Ethical Hacking Lab

Domain:

Social Engineering

Focus on Tools:

1)SET

Made by:

M Sameer Malik

LAB Contents

[Lab - Explore the Social Engineer Toolkit (SET) 3](#_Toc203368795)

[Objectives 3](#_Toc203368796)

[Background / Scenario 3](#_Toc203368797)

[Required Resources 3](#_Toc203368798)

[Part 1: Launching SET and Exploring the Toolkit 3](#_Toc203368799)

[Step 2: Examine the Available Social-Engineering Attacks. 5](#_Toc203368800)

[Part 2: Cloning a website to Obtain User Credentials 7](#_Toc203368801)

[Conclusion: 11](#_Toc203368802)

# Lab - Explore the Social Engineer Toolkit (SET)

## Objectives

Many exploits begin with a social engineering attack that is designed to obtain credentials or plant malware to create entry points into the target network. One of the tools used to perform these social engineering attacks is the Social Engineer Toolkit (SET), developed by David Kennedy.

* Launching SET and exploring the toolkit
* Cloning a website to obtain user credentials
* Capturing and viewing user credentials

## Background / Scenario

In this activity, you will clone a website and obtain user credentials. This activity is performed under carefully controlled conditions within a virtual environment. SET tools should only be used for penetration testing in situations where you have written permission to perform social engineering exploits.

In an actual penetration test, this procedure could be used to reveal problems with user security training and the need take measures to educate users about various types of phishing attacks.

## Required Resources

* Kali VM
* Internet access

## Part 1: Launching SET and Exploring the ToolkiT

## Step 1: Load the SET application.

1. Start Kali Linux using the username **kali** and the password **kali**. Open a terminal session from the menu bar at the top of the screen.
2. SET must be run as root. Use the **sudo -i** command to obtain persistent root access. At the prompt, enter the command **setoolkit** to load the SET menu system. The Social Engineering Toolkit can also be run from the **Applications >Social Engineering Tools >social engineering toolkit (root)** choice on the Kali menu.

┌──(kali㉿Kali)-[~]

└─$ **sudo -i**

[sudo] password for kali:

┌──(root㉿Kali)-[~]

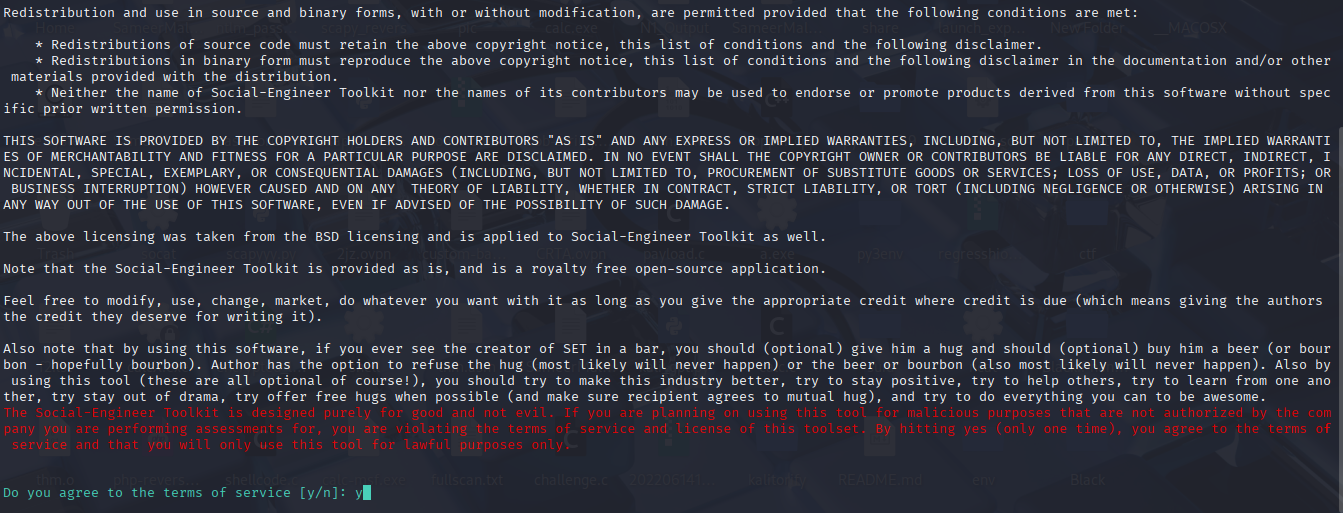
└─# **setoolkit**

If this is the first time that you have run SET, the license terms and conditions are displayed, and an agreement is required. Read the terms carefully.

