National College of Ireland

Ethical Hacking vs Smart Technology

Cybersecurity

2021/2022

Gareth Fitzgibbon

x18382503

x18382503@student.ncirl.ie

Ethical Hacking vs Smart Technology

Technical Report

Contents

Executive Summary

The purpose of this report is to provide detailed information about the project being undertaken this includes:

- Information regarding the project requirements that are necessary to complete the project successfully.
- The steps required to fulfil the requirements, use case diagrams to aid the users understanding of the project functionality.
- Examples of the software/tools that are used throughout the project.
- The project design plan and its implementation process.
- The projects user interface (UI).
- The plans for project testing and evaluation.
- The conclusion that can be made based on the evaluation results and overall project functionality.
- The project proposal and the reflective journals that have been completed at this stage of the project.

The major points covered in this report are the project requirements and the project functionality which includes the design and implementation sections of this report. The requirements section highlights the 6 high priority functional requirements that are necessary to the completion of this project and details the steps necessary for the user to meet those requirements. The Design section covers the basis of the project and details the structure of the design for the user. The implementation section covers how the design will be implemented and how this will affect the project and its functionality for the user and gives an example of how the user can perform the implementation process and perform functions when the project software is running. In summation, this report will cover all the

information required to understand why the project was created, who the project was created for, how the project can be used and how the project was designed and tested.

Glossary

Here I will be covering the meanings of some key terms that will be seen throughout this report:

- Kali Linux – a Linux distribution system derived from Debian that was designed for penetration testing and digital forensics.
- OS – Operating System
- SSH – Secure Shell: is a network protocol that allows users to securely access a device over a network that may not be secure.
- DoS Attack – Denial of Service Attack: an attack intended to disrupt or disconnect users from a network or machine by shutting it down.
- Raspberry Pi – is a cheap but powerful minicomputer roughly the size of a bank card that connects to a screen/monitor and uses a mouse and keyboard
- Bash Script - a plain text file that contains a series of commands normally typed by the user into the command line terminal.
- Terminal – known as the command line, allows for tasks on a computer to be automated without the use of a graphical user interface.
- GitHub – a platform used for hosting code and version control and teamwork/collaboration from anywhere in the world.

1.0 Introduction

1.1. Background

The purpose of this project is to test the security features of different smart devices and to show how the implementation of certain security features can prevent hackers from gaining access to a user's device. The use of smart technology in the household has been on the increase over the past few years, especially since the COVID-19 Global Pandemic. During the ongoing pandemic there has been a rise in the number of people working from home and this combined with the decline in individuals travelling has led to an increase in smart technology usage in the everyday home. The relevance of this information, is that with the increase in usage, has also seen a rapid increase in smart technologies in the home there has also been a rapid increase in the number of cyber-attacks. Reports of hacking have spiked worldwide. Once a hacker has penetrated an individual's smart device there are many different actions, they can perform that will negatively impact the victim and their security. With an increase in the number of individuals being attacked by cyber criminals, it is important to investigate how potentially vulnerable their devices are and how to patch these vulnerabilities to prevent them from being exploited.

1.2. Aims

The aim of this project is to conduct research into the various ways a hacker can perform reconnaissance on a network, and then use this information to gain unauthorized access to the network and its devices through a series of hacking methods. In order to make this project interactive for users the ultimate aim was to make this process automated so users can perform various reconnaissance techniques and attacks by simply choosing them from a menu. While successfully performing these hacks and creating a program to let users easily replicate them to test their own network and device security was the main aim, it was also important to discover how certain reconnaissance and hacking techniques can be prevented and to explain to users how to implement security features to better protect themselves and their devices. Therefore, making the project interactive was important as once users can perform these hacks on themselves and see how easy it is to exploit certain devices, they will have a stronger inclination to follow the security steps recommended to protect their information.

1.3. Technology

This Project was created using a Raspberry Pi Module 4 computer running the Kali Linux Operating System. Kali Linux is often referred to as an ethical hackers “Swiss Army Knife” and is one of the most popular Linux operating systems used in penetration testing. The latest version of Kali Linux (2021.4a) was downloaded and then flashed onto a micro-SD card using BalenaEtcher. A raspberry Pi is a crucial piece of technology for this project as it has a built-in wireless adapter and Bluetooth adapter meaning a Bluetooth USB adapter is not required. However, if a user wished to replicate this project or run the scripts without a Raspberry Pi, they could use VirtualBox and run the Kali Linux Operating System and configure a Bluetooth and Wireless Adapter connected to their machine. For this project, the Raspberry Pi will be used to run the Kali Linux Operating System and the command terminal will be used to download and access the bash script ‘scanndstrike’ which allows the user to perform network reconnaissance, Denial of Service (DoS) Attacks and Ethical Hacks with very little input or actions required and detailed instructions and information shared with the user about the process they choose to run. This process available through the bash script can be used by the user to identify the security vulnerabilities in a smart device or network and then exploit the vulnerabilities that are found to gain access to the device or network without permission or authorization from the owner. For this project, the Secure Shell (or SSH) protocol can also be used, Secure shell (SSH) protocol allows two different computers to communicate and share data. PuTTY is an application that was designed for this reason and is the application that can be used to establish the Secure Shell (SSH) connection between the Raspberry Pi computer and another computer.

1.4. Structure

Within this document we will cover six sections, these sections are the requirements, the User Interface (UI), the project design and implementation process, the testing process and lastly the project evaluation section. The evaluation section and the testing section will be used to show how the user performed testing of the project functionality and the results that were generated based on the testing process. The design process will allow the user to view the structure of the project and the implementation process will explain how this makes the project and its functionality available to the user. The user interface (UI) section will cover the user's interaction with the application throughout the project. Lastly, one of the first sections that will be covered in this report is the requirements section and this section displays a list of project goals that need to be completed in order for the project to be completed successfully with full functionality and will breakdown the processes involved in each of these requirements listed.

2.0 System

2.1. Requirements

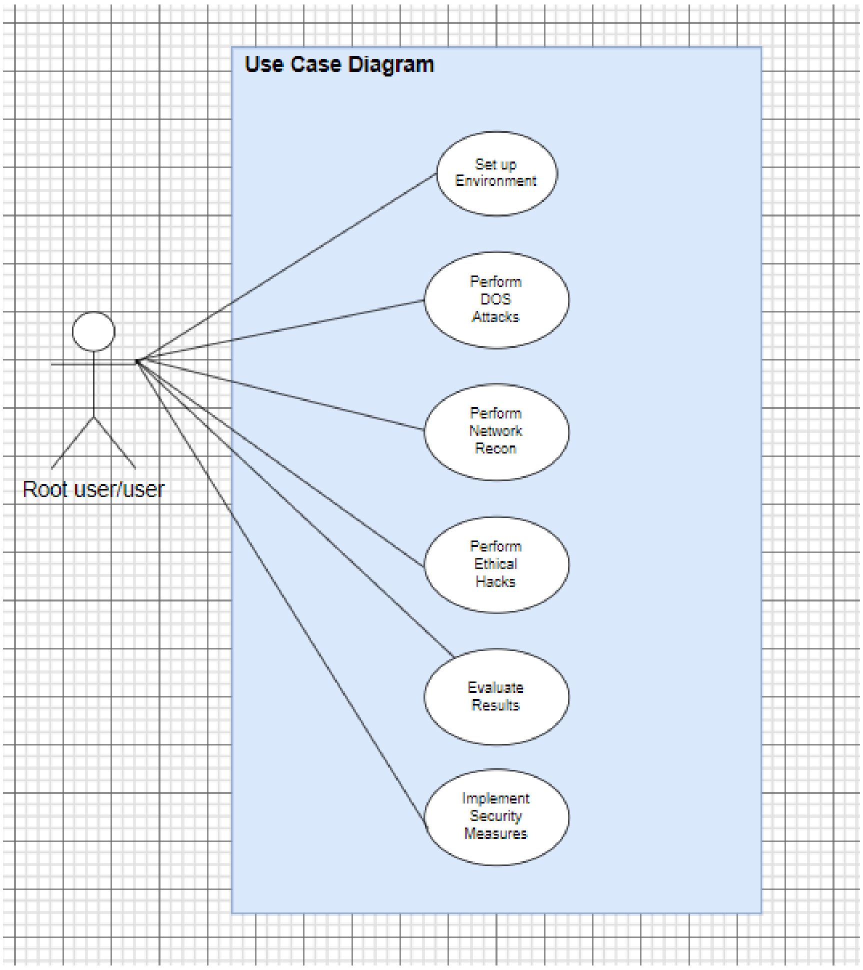
2.1.1. Functional Requirements

While this project was not originally created to be used by multiple users like an app or a website it has evolved and now involves the use of a bashscript which has been created for an interactive user experience which allows users to perform hacking techniques without needing a vast knowledge of hacking or penetration testing. In order to access this bash script and get the most effective use from it there are requirements that need to be met, these are:

- The Raspberry Pi will be capable of running Kali Linux
- The Raspberry Pi Kali Linux command line terminal will be accessible through Secure shell (SSH) connection
- Bash Scripts can be downloaded through command line terminal
- Bash Scripts can be given permissions on the device so they can be run without issue
- Main Bash Script can be run
- All modules can be run on Kali Linux such as the SSH Exploit that uses the Hydra and Nmap tools to gain unauthorized access to a device by breaking the Secure Shell (SSH) password or Wordlist creation using the crunch tool to create custom wordlists used with the ethical hacking modules.
- Menus within the script can be exited to return to the main menu

- Menus within the script can be opened and their content displayed
- Information gathered using reconnaissance, Denial of Service (DOS) and ethical hacking modules are be stored on the system
- Using the Raspberry Pi running Kali Linux OS a smart device or network is successfully penetrated
- Security Features are implemented to protect the previously vulnerable device or network
- Executing penetration tests on devices with additional security should result in failure
- The result of all processes running in the scripts are visible to the user

2.1.1.1. Use Case Diagram



2.1.1.2. Requirement 1 < Set up Environment>

2.1.1.3. Description & Priority

This section is of the upmost importance as the environment setup is essential for this project. Without the correct environment this project cannot be undertaken and if the environment is not set up correctly the application cannot run, and the scripts created will not be accessible. The environment setup for this project involves a Monitor/Screen, a Raspberry Pi Module 4 computer, the latest version of Kali Linux (Kali 2021.4 - 9th December 2021 - The fourth 2021 Kali Rolling release. Kernel 5.14. 0, Xfce 4.16.) and the files from https://github.com/Gareth-hub/EthichalHackingProject.git to fully set up the environment and allow the project to be run correctly.

2.1.1.4. Use Case <Set up Environment>

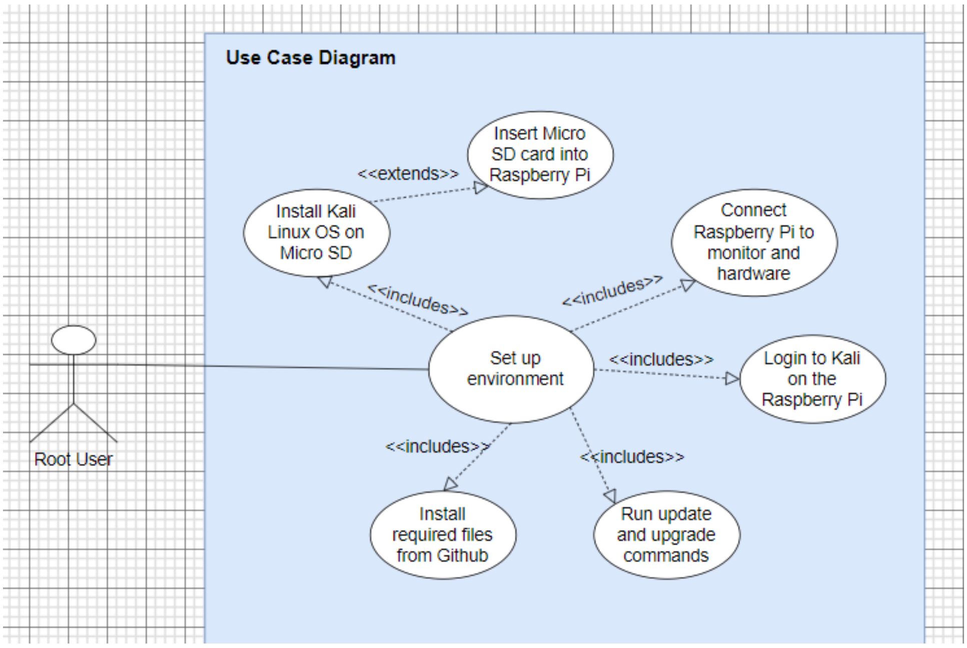
Scope

The scope of this use case is to show how the project environment is setup.

Description

This use case describes the process involved in setting up the project environment as the root user (admin).

Use Case Diagram


Use Case Diagram
Insert Micro SD card into Raspberry Pi
<<extends>>
Install Kali Linux OS on Micro SD
Connect Raspberry Pi to monitor and hardware
<<includes>>
<<includes>>
Set up environment
<<includes>>
Login to Kali on the Raspberry Pi
Root User
<<includes>>
<<includes>>
Install required files from Github
Run update and upgrade commands

Flow Description

Precondition

The user has the components required to set up the Environment, these components include Raspberry Pi 4 Computer, a MicroSD card with Kali Linux OS installed, a screen/monitor, all cables required for power and connectivity and internet connection to download the software.

Activation

This use case starts when the user obtains the components listed above and begins to create the project environment.

Main flow

1. The user obtains the required components (mouse, keyboard)
2. The user installs Kali Linux OS software onto a MicroSD card
3. The user inserts the MicroSD card into the Raspberry Pi and turns it on
4. Once the Raspberry Pi is running the Operating system the user is shown the login screen
5. The user enters the default login details
6. The user runs the Kali Terminal and runs the commands to update and upgrade the operating system
7. The user downloads the required software and grants permissions

Alternate flow

A1: <The users Raspberry Pi fails to run the OS software>

1. The Raspberry Pi shows an error light when attempting to run the Kali Linux OS
2. The Raspberry Pi cannot read the micro-SD card and its data
3. The user must reformat the SD card (wiping it clean) and reinstall the Kali Linux OS software
4. The use case continues from position 3 of the main flow

A2: <The user fails to install the required software>

1. The user does not download the required software for the software
2. The user must enter and run the commands to install the software
3. The use case continues from position 7 of the main flow

Exceptional flow

E1: <User fails to set up the Environment >

1. The user does not gather the correct components and cannot set up the environment

Termination

If the user successfully sets up the environment, updates/upgrades the application and downloads the software required then the set-up process is complete and the process terminates

Post condition

Success Conditions:

1) User obtains the correct components
2) User installs Kali Linux OS software on MicroSD

3) Raspberry Pi Computer successfully reads data on the MicroSD and runs Kali Linux
4) User can login to the application
5) User can update and upgrade the application software in the Kali terminal
6) User can download the required software and grant it permissions

Failure Conditions:

1) User obtains the incorrect components
2) Raspberry Pi cannot read the MicroSD card
3) Data on the MicroSD card not installed correctly
4) User denied permission to update or upgrade the application software
5) User denied permission to install the required software

2.1.1.5. Requirement 2 < Perform Network Reconnaissance >

2.1.1.6. Description & Priority

Once a user has set up their environment and can successfully run Kali Linux on their Raspberry Pi with the correct software installed, they can then run the scanndstrike bash script and choose the reconnaissance option. The Network reconnaissance menu shown to the user allows them to choose from six reconnaissance options Show IP, Quick Scan, Detailed Scan, DNS reconnaissance, IP Sweep and Ping Sweep. These modules available on the menu will allow a user to scan their target network using various reconnaissance techniques and all they will need is the Ip Address of their target which will be provided by the Show IP option which requires no user input. The ability to run network reconnaissance is highly important as not only can it provide detailed information about a target, but it can also help the user identify which of the ethical hacking modules will be most effective on their network and devices.

2.1.1.7. Use Case <Perform Network Reconnaissance>

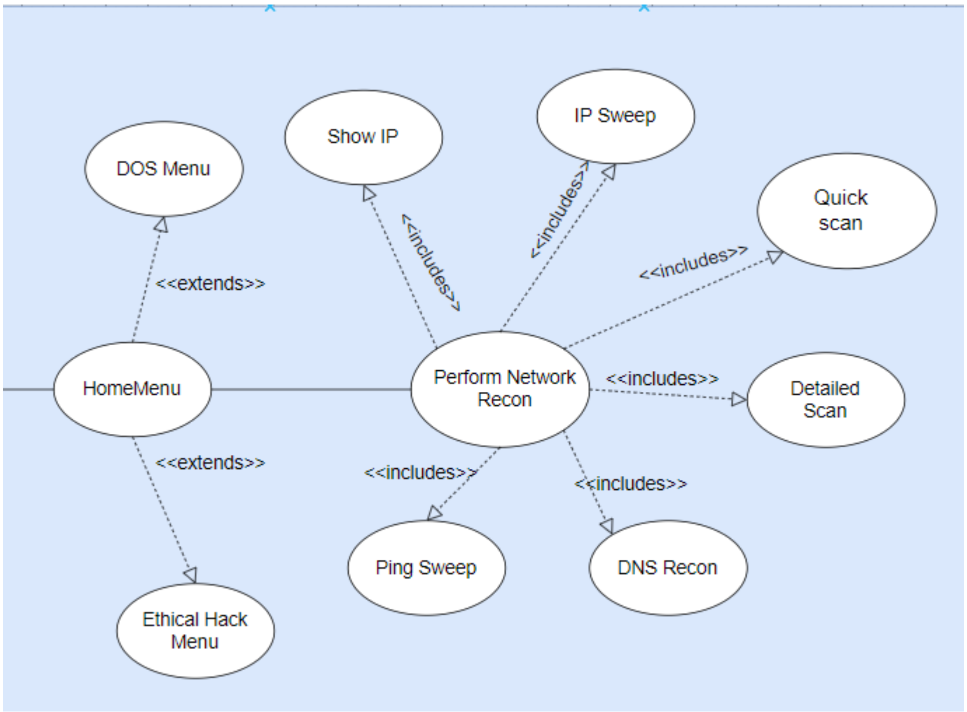
Scope

The scope of this use case is to show how the user can use the scripts automated modules to perform scans on a network to reveal useful information about it and the devices connected to it as well as reveal any vulnerabilities that could potentially be exploited.

Description

This use case describes the process involved in using the scanndstrike scripts modules and how they can be used by the user to perform reconnaissance on a target network or device and identify information about the target including any vulnerabilities that a hacker could exploit.

Use Case Diagram



Flow Description

Precondition

The user is logged into their Kali Linux system that has the required bash script (scandstrike) installed and has a terminal window open.

Activation

This use case starts when the user opens a terminal window in Kali Linux and wishes to run the scanndstrike script and uses its modules to perform reconnaissance on a target device or network in order to obtain additional information about the target including any potential vulnerabilities.

Main flow

1) The user finds the Kali Terminal icon on the home screen
2) The user opens the Kali Terminal window.
3) The user enters the command './scanndstrike' and presses enter to run the scanndstrike bash script and is taken to the script's main menu
4) The user selects the module they wish to run from the menu
5) The user waits for the script to prompt them for input or to display results
6) The information obtained in the reconnaissance is displayed to the user

7) The information gathered in the reconnaissance performed by the user is stored for later use.
8) The user can choose to run another reconnaissance module or return to the home menu.

Alternate flow

A1: <Bashscript fails to run on the user's device>

1) The user must ensure the required software has been downloaded
2) The user must check that the bashscript has permissions by running the command ‘sudo chmod +x ./scanndstrike’
3) The use case continues from position 3 of the main flow

A2: <Failed to scan the network or device>
1) The user is unable find a network or device with the chosen scanning tool
2) The user must ensure that the network or device they have selected is correct and within range
3) The user runs the show ip module to confirm their ip address
4) The use case continues from position 4 of the main flow

Exceptional Flow:
E1: <The user cannot perform network reconnaissance>
1) The user is not in range of any networks or connected to a network

E2: <The user cannot access the bash script>
1) The user is not able to grant permissions to the bash script.

E3: <The user cannot install the tools required for the script to run correctly>
1) The user does not have permission to update or install the software required for the script to run successfully .

Termination

1) The user is successfully able to perform reconnaissance the network or device of their choosing and see its potential vulnerabilities that may leave it open to exploitation.
2) The user fails to discover any local networks or devices to perform reconnaissance on.
3) The user is successfully able to perform reconnaissance the network or device of their choosing but is unable to find any vulnerabilities that may leave it open to exploitation.
4) The user presses Ctrl and c together to stop the module and exit the script

Post condition

Success Conditions:

1) User can run the bashscript
2) User can access the network reconnaissance menu

3) User can ping their own IP
4) User can perform a quick scan of their target network or device
5) User can perform a detailed scan of their target network or device
6) User can perform an ipsweep on their target network or device
7) User can perform a ping sweep on their target network or device
8) User can perform DNS scan on their target
9) User can run network reconnaissance modules on the network or device of their choosing
10) User will be shown the output from their chosen reconnaissance module
11) The user can then save the information gathered about the network or device they have targeted

Failure Conditions:

1) User cannot run the bash script
2) User cannot access the network reconnaissance menu
3) Module selected by the user does not run
4) Reconnaissance performed does not provide the user with any output
5) No networks or devices within range to perform reconnaissance
6) Network reconnaissance on chosen target does not run, throws error

2.1.1.8. Requirement 3 < Perform Denial of Service Attacks>

2.1.1.9. Description & Priority

This requirement enables the user to perform three types of Denial of Service (DOS) attacks on a network or machine of their choosing making it unreachable or unresponsive to its intended users. Denial of Service (DoS) attacks work by flooding a target with traffic or repetitively sending requests or information that causes the target to crash or become unresponsive. This requirement is of medium priority as while a user should be able to perform these attacks against a target of their choosing a user being able to perform network reconnaissance and ethical hacks are higher priorities. The reason scripts to automate Denial of Service (DoS) Attacks have been created is because Denial of Service (DoS) Attacks are an interesting part of penetration testing that are commonly performed after network reconnaissance and occasionally in preparation for hacking a target.

2.1.1.10. Use Case <Perform Denial of Service Attacks>

Scope

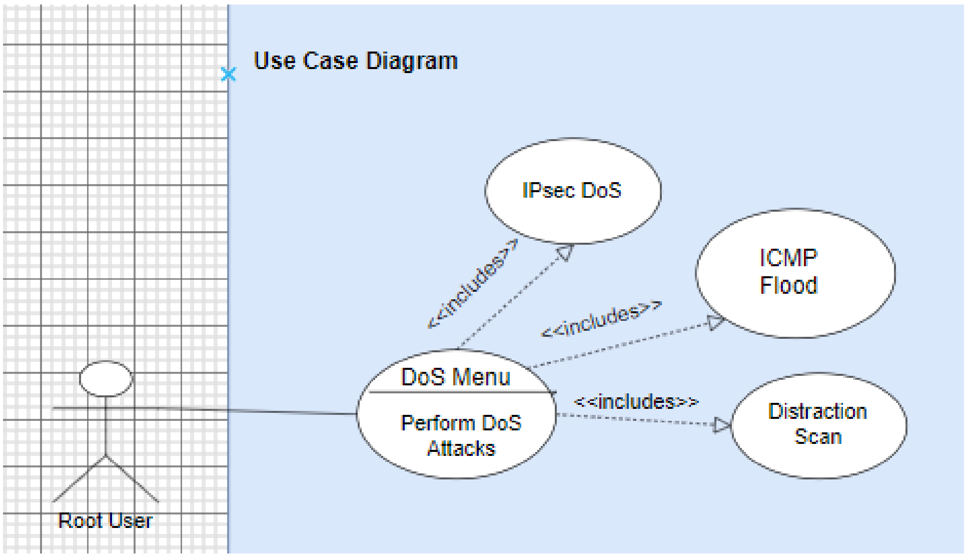
The scope of this use case is to show how the user can use Kali's preinstalled attacking tools to perform various attacks on a network or a device they wish to attack.

