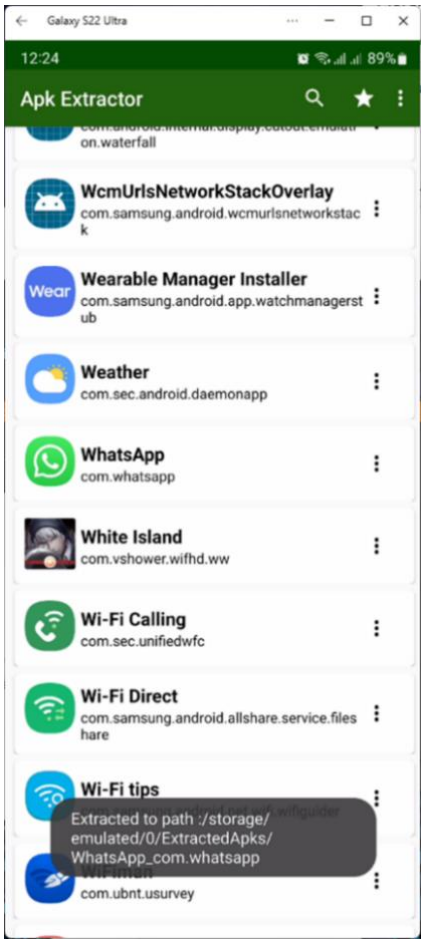


Figure 50: The APK Extractor application is installed on the mobile device

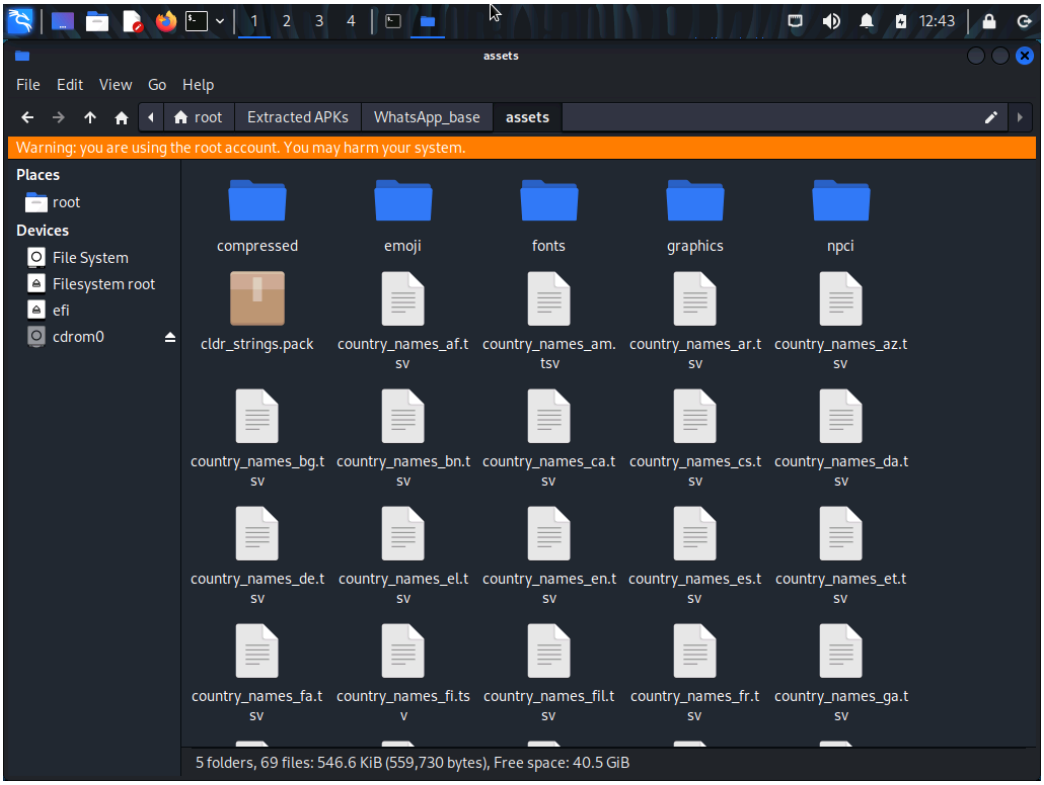


Figure 51: File hierarchy and structure of the APK file

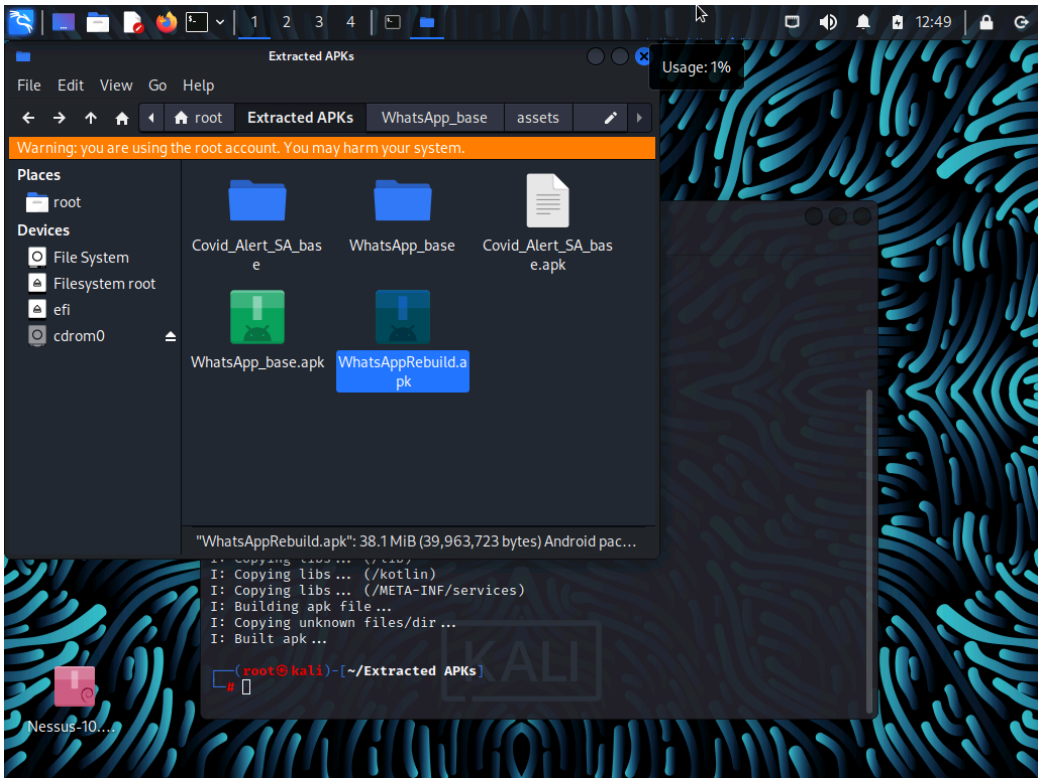


Figure 52: Reverse-engineered APK file

The reverse engineered APK file is now ready for deployment.

Hack Android device

This technique allows for the installation of a malicious APK file to enable full control over the mobile device. The attacker can then manipulate and extract data from the device.

A malicious APK file is created for deployment

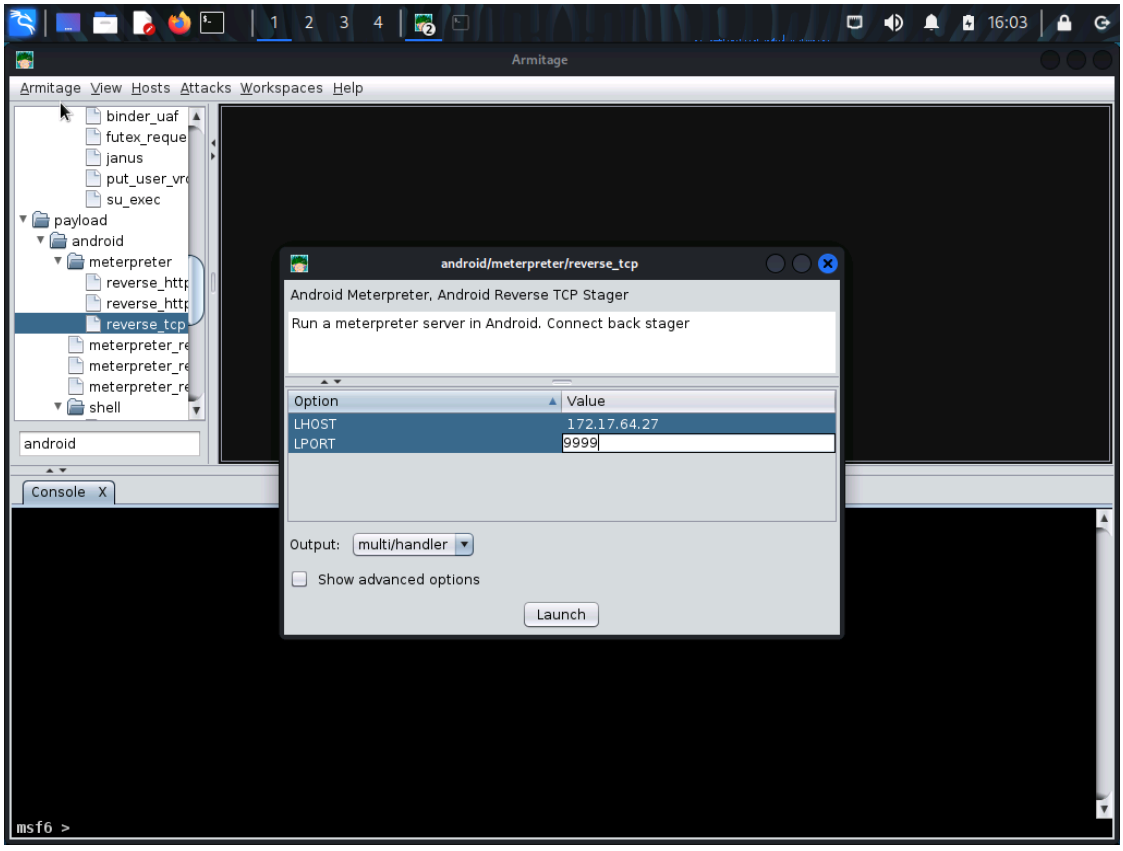


Figure 53: Creating a reverse TCP meterpreter session

A meterpreter session is then created by running Armitage to create a listening port with the same hostname and port number specified for the trojan APK. This is a reverse TCP meterpreter session.

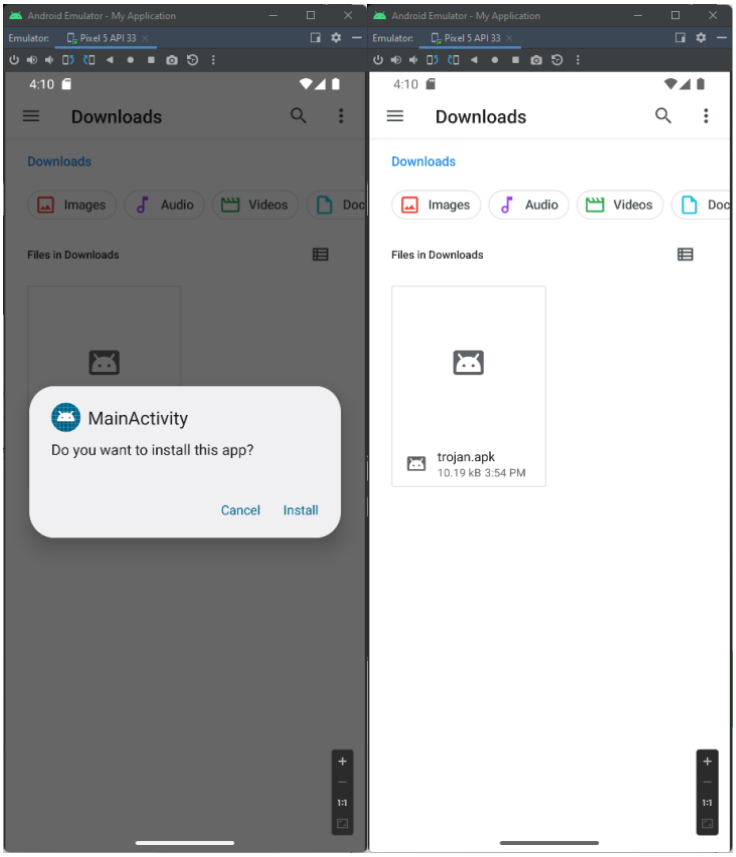


Figure 54: Installing Trojan APK on device

The malicious APK file is then installed on the mobile device.

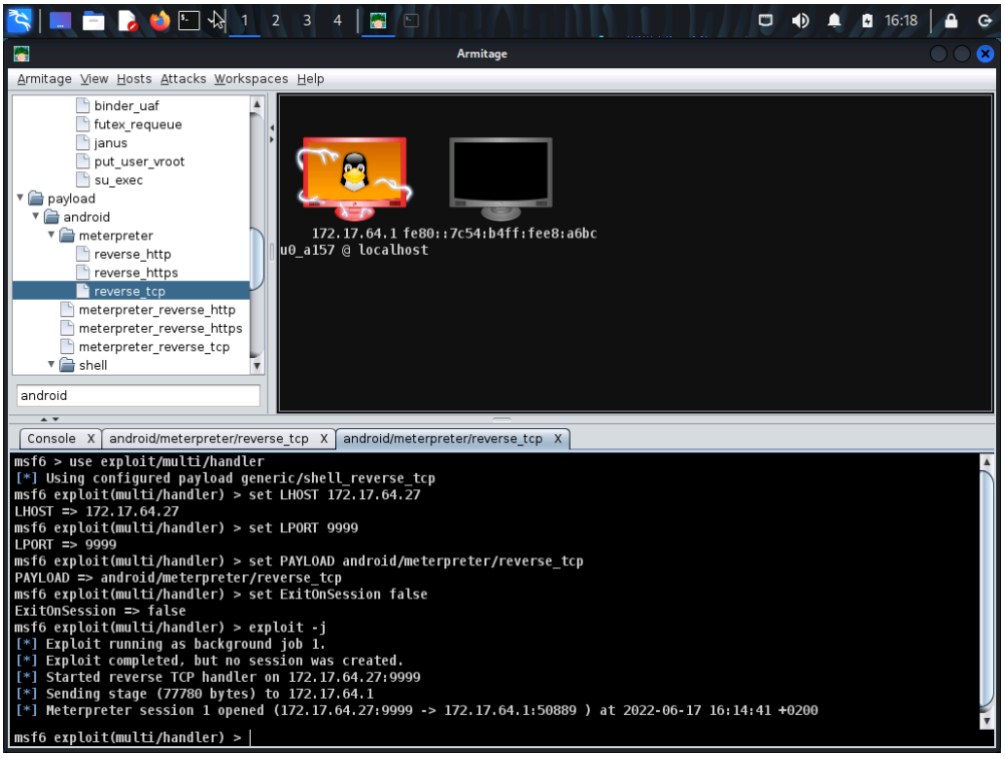


Figure 55: Device is visible on Armitage

The device is now visible on Armitage through the listening port that was created with the same hostname and port number specified for the trojan APK.

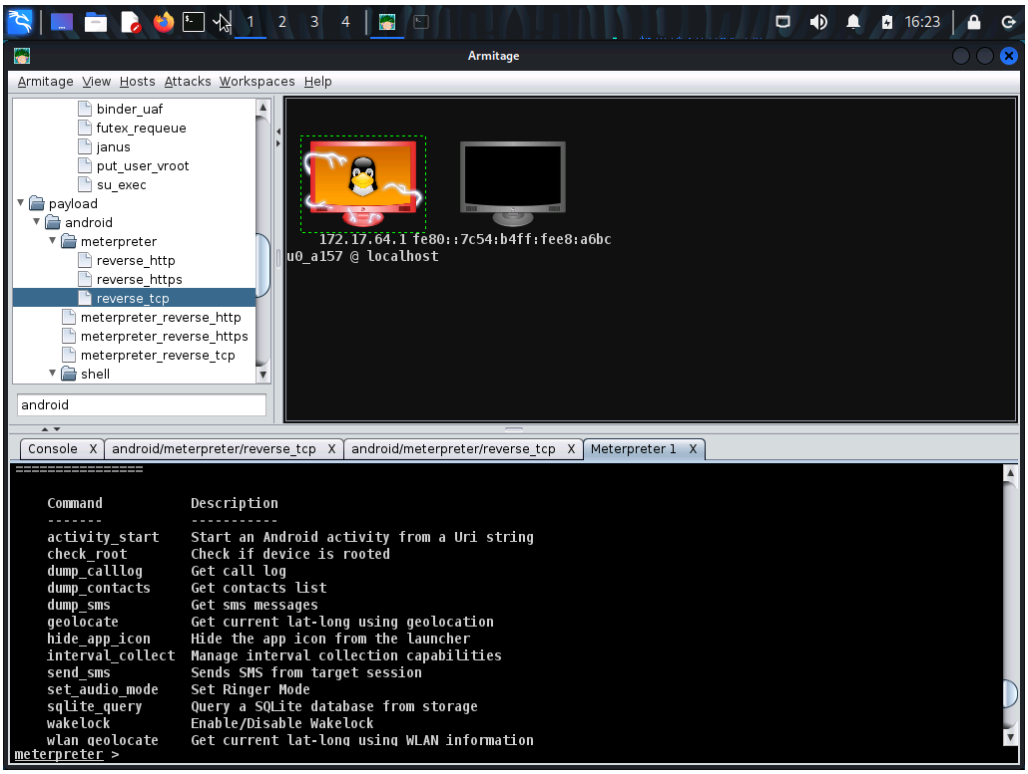


Figure 56: Command list of attacks

Conclusion

Conclusion on findings from the Botnet Attack

As a result of setting up and configuring the proposed Botnet Attack, we are presented with the following window, shown in Figure 57. We are prompted to enter the details of the target system, thus, within the correct situation there is a possibility for a Botnet attack, or account takeover, to target Eduvos.

