**Assignment 2**

**DPI 914**

**Lab 7**

**By: Buwaneka Hettiarachchi**

**SID: 104376165**

Table of Contents

[**Introduction** 3](#_Toc79445445)

[**Contract** 3](#_Toc79445446)

[**Permissions and restrictions** 3](#_Toc79445447)

[**Goals and Expectations** 3](#_Toc79445448)

[**Scenario Creation** 3](#_Toc79445449)

[**Individuals that deal with QED Inc.** 3](#_Toc79445450)

[**Individual 1** 3](#_Toc79445451)

[**Individual 2** 4](#_Toc79445452)

[**Individuals that work at QED Inc.** 4](#_Toc79445453)

[**Individual 1** 4](#_Toc79445454)

[**Individual 2** 4](#_Toc79445455)

[**Plan** 5](#_Toc79445456)

[**Bait** 5](#_Toc79445457)

[**Hook** 5](#_Toc79445458)

[**Diagram** 5](#_Toc79445459)

[**Attack Description** 6](#_Toc79445460)

[**Virtual Machines** 6](#_Toc79445461)

[**Hook** 6](#_Toc79445462)

[**Test** 7](#_Toc79445463)

[**Conclusion** 9](#_Toc79445464)

[Figure 1: The Diagram on how the attack will take place 5](#_Toc79446985)

[Figure 2: Black Eye tool is used to create the custom phishing website 6](#_Toc79446986)

[Figure 3: Mail server created to send the phishing Emails 7](#_Toc79446987)

[Figure 4: Attacker sent the Email to the Target Machine 7](#_Toc79446988)

[Figure 5: The Fake site will pop up 8](#_Toc79446989)

[Figure 6: Victim credentials shown in the attacker machine 8](#_Toc79446990)

# **Introduction**

This assignment focuses on performing a social engineering attack on the QED inc. The CEO of QED is concerned that the company has is a risk of being attacked by Social Engineering. Our team is hired to perform an actual Social Engineering attack on the company. This report will explain the step-by-step methods on how we are able to perform a successful Social Engineering attack on our target. The report goes through the following concepts.

1. Contract: The contract follows information on what the team is supposed to do, what they are not supposed to do and what are the expectations and goals of the CEO.
2. Scenario: The scenario is used to get the attention of the victim; this step will consist of our finding the right candidates as attacker and the targeted personnel for the attack.
3. Plan: The plan is used to preparate the Social Engineering attack on the victims, and we would use the information generated the scenario method and plan out the attack.
4. Attack Description: The Attack Description will be done in the Virtual machines and shown in a video demonstration.

# **Contract**

## **Permissions and restrictions**

* The team has the permission to search through the public information on their targets, but they do not have the permission to find any private information that are not available to the public (Financial Documents etc.)
* The team must solely work remotely and do not have any physical access to the company because that mean invasion of privacy (e.g.: Physical Social Engineering).
* The team has the permission to go with the phishing attack, but they are not permitted to do any other attack that might hinder the servers and the working environment of the company.

## **Goals and Expectations**

* The goal of this contract is for the Social Engineering attack to successful so that the CEO of QED can raise awareness amongst the working staff on the dangers of Social Engineering.

# **Scenario Creation**

## **Individuals that deal with QED Inc.**

### **Individual 1**

**Role Title:** Team Leader

**Service Supplied:** The team leader has the main priority on taking care of the network facilities and whether they are running smoothly, and he also is in charge of the whole contract and ensure that it is running without issues.

**Access:** The Team leader has the access to all the tools utensils that are used for the attack.

**Character:** The team leader is in charge of many duties throughout the contract, he must ensure that each and every member of the team are performing to the target, and it is important that he keeps a regular log so that if any problem arises it is easier to deal with. So, his character is mostly busy.

**Back story:** The bait will be sent to the Account Manager and steal his credentials to gather information of the recent clients they have been working. The Attack can be as simple as sending an E-mail that tells him to validate his user credentials, but the E-mail will have link that forwards the target into the phishing website which will gather their user information.