The scope of this use case is to show how the user can perform Denial of Service (DoS) Attacks on a target network or machine using the scanndstrike bash script in Kali Linux's terminal.

Description

The use case below describes the process involved in using the scanndstrike bash script the user has installed to perform Denial of Service (DoS) Attacks in the Kali command terminal against a target network or device to cause them to crash or become unreachable for users as long as the attack is running.

Use Case Diagram



Flow Description

Precondition

The user has installed software required and is capable of running the scanndstrike bash script and either knows their ip (target ip) or have run the IP scan modules to learn their network ip address as it crucial for this project that these attacks only be conducted on authorized networks for educational purposes. Once the target ip is known and the user will be able to perform the Denial of Service (DoS) attack of their choice from the DoS Menu.

Activation

The use case starts when the user wishes to run the scanndstrike script and use its automated Denial of Service (DoS) attack modules against a target network or machine to disrupt or crash it and make the users connected to the target unable to communicate with the target for the duration of the attack.

Main flow

1) The user is on the application home screen.
2) The user finds the Kali Terminal icon on the home screen.
3) The user opens the Kali Terminal window.
4) The user runs the scanndstrike bash script
5) The user navigates to the DoS Menu
6) The user enters a number corresponding with the module they wish to run
7) The user enters the details required by the chosen module
8) The user can then monitor the output for details on how the attack is affecting the target

Alternate flow

A1: <Failed perform Denial of Service (DoS) attack>
1) The user is unable run the Denial of Service (DoS) attack on their target
2) The system notifies the user of the reason(s) for failure and suggests potential solutions
3) The user attempts the solution(s) recommended by the system
4) The use case resumes the main flow from position 4

Exceptional flow

E1: < User Missing software >
1) The user does not have the software required by the Denial of Service (DoS) Module to perform the attack
2) The user performs an update of the applications on the system and installs any missing software
3) The use case resumes from position 4 of the main flow

E2: < User attacks their device running Kali Linux and cannot stop the Denial of Service (DoS) attack >
1) The user has attacked the machine running kali Linux and therefore cannot communicate to the terminal to make the module stop
2) The user can hold Ctrl and c to force stop the module and exit the script or reboot the machine
3) The use case resumes from position 3 of the main flow

Termination

1) The user is successfully able to run their chosen attack on the network or machine they are targeting, and once satisfied manually terminates the process.
2) The user fails to perform their chosen attack on their target device or network, and this terminates the process.

Post condition

Success Conditions:

1) The user can successfully perform the attack of their choosing on their target.
2) The user can successfully stop the attack
3) The user can view the output from the attack

Failure Conditions:

1) User cannot run the bash script
2) User cannot access the DoS Menu
3) User cannot run the Denial of Service (DoS) attack modules
4) User is unable to perform an attack on the network or device they have chosen to target
5) User is unable to stop the attack on chosen target

2.1.1.11. Requirement 4 <Perform Ethical Hacks>

2.1.1.12. Description & Priority

This Requirement is high priority as it is an essential part of this Project and is one of the overall goals of this project.

For this requirement, the user should be able to successfully perform any ethical hacks of their choice from the scanndstrike bash scripts Ethical Hack Menu. These ethical hacks performed by the user should result in the successful penetration of the target device or network and the user gaining access to hidden or sensitive information (this can be passwords, personal information, files, device information etc). Since one of the main aims of this project was to investigate the methods involved in ethical hacking and to successfully execute these methods to penetrate smart devices this requirement is an essential part of the project. Since every IoT device can be attacked in numerous ways the scanndstrike script was created to allow the user to attempt multiple types of ethical hacks depending on their target. The user has the ability to target routers, Bluetooth devices, Wi-Fi networks and devices as well as the option to create custom wordlists that can be used with these ethical hacks.

2.1.1.13. Use Case <Perform Ethical Hacks>

Scope

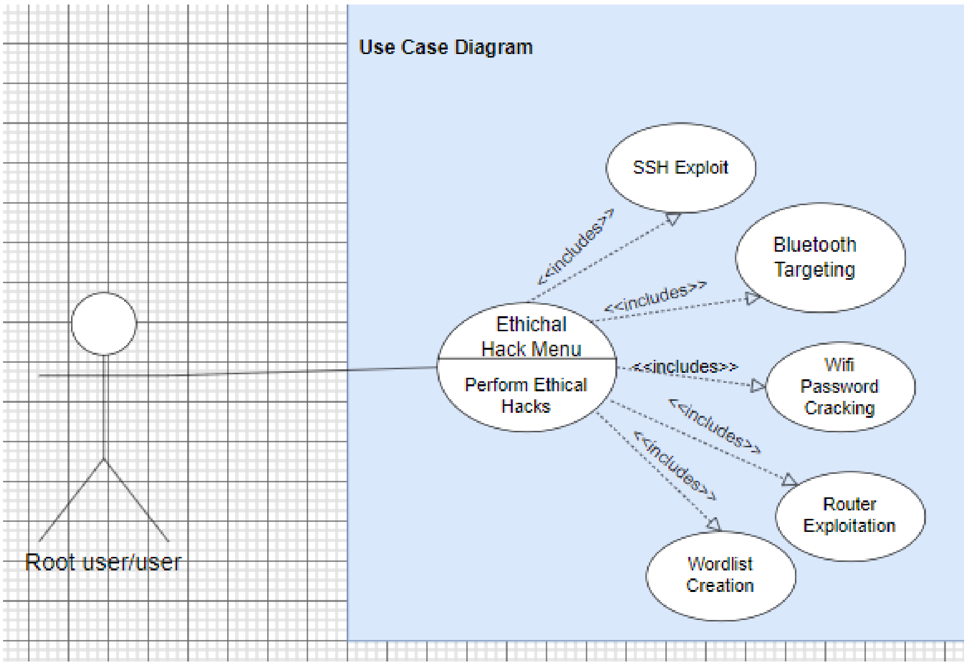
The scope of this use case is to shoe how the user can attempt to ethically hack a target smart device or network using Kali Linux and the scanndstrike script created for these hacks.

Description

This use case describes the process involved in using Kali's pre-installed hacking tools to successfully penetrate a smart device.

This use case describes the process involved in using a Raspberry Pi running Kali Linux OS to perform ethical hacks using the scanndstrike script from the project. While some modules within the bash script could be run through a virtual box supporting Kali Linux the majority of the ethical hacking modules require the use of a Raspberry Pi as it has built in adapters that are required for wireless and Bluetooth attacks.

Use Case Diagram



Flow Description

Precondition

The user is running Kali Linux on a Raspberry Pi or a virtual machine with a Bluetooth adapter configured. The user has set up their environment on Kali Linux and has downloaded the required software and given the scripts permissions so they can run without issues. The user knows the ip address of their target, if the user does not know this, they can use the ip scan tool within the network reconnaissance menu.

Activation

This use case starts when the user chooses to run the scanndstrike script and use its Ethical Hack modules to try and penetrate their network and its connected devices. In order to run a successful penetration test on a network or device the user must know things about their target such as the operating system the target is running, if the target has any open ports, if the target is up and running etc, this information can be simply gathered using the automated reconnaissance modules from the net reconnaissance menu before opening the ethical hack menu. Once the user has decided to run any form of ethical attack the use case is activated.

Main flow

1) The user is on the application home screen.
2) The user finds the Kali Terminal icon on the home screen.
3) The user opens the Kali Terminal window.
4) The user runs the scanndstrike bash script
5) The user navigates to the Ethical Hack Menu
6) The user enters a number corresponding with the module they wish to run
7) The user enters the details required by the chosen module
8) The user can then monitor the output for details on how the ethical attack is performing
9) The user continues to perform their chosen ethical on the target network or device and may implement other forms of ethical hacks until they have successfully breached the targets security and gained access
10) Depending on the ethical hack chosen the user may be able to execute commands and alter permissions, files etc on a target device or network.
11) The user can save the information gathered during the ethical hacking process

Alternate flow

1) A1: <The users ethical hack fails to penetrate the target>
2) The users ethical hack fails to penetrate the target
3) The system notifies the user of the reason(s) for failure and suggests potential solutions
4) The user attempts the solution(s) recommended by the system
5) The use case resumes the main flow from position 5

Exceptional flow

E1: < User fails to penetrate smart device >
1) The user runs the ethical hack modules but cannot gain access
2) Reconnaissance on the target reveals there are no vulnerabilities that can be exploited

3) The user attempts to perform ethical hacks regardless
4) The user fails to penetrate the target

Termination

1) The ethical hacking process terminates when a user has successfully penetrated the target device or network and has exploited its security vulnerabilities.
2) The process terminates when the user is unable to penetrate the target network device or exploit its potential security vulnerabilities.
3) The user pressing Ctrl and c will manually terminate the process but will also exit the script.

Post condition

Success Conditions:

1) User’s target device or network is within hacking range.
2) Users' reconnaissance of the target reveals valuable that can potentially be used when determining the best way to exploit the target
3) The user can successfully perform the ethical hacks of their choosing on their target.
4) The users hacking leads to successful penetration of the target's security
5) The user can then save the information gathered about the target device they have penetrated and any information or important data they may have gotten from penetrating their target.
6) The user can perform multiple ethical hacks on the target.

Failure Conditions:

1) The user is not in range of any networks or devices and does not have a target
2) The user cannot run the bashscript
3) The user enters the wrong commands/information during the ethical hacking process
4) None of the ethical hacks performed by the user are able to penetrate the target
5) The user is unable to store any of the information gathered during a successful hack

2.1.1.14. Requirement 5 < Secure Smart Devices>

2.1.1.15. Description & Priority

This requirement is of high priority as while this project is strongly focused on the ethical hacking process it also focuses on the methods that can be used to prevent certain vulnerabilities and decrease the likelihood of a user's devices or network being accessed by unauthorized parties. For this requirement, the user should be able to successfully implement security features on the previously penetrated smart device in order to successfully prevent it from being vulnerable to the same exploitation and protect it from further penetration and attacks from hackers and unauthorized users. Since this project is focused on Ethical hacking and smart (IOT) devices, the ability to prevent an attacker from gaining access or control over an IOT or smart device is an essential part of this project.

2.1.1.16. Use Case <Secure Smart Devices>

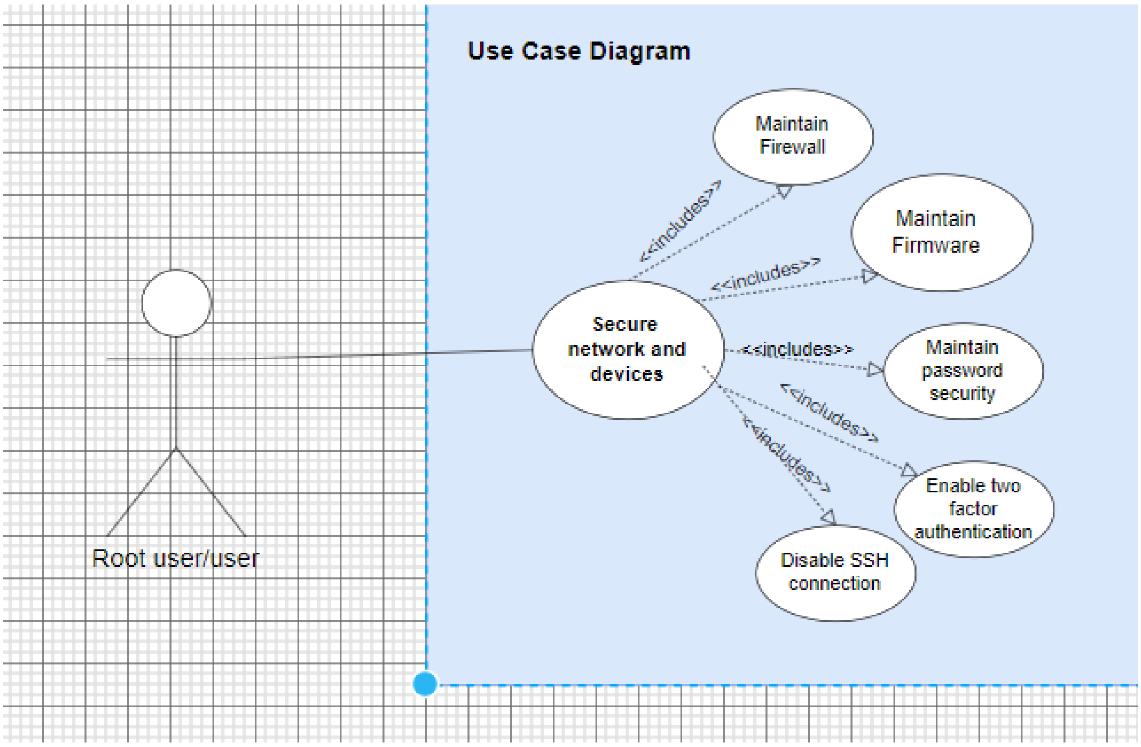
Scope

The scope of this use case is to show how the user can implement security measures and ensure potential vulnerabilities are fixed before a hacker has a chance to exploit them and gain access or control to their smart devices and confidential information. By implementing these security measures ethical hacks from the scanndstrike script that have been successful previously should now fail due to the previous vulnerabilities now being secured.

Description

This use case describes the process involved in implementing security features that can withstand a hacker using Kali Linux and the scanndstrike scripts modules and to successfully prevent the penetration of a target device or network.

Use Case Diagram



Flow Description

Precondition

The user owns a smart device and has permissions to access the devices network router and device settings.

The user owns a network, router or smart device and has permission to access the settings and execute administrative changes.

Activation

This use case starts when the user decides that their network and devices need additional or increased security against hackers and the types of attacks they commonly use against vulnerable networks and devices or if the user has previously been the victim of a cyber-attack which has led to their devices being exploited or their sensitive information exposed to unauthorized parties due to security vulnerabilities.

Main flow

1) The user decides to secure their smart device(s) in order to prevent it from being penetrated by a hacker's attacks
2) The user begins the securing process of their smart device
3) The user ensures all of their devices' firmware are up to date
4) The user replaces the current device passwords with strong, unique, and complex passwords

5) The user then disables remote access which will ensure that devices outside of the user's home network cannot connect to their smart devices remotely.
6) The user should then enable two factor authentication (2FA) on all apps and services possible to reduce the risk of unauthorized users gaining access, even if they have cracked the password or access key.
7) The user can maintain their firewall, this can involve using third party firewalls, updating their firewall etc.
8) By completing these steps, the user's network and devices will be more secure against ethical hacks and cyber attacks

Alternate flow

A1: <User's implements some of the security features>
1) The users choose to implement some of the security features
2) The user's smart device will have increased protection against penetration attacks
3) The user is less likely to have their device penetrated by a hacker's performed attacks
4) The user's smart device is not fully secure and not 'hack proof'

Exceptional Flow
E1: <No security measures are taken by the user>
1) The user chooses not to or does not have permission to add additional security to their network or devices.

Termination

1) The securing process terminates when the user implements all of the security measures or a select few they chose to implement on their network and devices.
2) The securing process terminates as the user does not add any security measures.

Post condition

Success Conditions:

1) The user can successfully implement the security features of their choosing on their smart device(s) or network.
2) The user's device displays increased security and previously discovered vulnerabilities have now been caught and are no longer exploitable.
3) The user's implementation of these security features leads to the successful prevention of penetration of the smart device or network.

Failure Conditions:

1) The user cannot implement the security features
2) The user security features implemented by the user do not stop the smart device from being penetrated
3) The security features implemented by the user lead to further vulnerabilities that can be exploited
4) The user removes previously implemented security features

2.1.1.17. Requirement 6 < Evaluate Results>

2.1.1.18. Description & Priority

While it may seem like this requirement is less of a priority than the other requirements it is also highly important as it allows the users to view the results of their work throughout all of the processes involved in this project. This requirement is quite essential to the overall system as without this requirement the user would not know whether certain requirements are functioning correctly or whether certain commands or scripts being run by the user are not functioning how they were supposed to. This requirement is particularly important when regarding requirements 2 (Perform Network Reconnaissance), 3(Perform Denial of Service (DoS) Attacks), 4(Perform Ethical Hacks) and 5(Secure Smart Devices). This requirement allows users to view the results of the modules they run and not only see how they run successfully but also what can be possibly causing unexpected or unwanted results. This requirement is also important for comparing the results of the network reconnaissance, Denial of Service (DoS) attacks and ethical hacks before and after security features have been implemented, if implemented correctly the user should notice differences in the results. Therefore, although not of the highest priority this requirement is still high in priority and is an essential requirement for this project.

2.1.1.19. Use Case <Evaluate Results>

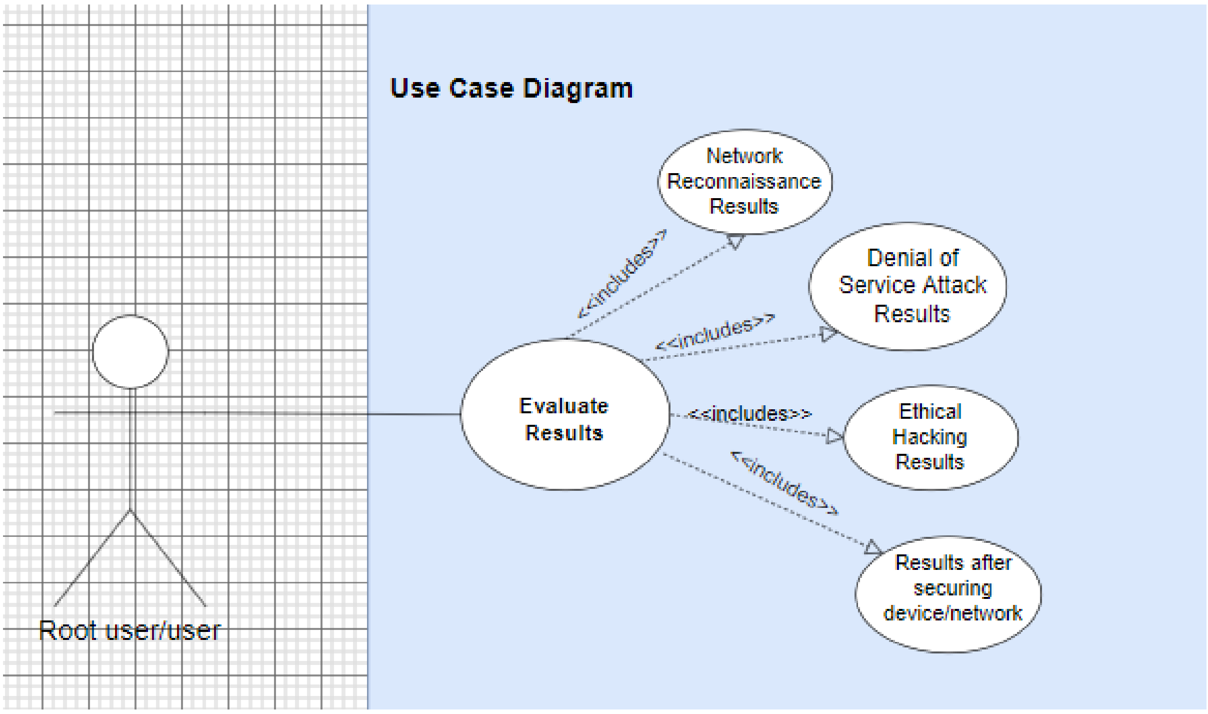
Scope

The scope of this use case is to show how the user can evaluate the results of the different functions of the project

Description

This use case describes how the user can evaluate the results given from the various processes.

Use Case Diagram



Flow Description

Precondition

The user has previously performed an action that is considered part of the requirement functionality as without an action performed there is nothing to evaluate.

Activation

This use case starts when the user decides they need evaluated the results of the processes that have been conducted up to that point and to examine the information that is accompanying these results. E.g., after the user has chosen to run a Quick Scan of a network from the Network Recon Menu, they can evaluate the results and can then determine whether more information is required or if they would like to proceed with running the Denial of Service or Ethical Hacking modules. The user may evaluate the results at any stage throughout the project once there is a result to evaluate, if no actions have been taken by the user, then there are no outcomes for the user to evaluate.

Main flow

1) The user chooses to evaluate the results of the processes that have been currently run on the application
2) The user is shown the success or failure of these processes
3) If applicable the user is also shown any information gathered during these process

4) The user can review these results and evaluate which process need to be improved and which of the processes perhaps might not work best for the project based on the requirements
5) The user can identify the processes that failed or did not return the required information and can analyse the data to potentially discover a solution or alternative way to perform these processes that may yield additional or improved results
6) The user can successfully evaluate the results associated with all processes and requirements.

Alternate flow

A1: <User attempts to evaluate a process that has not been performed>
1) The users choose to evaluate a requirement process that has not yet been attempted by the user
2) The user is shown an error message by the system as the results do not exist
3) The user is required to choose another requirement process to evaluate
4) The use case is resumed from point 1

Termination

1) The evaluation process terminates when the user finishes evaluating the results associated with the chosen requirement or requirement process or the user fails to select a valid process to evaluate or if the user chooses to evaluate a process that has not yet been performed by the user and therefore has no results to evaluate

Post condition

Success Conditions:

1) The user can successfully evaluate the processes and requirements of their choosing
2) When evaluating a process or requirement the user is shown the correct information regarding the outcome of the process and any information that was gathered during this process
3) If a previously run process is run again by the user, the evaluated results will reflect the outcome of the most recent version of the process and the data gathered by that most recent process.
4) The user can save the information reflected by the evaluation process in order to compare it to future evaluations of a requirement or its processes.

Failure Conditions:

1) The user cannot evaluate a process that has previously been completed
2) The evaluation result shown to the user is incorrect or lacking information

3) The user is shown an evaluation result for the wrong process
4) The user is shown an evaluation result for a process that has not yet been attempted by the user

2.1.2. Data Requirements

- The Raspberry Pi must be capable of reading the Kali Linux data from the microSD card in order to run the application.
- The Kali Linux Operating System will be capable of downloading and storing the bash scripts
- The Kali Linux Operating system will be capable of storing the information captured during network reconnaissance, Denial of Service (DoS) attacks or ethical hacks performed on target device or network.
- The Kali Linux Operating system will be capable of gathering data using the tools called upon by the bashscript
- The Kali Linux Operating system will be capable of displaying captured data to the user
- The Kali Linux Operating system will be capable of accepting and storing data input from the user
- The Kali Linux Operating system will output data gathered by the bashscript to users for the module they have chosen to run

2.1.3. User Requirements

- The user should have the ability to log into the application.
- The user should have the ability to use Kali's pre-installed tools.
- The user should have root control in the Kali Terminal.
- The user should be able to download the required software
- The user should be able to run the downloaded software
- The user should be able to execute all functions in the bash scripts
- The user should be able to exit the bash scripts
- The user should be able to perform scans for local networks or devices.
- The user should have the ability to perform network reconnaissance on their target device or network.
- The user should have the ability to perform Denial of Service (DoS) attacks on a device or network they are targeting.
- The user should have the ability to ethically hack their target network or device
- The user should have the ability to secure their network or device
- The user should have the ability to capture information about a target device and store it on the system for future use and evaluation.
- The user should be able to evaluate information stored on the system

2.1.4. Environmental Requirements

In order to recreate this environment, there are certain requirements that must be met by the user, for instance the user must have the components (mouse, keyboard, monitor/screen, connection cables) required to run the Raspberry Pi computer which includes a MicroSD card that can be formatted for the installation of the Kali Linux operating system this is because the user must have a Raspberry Pi computer capable of running Kali Linux OS (Operating System) software in order to perform the user requirements for this project. However, if someone wished to recreate this project without a Raspberry Pi, they could do so using VirtualBox, the latest version of Kali Linux software and a Bluetooth and Wireless adapter that can be connected and configured to their machine

Below are four images, the first two are of the Raspberry Pi 4 and micro-SD card with the Kali Linux Operating system on it. The second two images are of the environment set up and show all the components necessary for this project.