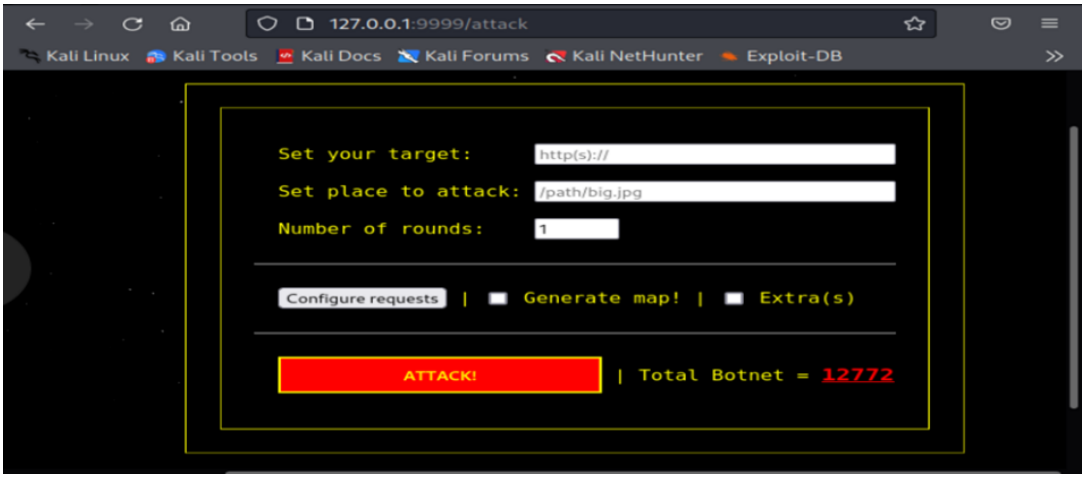


Figure 57: Launching a Botnet attack

Hack the box is used for the test site.

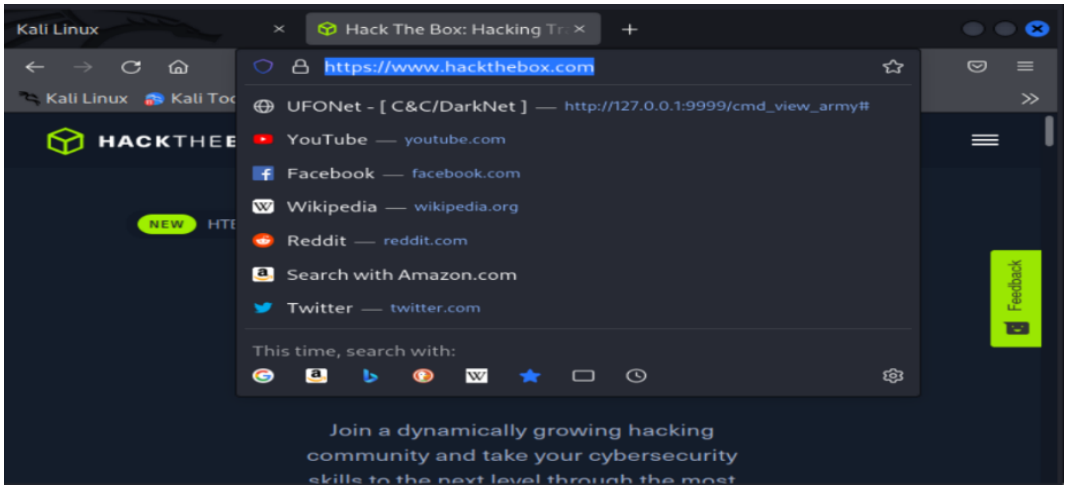


Figure 58: Hack the Box is used for testing

Hack The Box is stationed in the USA. A total of 5 botnets were launched within the region that Hack The Box is located in a timeframe of 4 minutes.

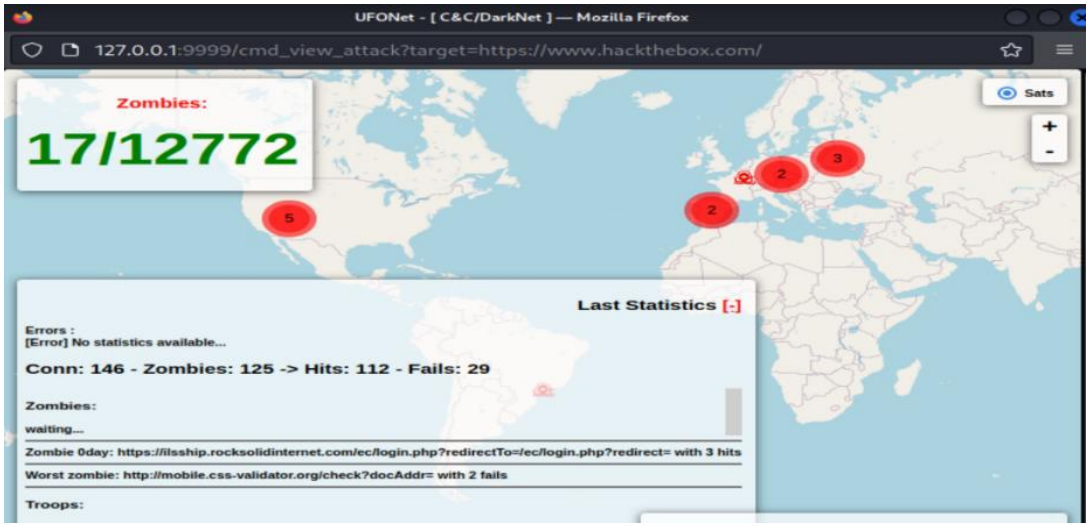


Figure 59: Launching Botnets

Hack the box URL is set as the target.

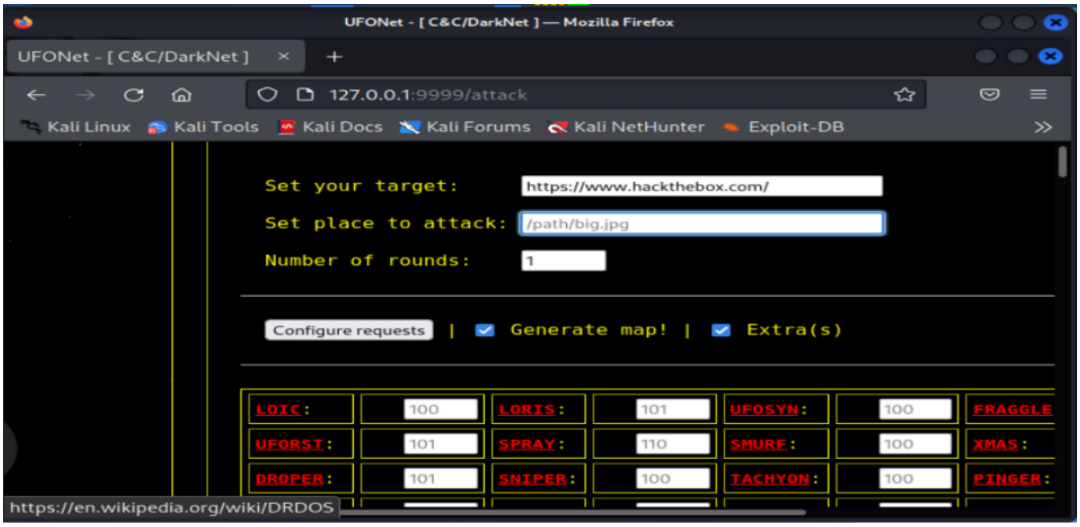


Figure 60: Set Botnet target

Conclusion on the findings from Simple Ways to Gain Access

In summary, we may conclude that the Mr Robot system, that was used to mimic a real world Eduvos system, has been accessed, as evident in the figures below, by utilising tools such as Nmap, Burp Suite, HYDRA, and other tools. Therefore, making it evident that these methods may be utilised in a real-world scenario to gain access to an Eduvos system.

Here we are able to see the Password and Usernames for the targeted system.

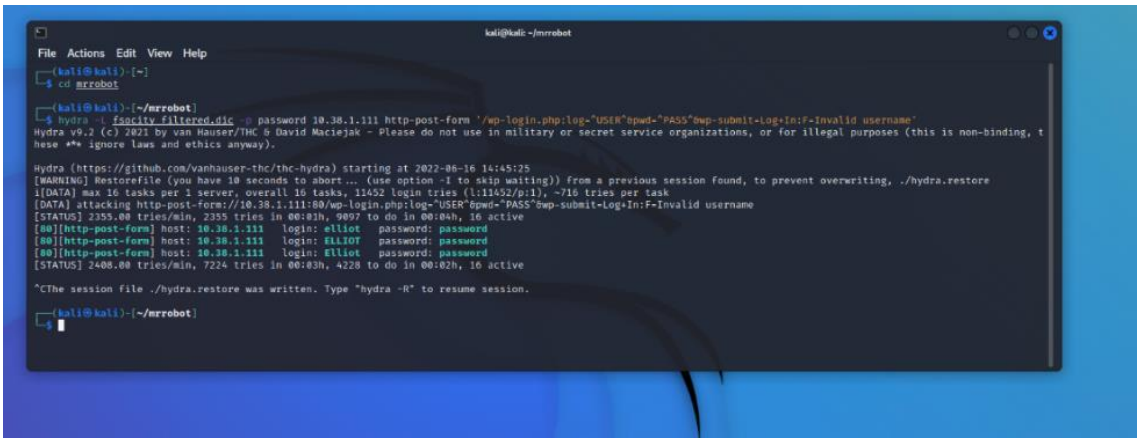


Figure 61: Running dictionary attack

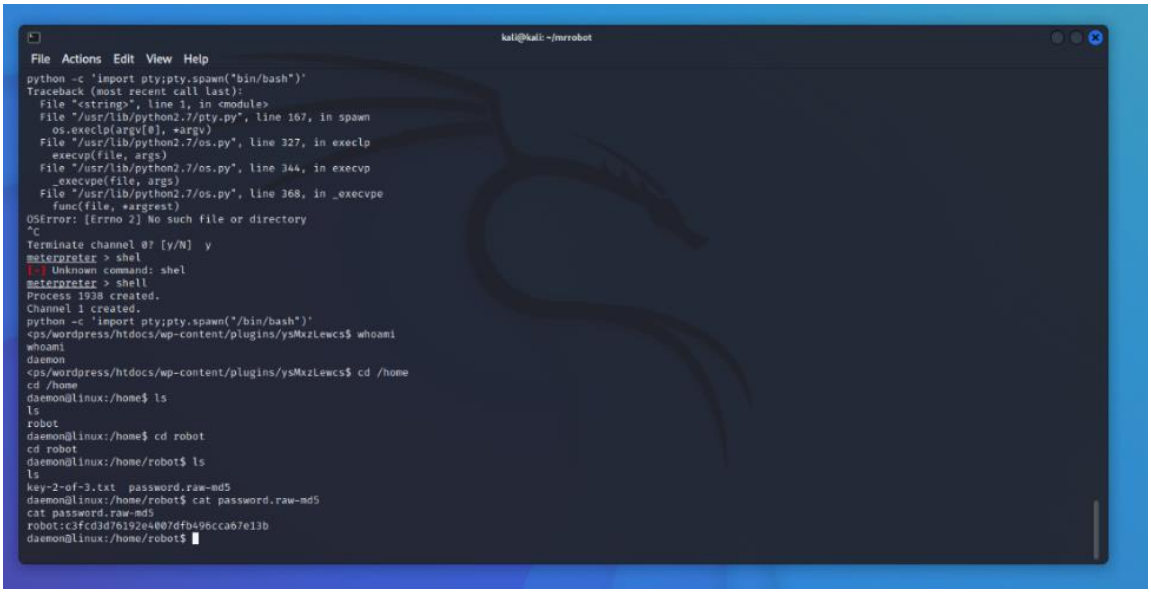


Figure 62: Results of attack

Conclusion on the findings from Attack Modern Wireless Networks

As seen in the above, Attack Modern Wireless Networks paragraph, a simulated watering hole attack was executed. As a result, we were able to easily obtain student data from their devices, seen in Figure 63, upon the student connecting to our network.

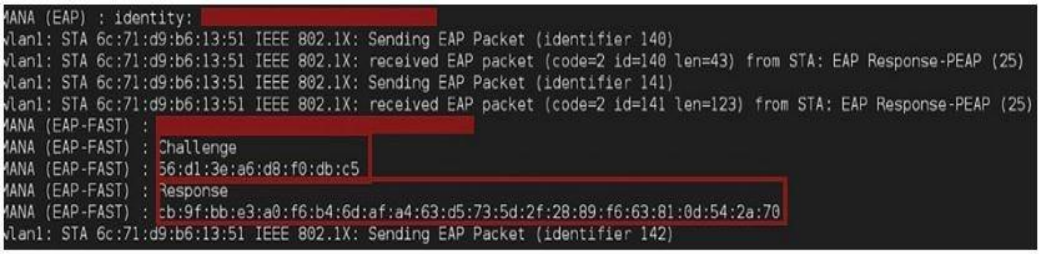


Figure 63: Watering hole attack

In 2016, unauthorized access points were discovered on average three times per location during Wi-Fi security testing. We discovered seven illicit access points functioning at the same time at one organization.

Attacks on such Wi-Fi networks, if successful, could offer attackers entry to LAN services and allow them to attack users of these hotspots. Our specialists discovered a wireless network that did not belong to the client organization during one test.

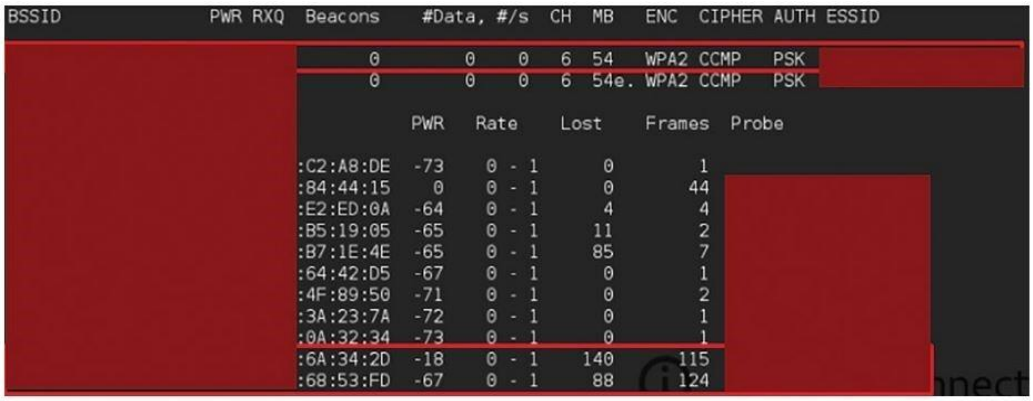


Figure 64: Results of watering hole attack

The Wi-Fi password at some businesses is built on the company's name or comparable information. As a result, attackers will have little trouble figuring out the password. They

can use specific software to undertake a tailored brute-force attack through the use of dictionary passwords.

Figure 65: Wi-Fi dictionary attack result

To exploit a WPS weakness, there is no need to configure anything; all you need is a PIN code to connect. This series of digits is frequently inscribed on the router's outside, visible to anybody who can get close enough to the equipment for a few seconds. Worse, these PINs are insecure. An attacker can simply join to the network by bruteforcing the PIN.

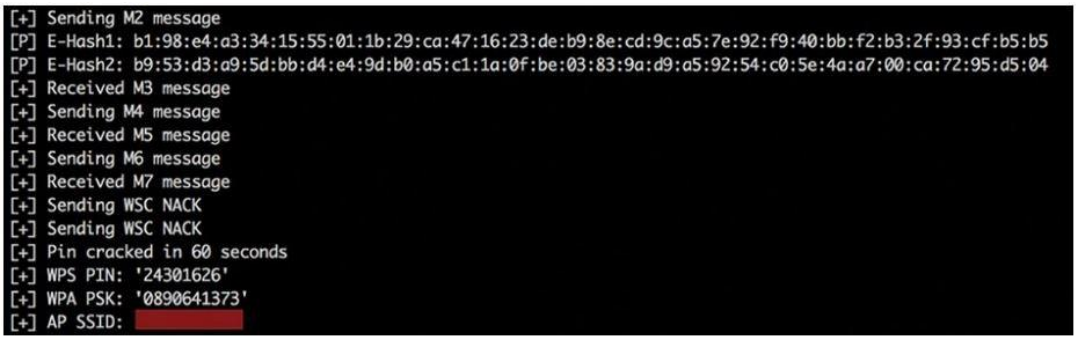


Figure 66: Bruteforcing the PIN

In researching insecure authentication, our testers came across a wireless network that uses an HTTPS webpage to get entry. The MAC address of the connected device is utilized to distinguish packets on the network following successful authentication. The user's MAC address is used to verify future connection attempts.

Our specialists deployed a rogue access point and their own equipment to show the danger, which routed user requests to the real access point. An employee's tablet was connected to the rogue access point, and the employee used a false Aruba Networks

authentication form to submit credentials. From that point on, our equipment relayed all of the user's network traffic to the access point, allowing us to listen in and add the MAC address of our "malicious" workstation to the whitelist. Our testers could also gain access to additional, more critical parts of the network via Wi-Fi connectivity.

Conclusion on findings from Web application Attacks

According to Nakar & Azaria (2019), SQL Injection attacks have been around for almost 2 decades. This is proof that data is valuable to individuals and organizations. Web Application Firewalls have fallen victim to this type of attack. The notion of smart SQL injections leverage systems such as Google searches, automation through botnets, and other sophisticated automated attacks (Chickowski, 2010). Figure 67 shows that it is not just one industry that is victim to SQL injections.

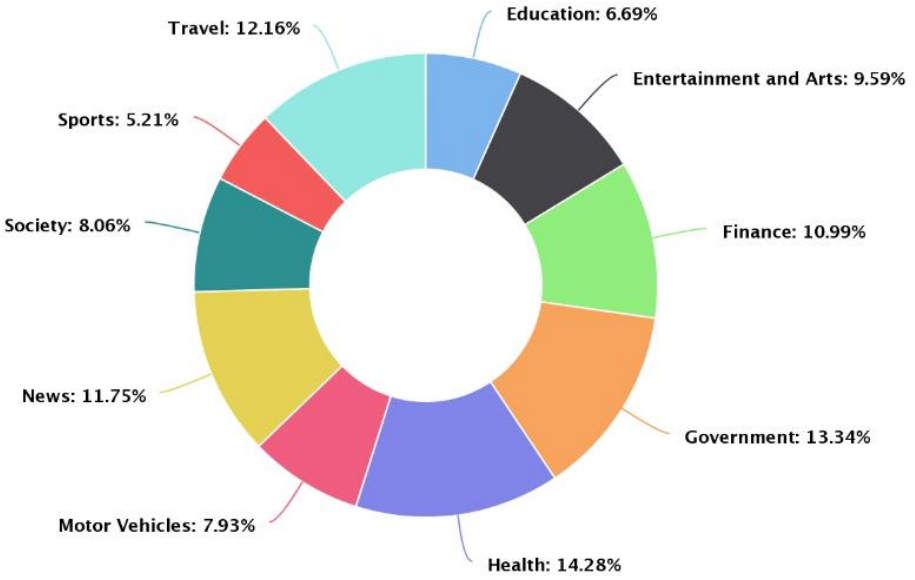


Figure 67: Attack distribution by industry

We were able to try and dump some information in the administrator database using this powerful tool. The figures below show that the user database has been exposed and can anytime be exploited.

