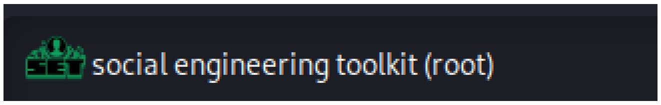
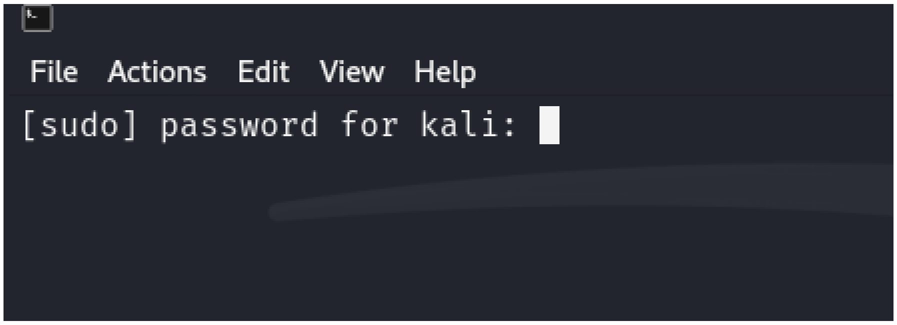
Description: This project aims to illustrate the process of executing a social engineering attack using techniques created by attackers. This project covers the use of the Social Engineering Toolkit (root) to clone a legitimate website. It explains how to distinguish between a real website and a fake one. The project shows how a victim might mistakenly enter sensitive information on a counterfeit website, and from the attacker's perspective, how this sensitive information is viewed through the terminal. Additionally, the project provides basic knowledge on how to prevent such attacks and emphasizes the importance of being cautious when entering personal information online.

Software and tools I use: social engineering toolkit (root), Kali Linux.

Project: In this project, I will open Kali Linux, which comes with a default software called the 'social engineering toolkit (root)'. I will use this toolkit to demonstrate a social engineering attack from the attacker's point of view.