Image 1 – Raspberry Pi MicroSD slot and MicroSD with Kali Linux software installed

Image 2 – Raspberry Pi Module 4 Computer with MicroSD card inserted

Image 3 – Raspberry Pi with components connected

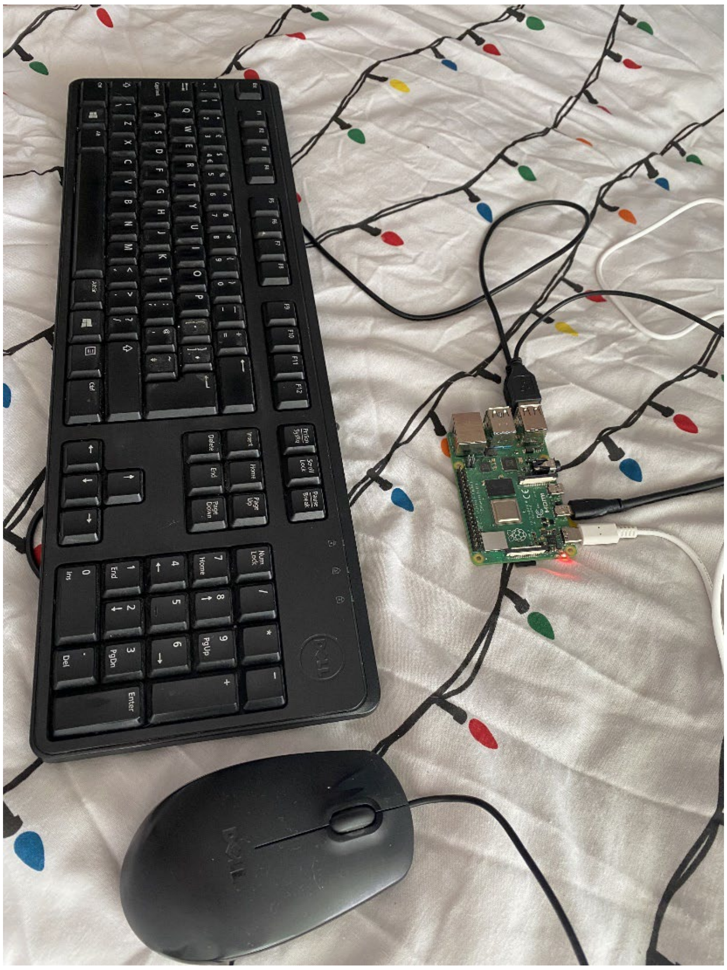


Image 4 – Raspberry Pi set up with all components running Kali Linux

2.1.5. Usability Requirements

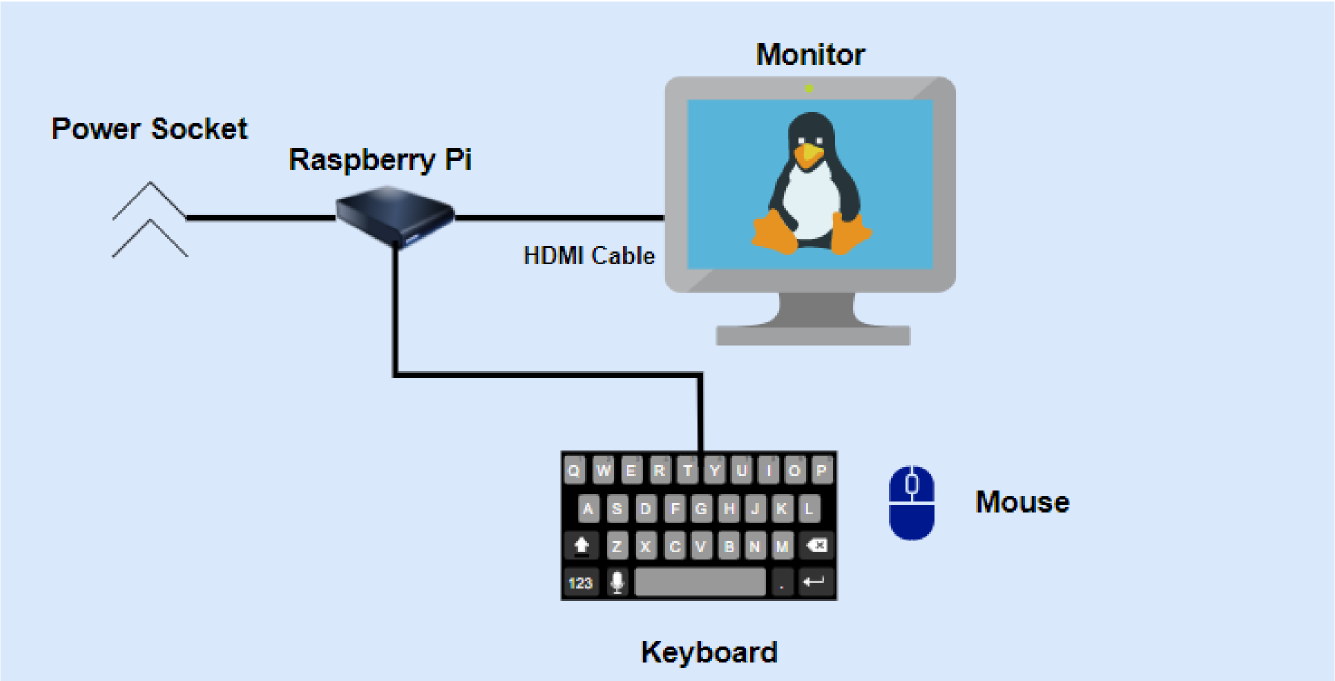
- The user needs to be able to login to Kali Linux
- The user needs to be able to install the software from GitHub and grant permissions
- The user needs to be able to run the bash script
- The bash script needs to display the menu and choices to the user
- The user needs to be able to interact with the scanndstrike script menus and modules
- The scanndstrike bash scripts needs to accept and use input from the user
- The scanndstrike script needs to exit when the user closes it
- The user needs to be able to exit the scanndstrike script
- The information gathered needs to be available to the user
- The user needs to follow the instructions laid out by the scripts
- The Kali Linux Operating system needs to have the required tools installed
- The user needs to be able to install tools needed for the scripts to run correctly

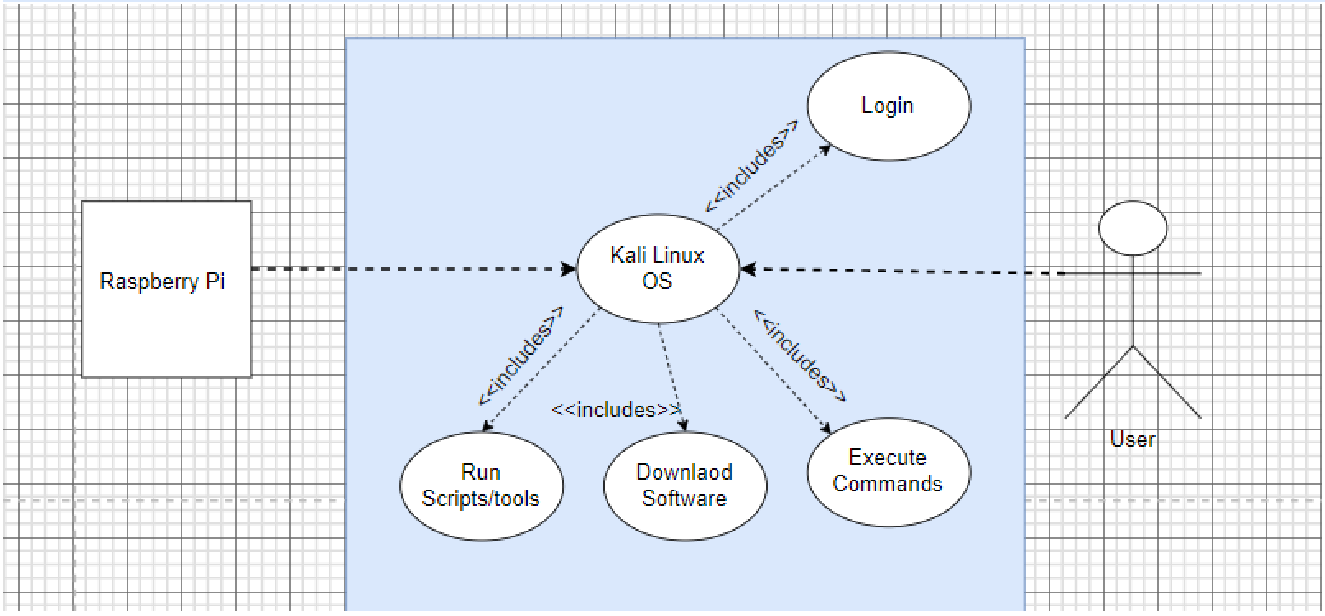
2.2. Design & Architecture

This project consists of four main components: The Raspberry Pi Module 4 computer, the Kali Linux operating system, the scanndstrike bashscript and a target.

The Raspberry Pi is used to run the Kali Linux operating system. The Kali Linux operating system is installed on a MicroSD and is inserted into the Raspberry Pi. The Raspberry Pi reads the data from the MicroSD and runs the operating system. The Kali Linux operating system comes with numerous preinstalled tools that will be called upon by the bashscript such as nmap, hydra and aircrack-ng.

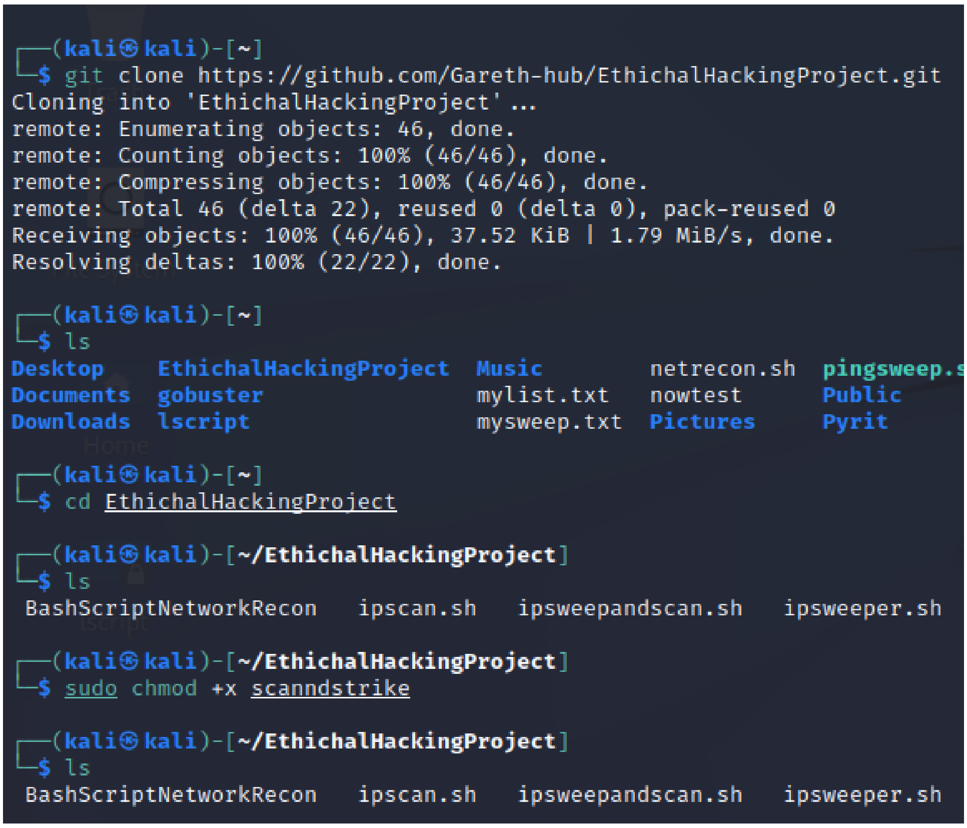
The bashscript is available to be downloaded from GitHub using the ‘wget’ command and will require permissions to be granted before it can run properly. Once installed and the permissions have been set the bashscript scanndstrike can be run, this will provide the user the option to perform 6 reconnaissance functions, 3 Denial of Service (DoS) attack functions and 5 Ethical hacking techniques. However, in order for these functions to be used a target is required. All functions will be directed towards this target network or device as since this project is conducted ethically the target should be a device or network belonging to the user. After the target has been successfully penetrated by the user through the use of the bashscript modules, security features will be implemented to protect the target which should prevent further successful penetration attempts. Below there are two images designed to display the architecture and design of the Project.





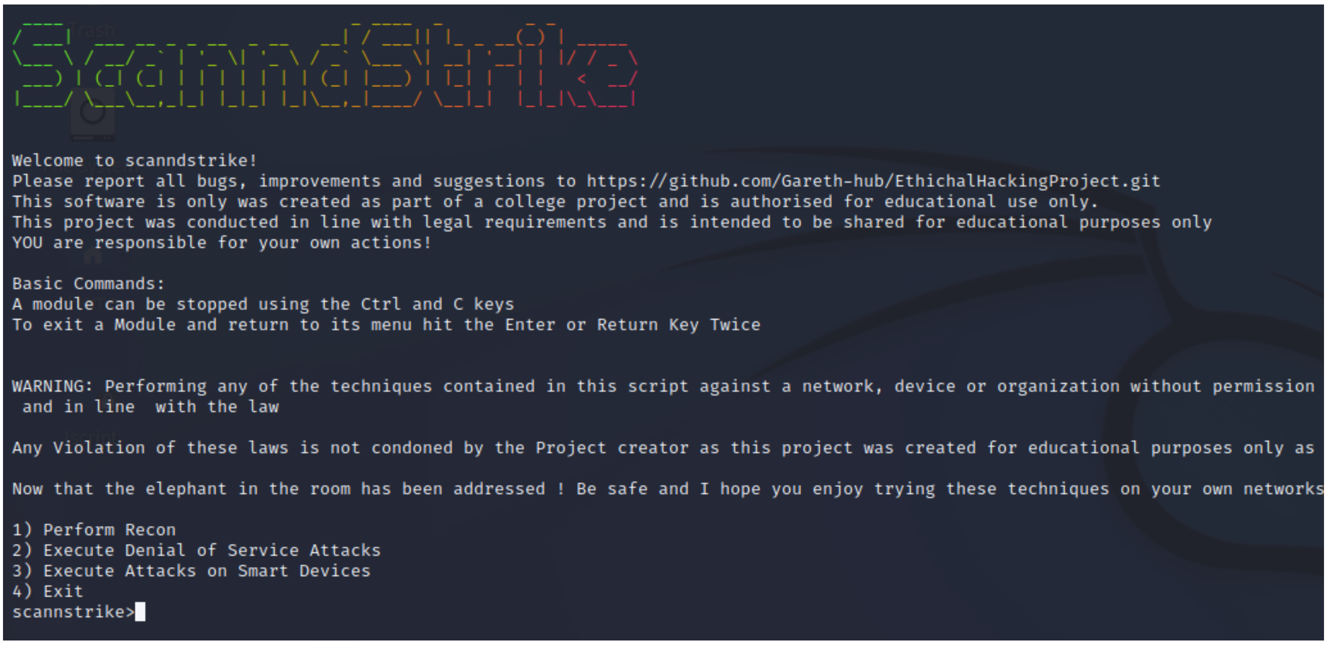
2.3. Implementation

The Kali Linux operating system is installed on a MicroSD so that it can be run by the Raspberry Pi Computer. This operating system comes with numerous tools that will aid in the penetration of networks and smart devices and this is why Kali is known as the 'Swiss Army Knife' of ethical hacking. One of the tools that will be used in this project is the network scanning tool Nmap. Nmap is a scanning tool that not only shows all the devices connected to a network but also returns information about the devices that are connected such as their operating system. While Kali Linux does come with various ethical hacking tools a script has been created to simplify the process of using them and provide users with an interface that requires little input to perform these ethical hacks using this amazing penetration testing/hacking tools. The Bash script that is the focus of this project is the scanndstrike script which the users must download from GitHub, this can be done using the ‘wget’ command followed by the link to the GitHub repository followed by the ‘sudo chmod +x scanndstrike’ command which will allow the script to be run on the user's machine. Once the script has been installed and permissions have been granted the user is ready to use the modules to perform Network Reconnaissance, Denial of Service attacks and Ethical Hacks on their target network or device.



```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/Gareth-hub/EthichalHackingProject.git
Cloning into 'EthichalHackingProject'...
remote: Enumerating objects: 46, done.
remote: Counting objects: 100% (46/46), done.
remote: Compressing objects: 100% (46/46), done.
remote: Total 46 (delta 22), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (46/46), 37.52 KiB | 1.79 MiB/s, done.
Resolving deltas: 100% (22/22), done.

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    EthichalHackingProject  Music        netrecon.sh  pingsweep.s
Documents  gobuster                mylist.txt   nowtest      Public
Downloads  lscript                 mysweep.txt  Pictures     Pyrit

┌──(kali㉿kali)-[~]
└─$ cd EthichalHackingProject

┌──(kali㉿kali)-[~/EthichalHackingProject]
└─$ ls
 BashScriptNetworkRecon   ipscan.sh   ipsweepandscan.sh   ipsweeper.sh

┌──(kali㉿kali)-[~/EthichalHackingProject]
└─$ sudo chmod +x scanndstrike

┌──(kali㉿kali)-[~/EthichalHackingProject]
└─$ ls
 BashScriptNetworkRecon   ipscan.sh   ipsweepandscan.sh   ipsweeper.sh
```

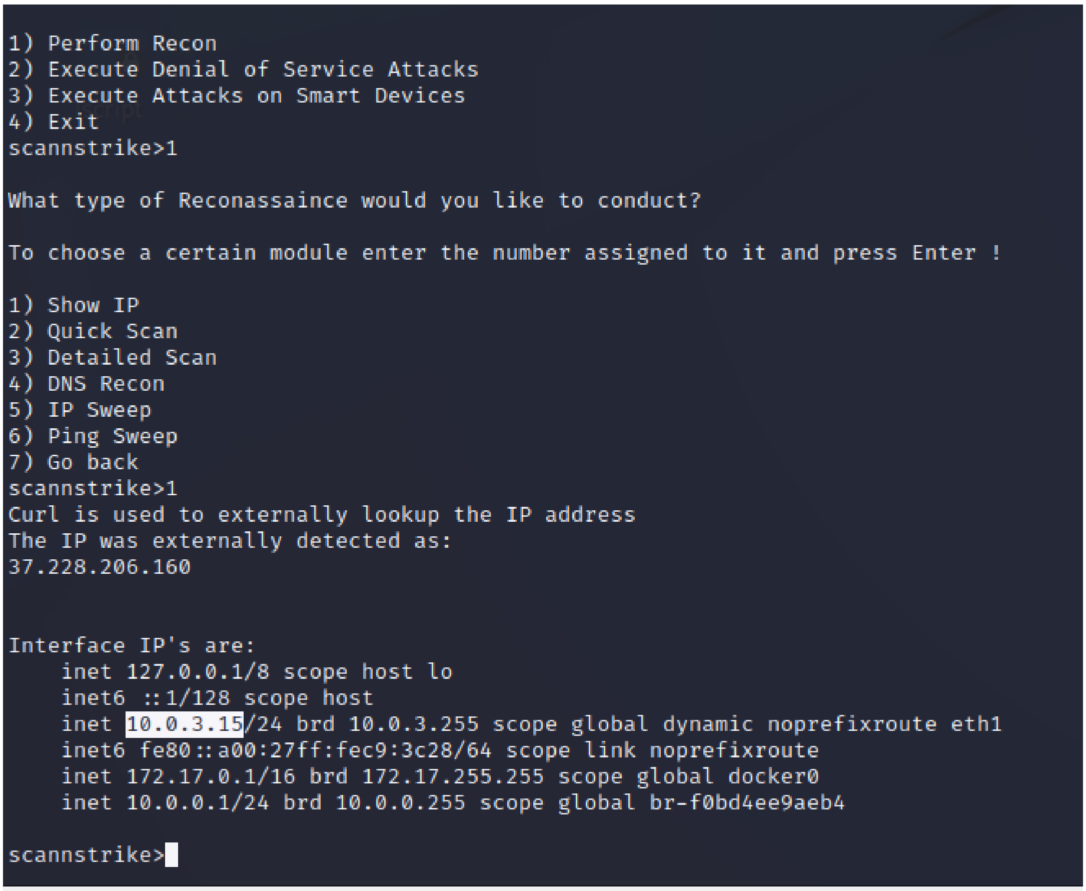
The command ‘./scanndstrike’ can then be run to launch the script to ensure it has been installed correctly and if so, the user should see the below image.



```
 ____                            _ ____  _        _ _        
/ ___|  ___ __ _ _ __  _ __   __| / ___|| |_ _ __(_) | _____ 
\___ \ / __/ _` | '_ \| '_ \ / _` \___ \| __| '__| | |/ / _ \
 ___) | (_| (_| | | | | | | | (_| |___) | |_| |  | |   <  __/
|____/ \___\__,_|_| |_|_| |_|\__,_|____/ \__|_|  |_|_|\_\___|


Welcome to scanndstrike!
Please report all bugs, improvements and suggestions to https://github.com/Gareth-hub/EthichalHackingProject.git
This software is only was created as part of a college project and is authorised for educational use only.
This project was conducted in line with legal requirements and is intended to be shared for educational purposes only
YOU are responsible for your own actions!

Basic Commands:
A module can be stopped using the Ctrl and C keys
To exit a Module and return to its menu hit the Enter or Return Key Twice


WARNING: Performing any of the techniques contained in this script against a network, device or organization without permission
 and in line  with the law

Any Violation of these laws is not condoned by the Project creator as this project was created for educational purposes only as

Now that the elephant in the room has been addressed ! Be safe and I hope you enjoy trying these techniques on your own networks

1) Perform Recon
2) Execute Denial of Service Attacks
3) Execute Attacks on Smart Devices
4) Exit
scannstrike>
```

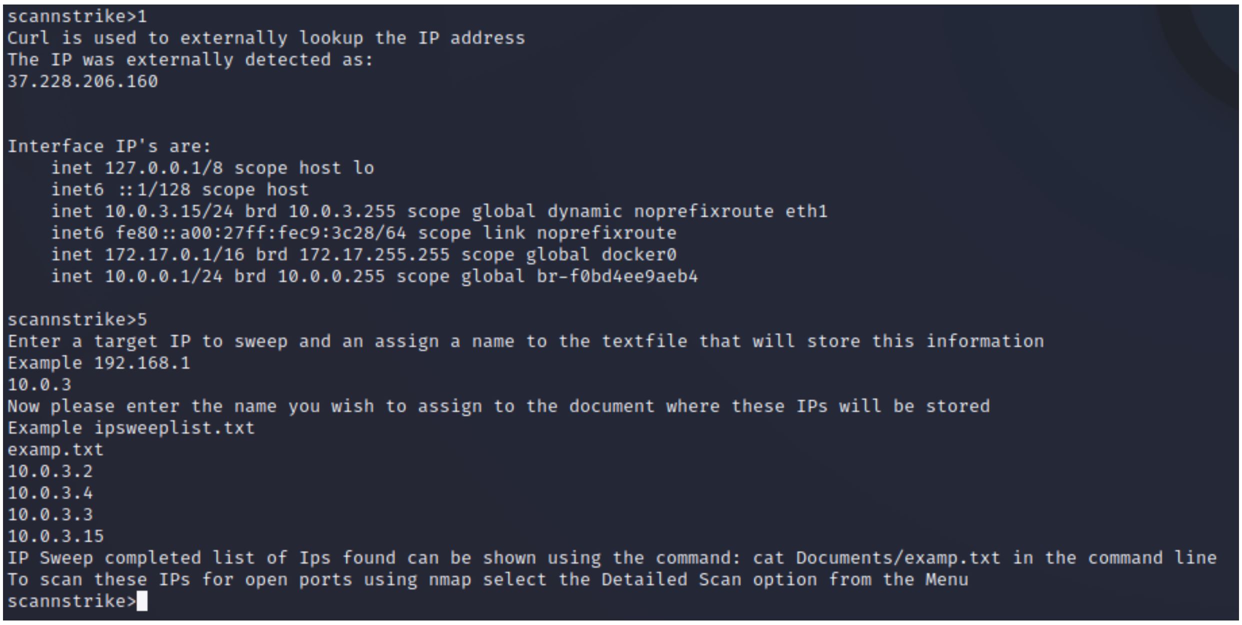
One of the main things a user needs to know to successfully run Network Reconnaissance, Denial of Service Attacks and Ethical Hacks is a target IP. Since this project is for educational purposes, the only IP being used should be one you have authorized access to, while your IP may not be known to you it can be found by navigating to the Recon Menu and selecting the Show IP module from the menu, this will give the output shown below which can then be used for the other modules such as the Quick Scan or IP Sweeper (also shown below).