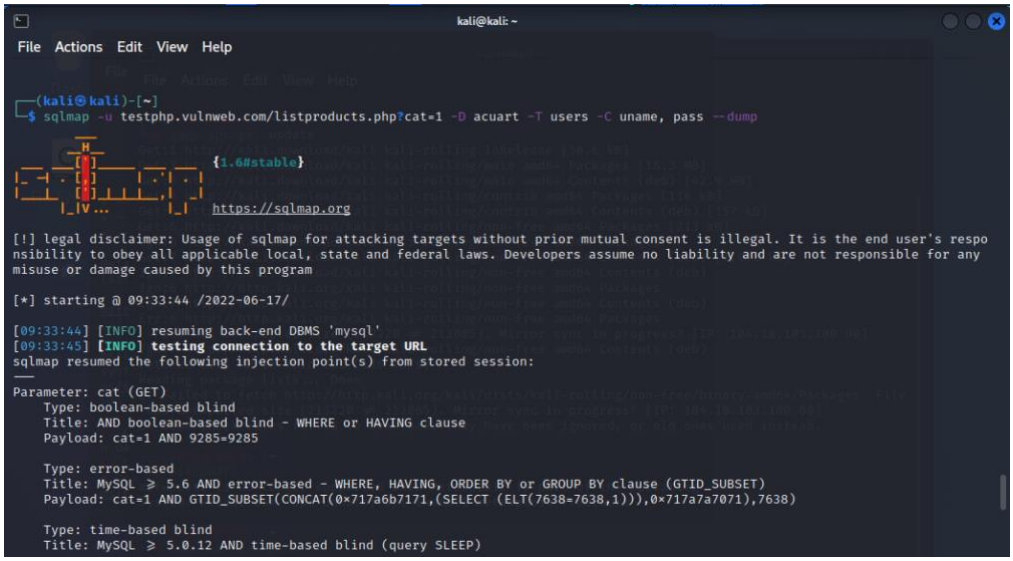


Figure 68: Querying database

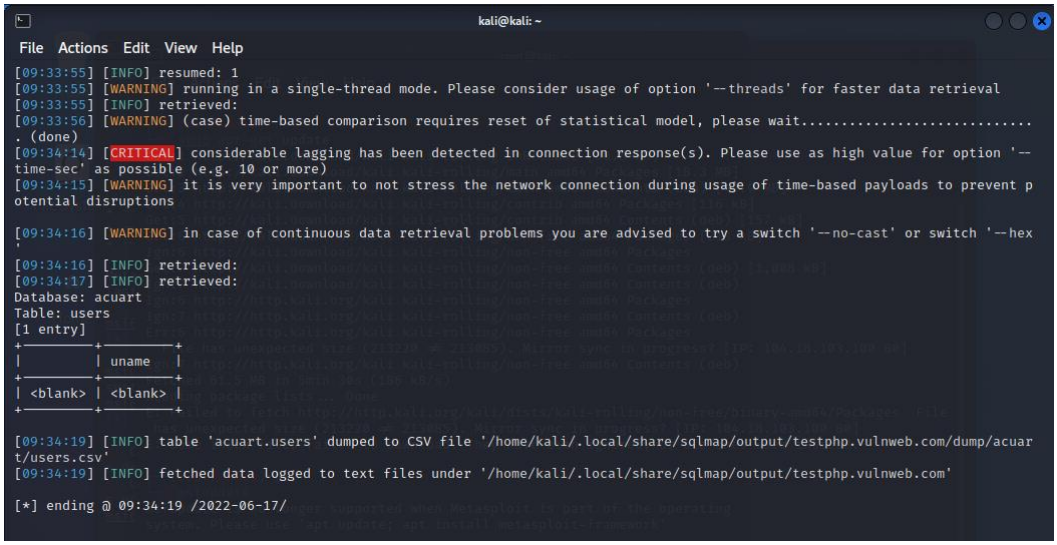


Figure 69: Dumping database contents

Conclusion on the findings from Mobile Phone Attacks

SSL encrypts information between the client and the server and provides authentication to ensure that the intended connection is established. This, however, is not enough when it comes to sufficiently securing applications, devices and information. Security measures must be implemented, and information must be encrypted from the application and code level. The necessity of keeping certificates and encryption protocols up to date are also important practices in ensuring trust and security (Wembley Partners, 2020).

The process of ensuring that mobile phone applications cannot be decompiled easily can be accomplished by obfuscating the programming code, using ProGuard or DexGuard, which encrypts strings, and can detect code tampering. The Native Development Kit (NDK) can be used to write libraries in C, and then import them into Java, which makes it more difficult for attackers to compromise applications (Berzinskas, 2020).

CHAPTER 5: ANALYSIS AND DISCUSSION OF THE RESULTS

Introduction

This research explores the grey areas within the scope of social engineering techniques with much focus placed on establishing a standard guideline about awareness of social engineering attacks that occur in the higher education sector. A hybrid approach was practically implemented focusing on botnet attacks, web application attacks, mobile phone attacks, modern wireless attacks, and simple ways to gain access. These are the social engineering methods used to conduct a comprehensive assessment report for the institution and enabling the institution to shy away from such attacks.

The issue of data sensitivity in universities is a huge grey area that needs to be addressed and dealt with immediately as stated by (Turner, 2018). With the rising concern of social engineering attacks in the education sector, our research demonstrates ways in which the majority of higher educational institutions fall victim to such attacks.

Before we conducted this research, we were very much aware of the current methods used in social engineering. The goal of this research is to demonstrate different techniques used in social engineering and to come up with guidelines to protect educational areas like campuses and higher learning institutions as well as showcase methods that hackers can use through social engineering.

Web applications could be fall victim to cyber-attacks due to misconfigured web servers, application design flaws and inappropriate validation (Burnham, 2021). SQL Injection is an old method yet still relevant as it deals with the most crucial part of individuals and organisations. According to Nakar & Azaria (2019), SQLi has more than 80% success rate

than other web application attacks. This attack might be overlooked but has cost many organisation millions for damage control.

The evolution of mobile devices, from a basic communication tool to a powerful, handheld computing device has led to a prolific increase in attacks against them and their users. Threats such as data breaches, social engineering and cryptojacking attacks are further enhanced by the research which builds on the growing number and types of threats by demonstrating practical techniques on how SSL sessions are decrypted, mobile applications are reverse engineered, and devices can be hacked using malicious software installed on the device (Yadav & Reddy, 2019:1543-1548).

Ways to gain access to a system, network and or mobile device allows one to judge and understand the vulnerability of said system, network and or device, as the ultimate goal of any penetration tester during an assessment is gaining access to the desired system or device (Srinivas, 2017). Thus, we had opted to implement and explore methods of gaining access, while using social engineering tactics as the basis of this research. This allows us to highlight and demonstrate how the data from social engineering techniques may be utilised by a potential attacker, or threat actor, to gain access to a targeted system or network.

A popular open-source botnet builder know as ‘BYOB’ was initially used for the creation of a botnet with an integrated crypto currency miner. However, the source code for the ‘botkit’ was unstable and prone to errors. This forced our team to create a command-and-control botnet from scratch. ‘All botnets follow a specific pattern while being developed. That pattern being a control and command style architecture.’ (Heron, 2019) The program used for the operating of the botnet server and its dependency's used python scripts. These scripts had to communicate via a covert channel to the client on the victim's machine (zombie computer). The botnet server and botnet client communicate over a secure channel and the server sends commands remotely to the target.

A simple bitcoin miner was written in python to be able to mine cryptocurrency on the infected computer without the victim's knowledge or consent. ‘This practice is known as

crypto-jacking, and it has surged in popularity in recent years. (Hwang, 2022). The botnet is loaded onto the victim's computer through a backdoor program coded in python 3 and executed through a virtual machine running kali Linux. The backdoor python script allows our team to install the botnet on the targeted machine.

Method DISCUSSION

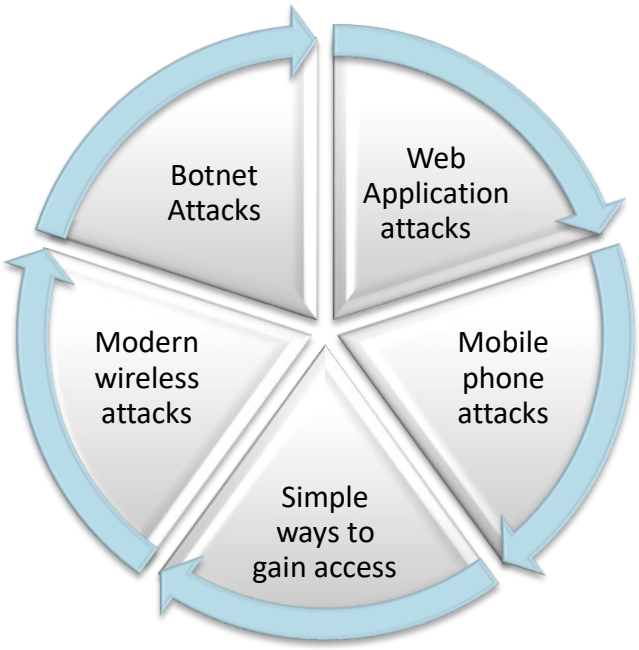


Figure 70: Method Discussion diagram

Collectively we chose the five above mentioned social engineering because we concluded that they were effective and most importantly efficient in executing our attacks. We chose Botnet attacks because this method is used to take over operations of vulnerable devices in order to control them remotely and launch a large-scale attack for malicious purposes. Web application attacks compromise the confidentiality of an organisation. As a group we also chose mobile phone attacks because this method also puts the user's data in jeopardy, people can install application that look legitimate but are malicious. Simple ways to gain access is also one the methods we chose because this method compromises an organizations system and its sensitive data. Lastly, we chose modern wireless attacks because this method aims to capture sensitive data transmitted across the network.

Related work discussion

The research paper titled Social Engineering by Jan-Willem Bullée and Marianne Junge was published in March 2020. This research paper was the most useful regarding the current project our team is undertaking. The research paper goes into detail pertaining to social engineering as well as its causes and how to protect oneself from cyber-attacks that use social engineering.

The research paper starts out by describing the definition of social engineering in detail. The paper then continues to talk about the notorious history of social engineering and various individuals that used it to their advantage like Kevin Mitnick, Stanley Mark Rifkin, and many other famous hackers. The research paper helped the team discover numerous social engineering attack and how they worked. The team members then decided each on a project that could benefit our research goals and some on the project's topics were derived from this research paper. “There are endless ways in which attackers can trick other humans for their benefit” (Douglas Rushkoff, 2020).

The social engineering attack that uses Voice Calls to defraud potential victims is the first social engineering attack mentioned in the research paper. “Social engineering via the telephone is also known as a phone scam, technical support scam, or cold call.” (Sheizaf Rafaeli, 2018) These attacks are extremely hard to get accurate data on but the Dutch Fraud Help Desk (an organization that collects reports on fraud) was contacted. In the period between 2015 and 2018, there were 4507 incidents reported, whereas 499 were victimized (11.1%). The total reported damage was €850,701, an average of over €1700 per victim. Because of the difficulty of measuring the effectiveness of these attacks the above data is only a rough estimate. The paper also contains useful information on steps that can be taken to reduce the effect of the social engineering attack.

After the phone scans the paper discusses Email fraud. This section helped the team greatly because it discusses how email scams are preformed and how to prevent them. The specific type of email scam that is discussed is a phishing attack. “Social engineering via email is often referred to as “phishing.” In email phishing, the target receives a malicious

email that tries to convince him or her to visit a fraudulent website. These websites often have only one goal: tricking people in sharing sensitive information.” (Clay Shirky, 2022) The conclusion is that email phishing's success is insecure and highly dependent on both the content and the context. Despite the many variances between the research, this provides a first indication of email phishing's general success.

The paper also discusses text message fraud. This topic is also useful for our research paper because our attack plan contains elements that pertain to weaknesses in mobile devices. Text message fraud is also known as a smishing or SMS phishing. This section describes three social engineering attacks via text message, one reasonably simple attack and two more sophisticated attacks. First, the target receives a message via WhatsApp from one of its contacts encouraging them to click and receive £100 worth of shop vouchers. The offender can install harmful software on the phone by clicking the link (McGoogan, 2016).

Second, a WhatsApp-based attack scenario seeks to steal money by impersonating a family member. The following is the modus operandi: The criminal notifies the victim that he or she now has a new phone number. This includes a profile photo of the individual who is being impersonated that match. The image is based on social media, familial relationships, and how individuals connect with one another (Fraudehelpdesk.nl 2018). Frequently, there is some chit conversation initially, followed by a request for assistance. There are bills that must be paid as soon as possible, and the internet banking system is having issues. You pay the expenses to assist a family member who is in need (Radar 2019). While you believe you are assisting, you become a victim.

Third, in this case, an offender uses SMS to get beyond an extra security layer (two-factor authentication (2FA)). A second factor (e.g., an SMS verification code) is required in 2FA in addition to a username and password. The verification code is sent to the phone number you provided during registration, adding an extra layer of security. By sending a cleverly designed SMS to the victim, the perpetrator can "bypass" this second component (Bullée & Junger, 2020) VCFA (verification code forwarding attack) (Siadati Kruger. 2017; Jakobsson Taylor 2018).

Analysis of result discussion

Botnet attack

The botnet attack was carried out using Kali Linux and the GitHub package “BYOB”. This however proved unsuccessful, and an alternative was used. A Botnet was built from scratch using python code. A primitive bitcoin miner was also created with the help of python. The botnet also has a simple key-logger installed using the python library: pynput. The botnet uses a standard botnet framework. That framework being a normal command and control style setup where the main test computer executes command for the bots to follow. These commands include installing a backdoor to the targeted machine, installing a python based crypto currency miner and a botnet to infect other computers on the network. The crypto-currency miner is operational and is capable of mining hashes for crypto currency.

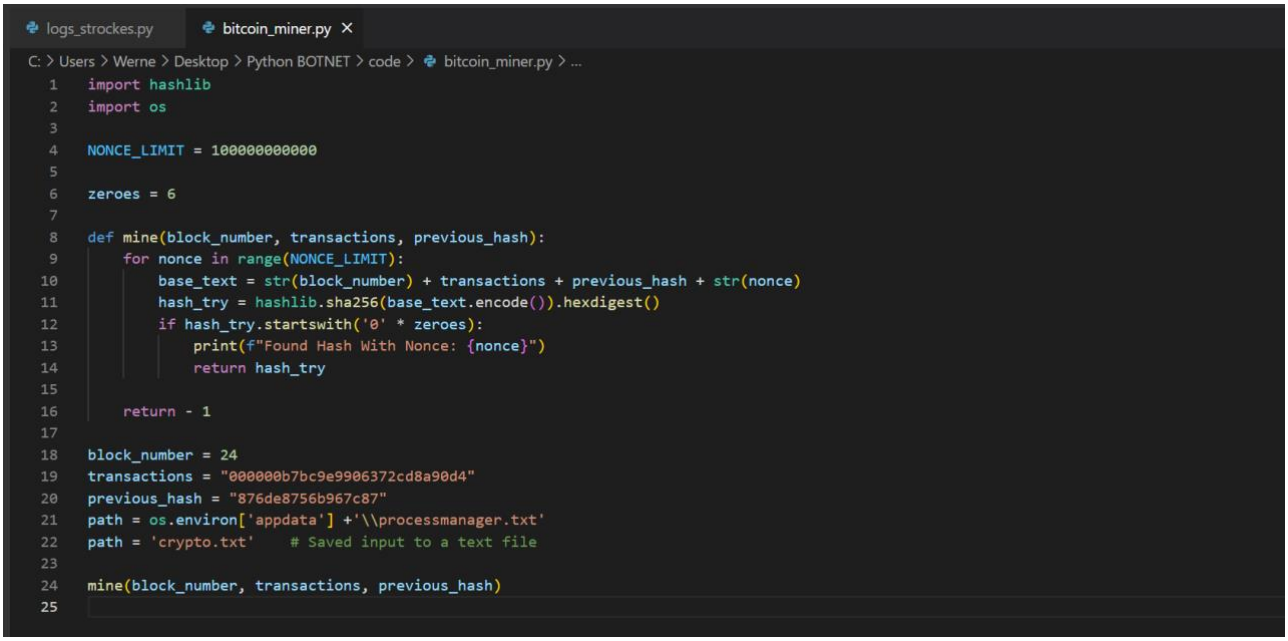


Figure 71: Crypto Miner Code

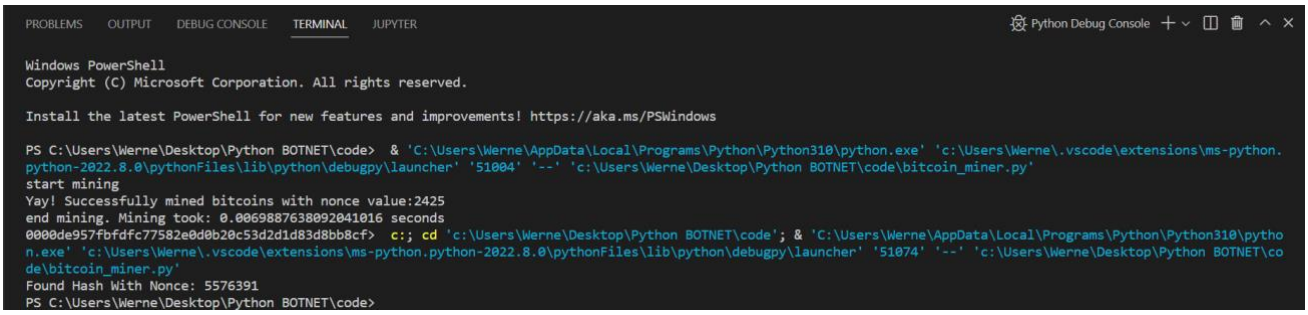


Figure 72: Running the Miner

The key logger is operational and is capable of saving its output to a text file.