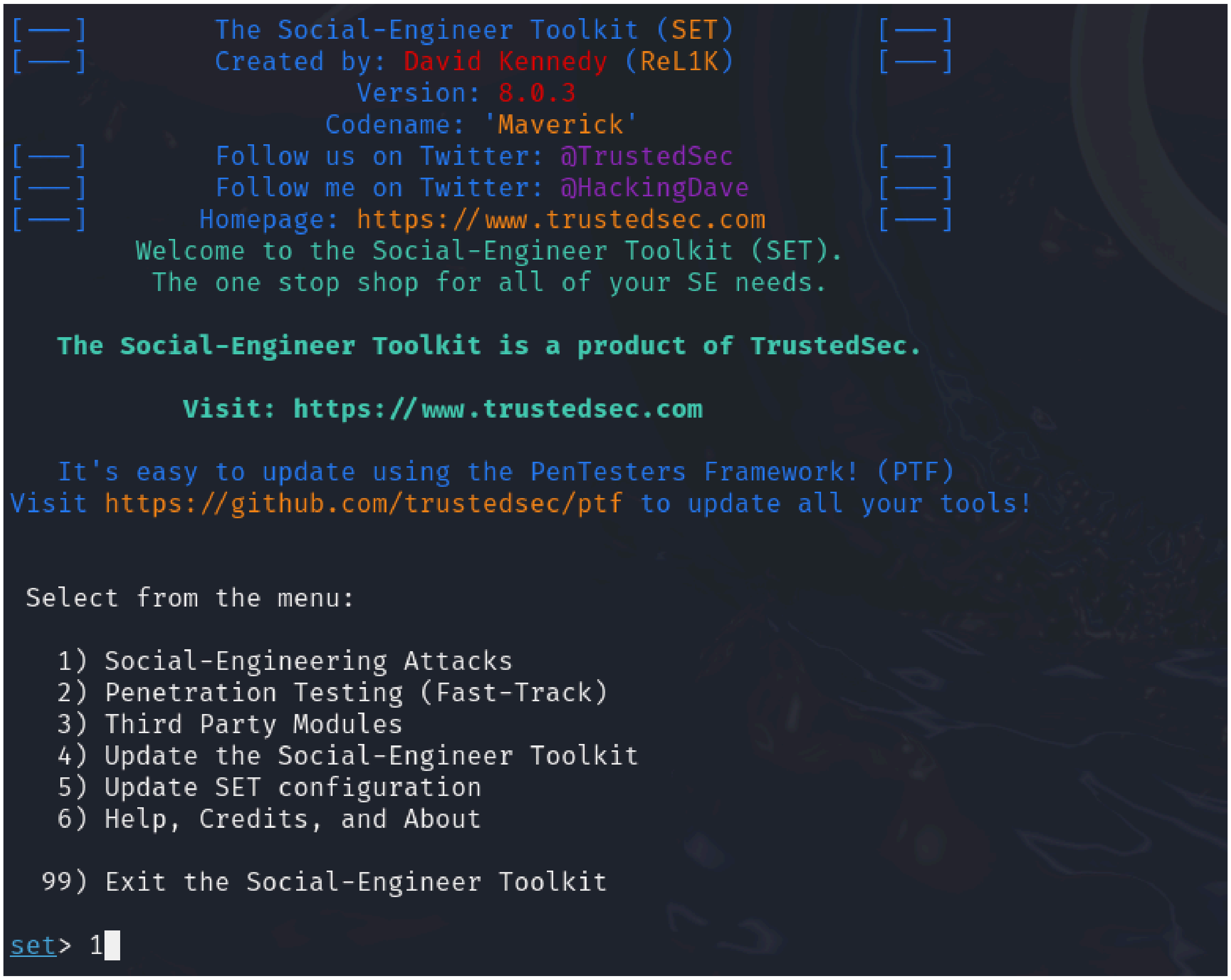


I will open it, and it will ask for my Kali Linux password to continue. I will enter my password to gain access.



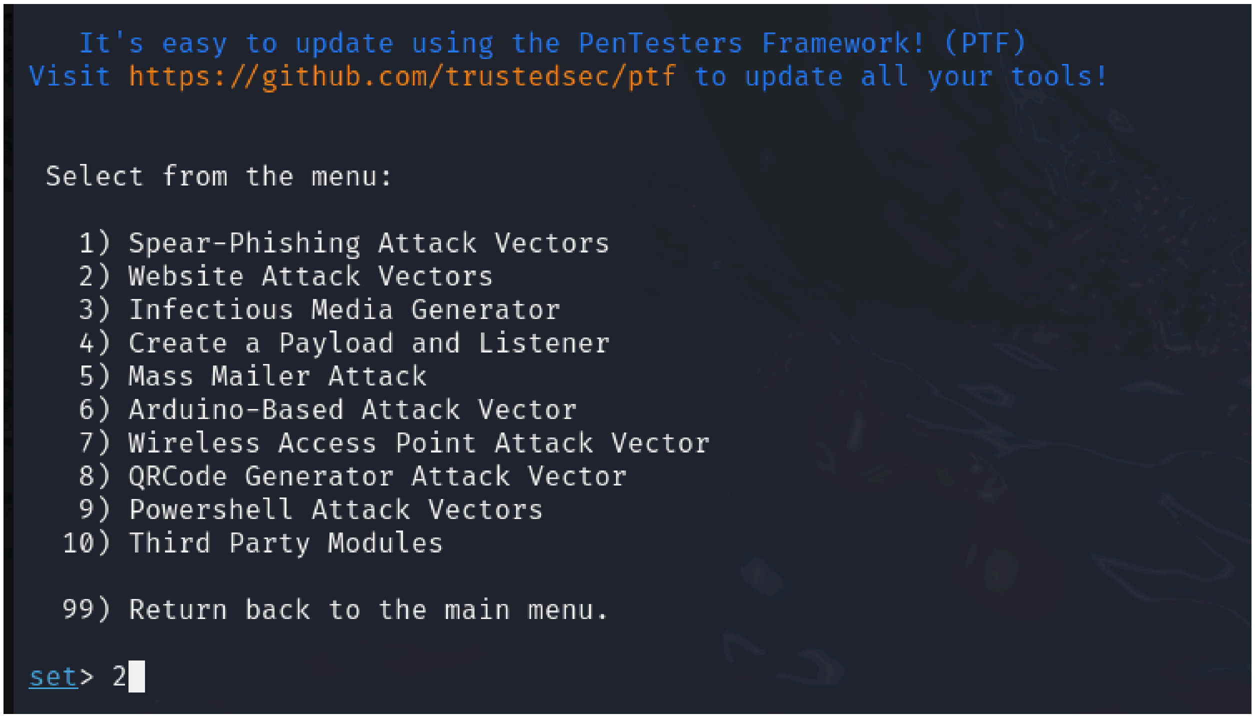
```
[sudo] password for kali:
```

It will open the application, which has a variety of options to choose from. For this project, I will select option 1, 'Social-Engineering Attacks'.