Show IP Module



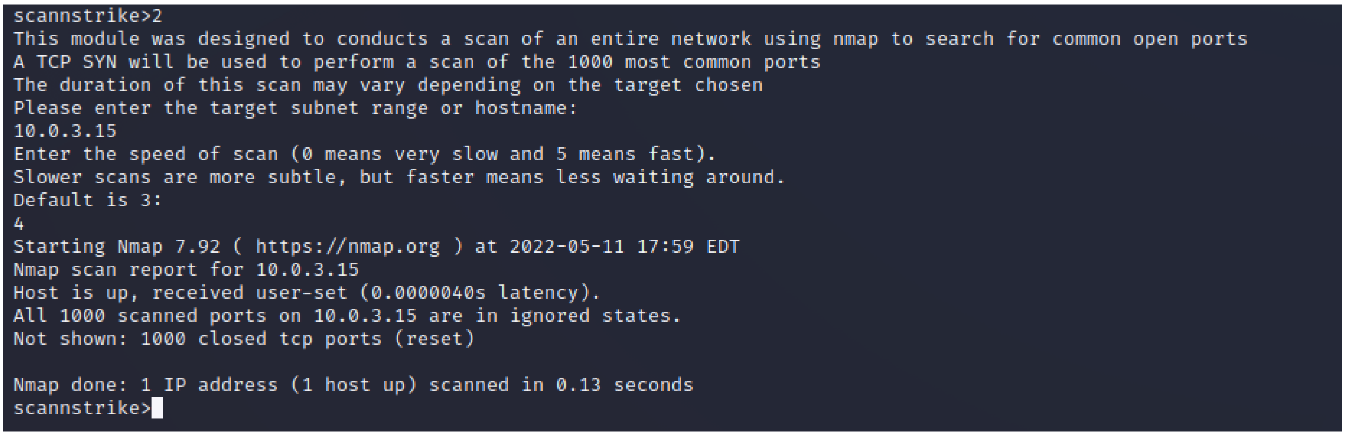
```
1) Perform Recon
2) Execute Denial of Service Attacks
3) Execute Attacks on Smart Devices
4) Exit
scannstrike>1

What type of Reconassaince would you like to conduct?

To choose a certain module enter the number assigned to it and press Enter !

1) Show IP
2) Quick Scan
3) Detailed Scan
4) DNS Recon
5) IP Sweep
6) Ping Sweep
7) Go back
scannstrike>1
Curl is used to externally lookup the IP address
The IP was externally detected as:
37.228.206.160


Interface IP's are:
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
    inet6 fe80::a00:27ff:fec9:3c28/64 scope link noprefixroute
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
    inet 10.0.0.1/24 brd 10.0.0.255 scope global br-f0bd4ee9aeb4

scannstrike>
```

IP Sweep Module



```
scannstrike>1
Curl is used to externally lookup the IP address
The IP was externally detected as:
37.228.206.160


Interface IP's are:
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
    inet6 fe80::a00:27ff:fec9:3c28/64 scope link noprefixroute
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
    inet 10.0.0.1/24 brd 10.0.0.255 scope global br-f0bd4ee9aeb4

scannstrike>5
Enter a target IP to sweep and an assign a name to the textfile that will store this information
Example 192.168.1
10.0.3
Now please enter the name you wish to assign to the document where these IPs will be stored
Example ipsweeplist.txt
examp.txt
10.0.3.2
10.0.3.4
10.0.3.3
10.0.3.15
IP Sweep completed list of Ips found can be shown using the command: cat Documents/examp.txt in the command line
To scan these IPs for open ports using nmap select the Detailed Scan option from the Menu
scannstrike>
```

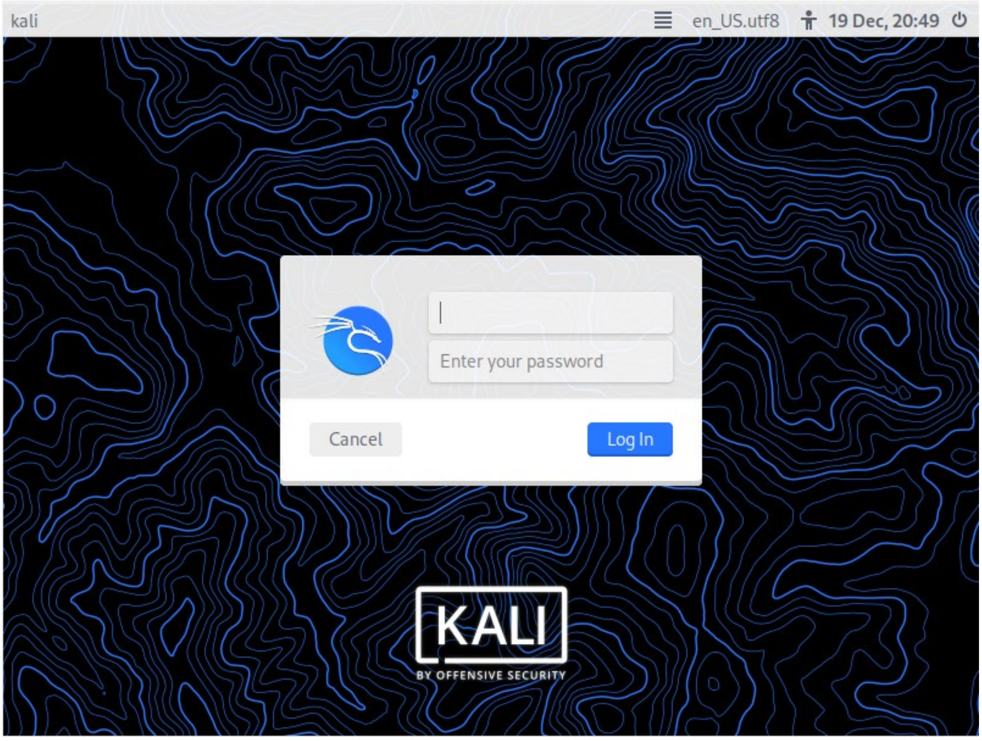
Quick Scan Module



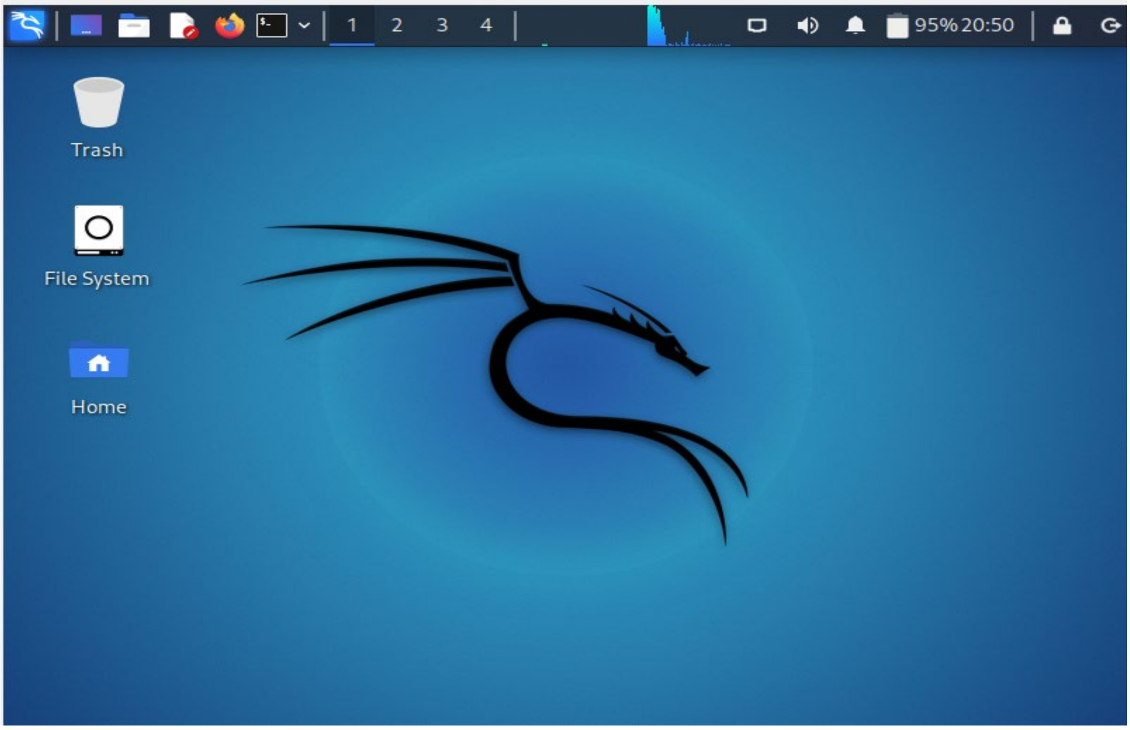
```
scannstrike>2
This module was designed to conducts a scan of an entire network using nmap to search for common open ports
A TCP SYN will be used to perform a scan of the 1000 most common ports
The duration of this scan may vary depending on the target chosen
Please enter the target subnet range or hostname:
10.0.3.15
Enter the speed of scan (0 means very slow and 5 means fast).
Slower scans are more subtle, but faster means less waiting around.
Default is 3:
4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-11 17:59 EDT
Nmap scan report for 10.0.3.15
Host is up, received user-set (0.0000040s latency).
All 1000 scanned ports on 10.0.3.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
scannstrike>
```

2.4. User Interface (UI)

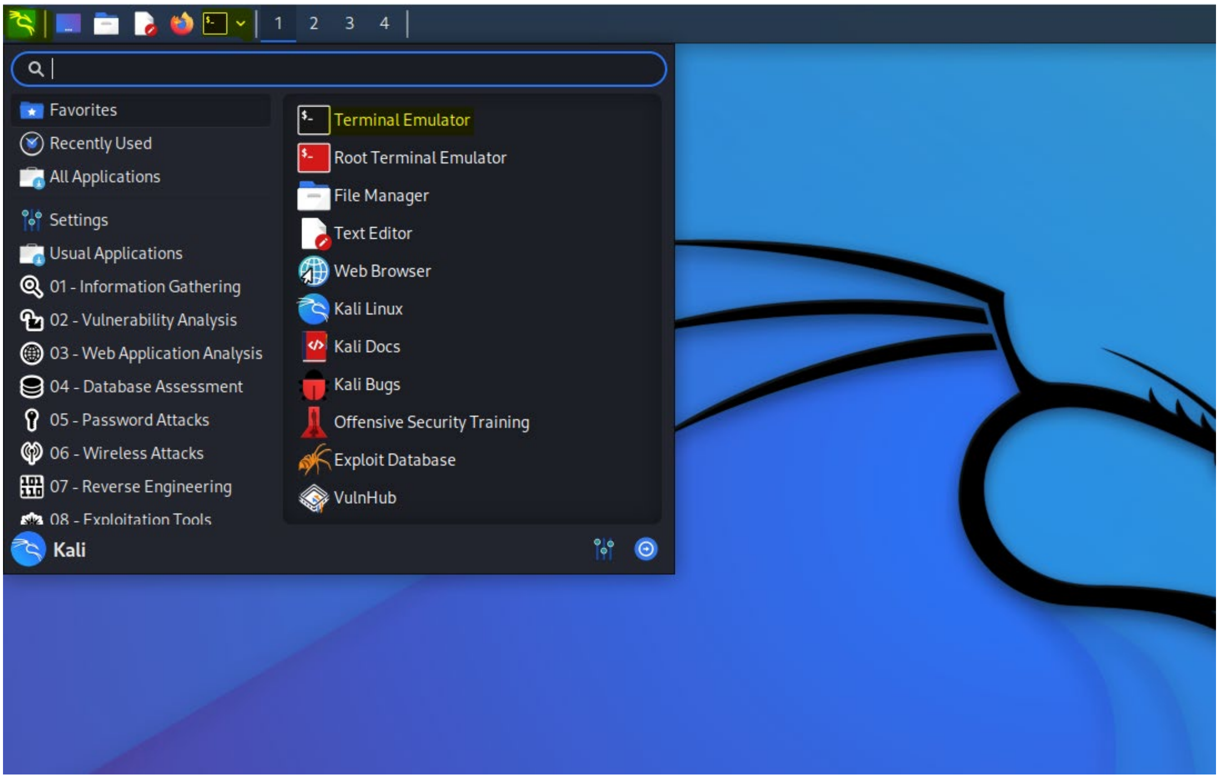
When Kali is run on the Raspberry Pi the user will be prompted to enter their username and password, by default the initial password and username are both: kali.



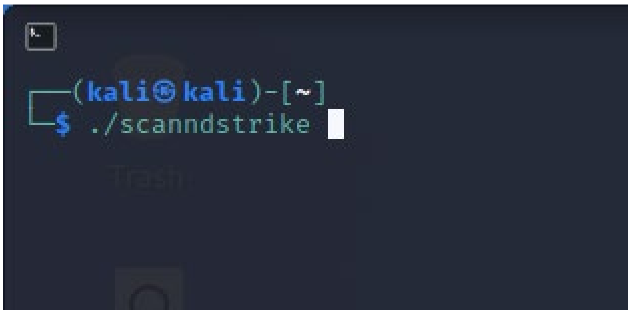
Once the username and password have been entered the user will be shown the Kali home screen (pictured below).



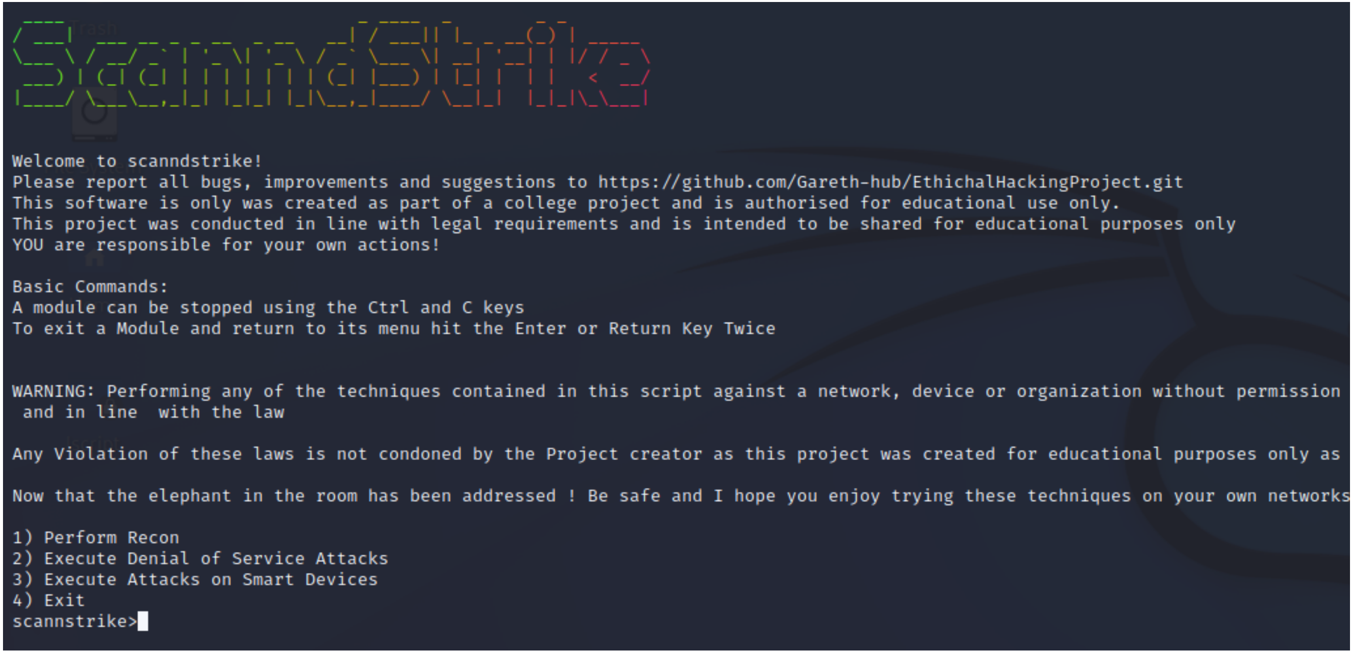
From here users can then navigate to the Kali Linux command terminal by clicking on the icon in the top left corner and selecting the Terminal Emulator from the list of suggested tools or by clicking on the black icon shown on the toolbar (this can be seen below).



Opening this Terminal Emulator (Terminal) allows the users to navigate to the scanndstrike bash script that is the focus for users (shown below).



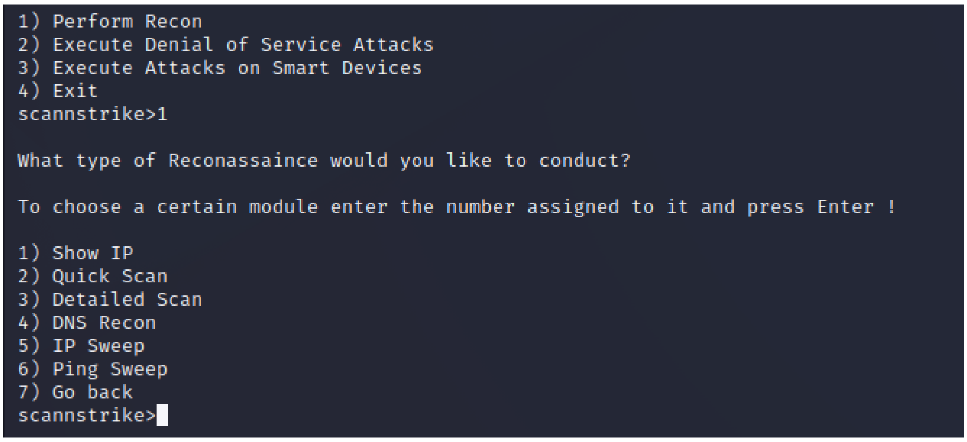
```
┌──(kali㉿kali)-[~]
└─$ ./scanndstrike
```



```
Welcome to scanndstrike!
Please report all bugs, improvements and suggestions to https://github.com/Gareth-hub/EthichalHackingProject.git
This software is only was created as part of a college project and is authorised for educational use only.
This project was conducted in line with legal requirements and is intended to be shared for educational purposes only
YOU are responsible for your own actions!

Basic Commands:
A module can be stopped using the Ctrl and C keys
To exit a Module and return to its menu hit the Enter or Return Key Twice


WARNING: Performing any of the techniques contained in this script against a network, device or organization without permission
 and in line  with the law

Any Violation of these laws is not condoned by the Project creator as this project was created for educational purposes only as

Now that the elephant in the room has been addressed ! Be safe and I hope you enjoy trying these techniques on your own networks

1) Perform Recon
2) Execute Denial of Service Attacks
3) Execute Attacks on Smart Devices
4) Exit
scannstrike>
```

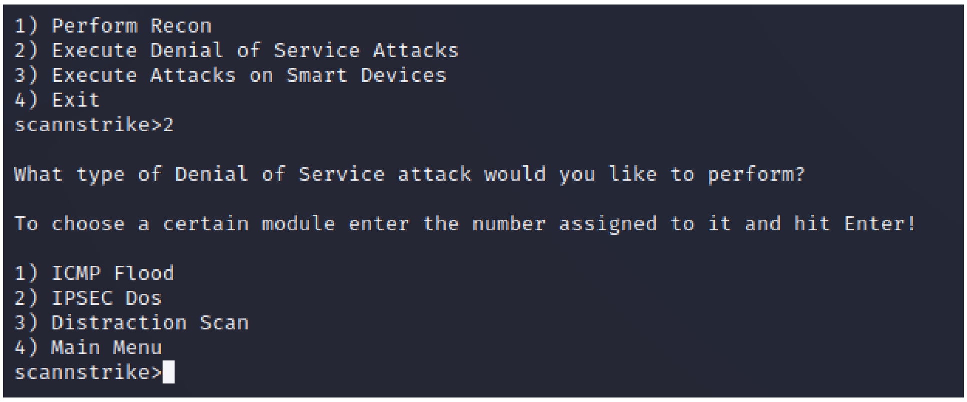
Now that the bash script is running users can choose what functions they would like to perform by choosing from the scanndstrike menu shown above. Within each of these sub menus is a list of modules the user can choose to run (shown below). These Modules are executed by the user and use Kali Linux's preinstalled tools such as nmap being used to perform a Quick Scan and Aircrack-ng being used to perform Wi-Fi password cracking.