1. After reading the disclaimer, enter **y** to accept the terms of service.

**The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.**

Do you agree to the terms of service [y/n]: **y**



The initial SET menu is displayed, as shown:

The Social-Engineer Toolkit is a product of TrustedSec.

  Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)

 Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks

2) Penetration Testing (Fast-Track)

3) Third Party Modules

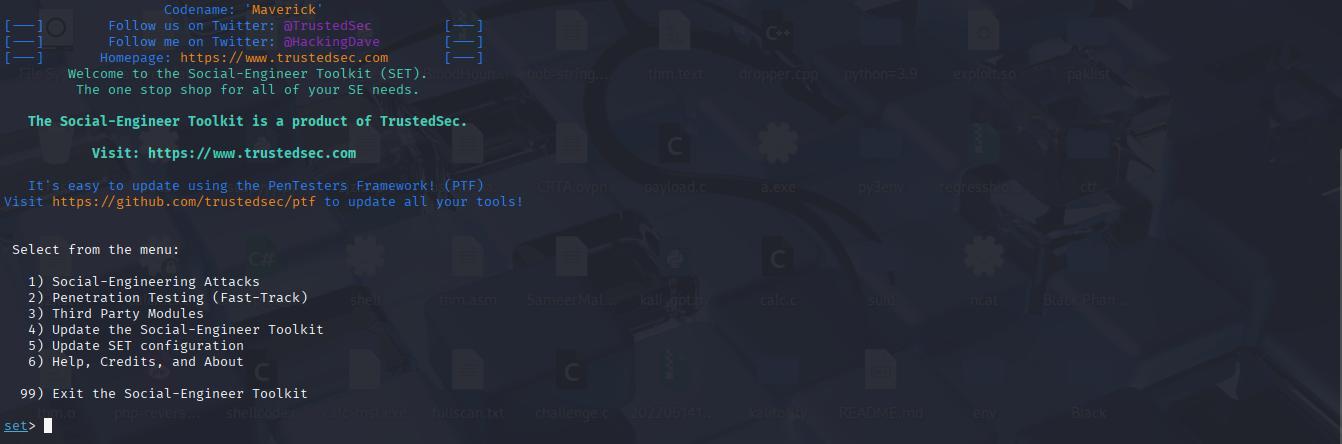
4) Update the Social-Engineer Toolkit

5) Update SET configuration

6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set>



## Step 2: Examine the Available Social-Engineering Attacks.

1. At the SET prompt, enter **1** and press **Enter** to access the Social-Engineering Attacks submenu.

set> **1**

Select from the menu:

  1) Spear-Phishing Attack Vectors

2) Website Attack Vectors

3) Infectious Media Generator

4) Create a Payload and Listener

5) Mass Mailer Attack

6) Arduino-Based Attack Vector

7) Wireless Access Point Attack Vector

8) QRCode Generator Attack Vector

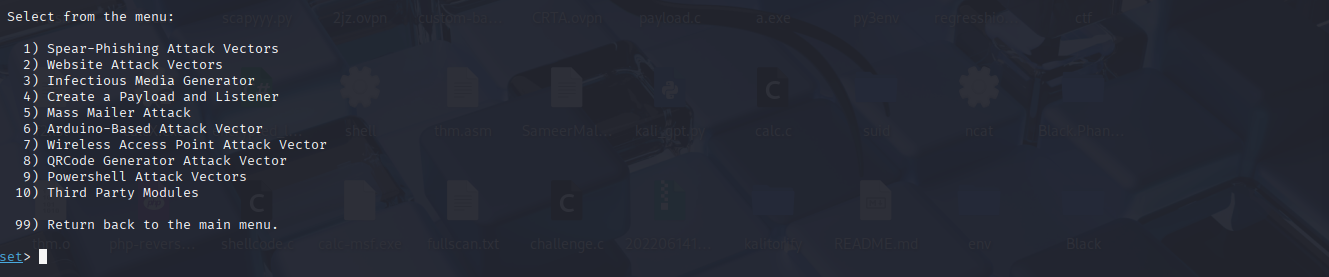
9) Powershell Attack Vectors

10) Third Party Modules

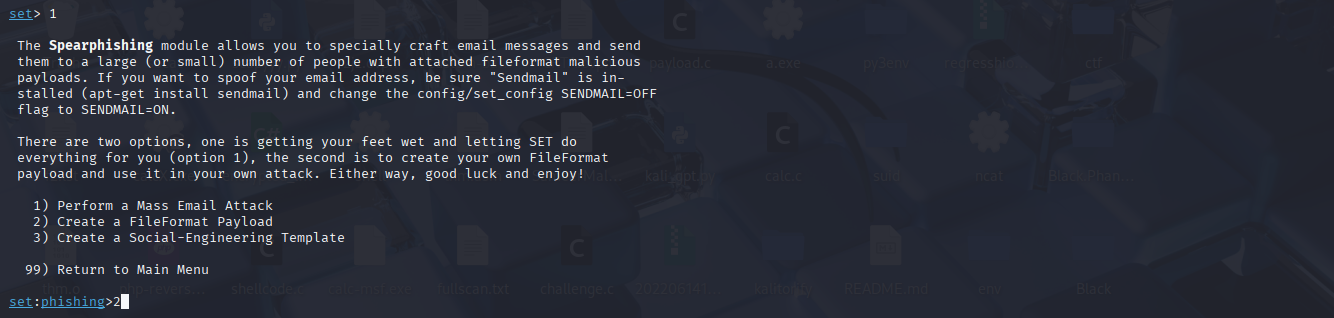
99) Return back to the main menu.

1. Select each option to see a brief description of each exploit and what the tool does for each.

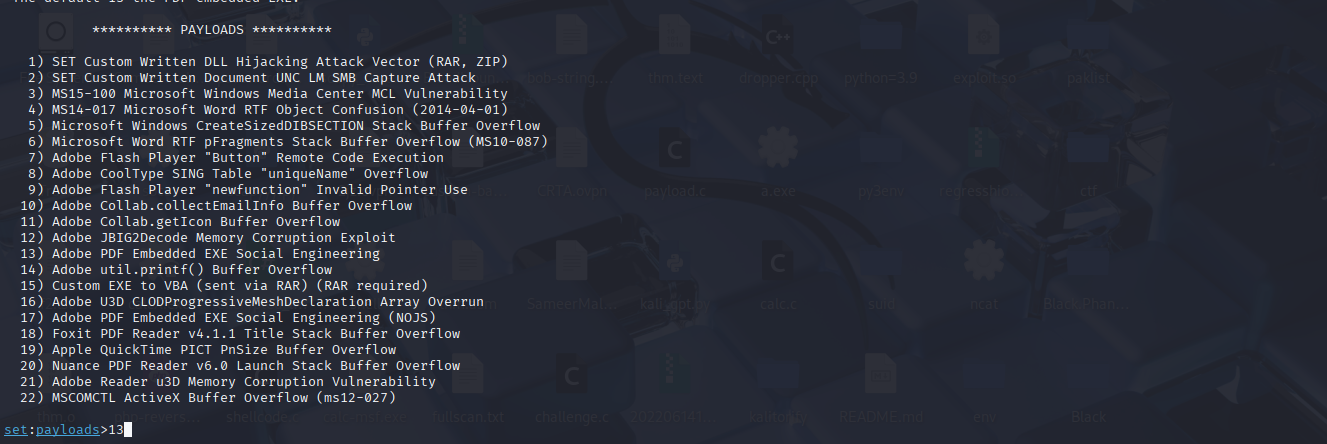
**Note**: Some options may not have a choice. In that case, use **CTRL-C** or enter **99**to return to the main menu.



