



Lab2: Social Engineering Penetration Testing Methodology

INFO40587: ETHICAL HACKING

Kevin Harianto | 991602128 | May 31, 2024

Contents

Contents	1
Executive Summary.....	2
Exercise 1: Conducting a Phishing Campaign Using Social Engineering Toolkit	3
Exercise 2: Conducting a Phishing Campaign Using OhPhish	8
Conclusion.....	11

Executive Summary

The objective of this module is to help students learn different techniques to gather information about a user. You will learn how to:

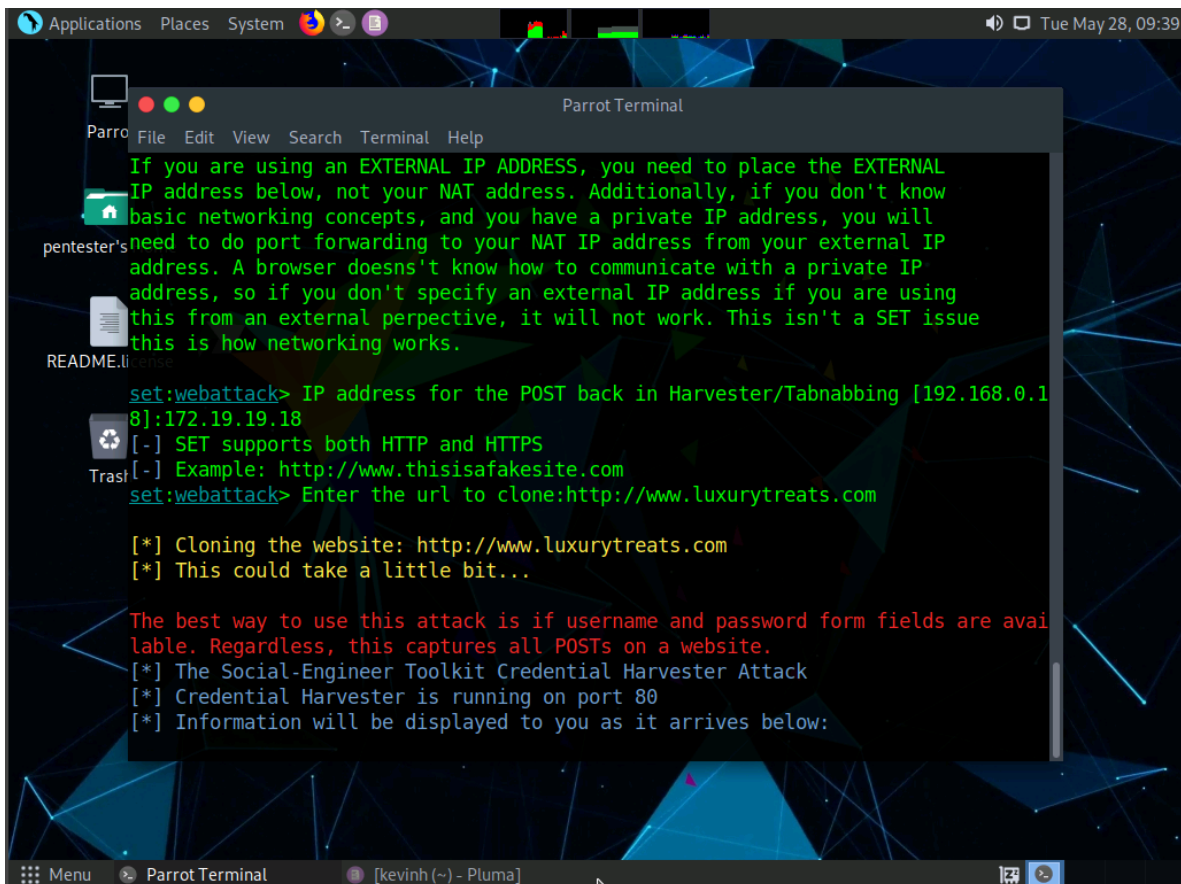
Conduct a Phishing Campaign Using Social Engineering Toolkit

Conduct a Phishing Campaign Using OhPhish

Exercise 1: Conducting a Phishing Campaign Using Social Engineering Toolkit

1.1 OUTPUT SCREENSHOTS

Exercise 1, Step 10: This application clones the webpage and waits for the victim(s) to enter their credentials.