Network Reconnaissance Modules



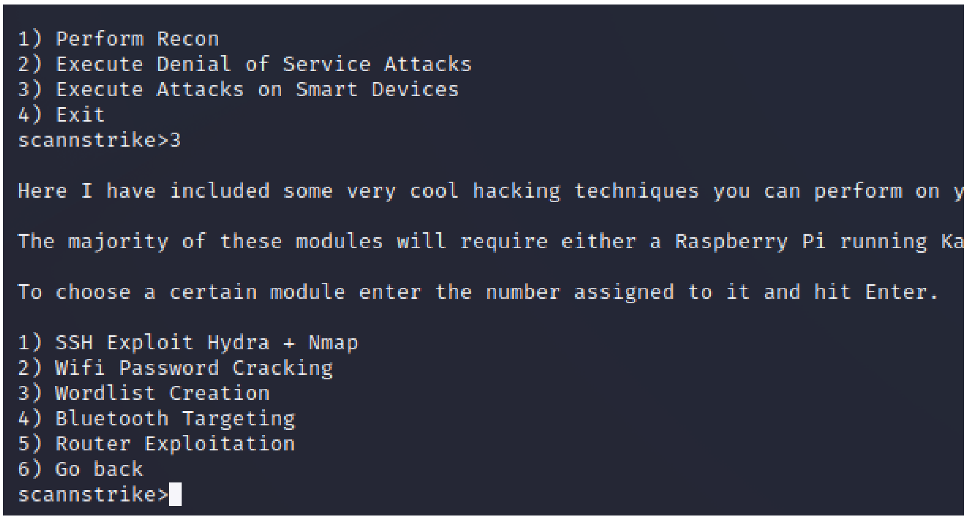
```
1) Perform Recon
2) Execute Denial of Service Attacks
3) Execute Attacks on Smart Devices
4) Exit
scannstrike>1

What type of Reconassaince would you like to conduct?

To choose a certain module enter the number assigned to it and press Enter !

1) Show IP
2) Quick Scan
3) Detailed Scan
4) DNS Recon
5) IP Sweep
6) Ping Sweep
7) Go back
scannstrike>
```

Denial of Service Attack Modules



```
1) Perform Recon
2) Execute Denial of Service Attacks
3) Execute Attacks on Smart Devices
4) Exit
scannstrike>2

What type of Denial of Service attack would you like to perform?

To choose a certain module enter the number assigned to it and hit Enter!

1) ICMP Flood
2) IPSEC Dos
3) Distraction Scan
4) Main Menu
scannstrike>
```

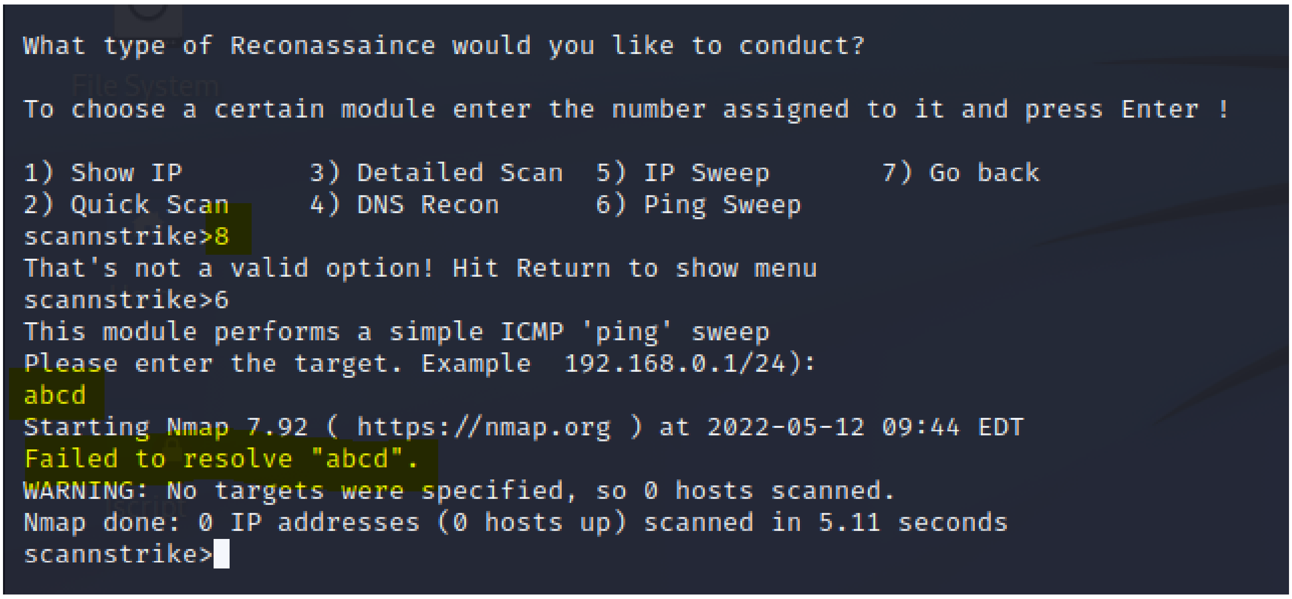
Ethical Hacking Modules



```
1) Perform Recon
2) Execute Denial of Service Attacks
3) Execute Attacks on Smart Devices
4) Exit
scannstrike>3

Here I have included some very cool hacking techniques you can perform on y

The majority of these modules will require either a Raspberry Pi running Ka

To choose a certain module enter the number assigned to it and hit Enter.

1) SSH Exploit Hydra + Nmap
2) Wifi Password Cracking
3) Wordlist Creation
4) Bluetooth Targeting
5) Router Exploitation
6) Go back
scannstrike>
```

2.5. Testing

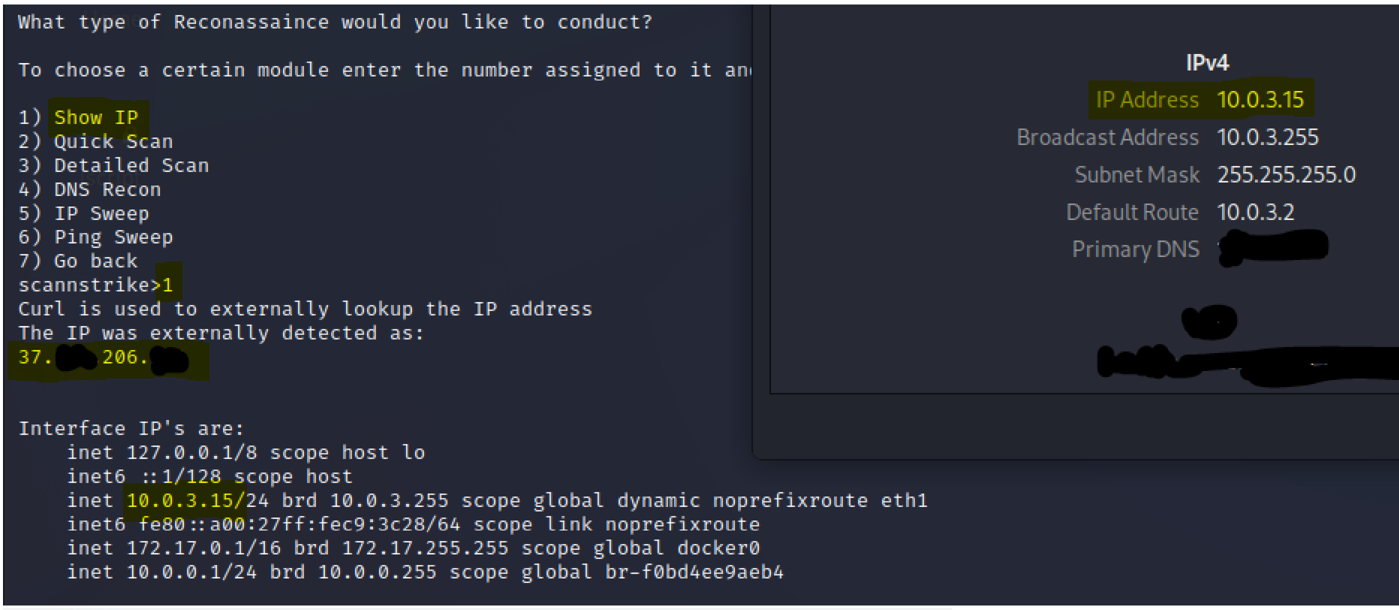
When it comes to using Kali Linux tools the best way to test them is to run them as any mistakes in the code that may stop them from running or missing packages/software is displayed to the user with an error message. Therefore, the best testing tool for this project is the Kali Linux terminal itself. From the example below there are two errors that can be seen 'Failed to resolve' and 'No targets were specified' these errors can occur when the user enters invalid input required for the module to run successfully.



```
What type of Reconassaince would you like to conduct?

To choose a certain module enter the number assigned to it and press Enter !

1) Show IP        3) Detailed Scan  5) IP Sweep       7) Go back
2) Quick Scan     4) DNS Recon      6) Ping Sweep
scannstrike>8
That's not a valid option! Hit Return to show menu
scannstrike>6
This module performs a simple ICMP 'ping' sweep
Please enter the target. Example  192.168.0.1/24):
abcd
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-12 09:44 EDT
Failed to resolve "abcd".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 5.11 seconds
scannstrike>
```

The plan for this project was to run all the Modules against the target network or device and evaluate the results and then do so again after security measures had been put in place and see which modules were affected. While some of the modules within the scanndstrike script can be stopped such as the (Secure Shell) SSH (Secure Shell) Attack on a machine or the Wi-Fi Password Cracking module, however modules such as Show IP and the majority of the network recon tools can evade firewalls and run effectively against a network. An Example of a test performed is verifying the information returned by the Modules the example below shows the Show IP module being run to detect the users IP Address (shown below as 37.XXX.206.XXX) as well as the machines IP Address. While below you will notice two sections of my IP Adress match the other two are covered as while this project is focused on ethical hacking and testing these tools, disclosing your personal IP Address is never a good idea as if hackers know your IP Address there are countless ways, they can use it against you.

Test of the Show IP Module

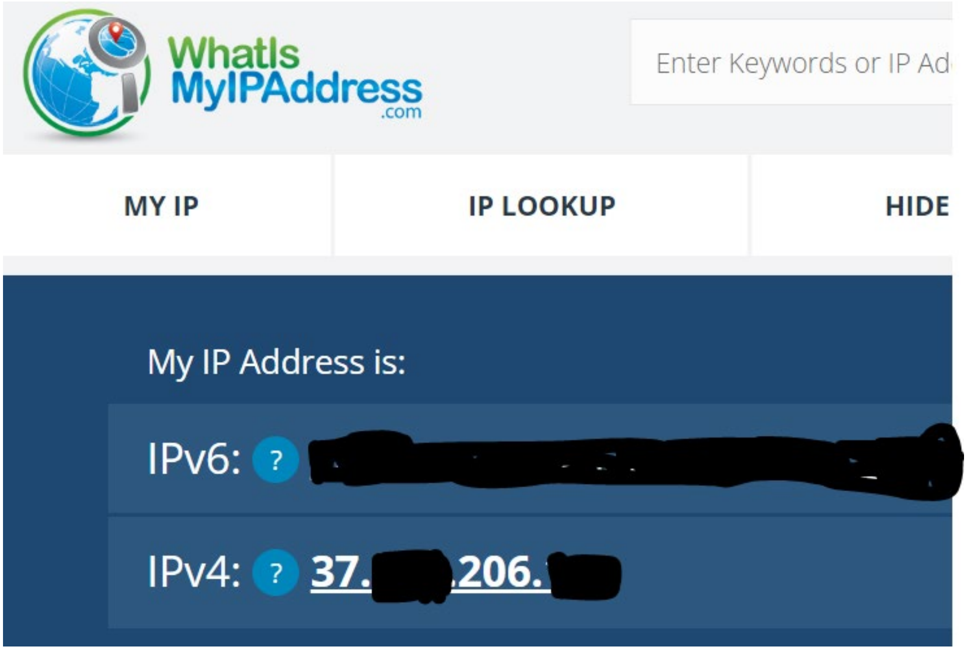


```
What type of Reconassaince would you like to conduct?

To choose a certain module enter the number assigned to it an

1) Show IP
2) Quick Scan
3) Detailed Scan
4) DNS Recon
5) IP Sweep
6) Ping Sweep
7) Go back
scannstrike>1
Curl is used to externally lookup the IP address
The IP was externally detected as:
37.[redacted]206.[redacted]

Interface IP's are:
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 10.0.3.15/24 brd 10.0.3.255 scope global dynamic noprefixroute eth1
    inet6 fe80::a00:27ff:fec9:3c28/64 scope link noprefixroute
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
    inet 10.0.0.1/24 brd 10.0.0.255 scope global br-f0bd4ee9aeb4
```

IPv4

IP Address	10.0.3.15
Broadcast Address	10.0.3.255
Subnet Mask	255.255.255.0
Default Route	10.0.3.2
Primary DNS	[redacted]

[redacted]



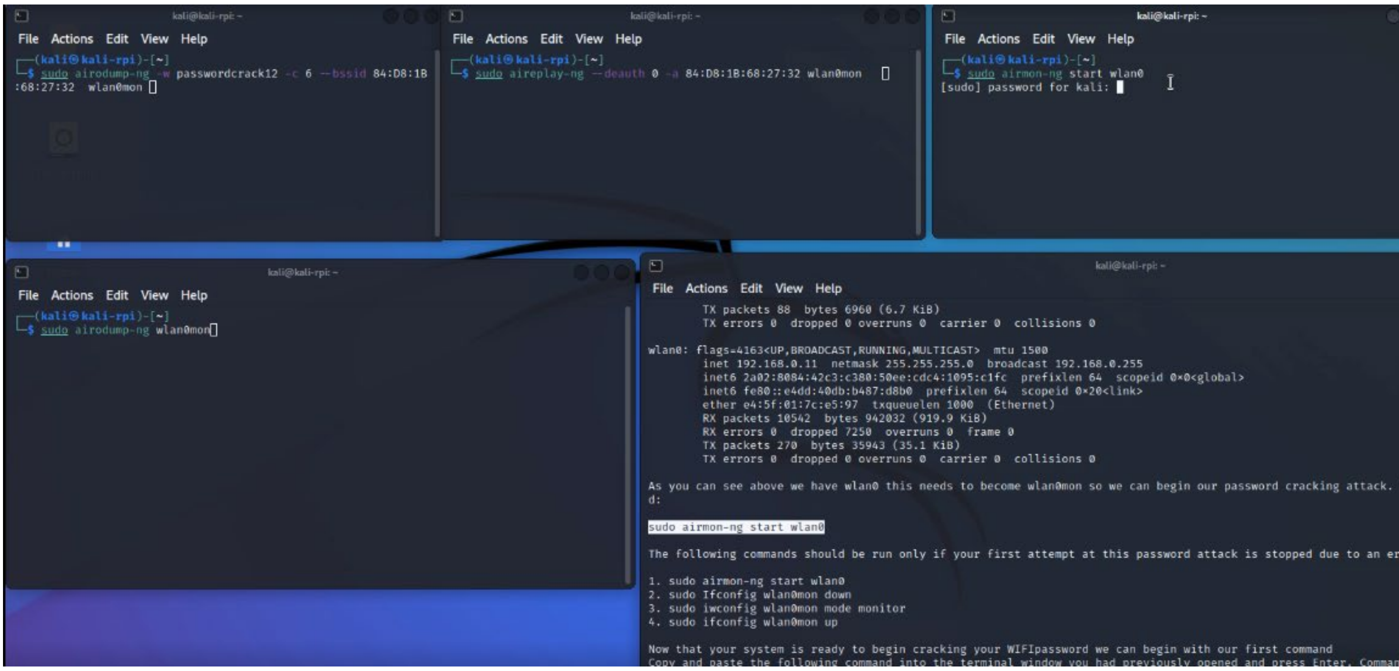
My IP Address is:

IPv6: ? [redacted]

IPv4: ? 37.[redacted]206.[redacted]

Another important module available for users is the Wi-Fi Password Cracking module which allows the user to take on a semi-automatic ethical hacking approach using aircrack-ng and its sub tools. While running this module does means some additional input is required by the user the input required is created for the user based on the data, they have entered about their target network. Below are screenshots taken during a Wi-Fi Password Crack on a Wi-Fi router that was used as a target after being granted authorization, these screenshots cover the processes involved in running this module and show how the module was tested. Since this project was conducted ethically and the target networks password was known a short wordlist was created to speed up the last step in the Wi-Fi password cracking process.

Testing the Wi-Fi Password Cracking Module



```
kali@kali-rpi: ~
┌──(kali㉿kali-rpi)-[~]
└─$ sudo airodump-ng -w passwordcrack12 -c 6 --bssid 84:D8:1B
:68:27:32  wlan0mon
```

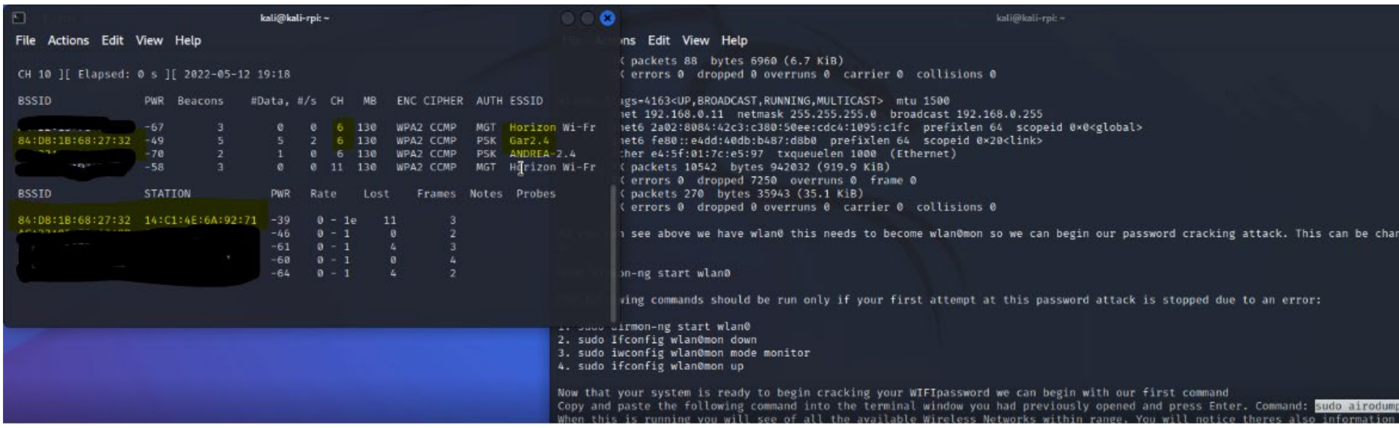
```
kali@kali-rpi: ~
┌──(kali㉿kali-rpi)-[~]
└─$ sudo aireplay-ng --deauth 0 -a 84:D8:1B:68:27:32 wlan0mon
```

```
kali@kali-rpi: ~
┌──(kali㉿kali-rpi)-[~]
└─$ sudo airmon-ng start wlan0
[sudo] password for kali:
```

```
kali@kali-rpi: ~
┌──(kali㉿kali-rpi)-[~]
└─$ sudo airodump-ng wlan0mon
```

```
kali@kali-rpi: ~
        TX packets 88  bytes 6960 (6.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.11  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 2a02:8084:42c3:c380:50ee:cdc4:1095:c1fc  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::e4dd:40db:b487:d8b0  prefixlen 64  scopeid 0x20<link>
        ether e4:5f:01:7c:e5:97  txqueuelen 1000  (Ethernet)
        RX packets 10542  bytes 942032 (919.9 KiB)
        RX errors 0  dropped 7250  overruns 0  frame 0
        TX packets 270  bytes 35943 (35.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

As you can see above we have wlan0 this needs to become wlan0mon so we can begin our password cracking attack.
d:

sudo airmon-ng start wlan0

The following commands should be run only if your first attempt at this password attack is stopped due to an er

1. sudo airmon-ng start wlan0
2. sudo Ifconfig wlan0mon down
3. sudo iwconfig wlan0mon mode monitor
4. sudo ifconfig wlan0mon up

Now that your system is ready to begin cracking your WIFIpassword we can begin with our first command
Copy and paste the following command into the terminal window you had previously opened and press Enter. Comman
```

Shown below is the output from the 'sudo airodump-ng wlan0mon' command which shows the user all the Wi-Fi networks within range along with details about the network such as their channel, security type, name etc. As you will see when the airodump command is run the target network for this test 'Gar2.4' is identified.

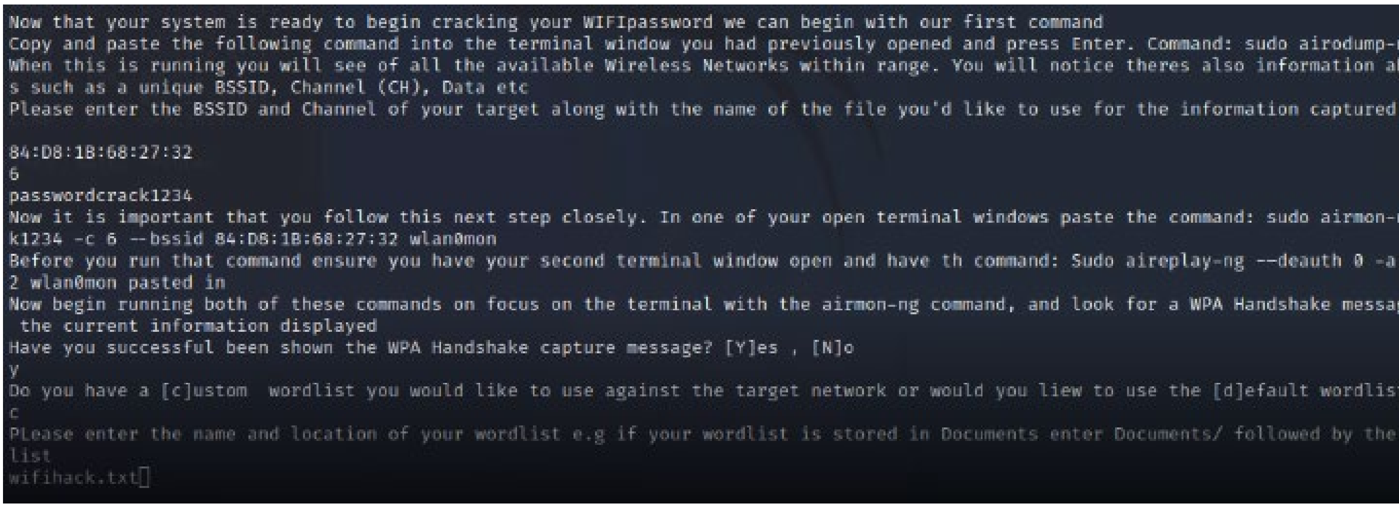


```
kali@kali-rpi: ~

CH 10 ][ Elapsed: 0 s ][ 2022-05-12 19:18

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

[redacted]         -67        3        0    0   6  130   WPA2 CCMP   MGT  Horizon Wi-Fr
84:D8:1B:68:27:32  -49        5        5    2   6  130   WPA2 CCMP   PSK  Gar2.4
[redacted]         -70        2        1    0   6  130   WPA2 CCMP   PSK  ANDREA-2.4
                   -58        3        0    0  11  130   WPA2 CCMP   MGT  Horizon Wi-Fr

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

84:D8:1B:68:27:32  14:C1:4E:6A:92:71  -39    0 - 1e    11        3
[redacted]                            -46    0 - 1      0        2
                                      -61    0 - 1      4        3
                                      -60    0 - 1      0        4
                                      -64    0 - 1      4        2
```

```
kali@kali-rpi: ~
ns  Edit  View  Help
( packets 88  bytes 6960 (6.7 KiB)
( errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
iet 192.168.0.11  netmask 255.255.255.0  broadcast 192.168.0.255
iet6 2a02:8084:42c3:c380:50ee:cdc4:1095:c1fc  prefixlen 64  scopeid 0x0<global>
iet6 fe80::e4dd:40db:b487:d8b0  prefixlen 64  scopeid 0x20<link>
her e4:5f:01:7c:e5:97  txqueuelen 1000  (Ethernet)
( packets 10542  bytes 942032 (919.9 KiB)
( errors 0  dropped 7250  overruns 0  frame 0
( packets 270  bytes 35943 (35.1 KiB)
( errors 0  dropped 0 overruns 0  carrier 0  collisions 0

i see above we have wlan0 this needs to become wlan0mon so we can begin our password cracking attack. This can be char

on-ng start wlan0

ving commands should be run only if your first attempt at this password attack is stopped due to an error:

1. sudo airmon-ng start wlan0
2. sudo Ifconfig wlan0mon down
3. sudo iwconfig wlan0mon mode monitor
4. sudo ifconfig wlan0mon up

Now that your system is ready to begin cracking your WIFIpassword we can begin with our first command
Copy and paste the following command into the terminal window you had previously opened and press Enter. Command: sudo airodump
When this is running you will see of all the available Wireless Networks within range. You will notice theres also information
```