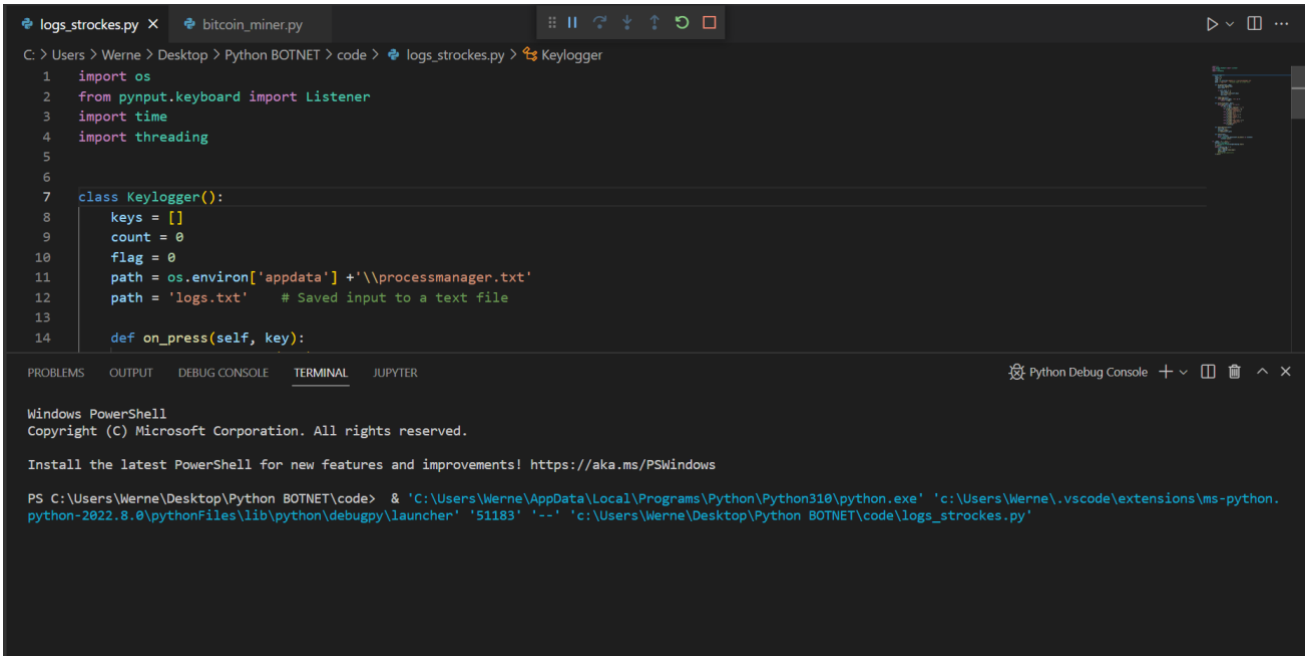


Figure 73: Keylogger code

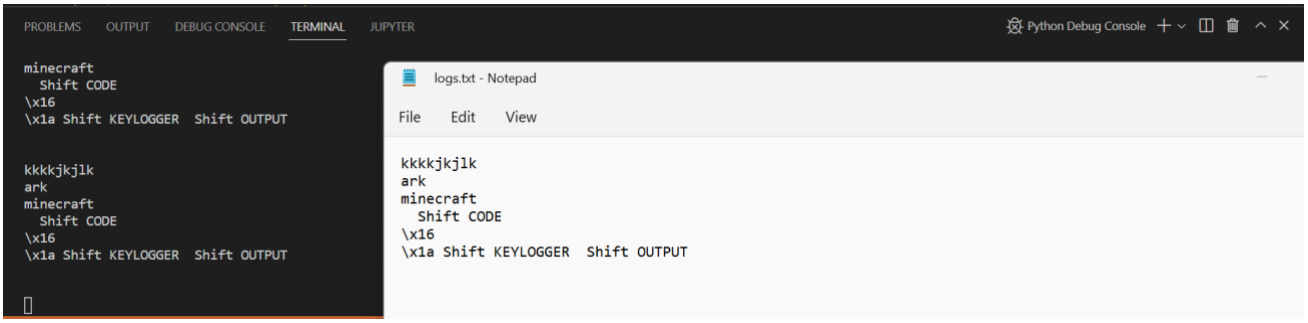


Figure 74: Keylogger output

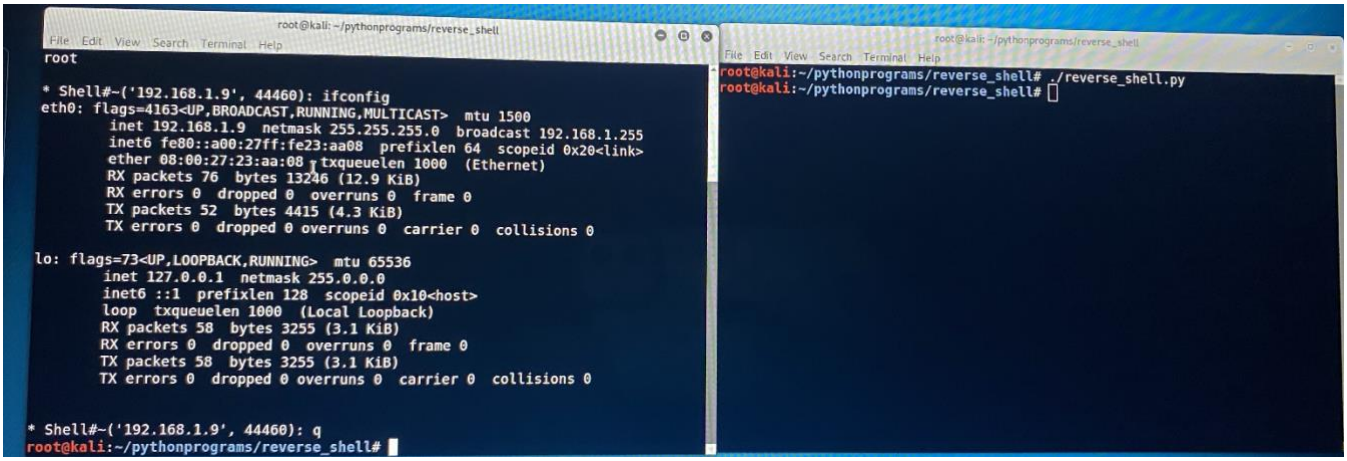


Figure 75: Botnet server command execution

Loading file onto target system.

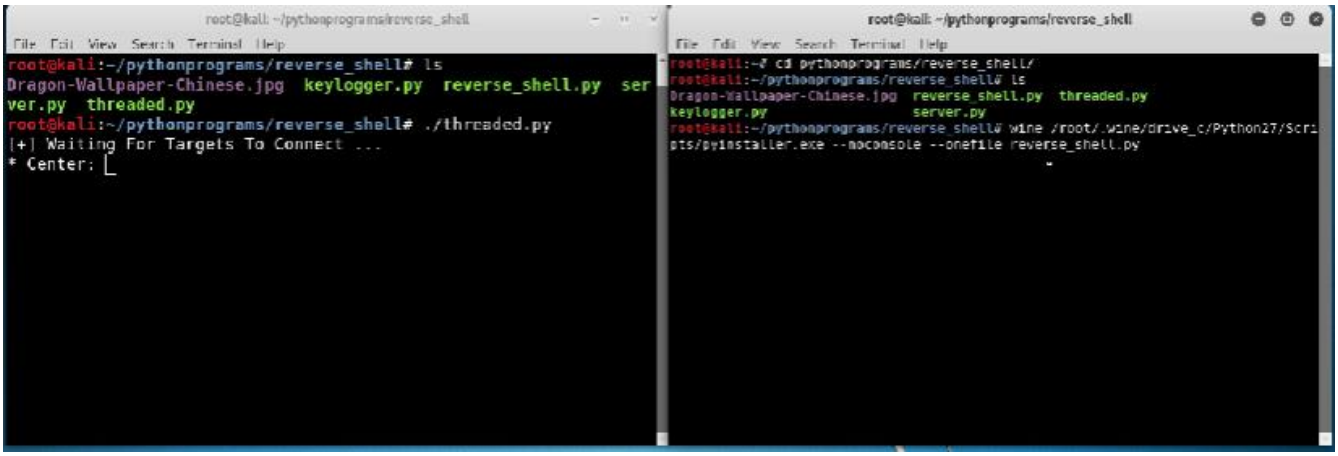


Figure 76: Exploiting target machine

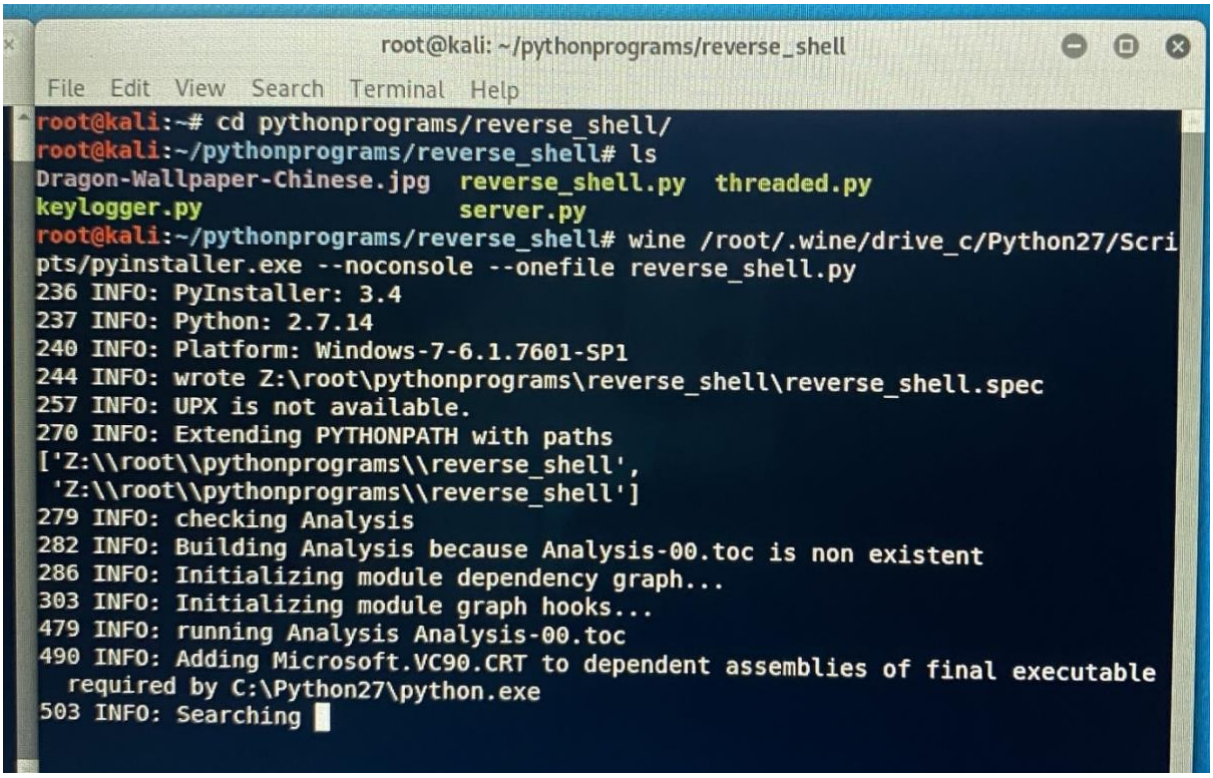


Figure 77: Reverse shell Python program

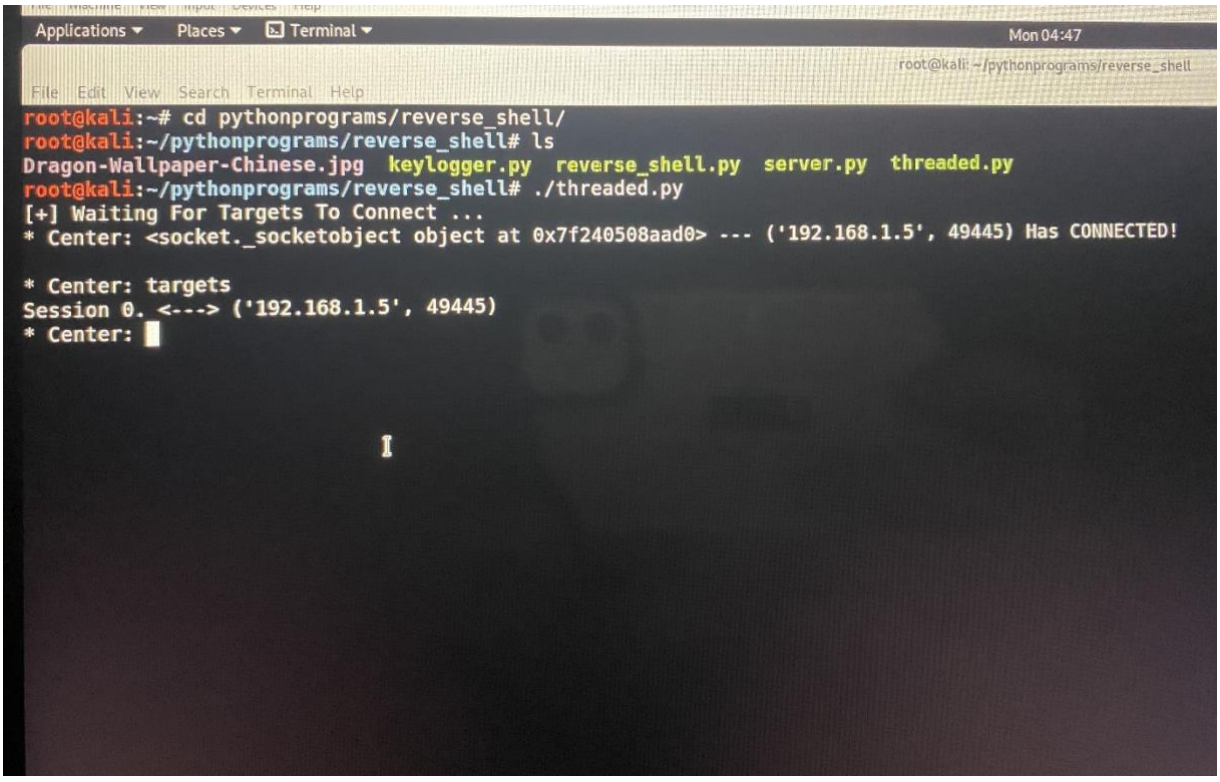


Figure 78: Connecting to target machine

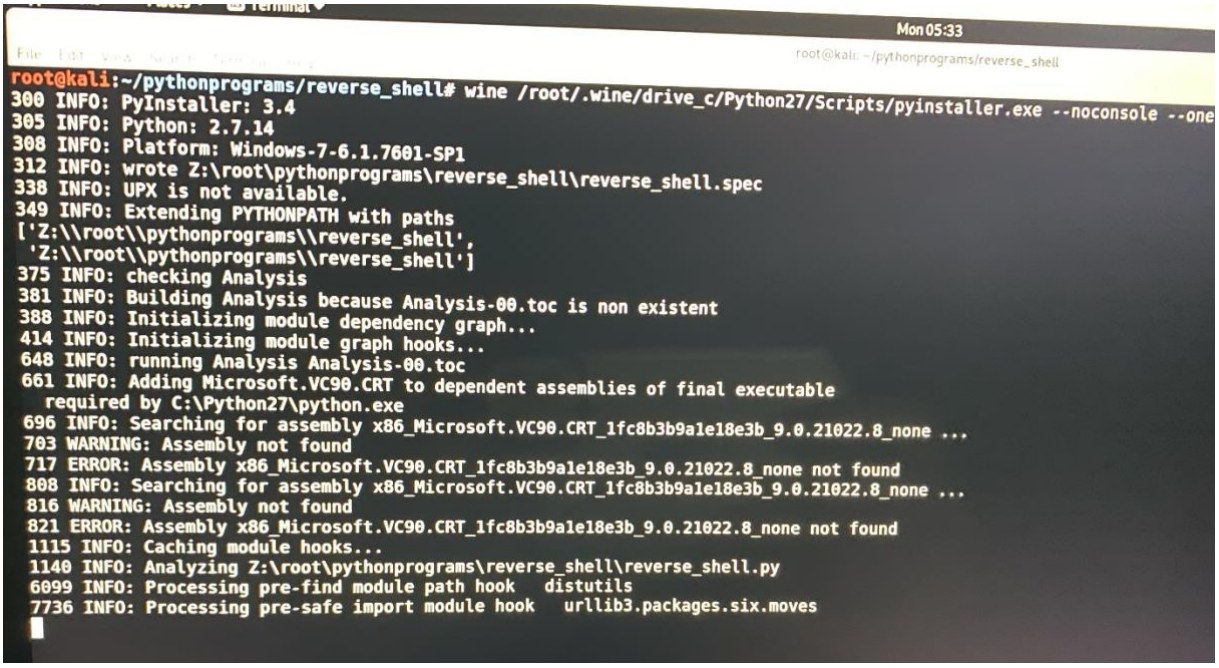


Figure 79: Compiling the Botnet

Simple ways to gain access

In order to highlight the dangers associated with Social Engineering, we had opted to launch a social engineering-based password attack. In which we had implemented the use of Kali Linux's Hydra, Metasploit, and Nmap applications. This had allowed us to enter any relevant information, collected via means of social engineering, such as a username and access the targeted system or account. This resulted in the group successfully gaining access to not only the webservice hosted on the targeted "Eduvos" virtual machine, but also the system itself, as seen in the figures below.