The screenshot shows a Parrot OS desktop environment. A Parrot Terminal window is open, displaying the output of the Social-Engineer Toolkit (SET). The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The output text is as follows:

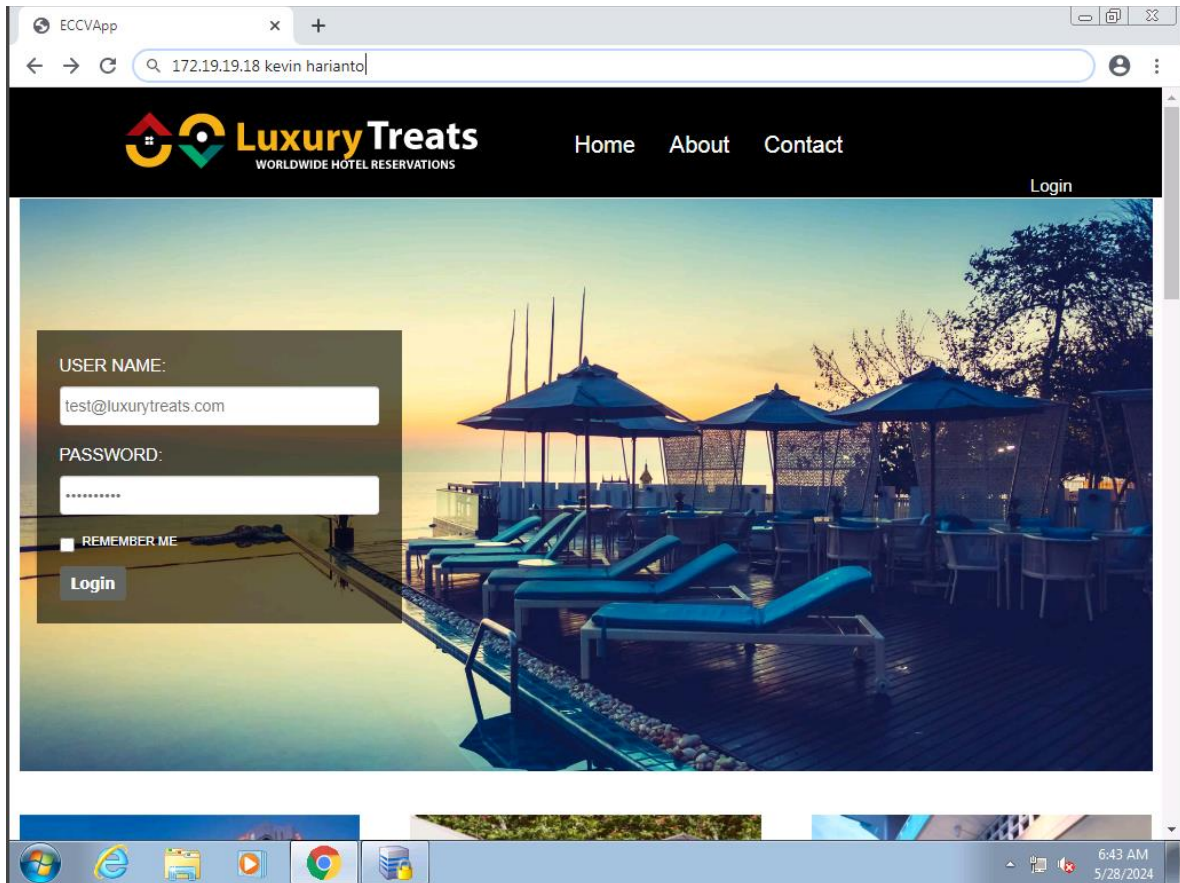
```
Parrot Terminal
File Edit View Search Terminal Help
pentester's
README.li
Trasl
set:webattack> If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, 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 [192.168.0.1
8]:172.19.19.18
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.luxurytreats.com

[*] Cloning the website: http://www.luxurytreats.com
[*] This could take a little bit...

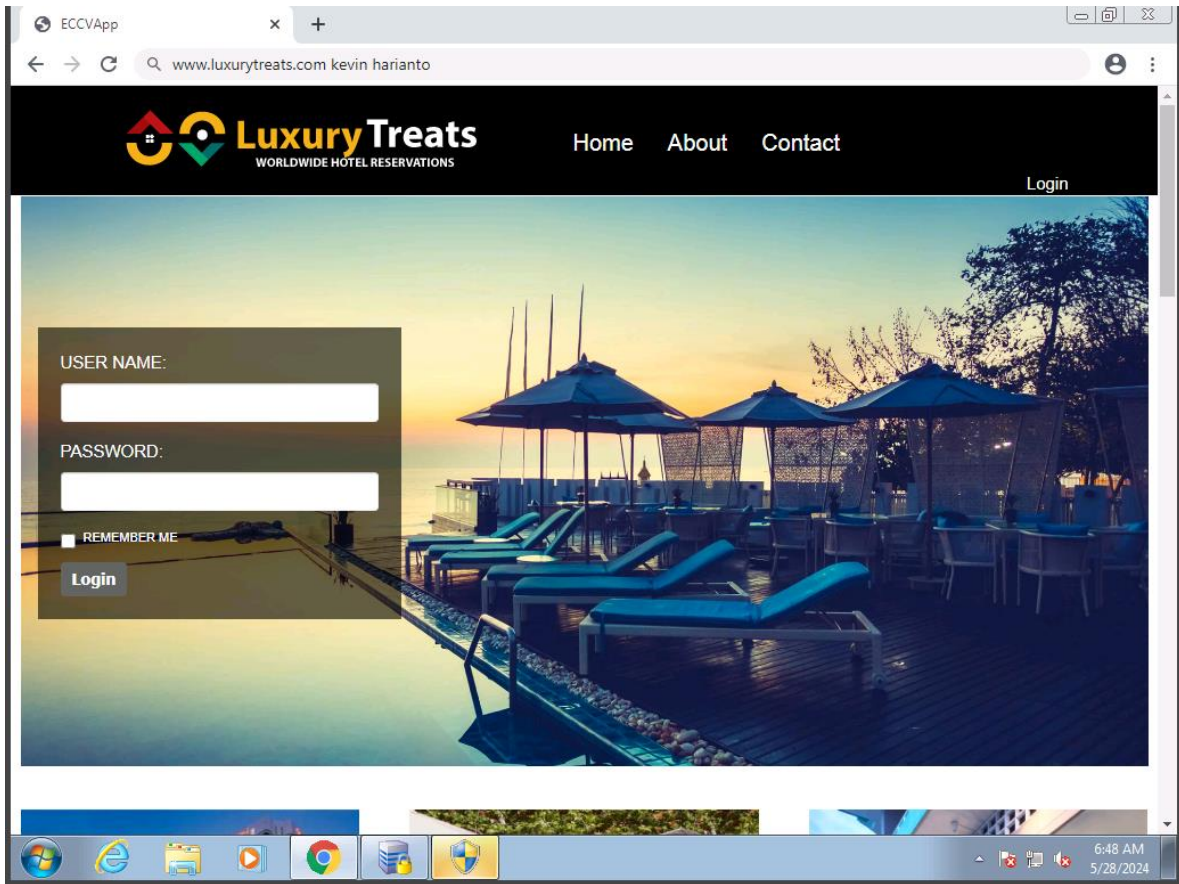
The best way to use this attack is if username and password form fields are avail