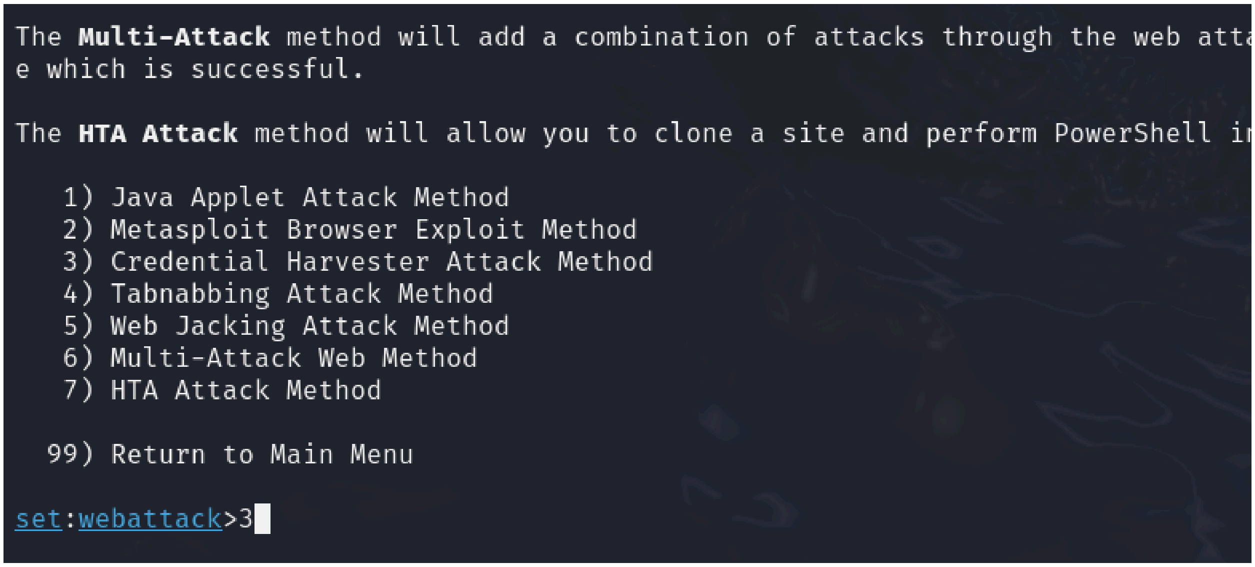
```
[---]        The Social-Engineer Toolkit (SET)          [---]
[---]        Created by: David Kennedy (ReL1K)          [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec          [---]
[---]        Follow me on Twitter: @HackingDave         [---]
[---]       Homepage: https://www.trustedsec.com        [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   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> 1
```

After choosing 'Social-Engineering Attacks', I will need to select the type of social engineering attack I want to perform. There are many options available. I will choose option 2, 'Website Attack Vectors', because I will be using a website to carry out the social engineering attack.



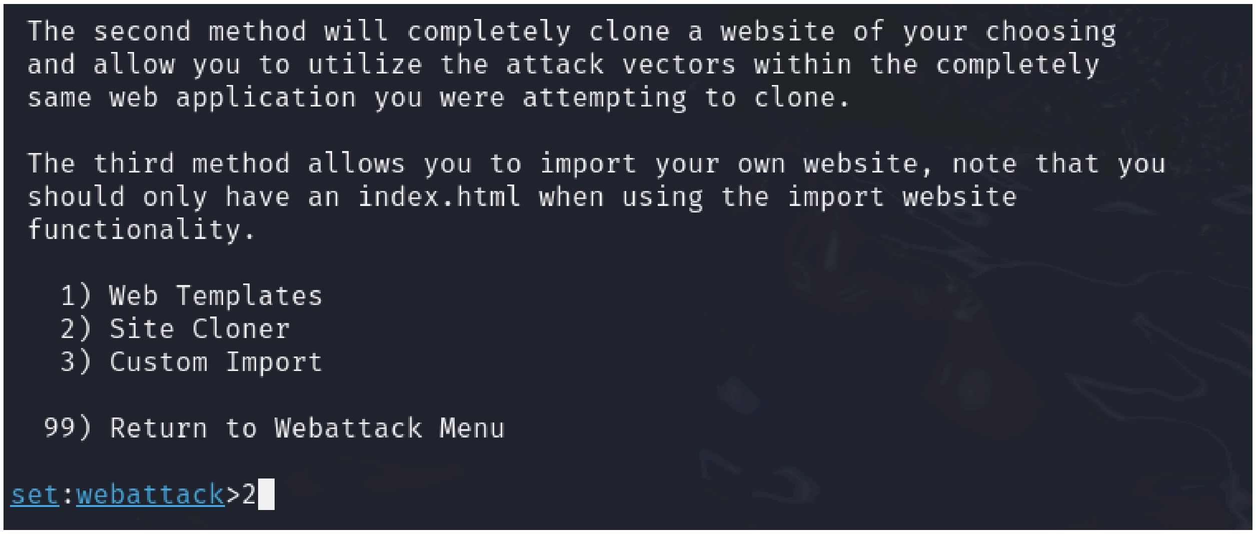
```
    It's easy to update using the PenTesters Framework! (PTF)
 Visit https://github.com/trustedsec/ptf to update all your tools!


  Select from the menu:

    1) 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.

 set> 2
```