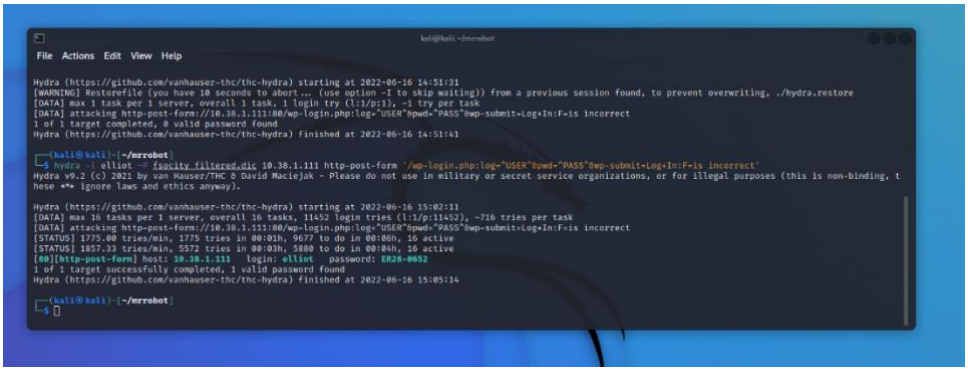


Figure 80: Gaining access to web service

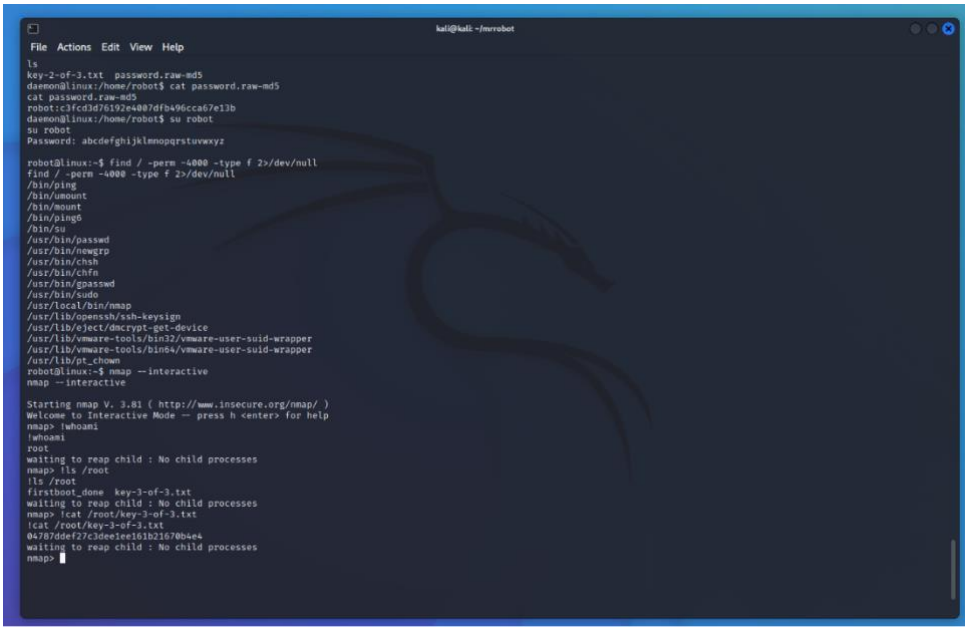


Figure 81: Gaining access to the system

Attack modern wireless networks

Make sure Kali Linux can detect your Wi-Fi card. The ifconfig command mat be used to search for wireless interfaces. We are focused only on the interface the begins with a “w”, but you should also see an Ethernet and loopback interface. Unless you have numerous wireless cards, wlan0 will likely be the wireless interface you wish to utilize.

The wireless interface will then be placed in monitor mode using aircrack-ng, allowing it to watch nearby and record wireless packets to aid the assault. The command listed below must be executed.

The program will then be capable to do calculations and data evaluations to crack the unsecure WEP protocol when we begin executing the dump command to capture packets from other wireless devices. The following commands are entered:

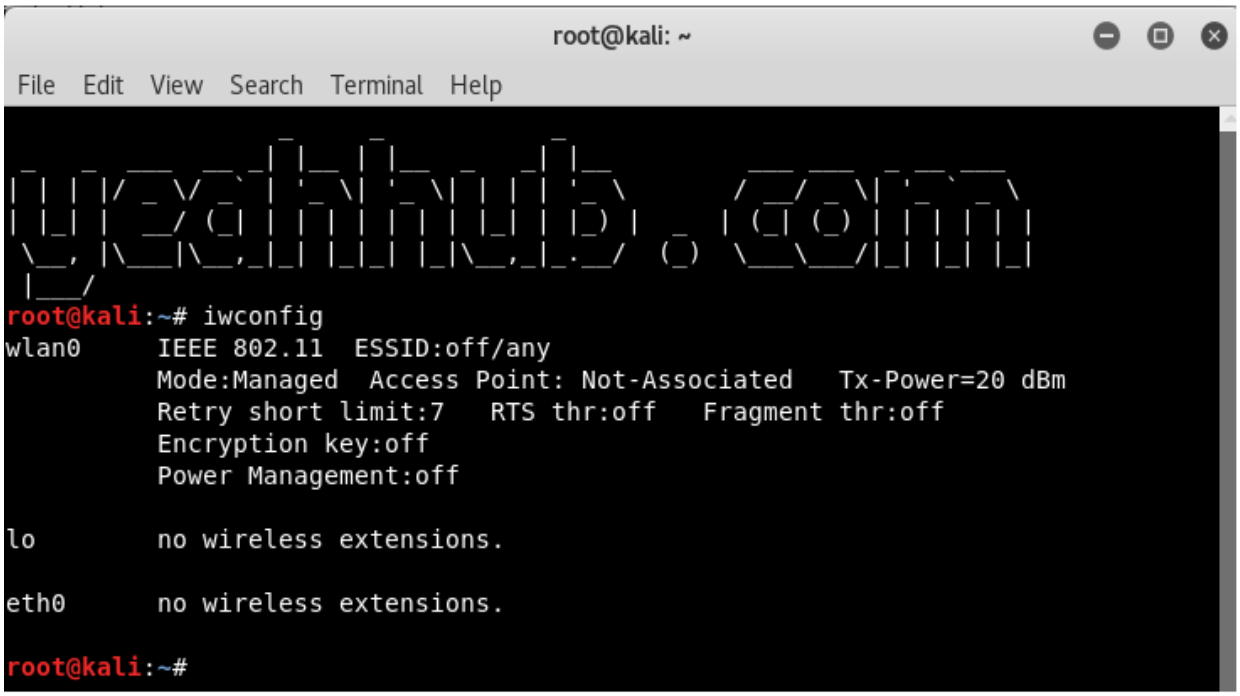


Figure 82: iwconfig

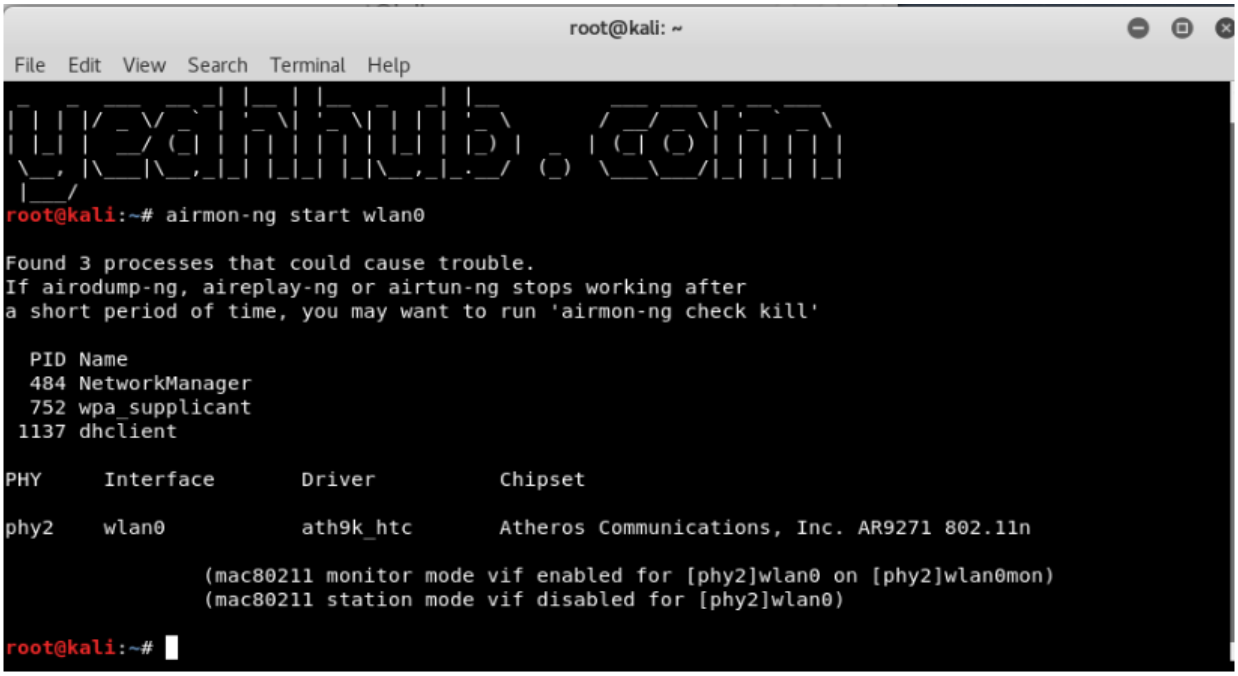


Figure 83: airmon-ng start wlan0

The wireless connection must be instructed to begin saving recorded wireless data depending on the network of your choice at this point. Don't forget to enter the following command with three crucial data points from the previous output:

- **airodump-ng –w [ESSID] –c [Channel] –bssid [BSSID] mon0**

Prior continuing with the next stages, you should obtain at least 10,000 packets. To transfer your data to a directory on your hard disk, execute the command:

- **airodump-ng mon0 –[file-name]**

By really employing the data that was obtained from the WEP device, you will want to complete the procedure' most crucial phase. Use the given order**.**

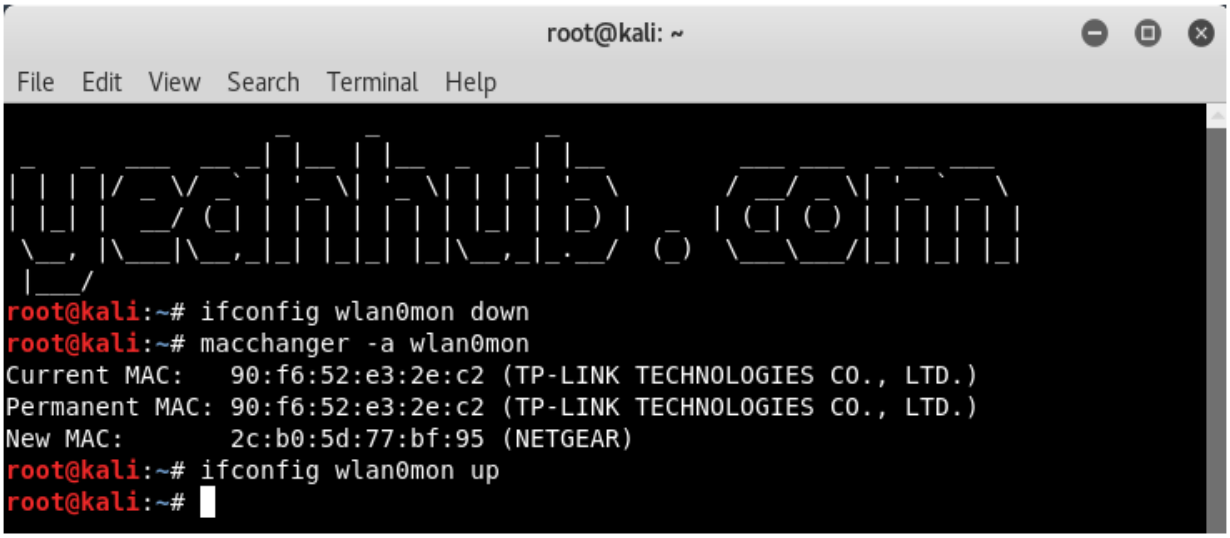


Figure 84: ifconfig wlan0mon up

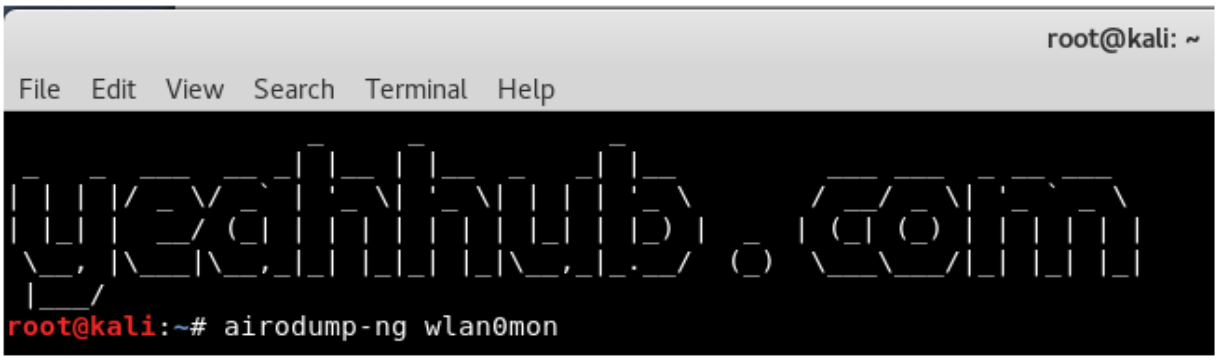


Figure 85: airodump-ng wlan0mon

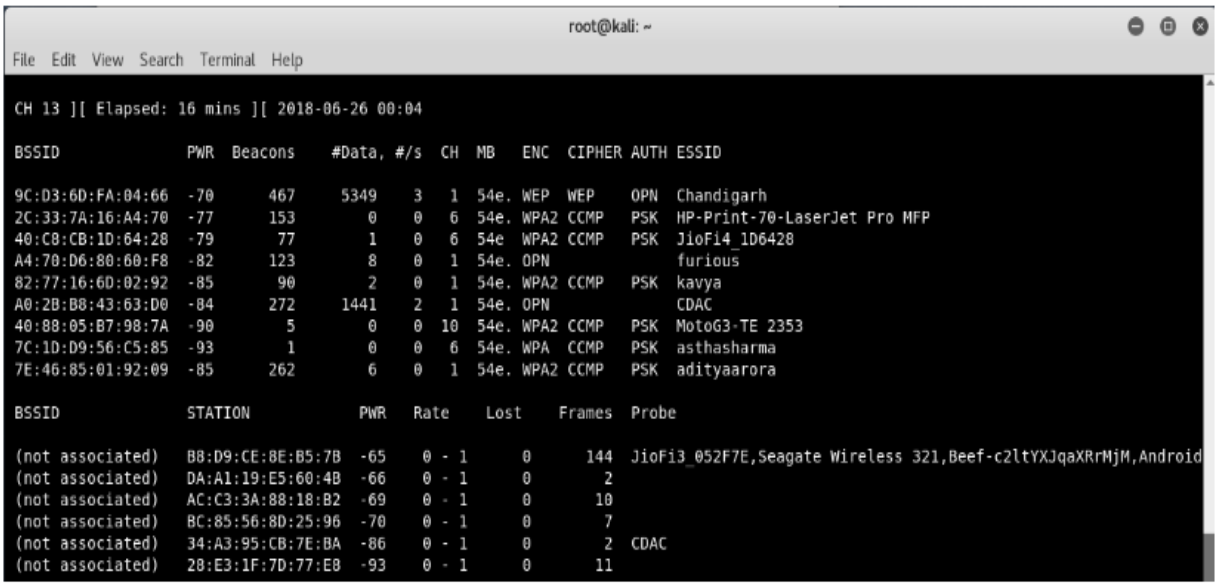


Figure 86: BSSID

Figure 87: airodump-ng -c <channel> –bssid <target mac> -w <filename> <interface name>