lable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

The desktop background features a dark blue geometric pattern. The terminal window is titled 'Parrot Terminal' and has a menu bar. The output text is color-coded: green for general instructions, yellow for status messages, and red for warnings or important notes. The terminal window is open over a desktop with various icons and a taskbar at the bottom.

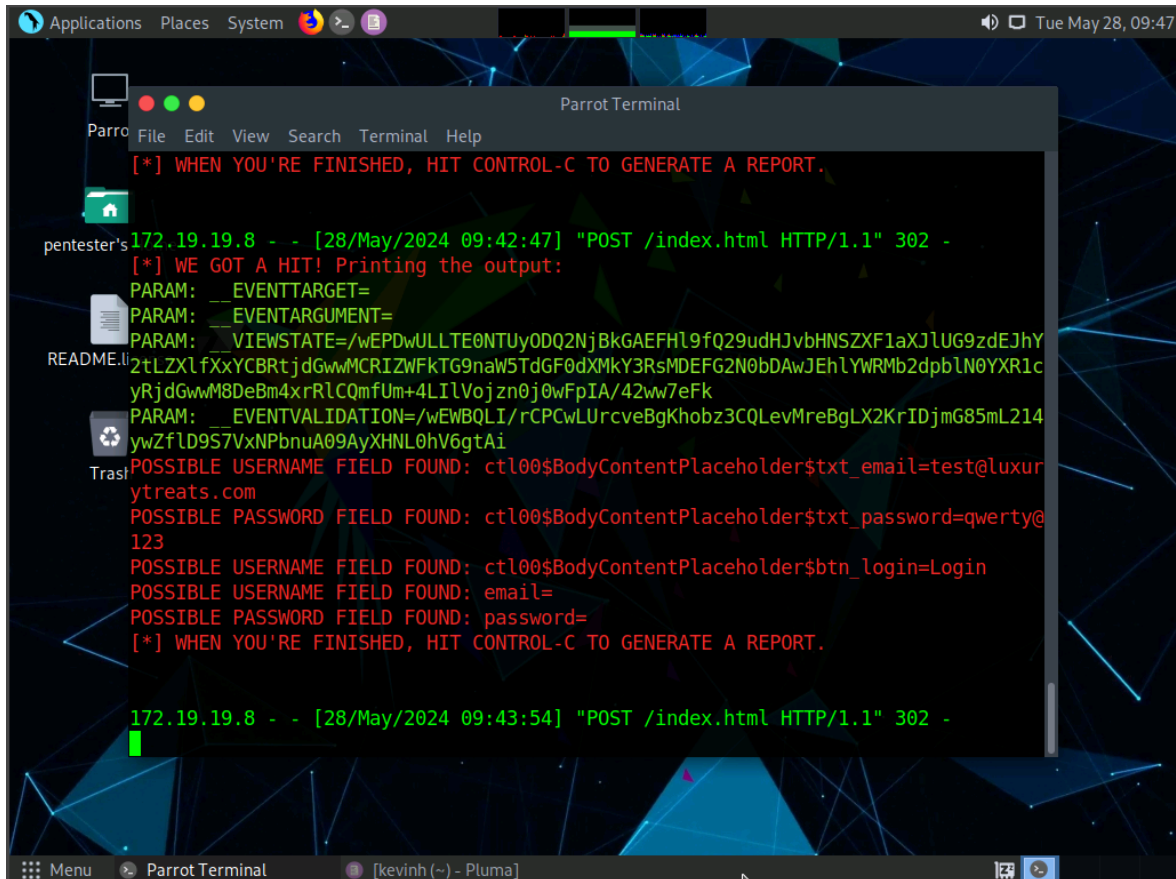
Exercise 1, Step 21: Enter the credentials to Log In to the website. Assume that you have an account in Luxurytreats website, and provide the details as below:



Exercise 1, Step 22: Once you enter the credentials, it does not log you into the website; instead, it redirects you to the legitimate page of luxurytreats.com. Close the Browser window