After selecting ‘Website Attack Vectors’, I will choose my method from the options provided. I will select option 3, the ‘Credential Harvester Attack Method’. This method allows the attacker to capture sensitive information, such as usernames and passwords when the victim enters their details on a fake website.



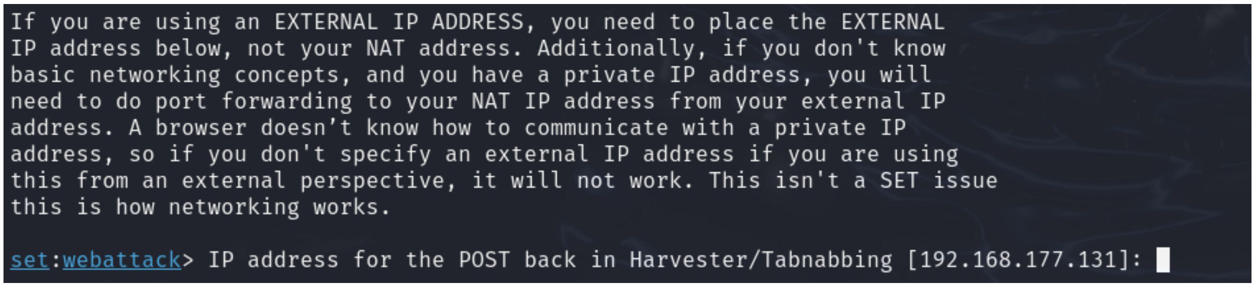
```
The Multi-Attack method will add a combination of attacks through the web atta
e which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell in

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

I will need to choose between using a website template or cloning a real website. Cloning a real website is a powerful option because it allows me to create a fake website that looks exactly like the original. I will select option 2, ‘Site Cloner’.



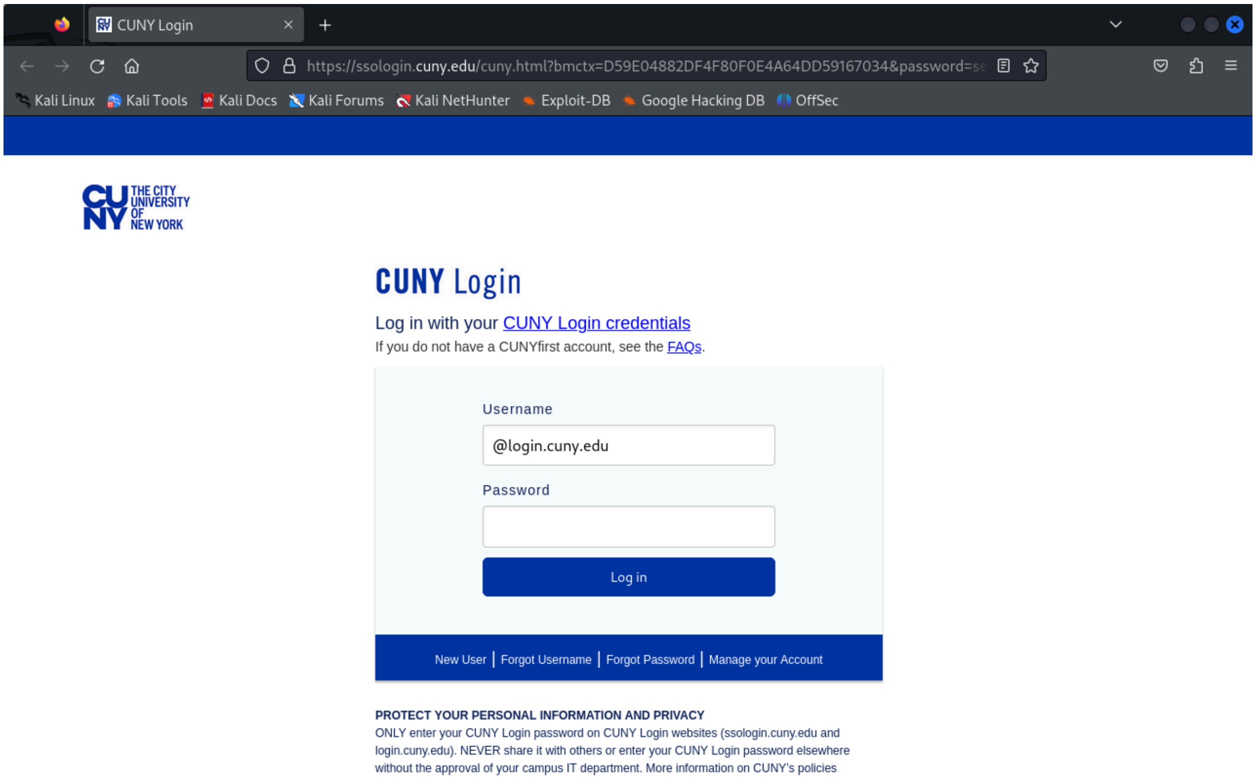
```
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