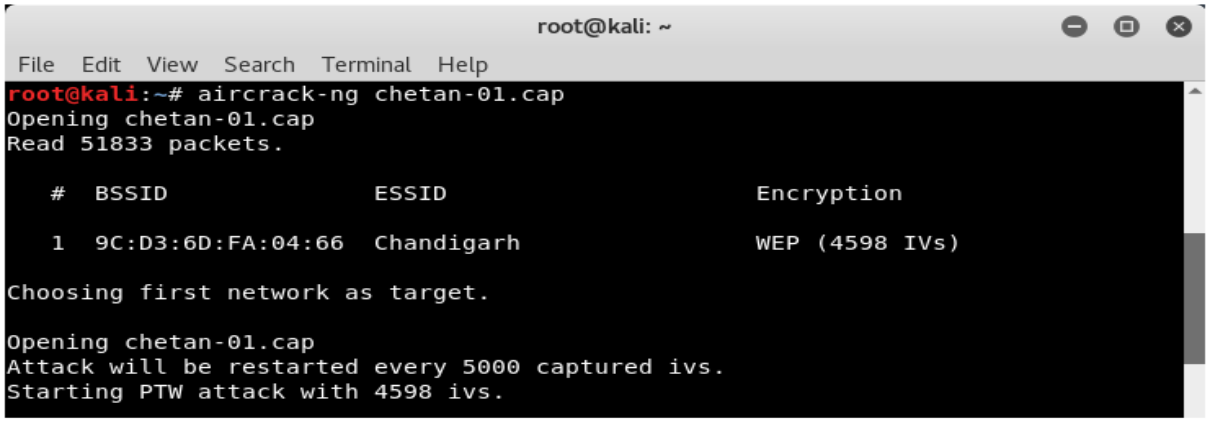


Figure 88: aircrack-ng <filename-01.cap>

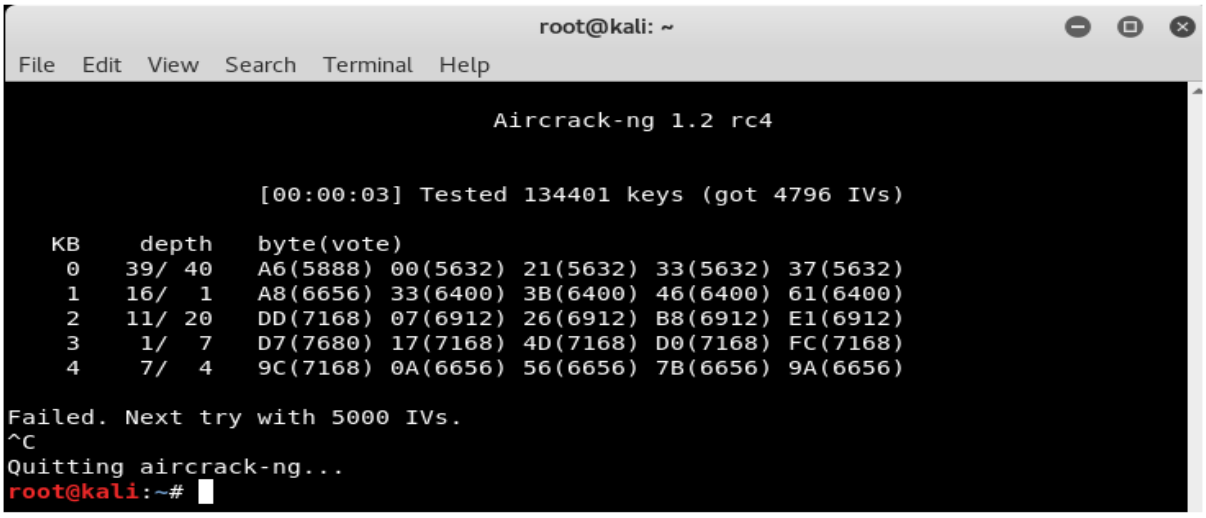


Figure 89: 4796 packets

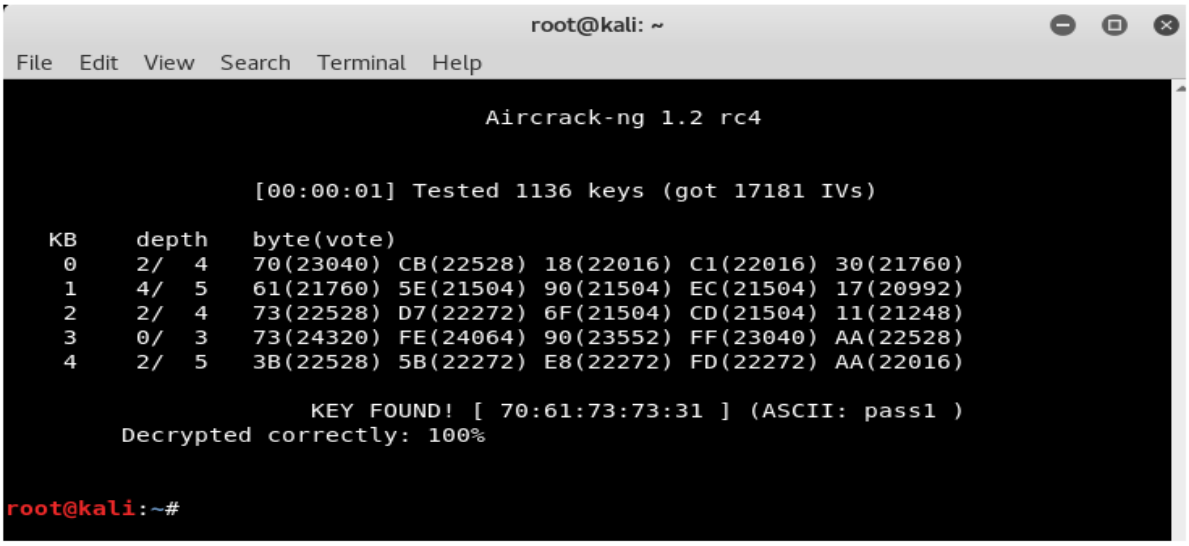


Figure 90: 17181 packets

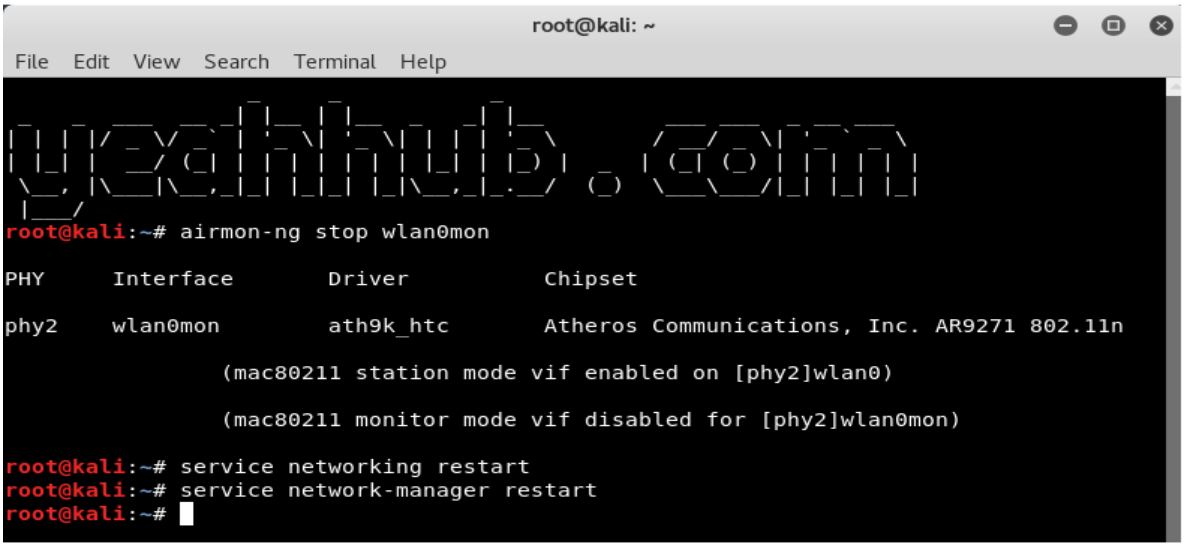


Figure 91: airmon-ng stop wlan0mon

Attack web applications

The approach of SQLi was executed using the Kali Linux virtual machine and one of its pre-installed penetration testing tools known as SQLmap. This tool has allowed us to gain unauthorised access into the web application database and make changes to it without any administrator rights.

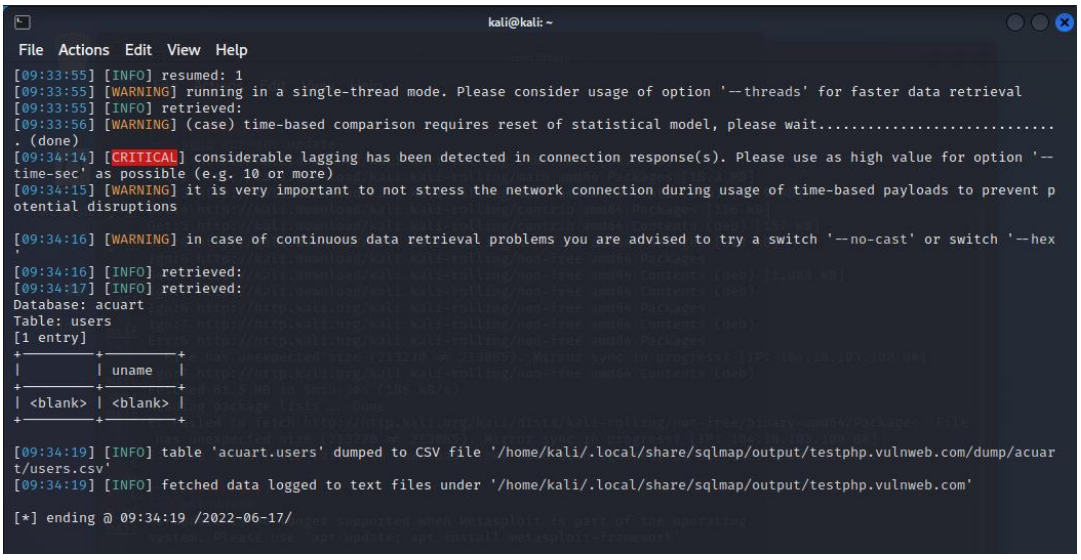


Figure 92: Web application attack outcome

Mobile phone attacks

Students and staff alike in tertiary institutions all use mobile devices to store critical information in some form. This presents another access point for potential attacks. The method of delivery for these attacks relies heavily on social engineering techniques where the user is coerced or falsely led to install an untrusted CA certificate or malicious APK file. The results once installed on the device have shown that information such as usernames, passwords and cookies can be extracted from decrypting an SSL session. The results also show that a trojan APK file can be successfully created and installed on a device, from where the device can be accessed and controlled. Another test showed that the WhatsApp APK file could be decompiled, and reverse engineered, where it can be published and deployed to devices.

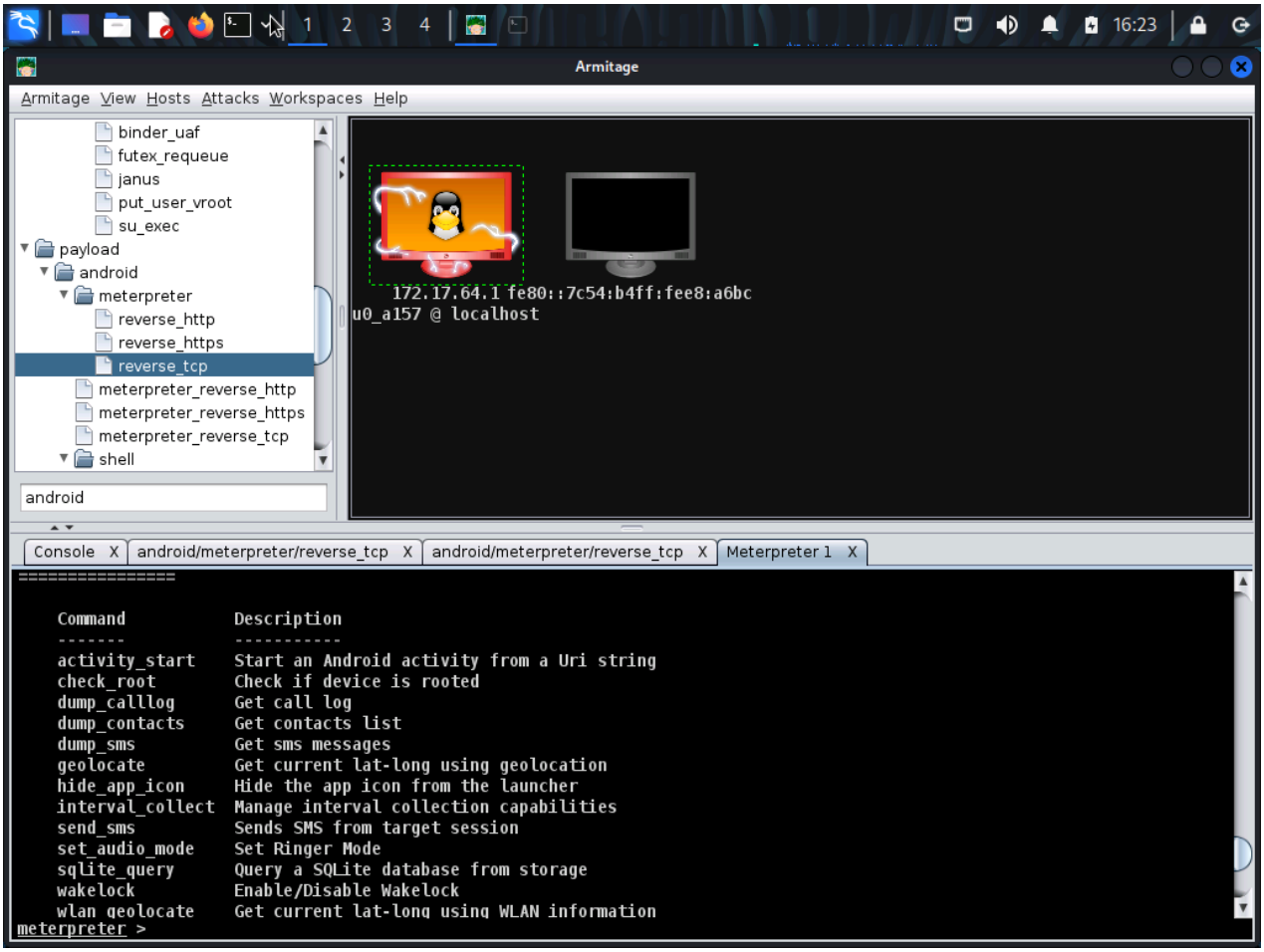


Figure 93: Successful trojan attack

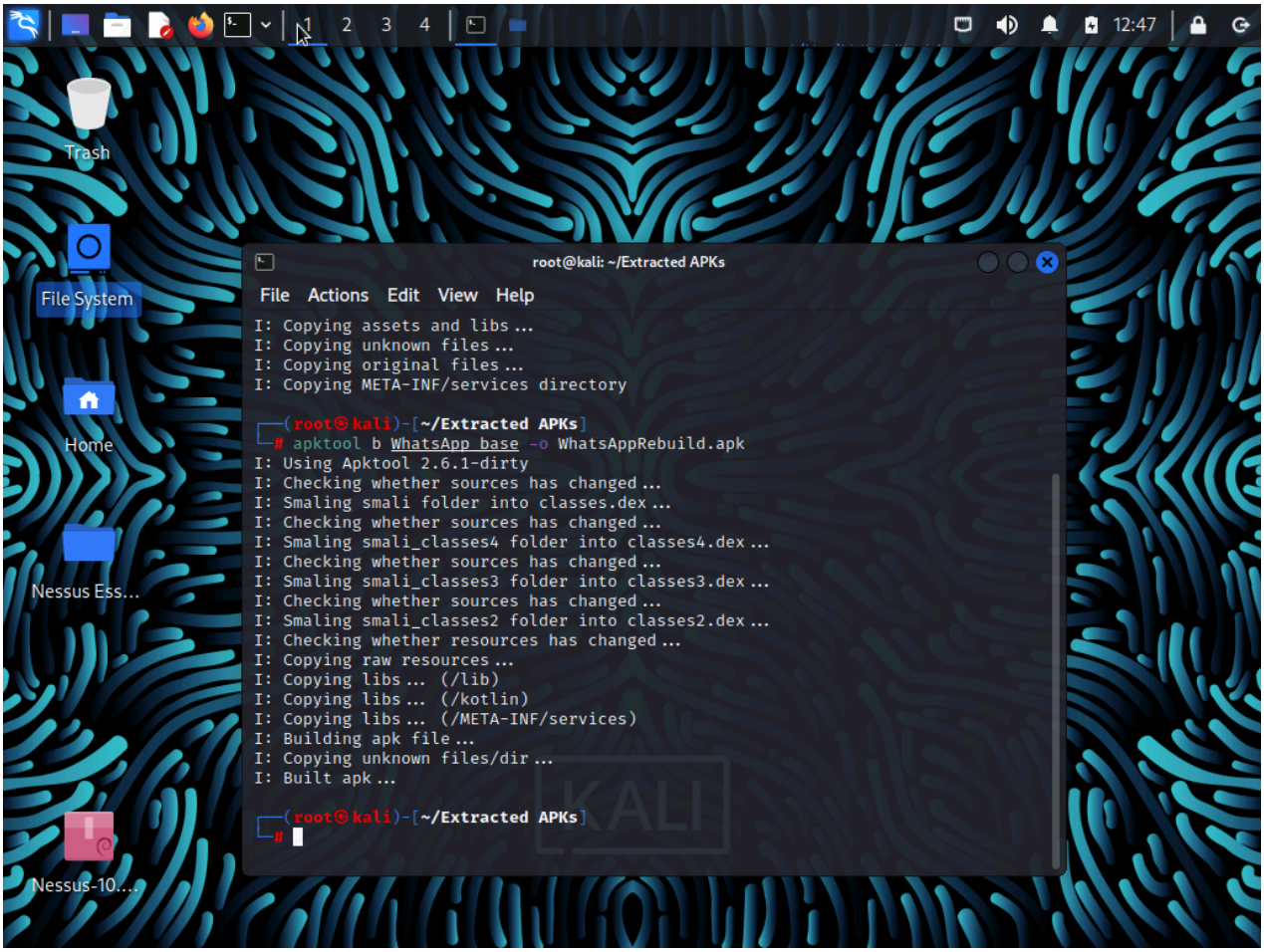


Figure 94: Reverse engineering WhatsApp APK

Conclusion

Projects	Effectiveness	Results	References
Botnet Attack	The botnet was effective in connecting to multiple hosts. The keylogger is successful in obtaining users key stocks. The bitcoin miner can mine crypto currency. The command-and-control server can give commands to multiple hosts.	The developed botkit used a python script to get back door access to the targeted machine. The back door allowed the team to deploy the botnet. The botnet used keylogger to steal user information. The botnet installed the python-based bitcoin miner to mine crypto currency.	Spamhaus's Q4 2021 Botnet Threat Update reported a 23% increase in botnet C&Cs (command and control) attacks from 2,656 in Q3 2021 to 3,271 in Q4 2021 (McCart, 2022). The NetScout 1H 2021 report also showed that adversaries use tracked botnet clusters worldwide to facilitate over 2.8 million DDoS (Distributed Denial of Service) attacks. Gafgyt and Mirai botnets made up more than half of these attacks (Ramirez, 2021). The most recent annual analysis from Cognyte examines the top four botnet markets, including Genesis, Russian Market, 2easy, and Amigos, on a macro level. Over 9 million stolen login credentials that were gathered between 2019 and 2021 were examined as part of our research. Login credentials are increasingly being sold on these marketplaces, with the total amount of stolen credentials reaching over 3.8 million in 2021 as opposed to 5.2 million sold in 2019 and 2020 combined. (Amir Barel 2020) The number of Mirai variations discovered in 2019 increased by 57%. Although Mirai variants are known to primarily compromise IoT (Internet of Things) devices using brute-force attacks, there was a rise in both attacks (51%) and web exploitation (87%) efforts in 2019 (Fruhlinger, 2018).

			2019 saw 300.000 notifications of Emotet botnet activity. In comparison to the same period in 2018, this resulted in almost 100.000 more victim alerts. Comparing the second halves of 2018 and 2019, researchers theorised that there was a 913 percent rise in the quantity of Emotet samples (Ikeda, 2021).
Simple ways to gain access	Simple ways to gain access, which was comprised of a host methods and techniques, was extremely effective in not only gaining access to the web services hosted but the device it was hosted on as well.	The executed password attack, utilising the data obtained from social engineering, allowed the group to not only gain access to the web services hosted on the Eduvos virtual machine, but also gain control of the device itself.	According to Branko (2022) a staggering 90% of passwords are vulnerable in some way to an attack to attack. A recorded 57% of compromised accounts still utilise the same password (Vojinovic, 2022). 27% of America has attempted to guess someone else's password, and shocking 17% are able to gain access, as documented by google (Johnson, 2021). An estimated 81% of data breaches stem from weak password security (Jovan, 2022).
Attack modern wireless networks	The security of WEP, a stream cipher, depends on never using the same key again. Unfortunately, as shown in multiple documented attacks, it is simple for an attacker to have the same key be used more than once	I could easily display a numerous amount of WEP's and with that start picking at those that support the most vulnerable portals.	According to Walter Gioko, there has been an increase to the benefits for using wireless networks but there are new threats that were not known with wired networks (Walter, 2020) Following (Logsign, 2020) we found the three most used network attack are Packet Sniffing, Rogue Access Point and Jamming. As indicated by (Noor & Hassan, 2013) there is a significant inclination in the intrusion of the network assault. In 2004 alone

	by replaying network data in a way that creates a huge number of packets. This makes it possible for a hacker to get the information required to figure out the encryption key and directly decrypt the network password.		there were 368 reported cases. From 2007 to 2011, there is a clear trend toward more intrusion-related assaults, which sees a high 861% rise. Best practices against wireless network attacks require you isolate the guest network, encrypt Wi-Fi-traffic with WPA2 or WPA3 creating secure SSID's and many more explained by (Cybersecurity Advice, 2021).
Attack web applications	The SQLi was successfully executed with no hassles and also had saved us enough time to proceed with other methods of attacks.	The SQLmap tool has allowed us to dump invalidated data into the administrator database without any form of authentication.	Based on the security measures mentioned by (Singh, 2021) Multi-layered, Holistic Security Solution is a good strategy to prevent SQLi. This includes penetration testing, security auditing and threat analysis. (Hannah, 2020) According to (Rob Rachwald, 2020) Web Application Firewalls (WAFs) and IPS are defending web applications from external attacks. As stated by (Hannah, 2020) sanitizing and escaping user input would prevent attackers from dumping malicious codes into the web scripts. It has been stated by (ptsecurity, 2019) that 82% of the vulnerabilities were found in web application code. Statistics and trends show that 50% of web application attacks were high in 2019 as stated by (ptsecurity, 2019).