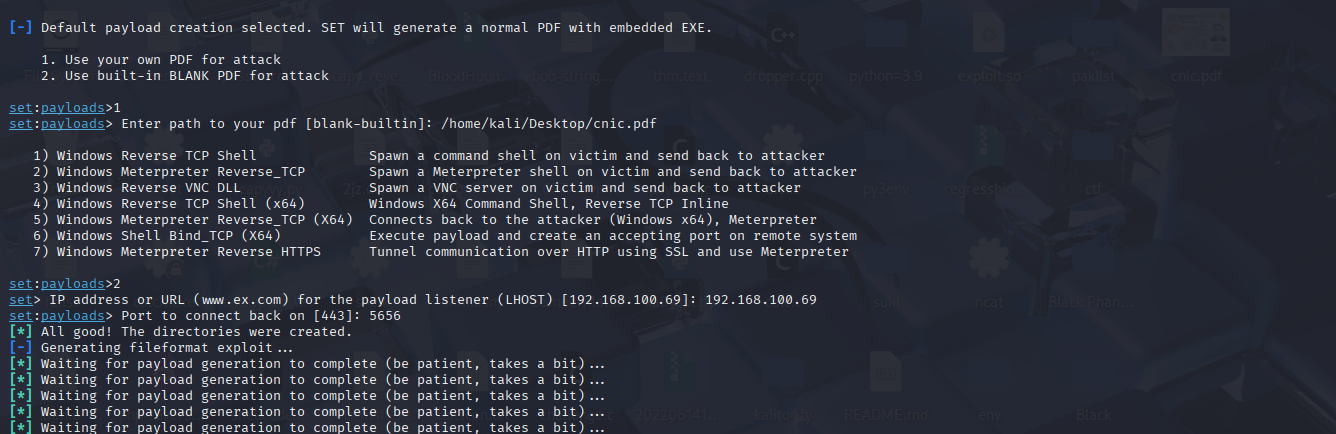
Here we will choose spear phishing.

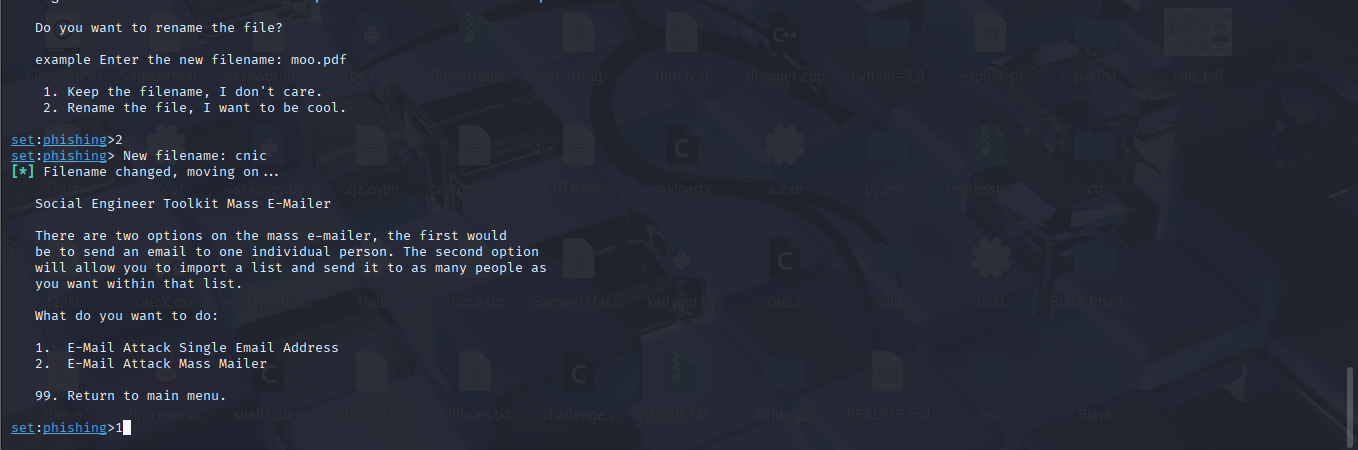


For this we will choose a File Format option what this does is that it stenographs a malware in a pdf or any other file. Now image sending a resume.pdf to an HR, embedded with a malware!



We can also create our own malware using msfvenom for this lab!