After that, it will ask for an IP address to create the fake website. Attackers usually purchase a domain for this type of attack, but for this project, I will use my Linux IP address (192.168.177.131) to create the cloned website so that no one else can access the attack. I will type nothing and press Enter.



```
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.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.177.131]:
```

It will ask which website I want to clone. For this project, I will use my CUNY College login page, and the website looks like this.


CUNY Login
https://ssologin.cuny.edu/cuny.html?bmctx=D59E04882DF4F80F0E4A64DD59167034&password=se
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
THE CITY UNIVERSITY OF NEW YORK

CUNY Login

Log in with your CUNY Login credentials

If you do not have a CUNYfirst account, see the FAQs.

Username

@login.cuny.edu

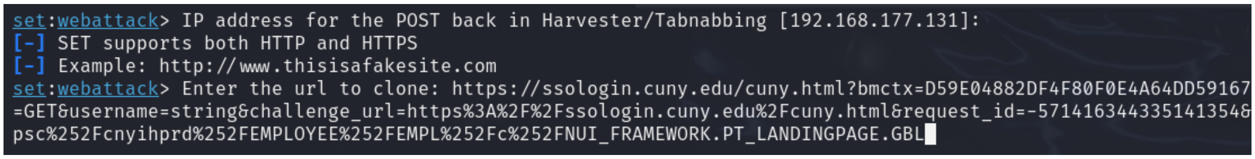
Password

Log in
New User | Forgot Username | Forgot Password | Manage your Account

PROTECT YOUR PERSONAL INFORMATION AND PRIVACY

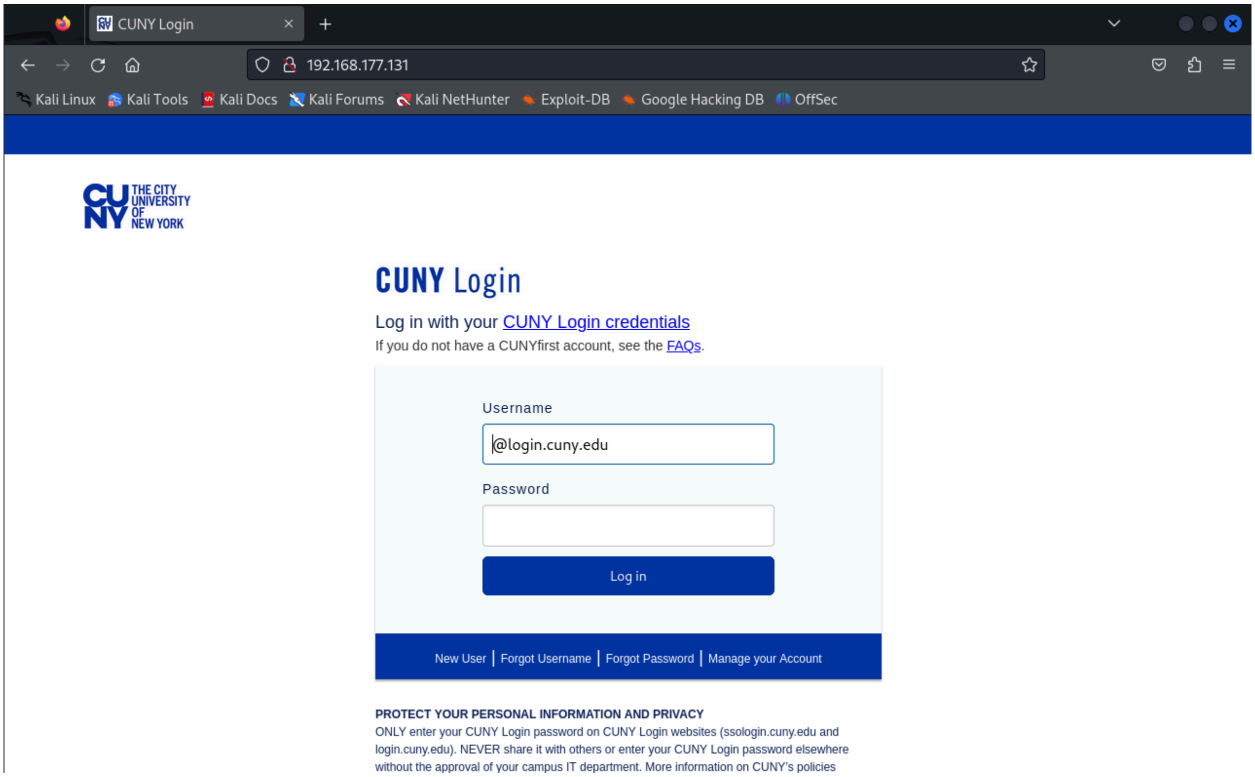
ONLY enter your CUNY Login password on CUNY Login websites (ssologin.cuny.edu and login.cuny.edu). NEVER share it with others or enter your CUNY Login password elsewhere without the approval of your campus IT department. More information on CUNY's policies

This is the real website because it starts with 'https' which indicates it is a secure website. This is one example of how to verify whether a website is genuine. It also has a secure lock sign. When attackers clone a website, they cannot replicate the 'https' security or the exact domain name. Instead, they create a fake domain and may alter the name by using uppercase or lowercase letters, adding numbers, or making other changes to keep it similar. While these alterations can be easy to spot, victims often fall for the scam due to carelessness or failure to verify the authenticity. I will copy the link to the real website and paste it into the application to create the clone.