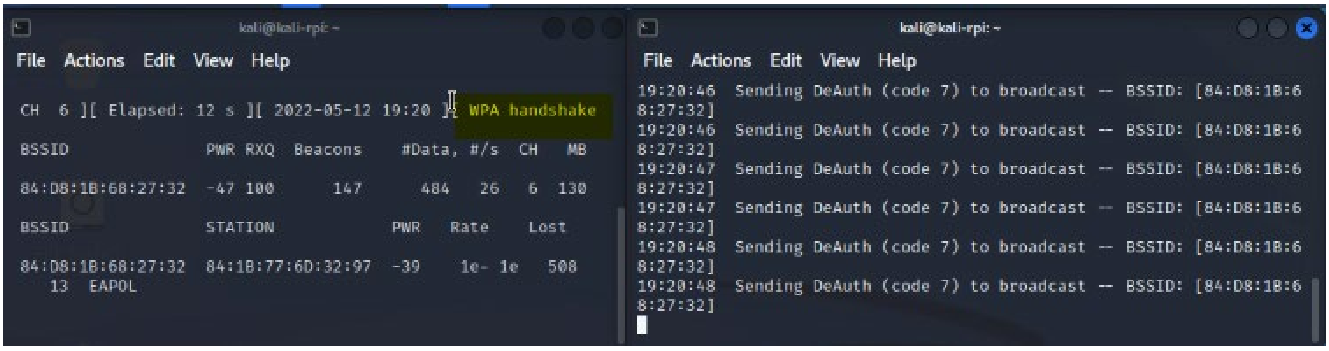
●

Now that the target network has been identified the user is asked to enter the network bssid, channel and name the file that will store any data gathered about this network. This input is then read by the script and used to create the next two commands that the user must run simultaneously as the 'sudo airmon-ng -w -c --bssid wlan0mon' command is used to provide the user with a live capture of the network and displaying the devices connected to it while the 'sudo aireplay-ng -–deauth 0 -a wlan0mon' command is used to perform a form of Denial of Service attack on the networks devices and interrupting the device connection to the router in the hopes of capturing the network password from the connecting device(s).



```
Now that your system is ready to begin cracking your WIFIpassword we can begin with our first command
Copy and paste the following command into the terminal window you had previously opened and press Enter. Command: sudo airodump-
When this is running you will see of all the available Wireless Networks within range. You will notice theres also information a
s such as a unique BSSID, Channel (CH), Data etc
Please enter the BSSID and Channel of your target along with the name of the file you'd like to use for the information captured

84:D8:1B:68:27:32
6
passwordcrack1234
Now it is important that you follow this next step closely. In one of your open terminal windows paste the command: sudo airmon-
k1234 -c 6 --bssid 84:D8:1B:68:27:32 wlan0mon
Before you run that command ensure you have your second terminal window open and have th command: Sudo aireplay-ng --deauth 0 -a
2 wlan0mon pasted in
Now begin running both of these commands on focus on the terminal with the airmon-ng command, and look for a WPA Handshake messa
 the current information displayed
Have you successful been shown the WPA Handshake capture message? [Y]es , [N]o
y
Do you have a [c]ustom  wordlist you would like to use against the target network or would you liew to use the [d]efault wordlis
c
PLease enter the name and location of your wordlist e.g if your wordlist is stored in Documents enter Documents/ followed by the
list
wifihack.txt
```

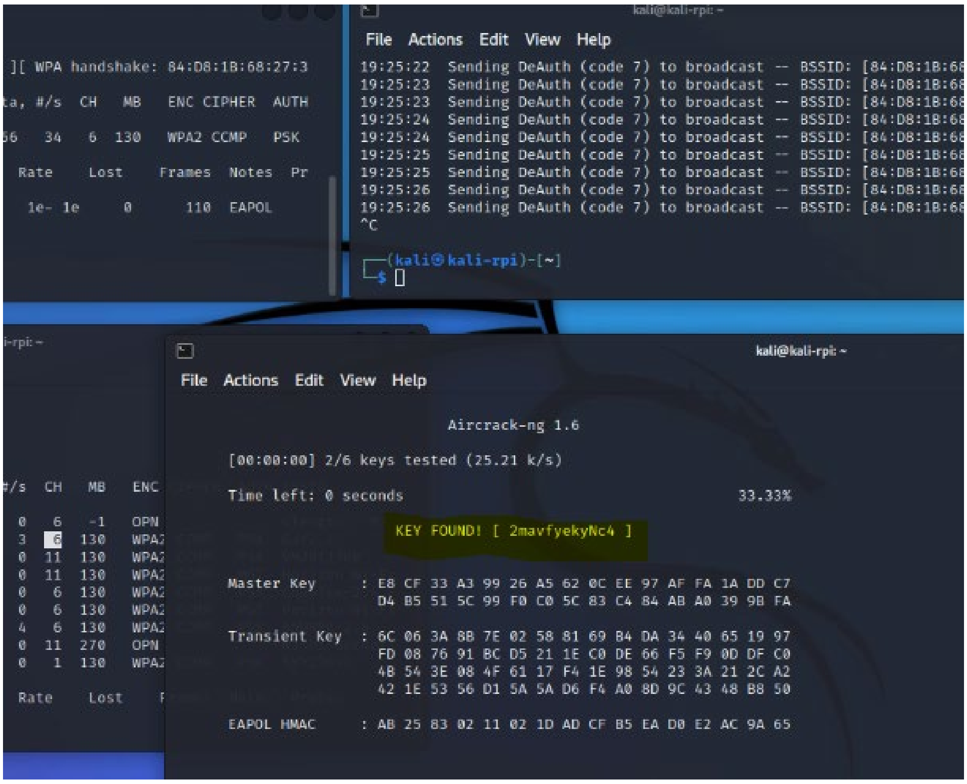
The capture of packets while a device is connecting to a network can lead to A WPA Handshake shown below which when used with a list of passwords that can crack weak, common or default passwords. The WPA handshake being captured can be seen below



```
 CH  6 ][ Elapsed: 12 s ][ 2022-05-12 19:20 ][ WPA handshake

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB

 84:D8:1B:68:27:32  -47 100      147      484   26   6  130

 BSSID              STATION            PWR   Rate    Lost

 84:D8:1B:68:27:32  84:1B:77:6D:32:97  -39    1e- 1e    508
    13   EAPOL
```

```
19:20:46  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:6
8:27:32]
19:20:46  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:6
8:27:32]
19:20:47  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:6
8:27:32]
19:20:47  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:6
8:27:32]
19:20:48  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:6
8:27:32]
19:20:48  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:6
8:27:32]
```

Once the WPA handshake is captured the information is stored in a file created with the filename given by the user and is then run with the wordlist chosen by the user. Again, since this test was performed on an authorized network a short password list was created for this test the results of which are shown below.



```
 ][ WPA handshake: 84:D8:1B:68:27:3

ta, #/s   CH   MB   ENC CIPHER  AUTH

56   34   6  130   WPA2 CCMP   PSK

 Rate    Lost    Frames  Notes  Pr

  1e- 1e    0      110  EAPOL
```

```
19:25:22  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:68
19:25:23  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:68
19:25:23  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:68
19:25:24  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:68
19:25:24  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:68
19:25:25  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:68
19:25:25  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:68
19:25:26  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:68
19:25:26  Sending DeAuth (code 7) to broadcast -- BSSID: [84:D8:1B:68
^C

┌──(kali㉿kali-rpi)-[~]
└─$ 
```

```
#/s  CH   MB   ENC

 0    6   -1   OPN
 3    6  130   WPA2
 0   11  130   WPA2
 0   11  130   WPA2
 0    6  130   WPA2
 0    6  130   WPA2
 4    6  130   WPA2
 0   11  270   OPN
 0    1  130   WPA2

 Rate    Lost    F
```

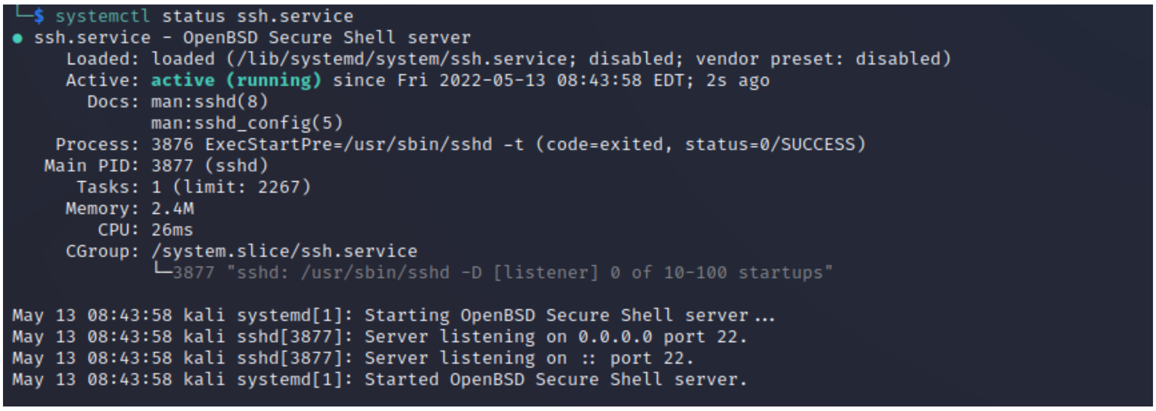
```
                              Aircrack-ng 1.6

      [00:00:00] 2/6 keys tested (25.21 k/s)

      Time left: 0 seconds                                      33.33%

                           KEY FOUND! [ 2mavfyekyNc4 ]


      Master Key     : E8 CF 33 A3 99 26 A5 62 0C EE 97 AF FA 1A DD C7
                       D4 B5 51 5C 99 F0 C0 5C 83 C4 84 AB A0 39 9B FA

      Transient Key  : 6C 06 3A 8B 7E 02 58 81 69 B4 DA 34 40 65 19 97
                       FD 08 76 91 BC D5 21 1E C0 DE 66 F5 F9 0D DF C0
                       4B 54 3E 08 4F 61 17 F4 1E 98 54 23 3A 21 2C A2
                       42 1E 53 56 D1 5A 5A D6 F4 A0 8D 9C 43 48 B8 50

      EAPOL HMAC     : AB 25 83 02 11 02 1D AD CF B5 EA D0 E2 AC 9A 65
```

While during this test the process of capturing the WPA handshake and cracking the target networks password was successful, even if the key was not found the test would be considered successful as all of the processes performed correctly and the user input was correctly stored and used to create the commands needed to send perform a deauthentication attack against the network and output live information about the network and its connected devices.

Testing Securing Smart Devices by disabling SSH connections

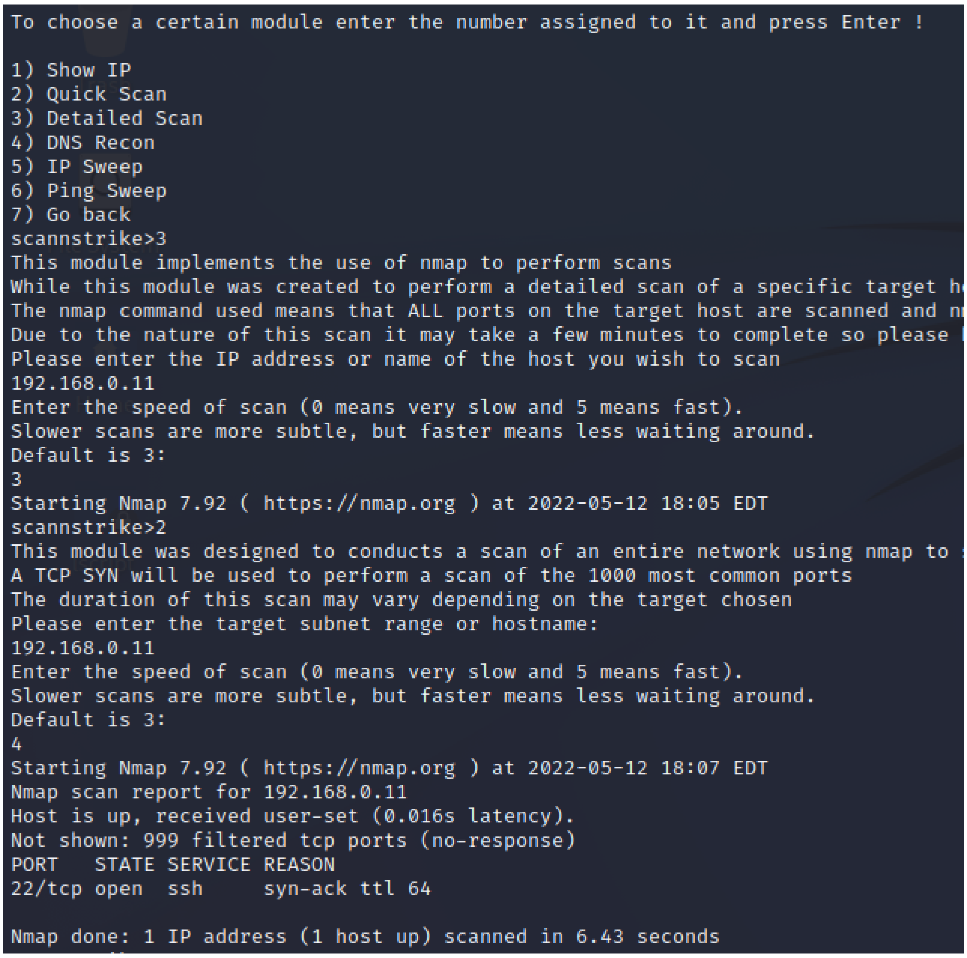
In order to determine whether or not disabling SSH connections on a machine will make it more secure it must first be tested to see if its SSH connections are enabled, are discoverable and what can be done once an open SSH connection is found. By running the Quick Scan Module and setting the target IP to the Kali Linux OS (Operating system) the scan reveals there is an open port for SSH connections.

Check if SSH Connections are enabled and active



```
└─$ systemctl status ssh.service
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
     Active: active (running) since Fri 2022-05-13 08:43:58 EDT; 2s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 3876 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 3877 (sshd)
      Tasks: 1 (limit: 2267)
     Memory: 2.4M
        CPU: 26ms
     CGroup: /system.slice/ssh.service
             └─3877 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 13 08:43:58 kali systemd[1]: Starting OpenBSD Secure Shell server...
May 13 08:43:58 kali sshd[3877]: Server listening on 0.0.0.0 port 22.
May 13 08:43:58 kali sshd[3877]: Server listening on :: port 22.
May 13 08:43:58 kali systemd[1]: Started OpenBSD Secure Shell server.
```

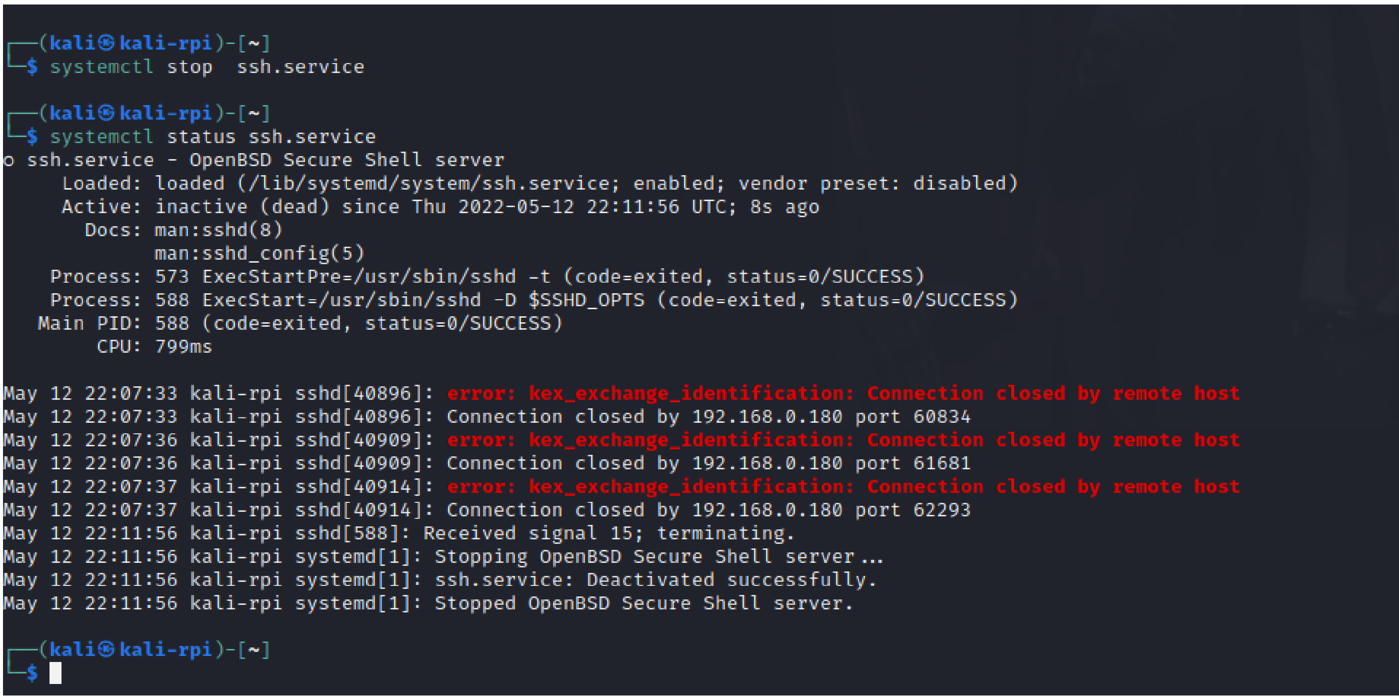
Quick Scan with SSH Connections active



```
To choose a certain module enter the number assigned to it and press Enter !

1) Show IP
2) Quick Scan
3) Detailed Scan
4) DNS Recon
5) IP Sweep
6) Ping Sweep
7) Go back
scannstrike>3
This module implements the use of nmap to perform scans
While this module was created to perform a detailed scan of a specific target h
The nmap command used means that ALL ports on the target host are scanned and n
Due to the nature of this scan it may take a few minutes to complete so please
Please enter the IP address or name of the host you wish to scan
192.168.0.11
Enter the speed of scan (0 means very slow and 5 means fast).
Slower scans are more subtle, but faster means less waiting around.
Default is 3:
3
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-12 18:05 EDT
scannstrike>2
This module was designed to conducts a scan of an entire network using nmap to
A TCP SYN will be used to perform a scan of the 1000 most common ports
The duration of this scan may vary depending on the target chosen
Please enter the target subnet range or hostname:
192.168.0.11
Enter the speed of scan (0 means very slow and 5 means fast).
Slower scans are more subtle, but faster means less waiting around.
Default is 3:
4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-12 18:07 EDT
Nmap scan report for 192.168.0.11
Host is up, received user-set (0.016s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64

Nmap done: 1 IP address (1 host up) scanned in 6.43 seconds
```

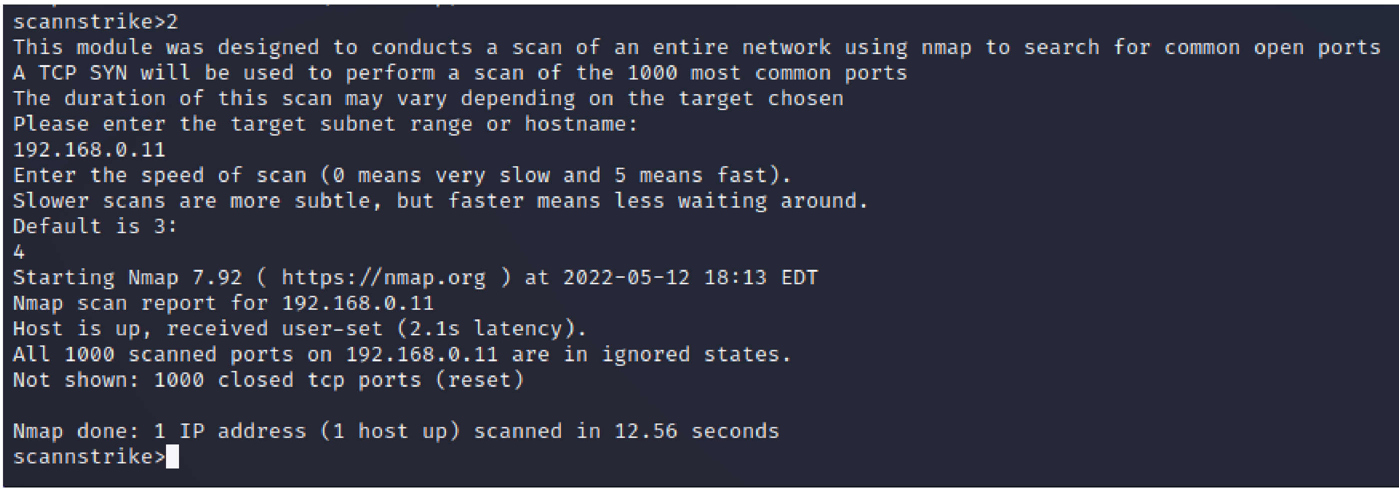
You can see above with SSH (Secure Shell) connections active on the target machine the hacker now has accesses to a vulnerability that could be exploit using the Ethical Hacking module SSH Exploit using Hydra + nmap. In order to avoid the possibility of being a victim to the exploitation of this vulnerability the user can remove the vulnerability altogether by disabling SSH connections.

Stop SSH Connections on your machine



```
┌──(kali㉿kali-rpi)-[~]
└─$ systemctl stop  ssh.service

┌──(kali㉿kali-rpi)-[~]
└─$ systemctl status ssh.service
○ ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: disabled)
     Active: inactive (dead) since Thu 2022-05-12 22:11:56 UTC; 8s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 573 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Process: 588 ExecStart=/usr/sbin/sshd -D $SSHD_OPTS (code=exited, status=0/SUCCESS)
   Main PID: 588 (code=exited, status=0/SUCCESS)
        CPU: 799ms

May 12 22:07:33 kali-rpi sshd[40896]: error: kex_exchange_identification: Connection closed by remote host
May 12 22:07:33 kali-rpi sshd[40896]: Connection closed by 192.168.0.180 port 60834
May 12 22:07:36 kali-rpi sshd[40909]: error: kex_exchange_identification: Connection closed by remote host
May 12 22:07:36 kali-rpi sshd[40909]: Connection closed by 192.168.0.180 port 61681
May 12 22:07:37 kali-rpi sshd[40914]: error: kex_exchange_identification: Connection closed by remote host
May 12 22:07:37 kali-rpi sshd[40914]: Connection closed by 192.168.0.180 port 62293
May 12 22:11:56 kali-rpi sshd[588]: Received signal 15; terminating.
May 12 22:11:56 kali-rpi systemd[1]: Stopping OpenBSD Secure Shell server...
May 12 22:11:56 kali-rpi systemd[1]: ssh.service: Deactivated successfully.
May 12 22:11:56 kali-rpi systemd[1]: Stopped OpenBSD Secure Shell server.

┌──(kali㉿kali-rpi)-[~]
└─$ 
```

Quick Scan Results after SSH Connections are stopped



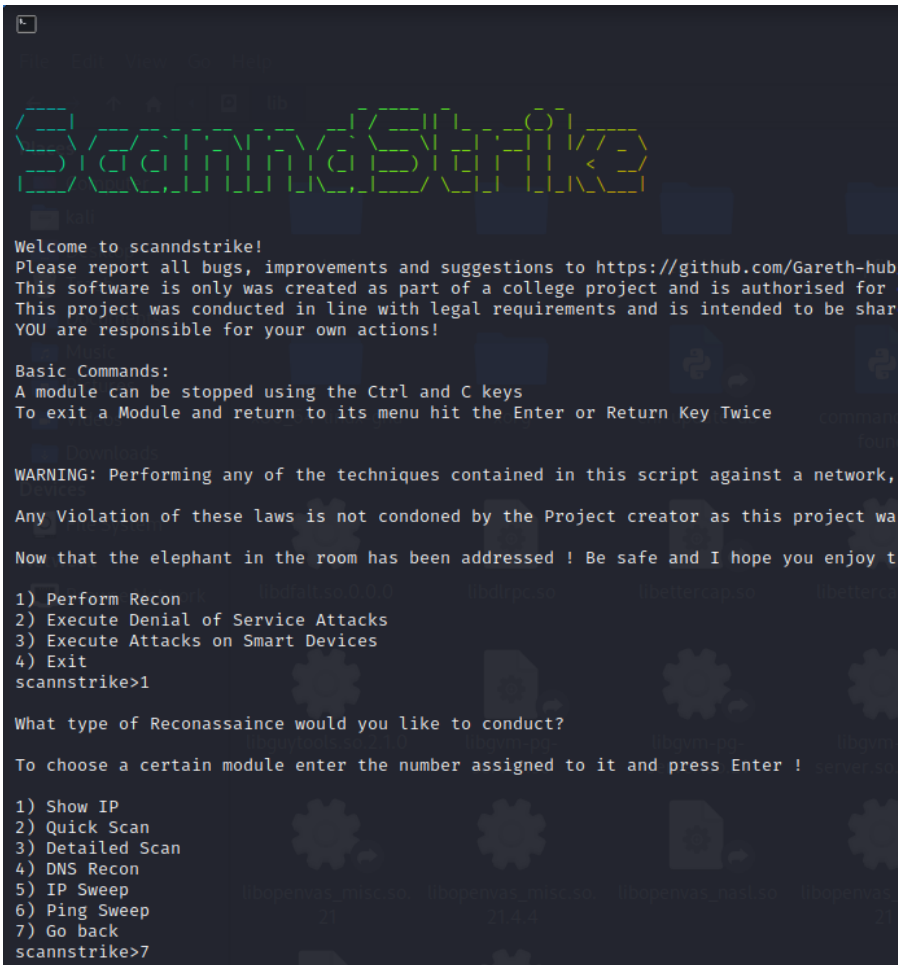
```
scannstrike>2
This module was designed to conducts a scan of an entire network using nmap to search for common open ports
A TCP SYN will be used to perform a scan of the 1000 most common ports
The duration of this scan may vary depending on the target chosen
Please enter the target subnet range or hostname:
192.168.0.11
Enter the speed of scan (0 means very slow and 5 means fast).
Slower scans are more subtle, but faster means less waiting around.
Default is 3:
4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-12 18:13 EDT
Nmap scan report for 192.168.0.11
Host is up, received user-set (2.1s latency).
All 1000 scanned ports on 192.168.0.11 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 12.56 seconds
scannstrike>
```

You can see from the images above after the security measure of disabling SSH (Secure Shell) connections has been implemented the target device that was previously vulnerable to a SSH Exploit is now secured. By running the quick scan of the target IP before and after implementing this security measure was a terrific way to test its effectiveness.