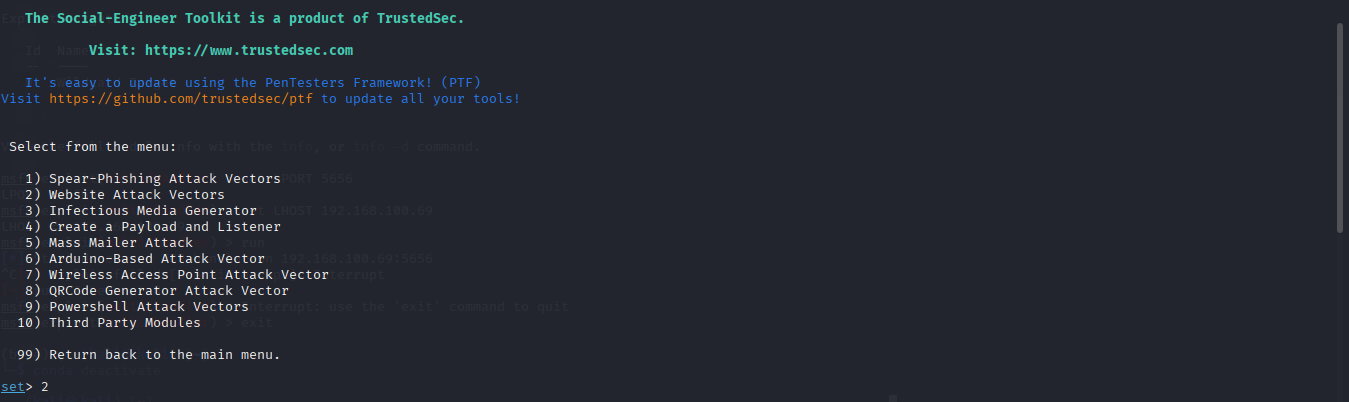


## Part 2: Cloning a website to Obtain User Credentials

In this part of the lab, you will create a perfect copy of the login page for a website. The fake login page will gather all credentials submitted to it and then redirect the user to the real website.

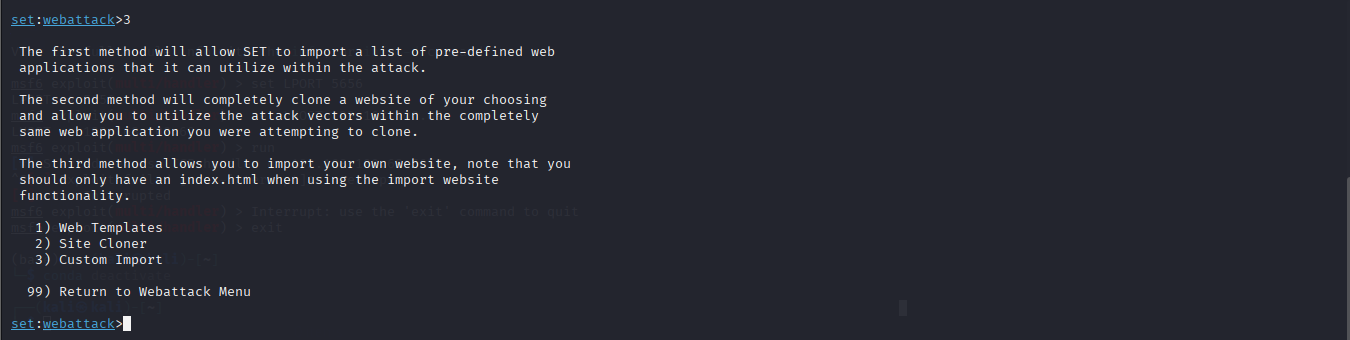
**Step 1: Investigate Web Attack Vectors in SET.**

1. From the Social-Engineering Attacks submenu, choose **2) Website Attack Vectors** to begin the web site cloning exploit.

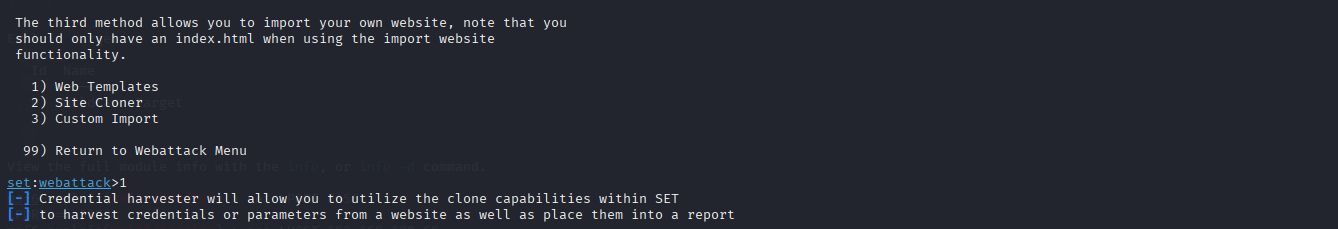


set> **2**

1. Review the brief attack description of each type of attack.



For now we will select first option you are encouraged to explore other options as well!