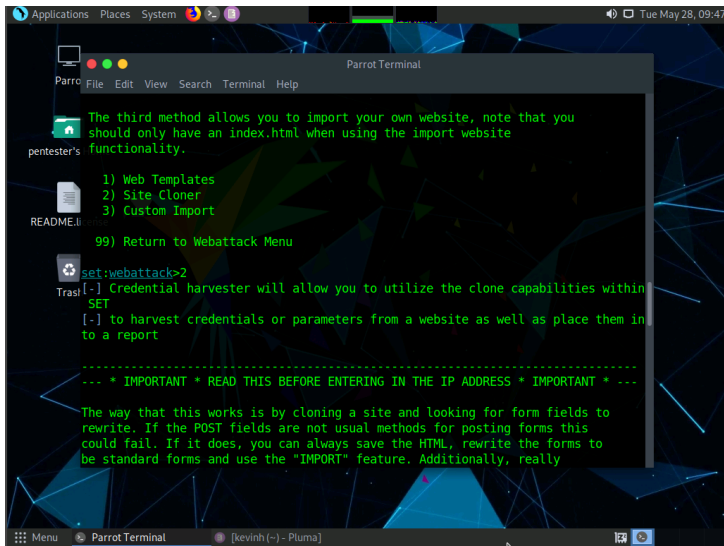
Exercise 1, Step 23: As soon as the victim (you) types in the credentials, and clicks Login, the social engineering toolkit fetches the entered credentials as shown in the screenshot which can be used by an attacker in real-time, to gain unauthorized access to the victim's account.



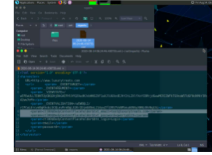
The screenshot shows a Parrot OS desktop environment. A terminal window titled "Parrot Terminal" is open, displaying the output of a social engineering toolkit. The terminal shows a successful POST request to /index.html, followed by a message indicating that credentials were found. The extracted credentials are listed as follows:

```
172.19.19.8 - - [28/May/2024 09:42:47] "POST /index.html HTTP/1.1" 302 -  
[*] WE GOT A HIT! Printing the output:  
PARAM: __EVENTTARGET=  
PARAM: __EVENTARGUMENT=  
PARAM: __VIEWSTATE=/wEPDwULLTE0NTUyODQ2NjBkGAEFHl9fQ29udHJvbHNSZXFlaXJlUG9zdEJhY  
2tLZXlfXxYCBrtjdGwwMCRIZWfKTG9naW5TdGF0dXMkY3RsMDEFG2N0bDAwJEhlYWRMb2dpblN0YXRlc  
yRjdGwwM8DeBm4xrRlCQmfUm+4LlVojzn0j0wFpIA/42ww7eFk  
PARAM: __EVENTVALIDATION=/wEWBQLI/rCPCwLUrcveBgKhobz3CQLvMreBgLX2KrIDjmG85mL214  
ywZfLD9S7VxNPbnuA09AyXHNl0hV6gtAi  
POSSIBLE USERNAME FIELD FOUND: ctl00$BodyContentPlaceholder$txt_email=test@luxur  
ytreats.com  
POSSIBLE PASSWORD FIELD FOUND: ctl00$BodyContentPlaceholder$txt_password=qwerty@  
123  
POSSIBLE USERNAME FIELD FOUND: ctl00$BodyContentPlaceholder$btn_login=Login  
POSSIBLE USERNAME FIELD FOUND: email=  
POSSIBLE PASSWORD FIELD FOUND: password=  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.  
  