The last form of testing conducted for this project was on the installation and running of the bash menu script from the user's end. Following the commands in the GitHub Repository the user should be able to install and run the scanndstrike bash menu script and access its three sub menus and their Modules. Below are screenshots taken during this testing.

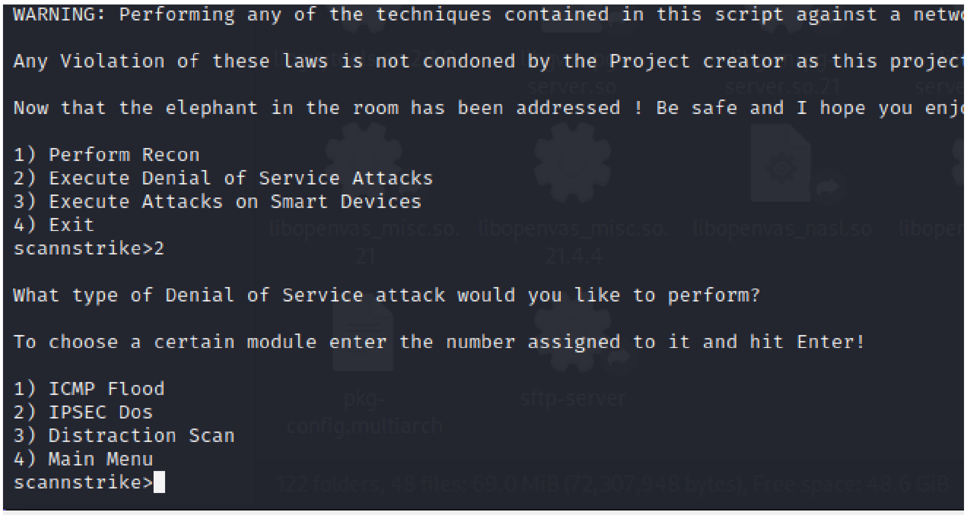
Main Menu of the ScanndStrike Bash Menu Script

This is the menu that users will see when they run the bash script and will allow them to navigate to the Network Reconnaissance, Denial of Service Attack and Ethical Hacking Menus that contain the required modules to perform various attacks on a target device or network.



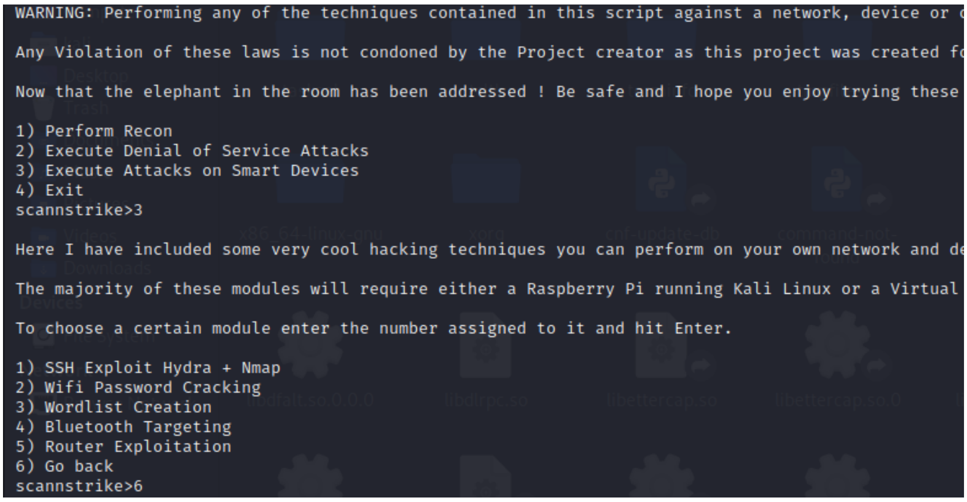
```
Welcome to scanndstrike!
Please report all bugs, improvements and suggestions to https://github.com/Gareth-hub
This software is only was created as part of a college project and is authorised for
This project was conducted in line with legal requirements and is intended to be shar
YOU are responsible for your own actions!

Basic Commands:
A module can be stopped using the Ctrl and C keys
To exit a Module and return to its menu hit the Enter or Return Key Twice


WARNING: Performing any of the techniques contained in this script against a network,

Any Violation of these laws is not condoned by the Project creator as this project wa

Now that the elephant in the room has been addressed ! Be safe and I hope you enjoy t

1) Perform Recon
2) Execute Denial of Service Attacks
3) Execute Attacks on Smart Devices
4) Exit
scannstrike>1

What type of Reconassaince would you like to conduct?

To choose a certain module enter the number assigned to it and press Enter !

1) Show IP
2) Quick Scan
3) Detailed Scan
4) DNS Recon
5) IP Sweep
6) Ping Sweep
7) Go back
scannstrike>7
```

Navigating to the Denial of Service Attack Menu



```
WARNING: Performing any of the techniques contained in this script against a netwo

Any Violation of these laws is not condoned by the Project creator as this project

Now that the elephant in the room has been addressed ! Be safe and I hope you enj

1) Perform Recon
2) Execute Denial of Service Attacks
3) Execute Attacks on Smart Devices
4) Exit
scannstrike>2

What type of Denial of Service attack would you like to perform?

To choose a certain module enter the number assigned to it and hit Enter!

1) ICMP Flood
2) IPSEC Dos
3) Distraction Scan
4) Main Menu
scannstrike>
```

Navigating to the Ethical Hacking Menu



```
WARNING: Performing any of the techniques contained in this script against a network, device or d

Any Violation of these laws is not condoned by the Project creator as this project was created fo

Now that the elephant in the room has been addressed ! Be safe and I hope you enjoy trying these

1) Perform Recon
2) Execute Denial of Service Attacks
3) Execute Attacks on Smart Devices
4) Exit
scannstrike>3

Here I have included some very cool hacking techniques you can perform on your own network and de

The majority of these modules will require either a Raspberry Pi running Kali Linux or a Virtual

To choose a certain module enter the number assigned to it and hit Enter.

1) SSH Exploit Hydra + Nmap
2) Wifi Password Cracking
3) Wordlist Creation
4) Bluetooth Targeting
5) Router Exploitation
6) Go back
scannstrike>6
```

2.6. Evaluation

This project was evaluated through the results outputted by each module run from the script, although the output provided by each module is dependent on the users target the functionality and automated processes do not change and are required to perform as expected in order to be considered successful. Through repeated testing of the bash menu script modules and the project, the results say that the project functions correctly based on its focus which is ethical hacking and smart devices. While this project does allow the user to perform a range of functions there are definitely steps that could be taken to increase this number and further scale this project into a larger Ethical Hacking Menu Script. However, since this project was created for educational and research purposes the current scale of the project and functionality meet the requirements for this project.

Scanndstrike Bash Menu Script Module Testing

Module Name	Number of Tests run	[S]uccess/[F]ailure	Tested on secondary Machine? Yes/No
IP Show	5	S	Yes
Quick Scan	5	S	Yes
Detailed Scan	5	S	Yes
Ip Sweep	5	S	Yes
Ping Sweep	5	S	Yes
DNS Recon	5	S	Yes
ICMP Flood	3	S	Yes
IPsec DOS	4	S	Yes
Distraction Scan	3	S	Yes
Wordlist Creation	3	S	Yes
SSH Exploit	5	S	Yes
Bluetooth Targeting	4	S	Yes
Router Exploitation	5	S	Yes
Wi-Fi Password Cracking	5	S	Yes

3.0 Conclusions

Advantages

The main advantage of this project is that it teaches users about the dangers of hacking and how easily their devices can be penetrated if not properly secured. If users are simply told this information the impact may not be as strong however, since this project allows them to actually test their own devices users may be shocked when seeing how vulnerable their devices are and how easily an unauthorized user can gain access without them knowing a thing. Another advantage of this project is that it shows users how simply security measures such as firewall maintenance, two factor authentication and disabling remote connections can rapidly decrease their risk of being a victim of a cyber-attack. Lastly, the final advantage of this project is that it requires user input and explains the processes to the user so they can understand what is occurring when they choose to run a module and they are actively involved in the process rather than just running modules without any notion as to what is happening when the module has been executed.

Disadvantages

The main disadvantage of this project is that it was only created for smart devices and networks the user is authorized to access certain modules could be used to attack websites or servers the user is not authorized to perform penetration tests against which could lead to trouble with the Law. Furthermore, since this project centres around the use of the bash menu script ‘scanndstrike’ if the repository on GitHub were to be deleted or the file corrupted for any reason users who had not yet downloaded the software would be unable to access the User Interface or engage in any attacks against their devices.

4.0 Further Development or Research

In order to further develop this project additional time and resources would be required, with this time and resources the project would concentrate on expanding this project from Ethical Hacking and Smart Technology to included websites too and would look to add modules that could be used for website penetration testing. Of course, with the given time and resources I would also look to create a vulnerable web application that users could use to practice their ethical hacking skills since not all users would have a website they would be authorized to use as a target. In summation, while happy with the project that has been created, given additional time and resources it would be interesting to scale the project to cover Website and webpage penetration testing and further educate users on how both sides of Ethical Hacking can be used with them.

5.0 References

References

Aircrack-ng.org, n.d. Aircrack-ng. *Aircrack-ng.*

Amigoscode, 2020. *Bash Script with Practical Examples | Full Course.* s.l.:s.n.

Freedman, M., 2022. 18 Ways to Secure Your Devices From Hackers. *BusinessNewsDaily,* 25 January.

Hira, Z., 2022. Shell Scripting for Beginners – How to Write Bash Scripts in Linux. *freeCodeCamp,* 31 March.

Kali.org, n.d. Hydra. *Kali.*

Kenlon, S., n.d. Getting started with Shell Scripting. *Opensource.com.*

Linuxtiwary.com, 2017. Firewall installation and configuration in Kali Linux. *Linuxtiwary,* 24 Novemeber.

Logsign Team, 2020. What is Ethical Hacking?. *Logsign,* 6 March.

nmap.org, n.d.

NullByte, 2018. *The Top 10 Things to Do After Installing Kali Linux on Your Computer [Tutorial].* s.l.:s.n.

NullByte, 2020. *Snoop on Bluetooth Devices Using Kali Linux [Tutorial].* s.l.:s.n.

Synopsys, n.d. What is Ethical Hacking?. *Synopsys.*

Techfigure, 2020. *Install NEW Kali Linux on a Raspberry Pi 4 - Mini Hacking Computer.* s.l.:s.n.

6.0 Appendices

6.1. Project Proposal

Project Proposal

Ethical Hacking vs Smart Technology

Bachelor of Science (Honours) in Computing

Cyber Security

Academic Year 2021/2022

Gareth Fitzgibbon

x18382503

x18382503@student.ncirl.ie

Contents

1.0 Objectives

Ethical hacking involves an unauthorized attempted to gain unauthorized access to an application, database, system, or data. Performing an ethical hack involves using the same methods as potential malicious hackers and is done to help identify any security flaws or vulnerabilities that a malicious hacker could exploit. Ethical hackers also known as 'White hats' will often reach out to an individual or organization once they have found these vulnerabilities and inform them how to fix their vulnerabilities. The aim of this project is to take on the role of an ethical hacker and investigate and examine smart technology to find vulnerabilities that can be exploited by malicious hackers. Once these vulnerabilities have been identified, the aim is exploit them using various hacking techniques until the smart device(s) have been successfully compromised and are now under the hacker's control. The purpose of this is to highlight how smart technology can be hacked and the dangers surrounding what a hacker can do once they have gained access to a user's device(s). Once a hacker has gained access to a user's device there are unlimited ways in which they can breach user details and compromise the device. Smart technology is on the rise and many new homes have incorporated some form of smart technology, whether that is an Alexa, smart tv, security camera, ring camera etc. According to an article on Nasdaq "people are actually buying homes today with an eye on the existing smart home tech that's already included" (Meredith Hirt Forbes Advisor, 2021) Since this technology is now becoming incorporated in our daily lives it is important to understand the risks associated with using this technology and how to prevent hackers from exploiting these vulnerabilities in these devices. Overall, the aim of this project is to successfully demonstrate the ability to compromise smart technology and from there how to successfully implement security protocols to protect the smart device from falling victim to a similar hack again.

2.0 Background

The reason this project is focusing on Smart Technologies is because we are on the cusp of a paradigm shift in terms of adopting smart technology without fully understanding the risks associated with it. From a cyber security standpoint, deciphering what is possible to ethically hack makes this interesting subject matter. Hacking has always been an interesting topic and today everything is becoming more reliant on smart technology and by combining the two and the idea to focus hacking smart technologies for the project was created. The project will show how smart tech can be hacked and how to prevent these hacks so other users will know how they can protect their devices and avoid being exploited by hackers. In order to meet the goals for the project it is important to determine the best method for hacking into a smart device and then putting this method into practice as well as implementing security measures afterwards to demonstrate how to stop the hack from occurring again. Determining the best method of hacking smart devices can be achieved by researching common methods and testing demonstrations and tutorials that are available for those that are new to ethical hacking

.

3.0 State of the Art

Current research suggests there is quite a few hacking forums online and YouTube channels that focus on hacking that highlight different hacking techniques. Although these channels/forums do go through ways to create your own method of hacking into smart devices, these methods are created for personal use as they are not really something that can be easily shared across devices. Most of these YouTube channels and online forums are created for educational purposes and do not supply you with any code but rather provide you with the tools and knowledge so that you can create your own code and complete the process they are demonstrating your own way. There may be some types of hacking applications online but there is no definitive method for hacking smart technologies and therefore this makes all smart device hacks unique as all are created by individuals with different ideas and thought processes. This enterprise aims to stand out from the rest as it is not something that has been looked at recently. Since there are many different methods online it provides an opportunity to test some of these to see which is best suited to the project. Research shows that since covid hit there has been a massive spike in cyber-attacks and hacking exploits as well as a rise in smart technology purchases and a spike in the number of people working from home using personal and company technology. According to an article published by TitanFile “Cybercrime is up 600% due to the COVID-19 pandemic” and “Remote work has increased the average cost of a data breach by $137,000.” (TitanFile, 2021). Therefore, this project stands out as it will be focusing on a problem that has been on the rise and will offer smart technology users an opportunity to create a more secure environment and reduce their risk of being victims of a hacking experience.

4.0 Technical Approach

After spending some time researching the possible development approaches, we have decided to use the Scrum approach for the project. Scrum is an agile development methodology used in the development of software and is adaptable, flexible, fast and encourages teams to learn through experiences and to self-organize while working on a problem, using past successes and failures as a learning experience. Agile is an interactive approach to software development and project management that focuses on delivering work in small fast increments with fewer issues. The Scrum method tends to work best for experienced and disciplined individuals or small teams as it requires a lot of self-management and self-organization. By using the Scrum method end goals can be broken down into smaller goals at the beginning of the project and can be worked through using sprints (fixed length iterations). Frequent meetings are also a critical part of the scrum approach as it is beneficial to perform tests on the project being developed to gather useful feedback and to see what changes could and should be made. To identify the requirements for this project firstly a project plan will need to be created and once the plan has been created, then through the process of brainstorming we can determine the possible approach to the project and the potential problems with this approach. Once the project requirements have been chosen, we can then begin to review and analyse them against the goals of the project and once these requirements have been finalized, we must work to manage these requirements throughout the project to ensure that these activities are being worked on and that will help us meet the requirement and to assess new requirements that emerge as a result of testing and/or quality checks. Once the requirement's gathering stage is done, the next step is to start determining the high-level milestones and creating a delivery plan with realistic timelines. Starting with high level milestones will provide a broad view of what the project entails, risks and assumptions to account for, skills required to deliver the project and probable resource and time requirements. Once the high-level milestones have been decided they can be broken down into parent, sub, and sub-sub tasks. By breaking down the tasks this will cover all aspects of task management for the project which entails:

- Planning task assignments
- Outlining/Classifying the tasks
- Creating estimated hours
- Identifying the inter dependencies in tasks
- Establishing the task linkages/relationships
- Visualizing the schedule for the overall project

The benefits of doing this are that resource and skill requirements become clear, progress tracking is easier, the true deliverables and their priority become clear, there is room for course correction and assumptions and risks can be verified and updated as the project progresses.

In summation this project will be developed using the Scrum development method as it is flexible, fast and encourages teams to learn through experiences and to self-organize while working on a problem, using past successes and failures as a learning experience. This method tends to work best for experienced and disciplined individuals or small teams as it requires a lot of self-management and self-organization. In order to gather the project requirements a project plan will be created, and the possible approaches will be determined, the requirements needed for these approaches can be reviewed to determine which of these requirements will work best and help achieve the project goal. After the requirements have been gathered the breakdown process will occur starting with the high-level milestones and working down from there to create manageable tasks and this will result in an estimated project delivery time.

5.0 Technical Details

The main operating system being considered for this project is Kali Linux and Command Line Interface (CMD) will also be used. These operating systems use C language and libraries. C is a general-purpose programming language that is ideal for the development of portable applications or firmware, it is a high-level programming language and was originally developed in the early years of the 1970's. While C can be harder to learn than some other programming languages (e.g., Java), it can do more and function faster than other languages due to its closeness to machine code. While all these operating systems use C and seem like suitable choices for my project Kali Linux seems to be the most utilised when it comes to hacking, as the operating system (OS) is specifically designed to best suit the needs of penetration testers and network analysts. Kali Linux comes with a wide range of pre-installed tools which can be extremely useful for ethical hacking with many ethical hackers calling Kali an ethical hackers "Swiss-Knife". Nmap is one of these preinstalled tools that can be used in the Linux command line for network exploring and for security checking, using Nmap allows you to scan the network you are connected to and discover what devices are connected to your network as well as a wide range of information about the devices connected to your network such as the operating services that the hosts are on. Nmap is a common tool used by cybersecurity professionals and hackers as it reveals information about your network in real time. Nmap is commonly used by hacker's scan networks for vulnerabilities that they can exploit such as open or uncontrolled ports.

To realise the project aim using a Raspberry Pi is under consideration as it can be used either to aid hacking a smart device or it can be programmed to act as the device the attacks will be targeted at and will then have security measures added to it in order to prevent the attack from occurring again. A Raspberry Pi is a tiny computer about the size of a stack of playing cards that can be plugged into a computer monitor or tv and uses something called 'a system on a chip' which integrated the GPU and CPU in a single integrated circuit with USB ports, RAM and other components such as a HDMI port soldered onto the board, making it an all-in-one package. Raspberry Pi's are capable minicomputers that can be programmed to do a wide variety of things using Python or Scratch. While using a Raspberry Pi may be a new challenge with this project, some thorough research has resulted in the discovery of various resources online including YouTube channels/videos and documentation that will aid in the initial use and programming of the Raspberry Pi. Python is one of the most used languages for programming Raspberry Pi's and is extensively used in the field of hacking for exploit writing and plays a vital role in the creation of malicious programs, hacking scripts and exploits. Raspberry Pi's are commonly programmed to be used as tools to aid hackers and given their small size they are easy hidden and provide hackers the opportunity to carry out attacks from various locations without much equipment or preparation. Raspberry Pi's can also be programmed to function as various smart devices such as smart tv's, Bluetooth speakers, cameras, Wi-Fi routers etc. They have a wide variety of possible uses and either way would be extremely useful for this project.

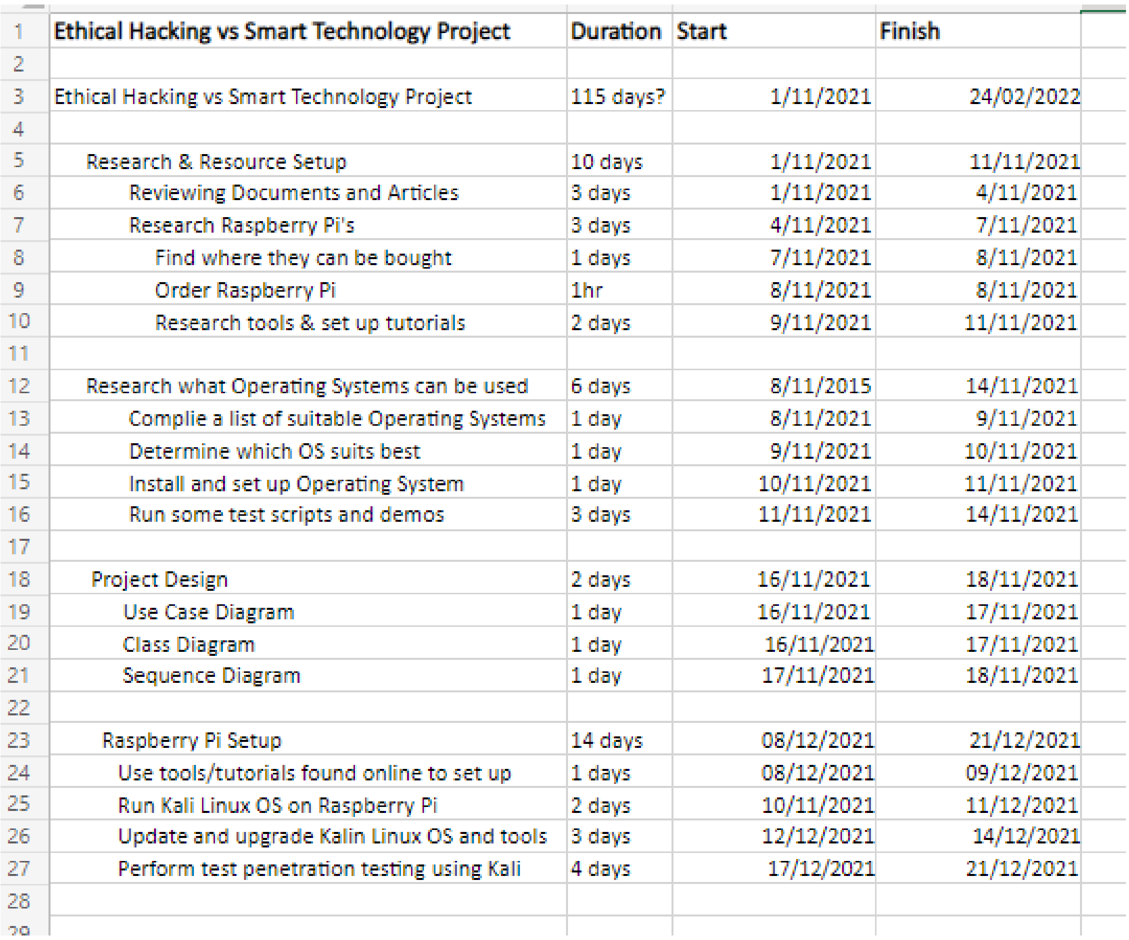
In summation the approach currently under consideration involves the use of Kali Linux, CMD (both of which use C programming language), Nmap which is one of the many useful hacking tools that comes with Kali Linux and a Raspberry Pi (which will be programmed using Python). As the project progresses the approach will be fluid but at this time this is the current approach that is under consideration and is being researched.