Mobile phone attacks	The three tests were highly effective in extracting information from the mobile device but is also highly dependent on the type of deployment method used, lowering the acceptance rate of installing unknown applications.	Decryption of the SSL session yielded access to data from real-time application usage on the device. The extracted APK file was successfully reverse-engineered, ready for deployment. The malicious APK file was successfully installed on the device, and a listening port was opened in Armitage on Kali Linux from where there was complete access to the device.	Malware applications are mostly distributed on social media websites or through SMS, in order to avoid any security screening (Castillo & Samani, 2021). Malware accounted for the largest share of attacks in 2021 at 80.69%, with adware second at 16.92%, and RiskWare at 2.38% (Shishkova & Kivva, 2022). Mogilevsky (2021) relates that 46% of organisations had their systems and information at risk of compromise due to at least one employee having downloaded a malicious mobile application. Verizon and Lookout reported a 37% increase in enterprise mobile phishing attacks in their annual security reports (Gontovnikas, 2021). Verizon reported that 93% of Android devices were running older, out-of-date operating systems (Verizon, 2021).

Table 8: Results and effectiveness of techniques

Recommendations

Projects	Threat Priority Level	Attack Indicators	Planned Action	Affected Stakeholders
Botnet Attacks	High level threat	Any unusual levels of internet traffic are often an indicator that a botnet is either attacking you or you have become part of a botnet.	In order to detect infections in devices, static analysis approaches can be useful. These are used to scan for malware signatures and other suspect connections to command-and-control servers that look for instructions and suspicious executable files when the device is not running any apps.	Because of the nature of a botnet, it spreads rapidly over the entire network and infects all computers on that network. The entire organization is at risk if a botnet infects their network.
Simple Ways to Gain Access	High level threat	No attack indicators.	The most common methods to mitigate, and or reduce, the chance of an attacker gaining access to the system, via a password attack, is to implement the utilisation of multifactor authentication and encourage frequent password changing.	Ways to gain access to a system is a category that comprises of various methods of attacking and intrusion. Thus, this large scope affects various, if not all stakeholders, within an institutional or organisational environment.
Attack Modern Wireless Networks	High level threat	An increasing loss of data.	The best choice you have is to change your router admin credentials, to set up stronger encryptions and keep your router updated.	This affects basically anybody that is connected to the internet wirelessly. This includes students, staff, groundskeeper and even a passer-by.

Projects	Threat Priority Level	Attack Indicators	Planned Action	Affected Stakeholders
Attack Web Applications	High level threat	Any changes in the database, without formal administration. Any changes in users' data without authorised access.	Input validation is one of the security measures to be taken by higher education institutes to protect themselves from this kind of attack.	Students, lectures, and staff would be highly affected by unauthorized changes in their confidential data. In this case, SQLi compromises the confidentiality and integrity of the user's data.
Mobile Phone Attacks	Medium level threat	An increase in mobile data usage. Majorly reduced performance of the phone. Abnormal battery drain. Pop-up advertisements .	Uninstalling suspicious applications, and at the worst-case reformatting the device will clear the malicious software. Users should, however, pre-empt these attacks by keeping their device up to date, encrypting their device, backing up their data, and only downloading applications from official sources and stores.	Students and staff are affected; however, the severity is dependent on the security measures each individual has in place on their device.

Table 9: Recommendations

Future work

Upon conducting our various projects to illustrate the dangers and lack of awareness associated with Social Engineering, and Social Engineering based attacks, within Eduvos' tertiary institute environment, the group had found various methods and tactics that could not be implemented in this research project, due to limiting factors, but may be utilised and incorporated into future iterations of research. These methods and tactics are stated and defined in the following paragraphs.

More integrating of A.I. (Artificial Intelligence) in social engineering as well as Voice transfer A.I. (Artificial Intelligence). New voice technology allows attackers to impersonate the sound of their chosen target. For example, a cybercriminal recently used voice imitation to defraud a company for $243,000. The social engineer utilized A.I. to mimic the voice of the CEO of a company and succeeded in transferring copious amounts of funds to their accounts (Tsukerman, 2020).

“Advanced Natural Language Processing (NLP) technology has allowed automated production of targeted phishing bots that outperform humans. They can successfully phish an astonishing two out of three users. These fully automated, A.I.-based phishing bots generate interesting tweets and then fools users into clicking on them.” (Gyansetu, 2021).

How to use A.I. to defend against social engineering; there are a plethora of A.I.-powered chatbots that work to resolve client difficulties. However, if a malicious A.I.-powered is taught to interact with humans in a polite and helpful manner, it can be used to find consumer complaints online and pose as a customer support bot attempting to resolve the issue. If someone falls for this ruse, they may be forced to provide critical information such as security question answers, passwords, or personal identifying information.

The group was able to successfully create functional botnets, but due to our lack of expertise and resources pertaining to botnet account takeovers we were unable to follow through on a coordinated Eduvos account takeover. This method of attack may be visited in future studies regarding botnet account takeovers.

Brute force attacks refer to manually entering various passwords in hopes of accessing a system or account. This method of password cracking, or hacking, has been identified by the group as too tedious and time consuming. Thus, this method, even though it is a plausible and functional method, was not explored by the group but may be implemented in future studies and practical applications.

Dictionary attacks refers to the utilisation of a diverse collection of possible passwords in attempt of gaining access to the targeted system or account. In the conducted research,

the group had identified and a limited number of possible passwords, this was done to limit the demanded processing capabilities. In future studies, a system with higher processing capabilities may be utilised to launch a dictionary attack that utilises a larger wordlist, such as KALI's Rockyou wordlist.

This research allows future instances of social engineering research to improve awareness around social engineering-based attacks, as it demonstrates the numerous ways in which these social engineering techniques and methods may be utilised in a practical scenario.

According to (James, 2018) Cross-Site Scripting is one of the most dangerous web application attacks, as it enables the attacker to inject malicious snippets of JavaScript in the web application without any form of validation. This method was not utilised in our research but would be revisited in future studies and bring forth successful results in future work.

The sheer number of mobile phones, and the fact that there are more phones than people in the world presents a major problem for security. Mobile device technology is ever expanding and evolving, resulting in newer techniques and methods of attacks. At present, only the current trends in the mobile security space can be researched and analysed, opening the way for further research into future issues (Ciber 4 All Team, 2021).

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

As a result of setting up and configuring the proposed Botnets, we are prompted to enter the details of the target system, thus, within the correct situation there is a possibility for a Botnet attack, or account takeover, to target Eduvos.

In simple ways to gain access, we may conclude that the Mr Robot system, that was used to mimic a real world Eduvos system, had been accessed by utilising tools such as Nmap, Burp Suite, HYDRA, and other tools. Therefore, making it evident that these methods may be utilised in a real-world scenario to gain access to an Eduvos system.

Within the Modern Wireless Network Attack framework, a simulated watering hole attack was executed. As a result, we were able to easily obtain student simulated data from their devices. Thus, making it increasingly evident a similar attack may be executed within an Eduvos campus, or environment.

As a result of conducting Mobile Phone Attacks, we may conclude that the SSL encrypts information between the client and the server and provides authentication to ensure that the intended connection is established. This, however, is not enough when it comes to sufficiently securing applications, devices and information. Security measures must be implemented, and information must be encrypted from the application and code level.

Within the field of Web Applications Attacks, we were able to gain unauthorised access to the targeted database and exploit the database's existing data. Thus, indicating towards the possibility of using similar tactics and techniques for exposing the actual Eduvos database, so that it can be exploited.

Therefore, it may be concluded, based on thew above evidence, that the incorporation of social engineering-based methods and techniques, and the above stated penetration testing framework, may be utilised to execute an attack, or gain sensitive information, within the Eduvos Institutional Environment.

BIBLIOGRAPHY

Alazri, A. S. (2015). *The awareness of social engineering in information revolution: Techniques and challenges*. Internet Technology and Secured Transactions, 198-201.

Aldawood, H. (2017). *Analysis and Findings of Social Engineering*. IEEEAccess, 9.

Aldawood, H., Alashoor, T. & Skinner, G., 2020. Does Awareness of Social Engineering Make Employees More Secure?. *International Journal of Computer Applications,* February, 177(38), pp. 45-49.

Alshoor Common Management Information Services and Protocol over TCP/IP (CMOT)". April 2019.

Alsulami, M. H. et al., 2021. Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. *Information,* 12 May, 12(5), pp. 1-13.

Amir Barel, *Keyloggers: How they work and how to detect them* (Part 1), Secure List, "Today, keyloggers are mainly used to steal user data relating to various online payment systems, and virus writers are constantly writing new keylogger Trojans for this very purpose." Retrieved June 24, 2022.

Barracuda (25 June 2020) *“InformationWeek Barracuda Rolls Out Spyware-Blocking Appliance”*.

Berzinskas, L., 2020. *Obfuscating Android Apps: Do you know your choices for protection?* [Online] Available at: https://proandroiddev.com/obfuscation-is-important-do-you-know-your-options-30b3ef396dfe
[Accessed 17 June 2022].

Borges, E., 2020. *The Social Engineering Toolkit*. [Online] Available at: https://securitytrails.com/blog/the-social-engineering-toolkit
[Accessed 09 June 2022].

Bosworth, Copper "Emotet uses parked domains to distribute payloads". How To Fix Guide. October 30, 2020. Retrieved June 24, 2022.

"botnet". Retrieved 17 June 2022. Available at: https://www.bing.com/searchq="botnet"&qs=n&form=QBRE&sp=-1&pq=botnet"&sc=8-7&sk=&cvid=C1EF0143265343C6A44FC921B4DBE62D
[Accessed 17 June 2022].

Branko K, 2022. *Impressive Password Statistics to Know in 2022*. [ONLINE] Available at: https://webtribunal.net/blog/password-stats/#gref.
[Accessed 24 June 2022].

Brian Contos, 2022. *From Rivals to BFF: WAF & VA Unite*. [ONLINE] Available at: https://owasp.org/www-pdf-archive/OWASP_Brian_Contos_WAF_and_VA_July2009_Final_PUBLIC.pdf.
[Accessed 03 June 2022].

Brian Prince | SecurityWeek.Com. 2022. Brian Prince | SecurityWeek.Com. [ONLINE] Available at: https://www.securityweek.com/authors/brian-prince.
[Accessed 03 June 2022].

Bullée, J. & Junger, M., 2020. Social Engineering. In: T. Holt & A. Bossler, eds. *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* s.l.:Springer Nature, pp. 2-21.

Burnham, K., 2021. *Web application attacks.* [Online]
Available at: https://www.mimecast.com/blog/web-application-attacks/

Campbell Douglas "*What is Cryptojacking? Defined, Explained, Explored* | Forcepoint". 24 January 2019. Retrieved June 24, 2022.

Carl Shirky. "Firewalls and fairy tales".; LOGIN: Vol 30, no. 1. Archive index at the Wayback Machine. Retrieved July 24, 2022

Castillo, C. & Samani, R., 2021. *McAfee Mobile Threat Report 2021*, San Jose: McAfee.
Chapple, M. & Seidl, D., 2018. *CompTIA PenTest+ Study Guide: Exam PT0-001.* 1st ed. Indianapolis: Wiley.

Checkpoint, 2021. *What is Ransomware?*. [Online]
Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/
[Accessed 19 May 2022].

Chan, Ethan (2019). "Circuit-level gateways". Security technologies for the World. Retrieved June 24, 2022

Chickowski, E., 2010. *SQL Injections Top Attack Statistics.* [Online]
Available at: https://www.darkreading.com/risk/sql-injections-top-attack-statistics
[Accessed 03 June 2022].

Ciber 4 All Team, 2021. *Cyber-attacks on mobile phones, the bloodletting that never stops*. [Online]
Available at: https://www.tarlogic.com/blog/cyber-attacks-on-mobile-phones/
[Accessed 24 June 2022].

CompTIA, n.d. *What Is Wireshark and How Is It Used?*. [Online] Available at: https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it
[Accessed 09 June 2022].

Crowdstrike, 2021. *10 Types of Social Engineering Attacks.* [Online]
Available at: https://www.crowdstrike.com/cybersecurity-101/types-of-social-engineering-

attacks/
[Accessed 05 April 2022].

Cybersecurity Advice, Internet Security, Mobile Security, Network Security, Web Filtering. [ONLINE] Available at: https://www.webtitan.com/blog/most-common-wireless-network-attacks/.
[Accessed 03 June 2022].

de Villiers, M., 2021. *SA schools targeted by cyber security threats.* [Online]
Available at: https://www.itweb.co.za/content/LPwQ57l6aokqNgkj
[Accessed 19 May 2022].

Douglas Rushkoff *2020 Circumvention Tool Usage Report*" (PDF). The Berkman Center for Internet & Society at Harvard University. October 2020. Retrieved July 24, 2022

Duarte, N., Coelho, N. & Guarda, T., 2021. *Social Engineering: The Art of Attacks*. s.l., Springer.

E. Frumento. (2016, February 1). *The role of Social Engineering in evolution of attacks*.

EASYDMARC. (2022, January 28). EasyDMarc. Retrieved from easydmarc.com: https://easydmarc.com/blog/how-does-social-engineering-affect-an-organization/

Eduvos, n.d. *About Eduvos.* [Online]
Available at: https://www.eduvos.com/about-eduvos/
[Accessed 19 May 2022].

Ernest Johnson, 2022. *Password Statistics That Will Change Your Online Habits* - Panda Security. [ONLINE] Available at: https://www.pandasecurity.com/en/mediacenter/tips/password-statistics/.
[Accessed 24 June 2022].

eSecurityPlanet. 2022. Peyton Engel, Author at eSecurityPlanet. [ONLINE] Available at: https://www.esecurityplanet.com/author/peyton-engel/.
[Accessed 03 June 2022].

Essuman, D., Boso, N. & Annan, J., 2020. Operational resilience, disruption, and efficiency: Conceptual and empirical analyses. *International Journal of Production Economics*, 12 April, 229(November 2020), pp. 1-11.

Faily, S., McAlaney, J. & Iacob, C., 2015. *Ethical Dilemmas and Dimensions in Penetration Testing.* s.l., s.n.

Federal Trade Commission, n.d. *The Antitrust Laws.* [Online]
Available at: https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/antitrust-laws
[Accessed 03 June 2022].

Firch, J., 2020. *How To Perform A Successful Network Penetration Test*. [Online]
Available at: https://purplesec.us/network-penetration-test/
[Accessed 19 May 2022].

Foresman, B., 2018. *Education ranked worst at cybersecurity out of 17 major industries.* [Online]
Available at: https://edscoop.com/education-ranked-worst-at-cybersecurity-out-of-17-major-industries/
[Accessed 03 June 2022].

Fraudehelpdesk.nl, 2018. *Aanzienlijke schade whatsapp-fraude.* [Online]
Available at: https://www.fraudehelpdesk.nl/aanzienlijke-schade-whatsapp-fraude/
[Accessed 03 June 2022].

Fruhlinger, J., 2018. *The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet.* [Online]

Available at: https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html
[Accessed 03 June 2022].

G. Nikhita Reddy, G. U. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies. *International Journal of Engineering and Technology*, 5.

GetNotify, n.d. *What is GetNotify*. [Online] Available at: https://www.getnotify.com/faq/#What_is_GetNotify
[Accessed 09 June 2022].

Goodin, Dan (24 May 2011). *"RSA won't talk? Assume SecurID is broken"*. The Register.

Gontovnikas, M., 2021. T*he 9 Most Common Security Threats to Mobile Devices in 2021*. [Online]
Available at: https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021/
[Accessed 24 June 2022].

g0tmi1k, 2022. *What is Kali Linux?*. [Online] Available at: https://www.kali.org/docs/introduction/what-is-kali-linux/
[Accessed 09 June 2022].

Gupta, B. B. (2017). *Fighting against phishing attacks: state of the art and future challenges*. ACM, 3629–3654.

Gyansetu, 2021. *What is Natural Language Processing? Intro to NLP in Machine Learning.* [Online]
Available at: https://www.gyansetu.in/what-is-natural-language-processing
[Accessed 22 June 2022].

Hadnagy and Willson An MIT graduate who brings years of technical experience to articles on; computers; Networking, Wireless. "What Is Transmission Control

Hannah, J., 2020. *Web Application Attack: What is it and How to Defend Against It?.* [Online]
Available at: https://www.techlila.com/web-application-attack/

Happ, Nathan "*New Cryptojacking Malware Variant Targeting Cloud Systems Discovered* - Infosecurity Magazine". 6 October 2020. Retrieved June 24, 2022.

Husein, 2020. *How to Perform a Phishing (whaling) attack via Emkei's Fake Mailer*. [Online] Available at: https://zsecurity.org/how-to-perform-a-phishing-whaling-attack-via-emkeis-fake-mailer/
[Accessed 09 June 2022].

Ikeda, S., 2021. *Emotet Malware Taken Down By Global Law Enforcement Effort, Cleanup Patch Pushed to 1.6 Million Infected Devices.* [Online]
Available at: https://www.cpomagazine.com/cyber-security/emotet-malware-taken-down-by-global-law-enforcement-effort-cleanup-patch-pushed-to-1-6-million-infected-devices/
[Accessed 03 June 2022].