172.19.19.8 - - [28/May/2024 09:43:54] "POST /index.html HTTP/1.1" 302 -
```


1.2 Questions



25. The report will be generated in the directory `/root/.set/reports` in xml format as shown in the screenshot. Save this report to the respective pentesting directory.



Question 4.1.1

Use the Social-Engineer Toolkit (SET) on the Parrot machine to sniff the credentials of a user on the Windows 11 machine. Apart from Site Cloner and Custom Import, what is the third method that SET offers to deploy a credential-harvesting attack vector?

Web Templates

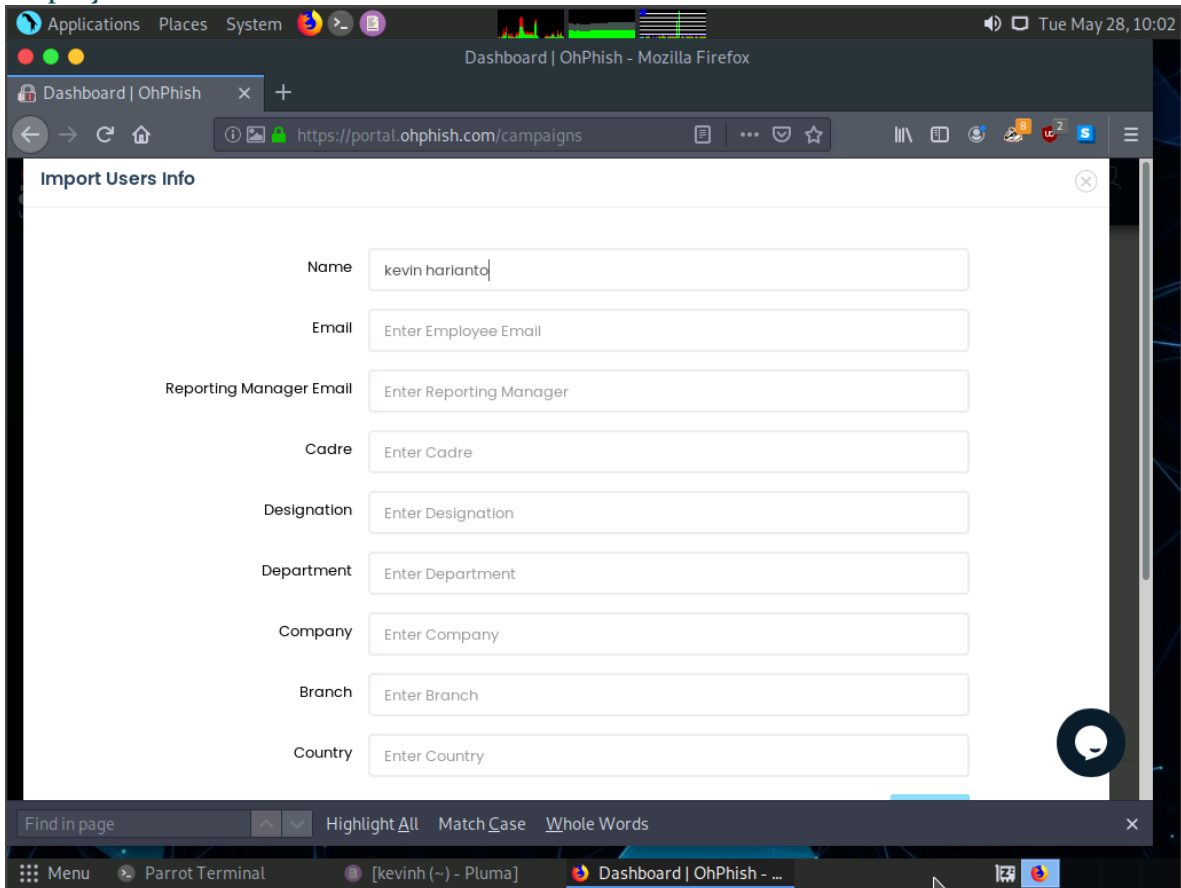
Score

✓ Correct

Exercise 2: Conducting a Phishing Campaign Using OhPhish

2.1 OUTPUT SCREENSHOTS

Exercise 2, Step 17: Import Users Info pop-up appears, enter the details of the target employee and click Add.



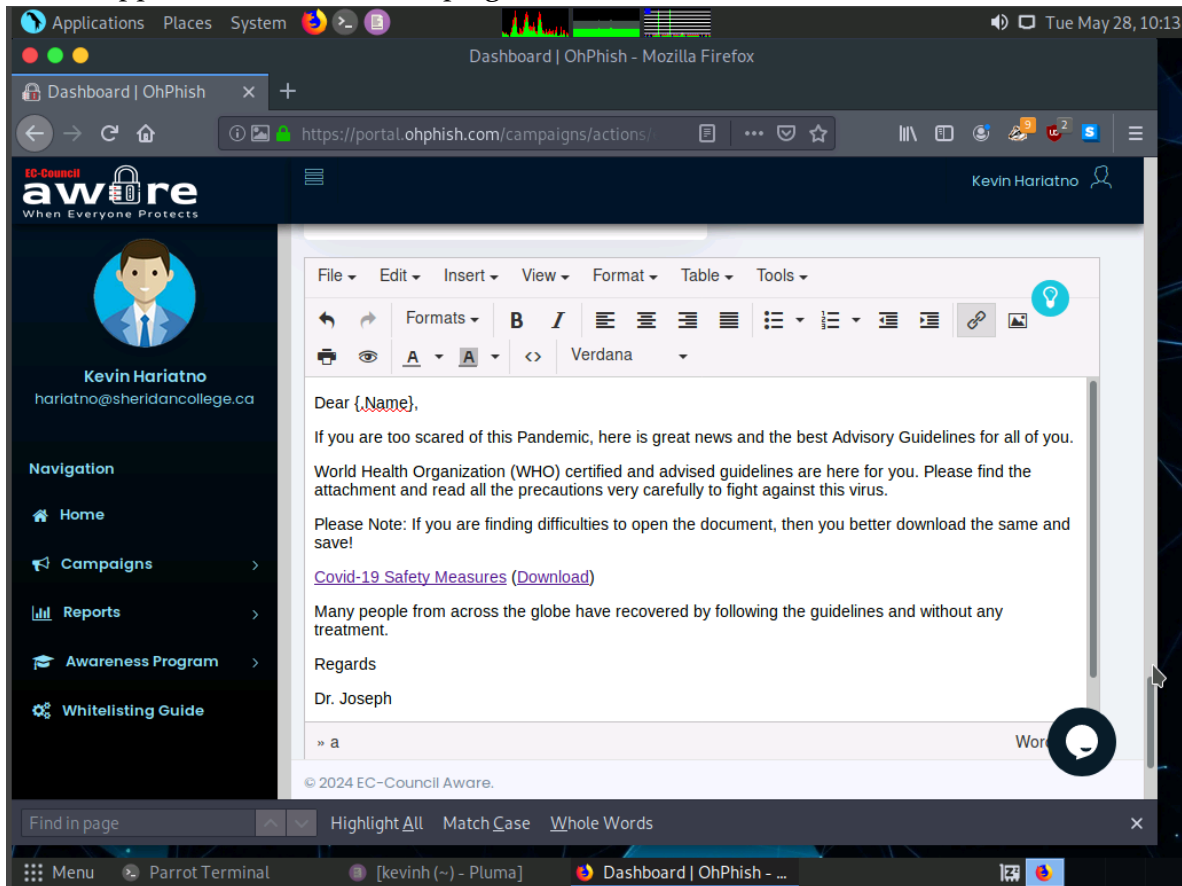
The screenshot shows a Mozilla Firefox browser window with the URL <https://portal.ohphish.com/campaigns>. A pop-up titled "Import Users Info" is displayed, containing a form with the following fields:

- Name: kevin harlanta
- Email: Enter Employee Email
- Reporting Manager Email: Enter Reporting Manager
- Cadre: Enter Cadre
- Designation: Enter Designation
- Department: Enter Department
- Company: Enter Company
- Branch: Enter Branch
- Country: Enter Country

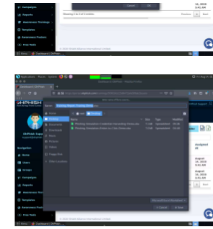
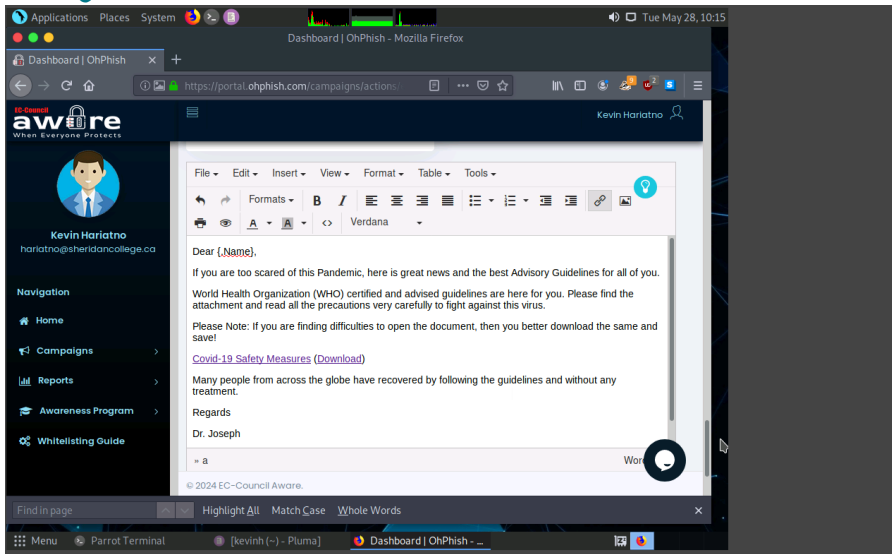