6.0 Special Resources Required

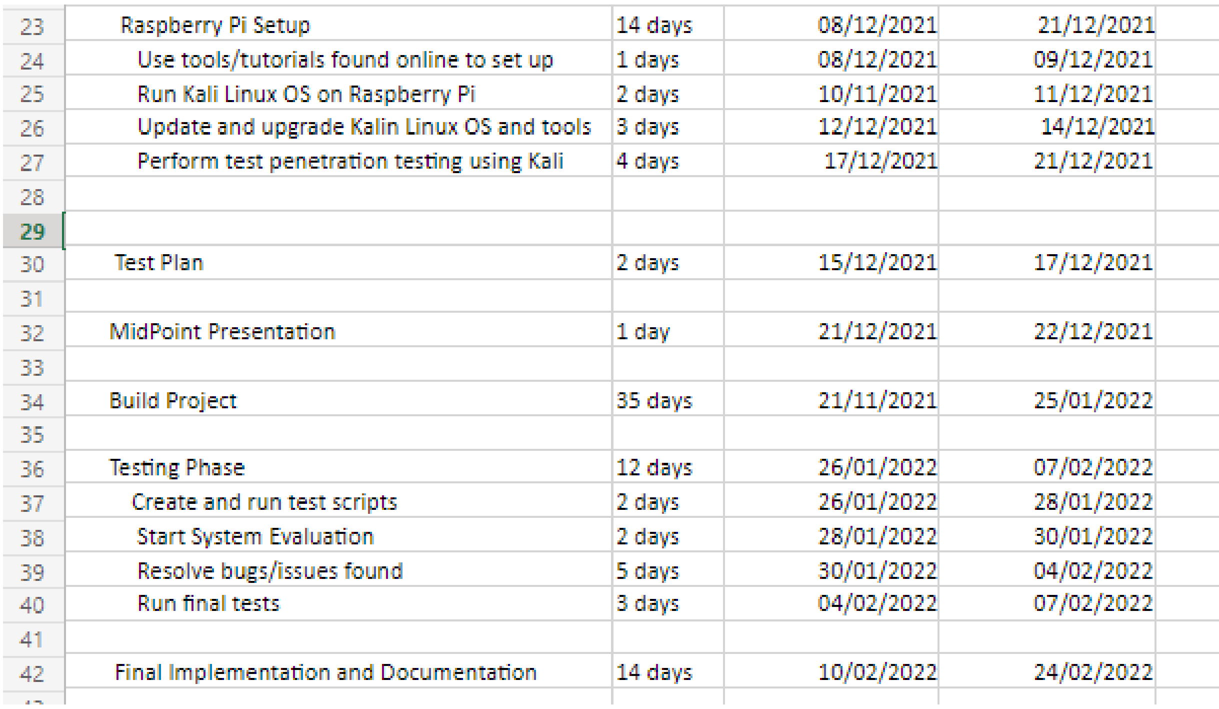
Based on the current planned approach for the project Raspberry Pi kit is required to meet the project aims. This is a special resource as it may not be something that can be gotten easily or for free as it will likely need to be ordered from amazon or another site that would sell the Raspberry Pi Kit with all the pieces that are required. A Raspberry Pi can be useful for the project in two ways, firstly it can be set up and programmed with Python to act as a portable hacking device and can be used to help orchestrate a series of attacks on the chosen target device(s) or alternatively the Raspberry Pi can be programmed to act as the smart device that will be targeted, whether that means programming it to be a Bluetooth Speaker or Smart Tv or one of the many other smart devices that are available. Then once the Raspberry Pi has successfully been programmed to function as a smart device, it will be possible to demonstrate how to perform the hack on the device before demonstrating how to implement certain security features that will help prevent hacks of that nature from occurring again. Once these security features have been implemented if the hack is attempted on the device again, it should result in failure. So, although it may be a special resource, it seems that the benefits of getting the Raspberry Pi for the project will outweigh the potential cost involved.

7.0 Project Plan

Below you will see the latest version of the project plan. This plan has been created to allow for some flexibility throughout the project and to act as a guide while working on the project. If this plan is followed correctly and allows for changes throughout the project, there should be no issues with getting the project complete and delivered with the desired outputs on time.



1	Ethical Hacking vs Smart Technology Project	Duration	Start	Finish
2				
3	Ethical Hacking vs Smart Technology Project	115 days?	1/11/2021	24/02/2022
4				
5	Research & Resource Setup	10 days	1/11/2021	11/11/2021
6	Reviewing Documents and Articles	3 days	1/11/2021	4/11/2021
7	Research Raspberry Pi's	3 days	4/11/2021	7/11/2021
8	Find where they can be bought	1 days	7/11/2021	8/11/2021
9	Order Raspberry Pi	1hr	8/11/2021	8/11/2021
10	Research tools & set up tutorials	2 days	9/11/2021	11/11/2021
11				
12	Research what Operating Systems can be used	6 days	8/11/2015	14/11/2021
13	Complie a list of suitable Operating Systems	1 day	8/11/2021	9/11/2021
14	Determine which OS suits best	1 day	9/11/2021	10/11/2021
15	Install and set up Operating System	1 day	10/11/2021	11/11/2021
16	Run some test scripts and demos	3 days	11/11/2021	14/11/2021
17				
18	Project Design	2 days	16/11/2021	18/11/2021
19	Use Case Diagram	1 day	16/11/2021	17/11/2021
20	Class Diagram	1 day	16/11/2021	17/11/2021
21	Sequence Diagram	1 day	17/11/2021	18/11/2021
22				
23	Raspberry Pi Setup	14 days	08/12/2021	21/12/2021
24	Use tools/tutorials found online to set up	1 days	08/12/2021	09/12/2021
25	Run Kali Linux OS on Raspberry Pi	2 days	10/11/2021	11/12/2021
26	Update and upgrade Kalin Linux OS and tools	3 days	12/12/2021	14/12/2021
27	Perform test penetration testing using Kali	4 days	17/12/2021	21/12/2021
28				



23	Raspberry Pi Setup	14 days	08/12/2021	21/12/2021
24	Use tools/tutorials found online to set up	1 days	08/12/2021	09/12/2021
25	Run Kali Linux OS on Raspberry Pi	2 days	10/11/2021	11/12/2021
26	Update and upgrade Kalin Linux OS and tools	3 days	12/12/2021	14/12/2021
27	Perform test penetration testing using Kali	4 days	17/12/2021	21/12/2021
28				
29				
30	Test Plan	2 days	15/12/2021	17/12/2021
31				
32	MidPoint Presentation	1 day	21/12/2021	22/12/2021
33				
34	Build Project	35 days	21/11/2021	25/01/2022
35				
36	Testing Phase	12 days	26/01/2022	07/02/2022
37	Create and run test scripts	2 days	26/01/2022	28/01/2022
38	Start System Evaluation	2 days	28/01/2022	30/01/2022
39	Resolve bugs/issues found	5 days	30/01/2022	04/02/2022
40	Run final tests	3 days	04/02/2022	07/02/2022
41				
42	Final Implementation and Documentation	14 days	10/02/2022	24/02/2022

8.0 Testing

System evaluation is the process of comparing the final system against its initial performance goals and performing ongoing testing in order to see if the system continues to meet those goals. In order to evaluate the system, it is important to first have a clear idea of the issue you are looking to investigate. Once this is done the next step is to look at the evidence, this means identifying how similar projects have worked in the past and understanding how they work in order to plan the project effectively. Logic models are a useful next step that can be created to display the ultimate goals of a project and be used as guide through the project. Logic models can be used display the resources that will be required to meet the short, medium and long-term goals of the project. Once a logic model has been created it can then be used to identify indicators that will test if the project is working based on the logic model. The last step involved in system evaluation is to analyse the data to test whether the project worked in accordance with the logic module and to assess how well the projects aims were met and how these aims may have changed throughout the project. One the main aims of this project is to take on the role of an ethical hacker and investigate and examine smart technology to find vulnerabilities that can be exploited by hackers, this will have to be tested by attempting to hack into a smart device and if the project is working in accordance with the logic model, then this process should be successful. Once this has been tested to a satisfactory level the evaluation process can continue and the next project deliverable can be tested. The next main aim of this project is to implement security features to prevent smart devices falling victim to these hacks again and this will have to be tested by attempting to hack into a smart device which has had security measures added and if the project is working in accordance with the logic model, then the hacker should be unable to find any security features that they could exploit to gain access to the device rendering the hack unsuccessful and the process of implementing the security features successful when compared to the logic model.

6.2. Reflective Journals

Supervision & Reflection Template

Student Name	Gareth Fitzgibbon
Student Number	x18382503
Course	Bachelor of Science (Hons) in Computing Specializing in Cybersecurity

Month: October

What?

Reflect on what has happened in your project this month?

This month I was brainstorming ideas for my software project. Once I had a couple of rough ideas, I created a list a slowly whittled down through the list to my best 3 ideas. Before doing further research into my potential project ideas, I first checked NCI’s 2021 Project Showcase to ensure that I was not looking into something that had already been done, after doing this I was down to two Ideas, Web Scraping was one of these ideas, and there was a lot of resources available online that could help me with this idea, but I was looking for something more challenging. Ultimately, after a lot of research and thinking I chose to focus on Smart Technologies for my Software Project. The reason that I chose to focus on Smart Technologies is because it is something new and something quite different compared to what I have worked on in the past. I feel like as a cyber security student it is an interesting topic and although it will be quite challenging, I am looking forward to working on it and getting to learn some new things. When I discussed the idea with my Security Principles lecturer, he seemed to think it was a good idea and as someone with experience in the world of hacking he told me that even though I would be very new to hacking, my idea was very feasible, and he was helpful enough to send me on some links that would be useful to my research and help me with my project. The project itself will revolve around hacking which is something I am very much new to and will be learning as I go.

So What?

Consider what that meant for your project progress. What were your successes? What challenges still remain?

Although I am sure we will be looking at some methods of ethical hacking throughout my next semester I will need to go off on my own before then and learn how to hack ethically. So far, I have come across some interesting videos/channels on YouTube related to the world of hacking though it has taken some time to whittle them down to a few useful resources. I am still currently performing research and learning about how to start hacking before I dive into the code. Although I have not yet started the coding portion of the project, yet I am not too worried as based on what my friends have told me that we are all in a comparable situation, although this provides some comfort, I am still feeling a bit nervous about the project overall as it revolves around something I have never tried before! Currently since I am still waiting for approval since I sent my project pitch I have decided just to stick to researching and trying to determine some achievable goals for this project. Once I have gotten approval for my project idea, I plan to choose which method(s) I to use to reach my goals for this project, but I know this will be a process of trial and error. When I first looked at the idea for this project, I did not feel overly confident, however after spending some time researching and after talking to some of my lecturers & colleagues, I feel more confident in the idea & although it seems different from some of my fellow students' ideas, and I think that it is a good thing. The

ideas of my colleagues will of course differ across the board as this project must relate to your chosen specialization and my colleagues are from a variety of specializations, now although this will affect their overall project I feel like the overall work and effort required will be the same across the board. I think that by choosing to undertake this project I am taking a risk by investigating and learning a new skill and I am hopeful that my risk is worth the reward. Currently I am still in my research/planning stage, however, I will soon need to start working on the programming side of this project as I am certain it will not be a short or easy challenge. I have gotten some tutorials bookmarked and some plans drawn up, but this may change over the course of the project. For next month I am planning to get to work on the coding portion of the project and practicing some demos with some different applications such as Kali & Linux to see which I am most comfortable working with, and which is best suited for my needs. I have created my project plans with a level of flexibility as I know my plans for next month might differ once the work begins next month.
Now What? What can you do to address outstanding challenges? In conclusion, most of the work that I have been doing this month has been research based and revolved around creating a plan for my project over the next few months. Initially I was quite nervous about the project as it is not something I have ever investigated or worked on before and does seem quite difficult and challenging topic for my project, however after spending the last few weeks doing my research and having spoken to some lecturers from NCI (National College of Ireland) as well as some colleagues and hearing about their projects and the challenges they will also face, I feel a bit more confident in my project and in myself. I have my plan created for next month and if I do not stray too far from that I think I will be able to achieve my goals for this project and produce the desired outcome. As long as I continue to work on researching for the project and commit to testing, I should not be capable of addressing any challenges that arise throughout the project.

Student Signature	Gareth Fitzgibbon

Supervision & Reflection Template

Student Name	Gareth Fitzgibbon
Student Number	X18382503
Course	Bachelor of Science (Hons) in Computing Specializing in Cybersecurity

Month: November

What?

Reflect on what has happened in your project this month?

This month I was conducting some additional research for my project. This involved reading articles/online journals regarding hacking and ethical hacking as well as watching multiple videos on sites like YouTube for examples of ethical hacking as well as tips for beginner hackers. I have also conducted some research on Raspberry Pi’s and saved some resources that I think will be useful for programming my Raspberry Pi. This month I spent some time comparing prices of Raspberry Pi kits and researching these kits and their components to see which type of Raspberry Pi kit would best suit my project needs. After a lot of time, I found a suitable (and affordable) Raspberry Pi kit on Amazon and ordered it on the 18th of November. Unfortunately, there was a problem with the sellers shipping method as the Raspberry Pi Kit did not arrive and Amazon refunded the purchase. Since then, I have ordered another kit which is due to arrive December 1st

So What?

Consider what that meant for your project progress. What were your successes? What challenges still remain?

. Although this means I will be starting to work on the Raspberry Pi later than previously planned. It allows me to work on the project documentation in the meantime and to practice with a few more tutorials before working on the Raspberry Pi itself. For the documentation I began by downloading the Technical Report Template from Moodle and going through each of the sections and making some scratch notes on what would be required for each of these sections. Once I had done this, I was able to separate the sections of the report I would be able to complete at various stages in the Project and the sections I could begin to undertake before working on the Raspberry Pi (when it arrives). Following this I then began to work on my project Documentation and will continue to do so up until my Raspberry Pi arrives and after it arrives, and I have been able to do some work on it and have been able to move towards a functional prototype for my Mid-Point Presentation.

Now What?

What can you do to address outstanding challenges?

In conclusion, most of the work that I have been doing this month has been research based and revolved around creating a plan for my documentation while waiting for the delivery of my Raspberry Pi Kit. While I

would have liked to have originally started working on my prototype sooner, the delivery setbacks have allowed me to focus more on the project documentation and research and I feel like this will benefit me overall. In order to create a working prototype, I plan to implement what I have learned from my research and use the resources I have made note of to further aid me in the prototype creation and testing before the Mid-Point presentation is due. As long as there are no further shipping issues and I follow the plan I have created for the project documentation I think I will be able to achieve my goals for the Mid-Point presentation and produce a thorough presentation and a functional prototype.

Student Signature	Gareth Fitzgibbon

Supervision & Reflection Template

Student Name	Gareth Fitzgibbon
Student Number	X18382503
Course	Bachelor of Science (Hons) in Computing Specializing in Cybersecurity

Month: December

What? Reflect on what has happened in your project this month? This month I was working on my Project prototype the Mid-Point Presentation, this involved practicing using Kali Linux's password cracking tools and perform a password attack to crack my own Wi-Fi routers password. I was also working on the technical report for the Mid-Point Presentation and updating my project plan to reflect the changes that were required due to the Raspberry Pi arriving later than expected. Once the Raspberry Pi arrived on December 8th, I began the steps involved in setting up the Kali Linux OS (Operating System) on the Raspberry Pi. Once Kali Linux was successfully running, I updated and upgraded the software before performing a scan for networks nearby. Once I found my own network, I began the process of attacking my own network, in order to do this, I first identified my Router ID and scanned it to see what devices are connected to its Wi-Fi. Once I had identified devices on the network, I was able to perform a form of DDOS (distributed denial of service) attack on network and capture a WPA handshake (this is what happens when a device is disconnected from the router and attempts to reconnect). Once I had done this successfully, I recorded the prototype and began to work on my Mid-Point Presentation slides.
So What? Consider what that meant for your project progress. What were your successes? What challenges still remain?

While waiting for my Raspberry Pi to arrive I was able to start working on my Technical Report for the project and practice using Kali Linux OS (Operating System) tools on Desktop. Once the Raspberry Pi finally arrived, I was able to successfully install and run Kali Linux OS and use Kali’s tools to practice Wi-Fi and password attacks. The challenge of hacking into a smart device still remains, however I have been able to crack my WIFI's password and identify smart devices connected to my network.

Now What?

What can you do to address outstanding challenges?

In conclusion, most of the work that I have been doing this month has revolved around the documentation required for the Mid-Point Presentation and creating a functional project prototype. While I would have liked to have originally started working on my prototype sooner, the delivery setbacks have allowed me to focus more on the project documentation and research so when it finally arrived, I was able to dive straight into prototyping and testing. Now having completed the requirements for the Mid-Point Presentation I still have to successfully penetrate and then protect a smart device. Now that I have Kali Linux functioning on the Raspberry Pi I can continue to perform known penetration testing methods in attempt to successfully penetrate a smart device.

Student Signature	Gareth Fitzgibbon

Supervision & Reflection Template

Student Name	Gareth Fitzgibbon
Student Number	X18382503
Course	Bachelor of Science (Hons) in Computing Specializing in Cybersecurity

Month: January

What?

Reflect on what has happened in your project this month?

This month I continued to do some research for my project that may help with working on the Raspberry Pi remotely and creating a better SSH (Secure Shell) connection. This involved researching different types of software such as VirtualBox which allows you to run Kali Linux on your device and connect to a device remotely that is running a Kali Linux OS. I also took some time to review my project plan and researched some ideas I had over Christmas that I thought may work well with or improve my project. I have been analyzing the documentation I have worked on so far as well as the documents that I need to complete for the next stage of the project

So What?

Consider what that meant for your project progress. What were your successes? What challenges still remain?

The challenge of hacking into a smart device remains, however I have been able to crack my WIFI's password and identify smart devices connected to my network. I have discovered some methods in my research that I am currently putting to the test and that will hopefully result in the successful penetration of a smart device. As far as project progress goes, I think I am still on track with my project plan and completion should not be an issue. Currently my focus is switched to the project documentation as I would like to have it finished as soon as possible which will make for easier editing and changes once the project is completed

Now What?

What can you do to address outstanding challenges?

Most of the work that I have been doing this month has revolved around the documentation required for the project and researching some new penetration methods using Kali's tools. Since I have Kali Linux functioning on the Raspberry Pi I can continue to perform known penetration testing methods in attempt to successfully penetrate a smart device. I will also continue to work on the project documentation updating it and making changes as the project changes throughout the process. In conclusion, I will continue to work on the project documentation and researching penetration methods that will be helpful to my project.

Student Signature	Gareth Fitzgibbon

Supervision & Reflection Template

Student Name	Gareth Fitzgibbon
Student Number	X18382503
Course	Bachelor of Science (Hons) in Computing Specializing in Cybersecurity

Month: February

What?

Reflect on what has happened in your project this month?

Thia month I have been revising my project plan and testing some interactive scripts that may be suitable for my project. This has involved watching YouTube videos, reading articles, and writing/running these scripts on Kali Linux. I have also been following my Penetration Testing labs which have been focused on using Kali Linux's tools and performing various attacks. With upcoming CA's and other project work I have been mainly working on making the project more interactive and ensuring that all my required documentation is complete. This included completing my project showcase profile which has now met the requirements to be approved and locked pending any future changes made by me.

So What?

Consider what that meant for your project progress. What were your successes? What challenges still remain?

As far as project progress goes, I think I am still on track with my project plan and completion should not be an issue. My focus this month was the project documentation as I would like to have it finished as soon as possible, which will make for easier editing and changes once the project is completed. Although having gotten feedback from my project supervisor I have been researching and testing scripts that I can implement to make the project more interactive. I am still in the process of determining which type of scripts would be best suited regarding adding interactive scripts to my project. Therefore, the challenge remains to add the chosen interactive features to my project and to perform other methods of penetration testing on smart devices.

Now What?

What can you do to address outstanding challenges?

This coming month I am planning to continue working on my project documentation as well as deciding which interactive scripts I will be using going forward. I will also be doing some further research into security measures that can be taken once a smart device has been successfully penetrated. This month will be quite busy with other Modules CA's coming up shortly, therefore my focus will be more directed to revision for my other modules. However, I do have a planned workload for the project this month that will keep me on track with my project plan. In conclusion, I will continue to work on the project documentation and researching penetration methods and interactive scripts that will be helpful to my project.

Student Signature	Gareth Fitzgibbon

Supervision & Reflection Template

Student Name	Gareth Fitzgibbon
Student Number	X18382503
Course	Bachelor of Science (Hons) in Computing Specializing in Cybersecurity

Month: March

What?

Reflect on what has happened in your project this month?

This month I have been more focused on my other modules rather than my project, this is due to ongoing CA's and TABA's which are due within the first two weeks of April. Although I have diverted some attention away from my project, for those reasons, I still have been working on it and thinking of ways to improve the project based on feedback from my project supervisor. I have spent a lot of time performing research on ways to add some more interactive features to my project and testing these ideas in accordance with my project

plan. However, I am still in this process as I would like to do thorough checks before ruling anything out completely. I have also kept up with my project documentation and made changes where applicable.	
So What? Consider what that meant for your project progress. What were your successes? What challenges still remain? As far as project progress goes, I think I am still on track with my project plan and completion should not be an issue. My focus this month was to continue researching and testing features for the project based on the feedback from my project supervisor in order to improve the overall quality of the project. Though there have been some successes with the project I am still working on getting things to run cohesively and naturally this will take time. Although I have also been focusing on my other modules and their CA's/TABA's this month I am happy with the work and progress I have made on the project so far. Therefore, the challenge remains to add the chosen interactive features to my project and to perform other methods of penetration testing on smart devices.	
Now What? What can you do to address outstanding challenges? This coming month I am planning to continue working on my project documentation as well as working on implementing interactive scripts/features to my project. I will also be doing some further research into security measures that can be taken once a smart device has been successfully penetrated. This month I will be concluding my other modules which will give me a lot more time to spend on the project. I am currently revising my project plan and creating a plan that works best for me and will allow me to efficiently spend time working on the project In conclusion, I will continue to work on the project documentation and researching penetration methods and interactive scripts that will be helpful to my project.	
Student Signature	Gareth Fitzgibbon

6.3. Other materials used