--- \* IMPORTANT \* READ THIS BEFORE ENTERING IN THE IP ADDRESS \* IMPORTANT \* ---

The way that this works is by cloning a site and looking for form fields to

rewrite. If the POST fields are not usual methods for posting forms this

could fail. If it does, you can always save the HTML, rewrite the forms to

be standard forms and use the "IMPORT" feature. Additionally, really

important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL

IP address below, not your NAT address. Additionally, if you don't know

basic networking concepts, and you have a private IP address, you will

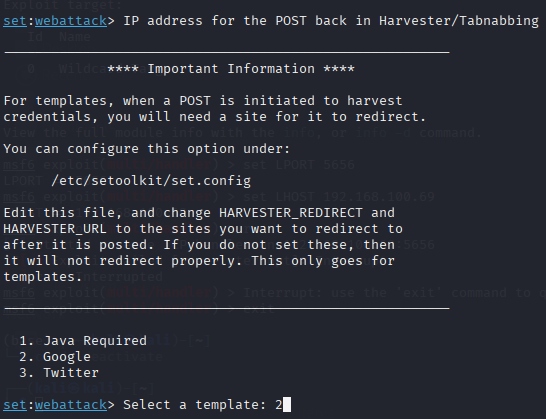
need to do port forwarding to your NAT IP address from your external IP

address. A browser doesn’t know how to communicate with a private IP

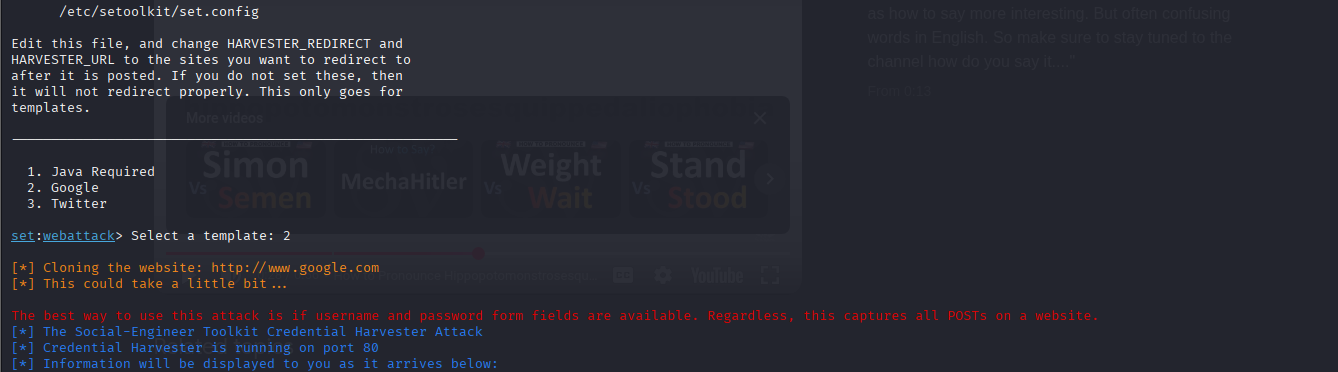
address, so if you don't specify an external IP address if you are using