A search bar at the bottom of the pop-up contains the text "Find in page" and options for "Highlight All", "Match Case", and "Whole Words". The browser's taskbar at the bottom shows several open applications, including "Menu", "Parrot Terminal", "[kevinh (~) - Pluma]", and "Dashboard | OhPhish - ...". The system clock in the top right corner indicates "Tue May 28, 10:02".

Exercise 2, Step 28: Click on Safety Measures. If a pop-up appears, stating that a Suspicious link has been detected, and it leads to an untrusted site, click Proceed

NOTE: Emails sent were automatically being deleted/cleared and was unable to receive the Phishing emails. Despite sending the test email as well and launching the campaign itself. I was still able to successfully create the campaign itself based on the app but not test the campaign itself.



2.2 QUESTIONS



87. This way, you can conduct phishing campaigns in organizations and create awareness among employees, to secure themselves and the organization from social engineering attacks.

Question 4.2.1

Conduct a phishing campaign against an organization's security using OhPhish. Flag submission is not required for this task; enter "No flag" as the answer.

No flag

Score

✓ Correct

Conclusion

In conclusion, I have successfully learned about the possibilities of using parrot's SET tools to create phishing campaigns to steal user's account username and passwords. I have also learned about how to leverage GUI Tools to create monitorable phishing campaigns using easy templates and simplified email lists.