### **Individual 2**

**Role Title:** Security Researcher

**Service Supplied:** The security researcher keeps up-to date information on all the threats and risks in the IT environment. He can provide services that are new and updated.

**Access:** He should have access to Internet so that he can get information on the latest threats and attacks happening around. He also needs access to various platforms and software, so that he can test these new attacks on them.

**Character:** He should constantly be alerted on new technologies, and he needs to be up-to date with all of them, making him a busy individual.

**Back story:** Can send an Email, that will have a malicious code hidden in it, the bait will be the Senior Network Administrator of the company because then the security researcher can identify the specific clients that are using the specific network in the company.

## **Individuals that work at QED Inc.**

### **Individual 1**

**Title:** SeniorNetwork Administrator

**Role:** The Network Administrators are responsible in the maintaining the network of the organization and try to implement a Network hardening method into the system.

**Access:** They have access to all network devices in the company, these can be devices such as routers, switches, and cable management etc.

**Reason:** Because, they have all information of the specific user who use the company sites, by intercepting the Network Admin, the security researcher can ideas of the key employees working in the company.

### **Individual 2**

**Title:** Account Manager

**Role:** The account manager is in charge of dealing with the communication and dealing with the company clients and also responsible for the management of the company sales.

**Access:** Should have information on clients and other information such as yearly sales.

**Reason:** Because The Account Manager has all the information on the clients, which might be important.

# **Plan**

## **Bait**

The Bait in this Social Engineering attack is to send an Email to the target letting him know that his account is not properly verifies by the mail server. So, the attacker uses a fake URL to the target letting him know that he should provide his account details so that his Email will be “verified”. To show a sense urgency, we are informing our target that if he failed to do so, his user account will be deactivated from the system, furthermore, we have added a time limit so that the target will give more attention to the Email

## **Hook**

The hook in this attack is that he is not a verified Email user, this means that if he fails to make his user account verified to the company, he will lose his access to his account. This creates an urgency in his situation because his user account has important information that is confidential to the public. So, he will immediately act on it and supply his account information to the given URL.

## **Diagram**

**![Diagram

Description automatically generated with low confidence]()**

Figure : The Diagram on how the attack will take place

# **Attack Description**

## **Virtual Machines**

* Attacker Machine: Used a Kali Linux virtual machine and installed the black eye GIT repository to make custom Phishing websites. The Machine has the ability to use the mail server.
* Target Machine: Ubuntu Virtual Machine that has the ability to use the mail server.
* Mail Server: Ubuntu Virtual Machine that has Mail cow UI installed through the use of Docker.
* Server: Ubuntu Virtual Machine as the webserver.

## **Hook**

To create the hook, we needed the Black eye tool from the GIT repository. Then we create a custom phishing website, the figure below shows the link that is highlighted in white.

Graphical user interface

Description automatically generated

Figure : Black Eye tool is used to create the custom phishing website

A screenshot of a computer

Description automatically generated

Figure : Mail server created to send the phishing Emails

## **Test**

Graphical user interface, text, application

Description automatically generated

Figure : Attacker sent the Email to the Target Machine

A screenshot of a computer

Description automatically generated

Figure : The Fake site will pop up

A screenshot of a computer

Description automatically generated

Figure : Victim credentials shown in the attacker machine

First, the attacker sends the email to the victim using the mail server, in the email, the attacker has given all the information such the reasoning for the email and the link that will forward the target to the fake website. Then the target will provide their user credentials thinking that they will be verified when they click on the submit button. Figure 6 shows all the user credential information such as the target’s account and their password, which is Jason\_123.

# **Conclusion**

In conclusion, this assignment discusses about the practicality of Social Engineering attacks, as shown through the virtual machines. This assignment is fully based on our team following the regulations given to us by the CEO of QED Inc. and from the scenarios we generated, we created one of them and did a practical method in the virtual machines. Furthermore, this assignment further enhances our knowledge on Social Engineering.