Inyoung Hwang, 2022. *What is cryptojacking? How to detect mining malware* - MediaFeed. [ONLINE] Available at: https://mediafeed.org/what-is-cryptojacking-how-to-detect-mining-malware/.
[Accessed 03 June 2022].

Ivana Vojinovic,. 2022. *Save Your Data with These Empowering Password Statistics* | DataProt. [ONLINE] Available at: https://dataprot.net/statistics/password-statistics/.
[Accessed 24 June 2022].

Ivankova, N., Creswell, J. & Stick, S., 2020. Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice. *Field Methods. Retreived 7 June 2022*

James, P., 2018. *Top Five Most Common Web Application Attacks That Affecting Websites.* [Online]
Available at: https://gbhackers.com/web-application-attacks/#:~:text=Top%205%20Most%20Common%20Web%20Application%20Attacks%20That,...%205%20SQL%20Injection.%20...%206%20Malware.%20

JavaTpoint, 2021. *Post Exploitation Concept*. [Online]
Available at: https://www.javatpoint.com/post-exploitation-concept
[Accessed 19 May 2022].

Jovan, 2022. *21 Must-Know Weak Password Statistics for Utmost Security*. [ONLINE]
Available at: https://kommandotech.com/statistics/weak-password-statistics/.
[Accessed 24 June 2022].

Julie Bort. 2022. *Attack of the killer bots* - ARN. [ONLINE] Available at: https://www.arnnet.com.au/article/189967/attack_killer_bots/.
[Accessed 03 June 2022].

Kshetri, N., 2021. *Cybercriminals use pandemic to attack schools and colleges.* [Online]
Available at: https://iowacapitaldispatch.com/2021/09/21/cybercriminals-use-pandemic-to-attack-schools-and-colleges/
[Accessed 19 May 2022].

Kurt Thomas, F. L. (2017). *Data Breaches, Phishing, or Malware?: Understanding the Risks of Stolen Credentials*. ACM, 1421–1434.

Kyeremeh, K., Bright, B. K. & Matilda, A. F., 2019. *A Study into the Social Engineering Risk and Its Effects in the Public Institutions in Ghana,* s.l.: Elsevier.

"Lance Whitney Named Editor in Chief of PC Magazine Network". adage.com. 2019-04-11. Retrieved 2022-06-03.

Lance Whitney. 2022. *How to combat the latest and most aggressive botnets and malware* | TechRepublic. [ONLINE] Available at: https://www.techrepublic.com/article/how-to-combat-the-latest-and-most-aggressive-botnets-and-malware/.
[Accessed 03 June 2022].

Lastdrager, E., 2014. Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science,* 03 September, 3(9), pp. 1-10.

Learning Center. 2022. *What is Penetration Testing* | *Step-By-Step Process & Methods* | Imperva. [ONLINE] Available at: https://www.imperva.com/learn/application-security/penetration-testing/.
[Accessed 03 June 2022].

Live botnet threats worldwide | Spamhaus Technology. 2022. *Live botnet threats worldwide* | Spamhaus Technology. [ONLINE] Available at: https://www.spamhaus.com/threat-map/.
[Accessed 03 June 2022].

Logsign, 2020. *Types of Wireless Network Attacks.* [Online]
[Accessed 05 June 2022].

Loukas, Keith (October 22, 2018). *"The OSI model explained: How to understand (and remember) the 7 layer network model"*. Network World. Retrieved June 5, 2022.

Maltego, n.d. *What is Maltego?* . [Online] Available at: https://www.maltego.com/maltego-faq/#what-is-maltego
[Accessed 09 June 2022].

McCart, C., 2022. *15+ Shocking botnet statistics.* [Online]
Available at: https://www.comparitech.com/blog/information-security/botnet-statistics/
[Accessed 03 June 2022].

McGoogan, C., 2016. *WhatsApp users targeted with £100 Sainsbury's scam - how to protect yourself.* [Online]
Available at: https://www.telegraph.co.uk/technology/2016/10/25/whatsapp-users-targeted-with-100-sainsburys-scam---how-to-protec/
[Accessed 03 June 2022].

Michael Dibna Hummingbird networks 2019 *How attackers use social engineering in the real world*. Social Engineering handbook.

MODERN DAY ATTACKS ON WIRELESS NETWORKS. [ONLINE] Available at: https://www.academia.edu/29615663/MODERN_DAY_ATTACKS_ON_WIRELESS_NETWORKS_docx.
[Accessed at 03 June 2022].

Mogilevsky, O., 2021. *Check Point's Mobile Security Report 2021: Almost Every Organization Experienced a Mobile-related Attack in 2020*. [Online]
Available at: https://blog.checkpoint.com/2021/04/12/check-points-mobile-security-report-2021-almost-every-organization-experienced-a-mobile-related-attack-in-2020/
[Accessed 24 June 2022].

Moulder 2019. *"Pen Testing Types explained"*. Internal Cyber Security Rulebook. Retrieved 2022-06-03.

Mouton, F., Malan, M. M., Leenen, L. & Venter, H., 2014. Social Engineering Attack Framework. *Information Security for South Africa*, pp. 1-9.

Muncaster (2018-03-15). "*Hospital to punish snooping on Spears*". Los Angeles Times. Retrieved 2022-04-07.

Nakar, O. & Azaria, J., 2019. *SQL injection attack: so old but still so relevant.* [Online] Available at: https://www.imperva.com/blog/sql-injection-attacks-so-old-but-still-so-relevant-heres-why-charts/
[Accessed 03 June 2022].

Najera-Gutierrez, G., Ansari, J. A., Teixeira, D. & Singh, A., 2019. *Improving your Penetration Testing Skills*. 1st ed. s.l.:Packt Publishing.

Nataliya V. Ivankova, John W. Creswell and Sheldon L. Stick, 2022. *Using Mixed-Methods Sequential Explanatory Design*. [ONLINE] Available at: https://www.dedoose.com/publications/using%20mixed-methods%20sequential%20explanatory%20design%20from%20theory%20to%20practice.pdf
[Accessed 03 June 2022].

Nguyen, T. H. & Bhatia, S., 2020. Higher Education Social Engineering Attack Scenario, Awareness & Training Model. *Journal of The Colloquium for Information Systems Security Education,* 8(1), pp. 1-8.

Nmap, n.d. *Nmap: Discover your network*. [Online] Available at: https://nmap.org/
[Accessed 11 June 2022].

Noor, M. & Hassan, W., 2013. Wireless Networks: Developments, Threats and Countermeasures. *International Journal of Digital Information and Wireless Communications,* 3(1), pp. 125-140.

Obbayi, L., 2019. *A brief introduction to the Nessus vulnerability scanner*. [Online] Available at: https://resources.infosecinstitute.com/topic/a-brief-introduction-to-the-nessus-vulnerability-scanner/
[Accessed 10 June 2022].

ostec. (2018, May 17). *ostec*. Retrieved from ostec.blog: Available at: https://ostec.blog/en/general/social-engineering-impacts/

Pandhya, A. & Lodha, P., 2021. Social Connectedness, Excessive Screen Time During COVID-19 and Mental Health: A Review of Current Evidence. *Frontiers in Human Dynamics,* 22 July, Volume 3, p. 2.

Pike, R., 2013. The “ethics” of teaching ethical hacking. *Journal of International Technology and Information Management,* 04 November, 22(4), pp. 67-75.

ptsecurity, 2019. *Web Application vulnerabilities and threats attacks statistics for 2019.* [Online]
Available at: https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/

PurpleSec. 2022. *2021 Cyber Security Statistics: The Ultimate List of Stats, Data & Trends* | PurpleSec. [Online]
Available at: https://purplesec.us/resources/cyber-security-statistics/
[Accessed 04 April 2022].

Radar de Kolf. "Intel Management Engine, Explained: The Tiny Computer Inside Your CPU". How-To Geek. Retrieved June 24, 2022.

Rafaeli Standler "*Bitcoin Mining*". BitcoinMining.com. Archived from the original on 30 April 2020. Retrieved 17 July 2022. A Complete Guide to Cryptocurrency Trading for Beginners | Binance Academy

Ramirez, R., 2021. *Gafgyt is a botnet that uses Mirai DDoS modules.* [Online]
Available at: https://truxgoservers.com/blog/gafgyt-is-a-botnet-that-uses-mirai-ddos-modules/
[Accessed 03 June 2022].

Ravie Lakshmanan, 2022. *FritzFrog P2P Botnet Attacking Healthcare, Education and Government Sectors*. [ONLINE] Available at: https://thehackernews.com/2022/02/fritzfrog-p2p-botnet-attacking.html. [Accessed 03 June 2022].

Richey, R.C. (2018). *"Reflections on the 2008 AECT Definitions of the Field"*. TechTrends. Springer Science and Business Media LLC. 52 (1): 24–25.

Richmond, R., 2011. *The RSA Hack: How They Did It.* [Online] Available at: https://archive.nytimes.com/bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/ [Accessed 22 May 2022].

Rob Rachwald, K. C., 2020. *Review: Analyzing the effectiveness of WAF.* [Online] Available at: https:///blog/review-analyzing-the-effectiveness-of-web-application-firewalls/

Robert Braden, ed. (October 2020). "RFC 1123: Requirements for Internet Hosts – Application and Support". Network Working Group of the IETF.

Rouse, M., 2006. *Definition social engineering.* [Online] Available at: http://www.searchsecurity.techtarget.com/definition/social-engineering [Accessed 03 June 2022].

Rubin, J. & Chisnell, D., 2008. *How to Plan, Design, and Conduct Effective Tests*. 2nd ed. Indianapolis: Wiley Publishing, Inc.

Russell, Stuart J.; Norvig, Peter (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Hoboken: Pearson. ISBN 9780134610993. LCCN 20190474.

Sahri, Z. et al., 2014. Implementing IT Security Penetration Testing in Higher Education Institute. *Australian Journal of Basic and Applied Sciences*, 17 June, 8(21), pp. 67-72.

Security Boulevard. 2022. *The High Cost of Phishing in K-12 Schools - Security Boulevard*. [Online] Available at: https://securityboulevard.com/2021/07/the-high-cost-of-phishing-in-k-12-schools.
[Accessed 19 May 2022].

Scheier, Smith "Service Name and Transport Protocol Port Number Registry". Internet Assigned Numbers Authority. 19 May 2018. Retrieved June 24, 2022.

Sheizaf Frank, "Bogus story: no Chinese backdoor in military chip". blog.erratasec.com. Retrieved 24 July 2022.

Shishkova, T. & Kivva, A., 2022. *Mobile malware evolution 2021*. [Online]
Available at: https://securelist.com/mobile-malware-evolution-2021/105876/
[Accessed 24 June 2022].

Siadati Kruger, (December 24, 2019). "*Emotet Reigns in Sandbox's Top Malware Threats of 2019*". Bleeping Computer. [Accessed 24 June 2022]

Simon Heron. 2022. . [ONLINE] Available at: https://dl.acm.org/doi/10.1016/S1353-4858%2807%2970045-4.
[Accessed 03 June 2022].

Singh, R., 2021. *10 Best Practices to Prevent Web Application Attacks.* [Online]
Available at: https://www.indusface.com/blog/what-are-the-best-security-practices-to-protect-against-the-main-types-of-attacks-on-web-applications/

Srivanas, 2022. *Process: gaining and elevating access* - Infosec Resources. [ONLINE]
Available at: https://resources.infosecinstitute.com/topic/process-gaining-and-elevating-access/.
[Accessed 22 June 2022].

Tam, T., Rao, A. & Hall, J., 2020. The Invisible COVID-19 Small Business Risks: Dealing with the Cyber-Security Aftermath. *Digital Government: Research and Practice,* 29 December, 02(02), pp. 2-3.

TechRepublic. [Online] Available at: https://www.techrepublic.com/article/how-phishing-attacks-are-targeting-schools-and-colleges/.
[Accessed 19 May 2022].

TekhiToday, 2021. *Can Artificial Intelligence and Machine Learning be used for Penetration Testing?.* [Online]
Available at: https://www.tekhitoday.com/can-artificial-intelligence-and-machine-learning-be-used-for-penetration-testing/
[Accessed 02 June 2022].

"Thingbots: The Future of Botnets in the Internet of Things". Security Intelligence. 20 February 2019. Retrieved 17 June 2022. Available at: https://www.bing.com/ck/a?!&&p=1926cb625d84752c4c90bb41a38877589b2beaa6f8587eaca2e982dfdda53b5bJmltdHM9MTY1NTQ3NzQxNSZpZ3VpZD1kZTYyYjU1Yy1iMjliLTQyMzgtOTg3Mi00MTYxNjk1OTBiZjUmaW5zaWQ9NTEzNA&ptn=3&fclid=cc38b2bbee
[Accessed 17 June 2022].

Tsukerman, E., 2020. *How artificial intelligence is changing social engineering.* [Online]
Available at: https://resources.infosecinstitute.com/topic/how-artificial-intelligence-is-changing-social-engineering/
[Accessed 14 June 2022].

Turner, B., 2018. *Social Engineering attacks on rise in higher education..* [Online]
Available at: https://it.wisc.edu/cybersecurity/social-engineering-attacks-on-the-rise-in-higher-education/

tutorialspoint, n.d. *Penetration Testing Tutorial: What is PenTest?.* [Online]
Available at: https://www.tutorialspoint.com/penetration-testing-tutorial-what-is-pentest
[Accessed 30 May 2022].

Types of Wireless Network Attacks. [ONLINE] Available at:
https://www.logsign.com/blog/types-of-wireless-network-attacks/.
[Accessed 03 June 2022].

Ugoani, J. N. (January 2019). 232 © 2019 Conscientia Beam. All Rights Reserved. ACTIVITY COST MANAGEMENT AND ITS EFFECT ON ENTERPRISE PRODUCTIVITY . *International Journal of Business, Economics and Management*, 16. Available at:
https://www.researchgate.net/publication/335423533_Activity_Cost_Management_and_its_Effect_on_Enterprise_Productivity

Velusamy, R. (September 2018). An Overview: Watering Hole Attack. *International Journal for Scientific Research & Development*, 3. Available at:
https://www.researchgate.net/publication/327498192_An_Overview_Watering_Hole_Attack

Venkatasha, S., Reddy, K. & Chandavarkar, B., 2021. Social Engineering Attacks During During the COVID-19 Pandemic. *SN Computer Science,* 2(78), pp. 3-4.

Verizon, 2019. *Data Breach Digest 2018: Studies in cyber crime.* [Online]
Available at: https://www.verizon.com/business/resources/reports/data-breach-digest/
[Accessed 15 May 2022].

Verizon, 2021. *2021 Data Breach Investigations Report.* [Online]
Available at: https://www.verizon.com/business/resources/reports/dbir/interactive/
[Accessed 04 April 2022].

Verizon, 2021. *Mobile Security Index 2021,* s.l.: Verizon.

Verizon Business. 2022. *2022 Data Breach Investigations Report* | Verizon. [ONLINE] Available at: https://www.verizon.com/business/resources/reports/dbir/. [Accessed 26 May 2022].

Wai, T., 2001. *Conducting a Penetration Test on an Organization*. [Online] Available at: https://www.sans.org/white-papers/67/ [Accessed 26 May 2022].

Wang, L. & Kou, H., 2012. A Research of Behavior-Based Penetration Testing Model of the Network. Xi'an, *IEEE*, pp. 1680-1683.

Wembley Partners, 2020. *SSL Certificates and Strong Encryption Matter*. [Online] Available at: https://www.wembleypartners.com/post/why-are-ssl-certificates-and-encryption-standards-often-overlooked [Accessed 17 June 2022].

Wierckx, S., 2021. *7 advantages of penetration testing*. [Online] Available at: https://www.toreon.com/7-advantages-of-penetration-testing/ [Accessed 19 May 2022].

Wireless Networks: Developments, Threats and Countermeasures. [ONLINE] Available at: https://www.researchgate.net/publication/328090396_Wireless_Networks_Developments_Threats_and_Countermeasures. [Accessed at 03 June 2022].

Wireshark, n.d. *About*. [Online] Available at: https://www.wireshark.org/ [Accessed 09 June 2022].

Worth, Robert (25 June 2019). *"Terror on the Internet: The New Arena, The New Challenges"*. New York Times Book Review: 21. Retrieved 7 June 2022.

Yadav, A. M. & Reddy, B. I., 2019. Android Device Attacks and Threats. *International Research Journal of Engineering and Technology (IRJET)*, July, 6(07), pp. 1543-1548.

Yury Geiler, Nadav Avital, 2022. *How Account Takeover Botnets Outsmart Traditional Security Controls* | Imperva. [ONLINE] Available at: https://www.imperva.com/blog/how-account-takeover-botnets-outsmart-traditional-security-controls/.
[Accessed 03 June 2022].

APPENDICES

Appendix 1

Ethical clearance form part 1

PROJECT DETAILS			
Title and sub-title of project Investigating Social Engineering Techniques to Generate a Comprehensive Risk Assessment Report for Eduvos Potchefstroom Campus			
SUPERVISOR		**CO-SUPERVISOR**	
Name and surname Eric Chemhere		Name and surname	
Qualification (e.g. PhD, etc.) Msc x2, PGDp, BSc		Qualification (e.g. PhD, etc.)	
Institution where based Eduvos Potch Campus		Institution where based	

Purpose of Research (Mark with X)							
Non-degree	Diploma	Bachelor's	Honours	Postgraduate certificate or diploma	Master's	Doctorate	Post-doctorate
		x					

Research Method (Mark with X)			
Qualitative	Quantitative	Mixed methods	Other (Please specify)
		x	

Appendix 2

Ethical clearance form part 2

FUNDING OF RESEARCH PROJECT

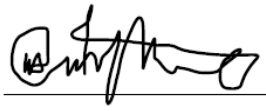
Please provide details of how the research project is being funded, and indicate any expectations that the sponsor may have.

NO SPONSORS

STATUS OF RESEARCH PROJECT

Proposal defended?	Yes X	No	N/A	**Fieldwork started?**	Yes	No	**Pilot study/ fieldwork concluded?**	Yes	No

APPLICANT

Date: 04/05/2022 Signature: 

HEAD OF PROGRAMME

Approval of Research Ethics Committee

[X] Yes, Clearance Number: ITNPA3G1

[ ] No

Appendix 3

Ethical clearance form part 3

Reasons:
Research objectives deemed neccesary for research to be undertaken thereby research has been approved

Date: 04/05/2022 Signature: N.Makuvaza