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.177.131]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://ssologin.cuny.edu/cuny.html?bmctx=D59E04882DF4F80F0E4A64DD59167
=GET&username=string&challenge_url=https%3A%2F%2Fssologin.cuny.edu%2Fcuny.html&request_id=-5714163443351413546
psc%252Fcnyihprd%252FEMPLOYEE%252FEMPL%252Fc%252FNUI_FRAMEWORK.PT_LANDINGPAGE.GBL
```

To access the cloned website I created for a social engineering attack, I will open a browser and use my Linux IP address.



CUNY Login

Log in with your CUNY Login credentials

If you do not have a CUNYfirst account, see the FAQs.

Username

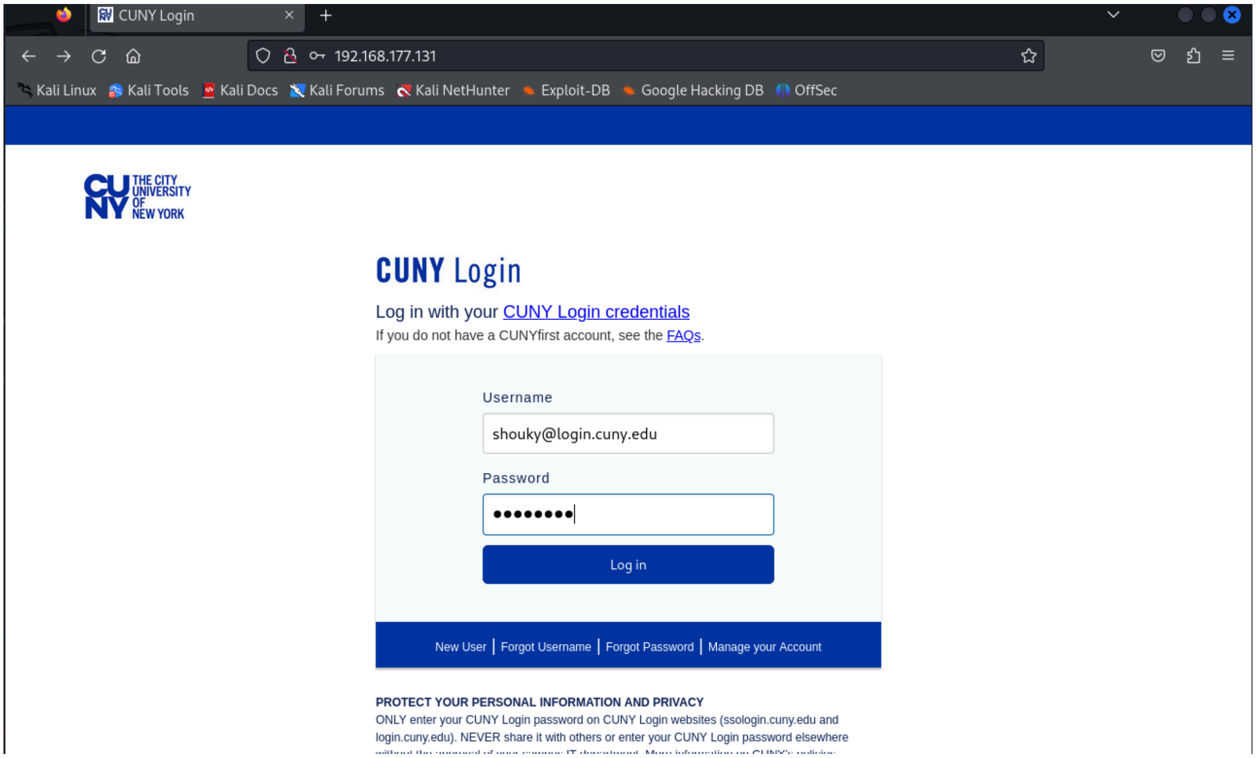
@login.cuny.edu

Password

PROTECT YOUR PERSONAL INFORMATION AND PRIVACY

ONLY enter your CUNY Login password on CUNY Login websites (ssologin.cuny.edu and login.cuny.edu). NEVER share it with others or enter your CUNY Login password elsewhere without the approval of your campus IT department. More information on CUNY's policies

At first glance, It looks like a real website. Nobody can get that it is a fake website by looking at the login information. But if I look at the website address, However, by checking the website address, it becomes clear that the site is fake. Even the lock sign has a red line on it. That tells that it is not a secure website. The real website has a lock sign but no red line on it. In the website address, it will show my Linux IP address which means that the website address is wrong. Attacker is not going to use their linux ip address but they will temper the website by adding uppercase and lowercase. To test the clone website I will put a fake username and fake password to see if I can capture the information.



CUNY Login

Log in with your CUNY Login credentials

If you do not have a CUNYfirst account, see the FAQs.

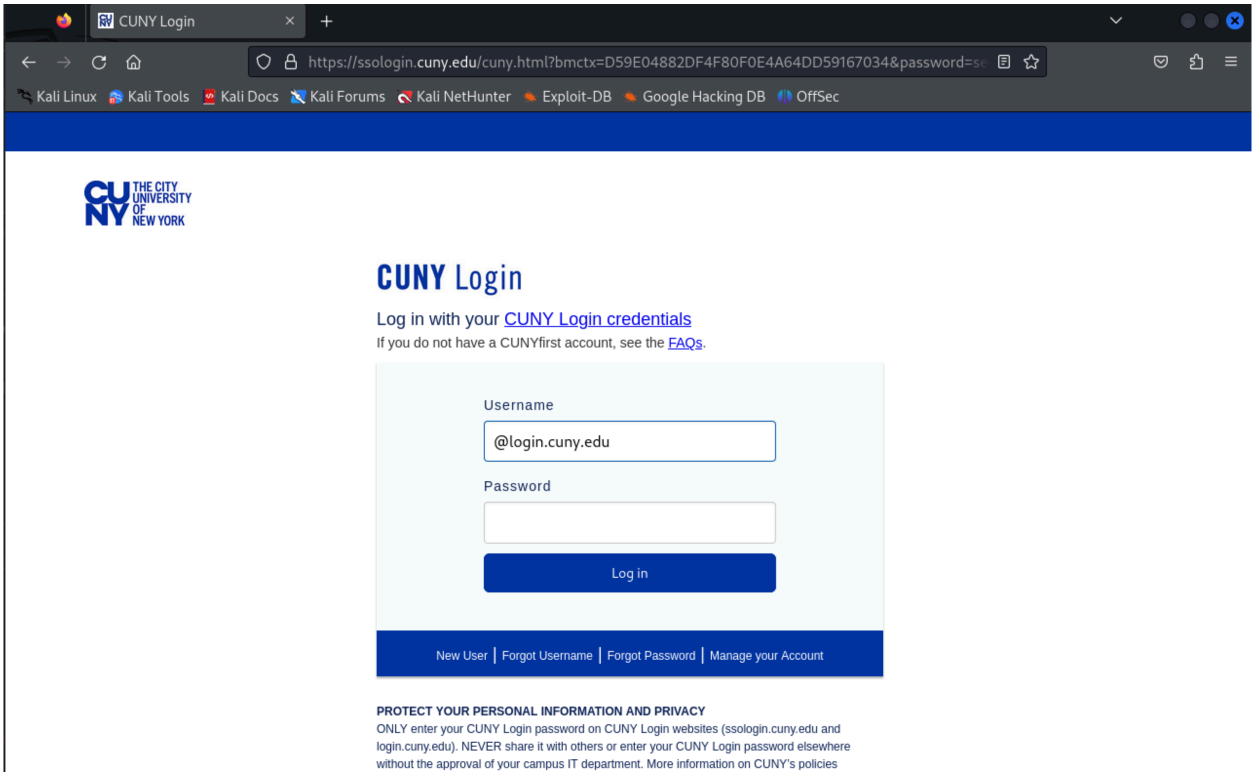
Username: shouky@login.cuny.edu

Password: ••••••••

Log in
New User | Forgot Username | Forgot Password | Manage your Account

PROTECT YOUR PERSONAL INFORMATION AND PRIVACY