this from an external perspective, it will not work. This isn't a SET issue

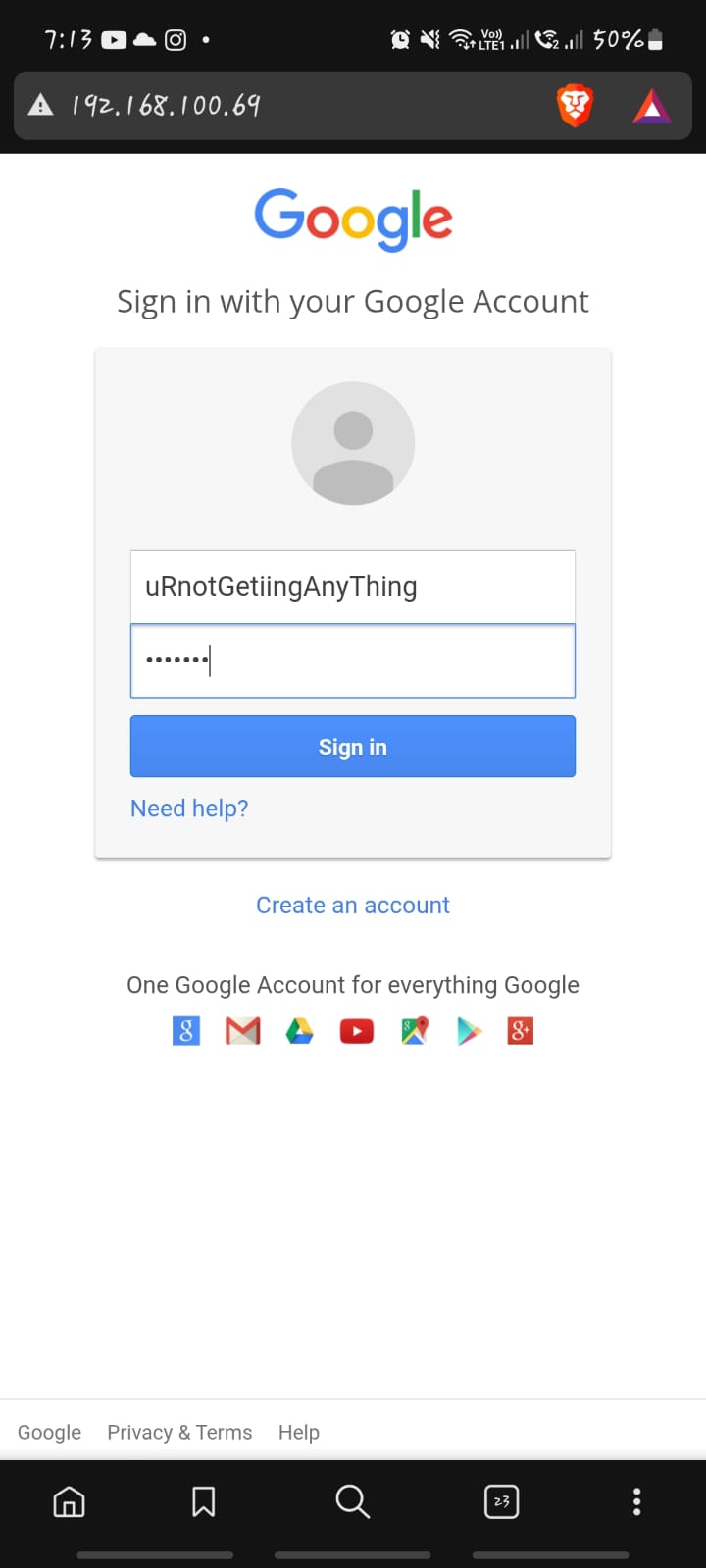
this is how networking works.



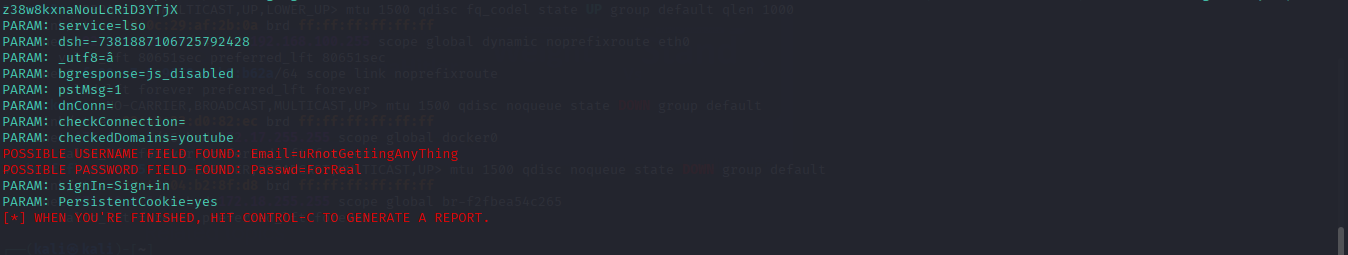
After that I selected a Google template to continue with you can either choose pre built templates or even clone login page!



I used my phone as the victim machine to demonstrate how this works:



And on the attacker machine we have plain text credentials!



## Conclusion:

This lab aimed to provide the fundamental aspects of how phishing attacks are initiated and how easily they can entice an untrained employee to click and prove that humans are the weakest link in any company. There are a lot of other tools out there which perform similar function but in an improved way such as Rubik phish, Go phish etc. Moreover, these links can be masked by using a URL shortener such as bit.ly.