ONLY enter your CUNY Login password on CUNY Login websites (ssologin.cuny.edu and login.cuny.edu). NEVER share it with others or enter your CUNY Login password elsewhere without the approval of your campus IT department. More information on CUNY's policies:



https://ssologin.cuny.edu/cuny.html?bmctx=D59E04882DF4F80F0E4A64DD59167034&password=se

CUNY Login

Log in with your CUNY Login credentials

If you do not have a CUNYfirst account, see the FAQs.

Username

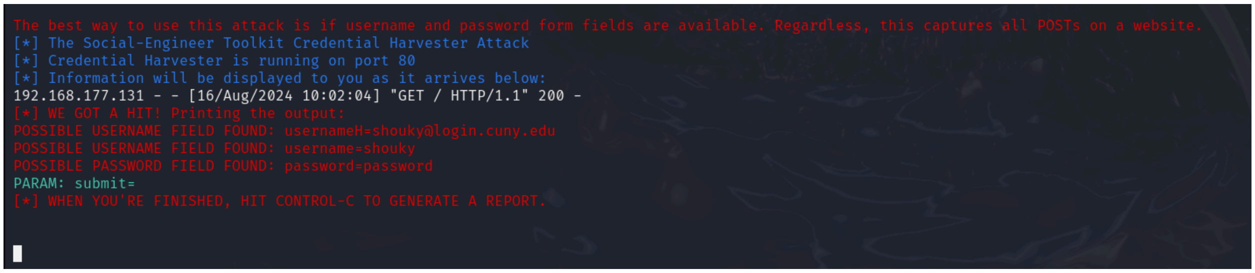
@login.cuny.edu

Password

PROTECT YOUR PERSONAL INFORMATION AND PRIVACY

ONLY enter your CUNY Login password on CUNY Login websites (ssologin.cuny.edu and login.cuny.edu). NEVER share it with others or enter your CUNY Login password elsewhere without the approval of your campus IT department. More information on CUNY's policies

After entering a fake username and password, it redirects to the real website like nothing happened. Victims will think that they made a mistake putting the information but when they try a second time, they will access the real website. Victims will have no idea what is happening. Now I will open the application terminal to see if I can capture the username and password.



```
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.177.131 - - [16/Aug/2024 10:02:04] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: usernameH=shouky@login.cuny.edu
POSSIBLE USERNAME FIELD FOUND: username=shouky
POSSIBLE PASSWORD FIELD FOUND: password=password
PARAM: submit=
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

In the terminal, it captured the username and password. The username is ‘shouky’ and the password is ‘password’. That’s how attackers do social engineering attacks. It is the most popular attack right now because anyone can fall for this trap. So it is important to judge website by looking at the website link. It is not a good idea to click any link from the email that asks to log in. If it is necessary to open then it is a good idea to go to the website and log in to the real website by looking at the website link and ‘https’.