Social Engineering Write-Up

Name: ZAHIDAH AZ-ZAHRA BINTI SAFARIZAM

ID: 52215226218

Platform: TryHackMe

Exercise 1: Phishing-Merry Clickmas

1. Objective

The objective of this exercise is to understand how to use the Social-Engineer Toolkit to send phishing emails and harvest credentials by mimicking legitimate login page.

2. Tools/Platform Used
   - TryHackMe
   - Social-Engineer Toolkit (SET)

3. Steps Taken

1. Set up a local environment to simulate a credential collection server.

2. Verified the server connection through a web browser.

3. Used the Social-Engineer Toolkit (SET) to explore social engineering attack options.

4. Selected an email-based phishing attack scenario within the tool.

5. Created a realistic phishing email scenario with a convincing subject line.

6. Configured the email content to include a link to a simulated login page.

7. Observed how user interaction with the phishing email could lead to credential capture.

8. Monitored the server to understand how phishing attacks collect user input.

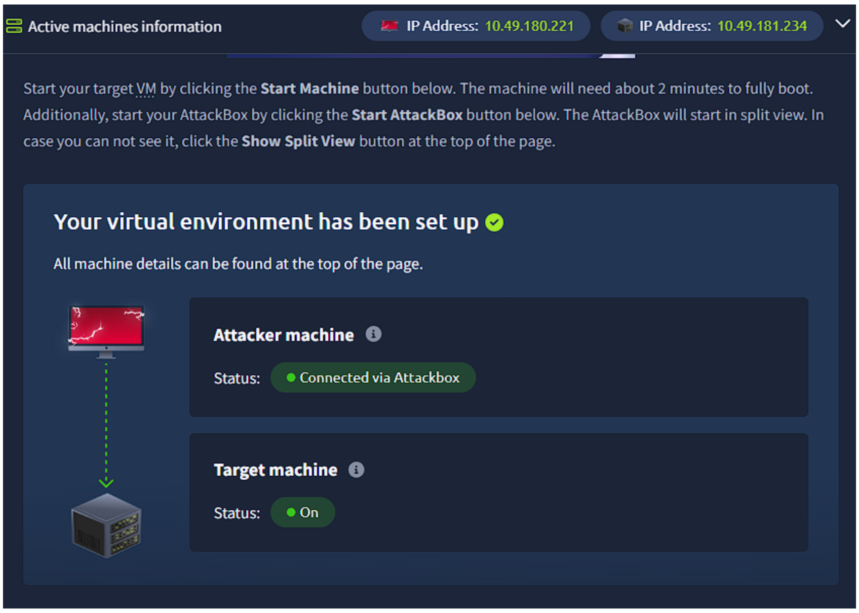
9. Harvest the credentials from target users by using username and password capture.

4. Findings/What I learned
   - Human manipulation plays an important role in phishing attacks, especially through convincing messages and legitimate-looking sender email addresses.
   - Create fake login pages and phish email using the configured SMTP server
   - The Social-Engineer Toolkit (SET) supports various types of social engineering attacks and helps demonstrate how phishing campaigns are created.

5. Conclusion

This exercise gave exposure and awareness education on social engineering attacks by using Social Engineering Toolkit (SET) and showed how simple techniques can be used to deceive users.

6. Evidence


Active machines information
IP Address: 10.49.180.221
IP Address: 10.49.181.234

Start your target VM by clicking the **Start Machine** button below. The machine will need about 2 minutes to fully boot. Additionally, start your AttackBox by clicking the **Start AttackBox** button below. The AttackBox will start in split view. In case you can not see it, click the **Show Split View** button at the top of the page.

Your virtual environment has been set up

All machine details can be found at the top of the page.

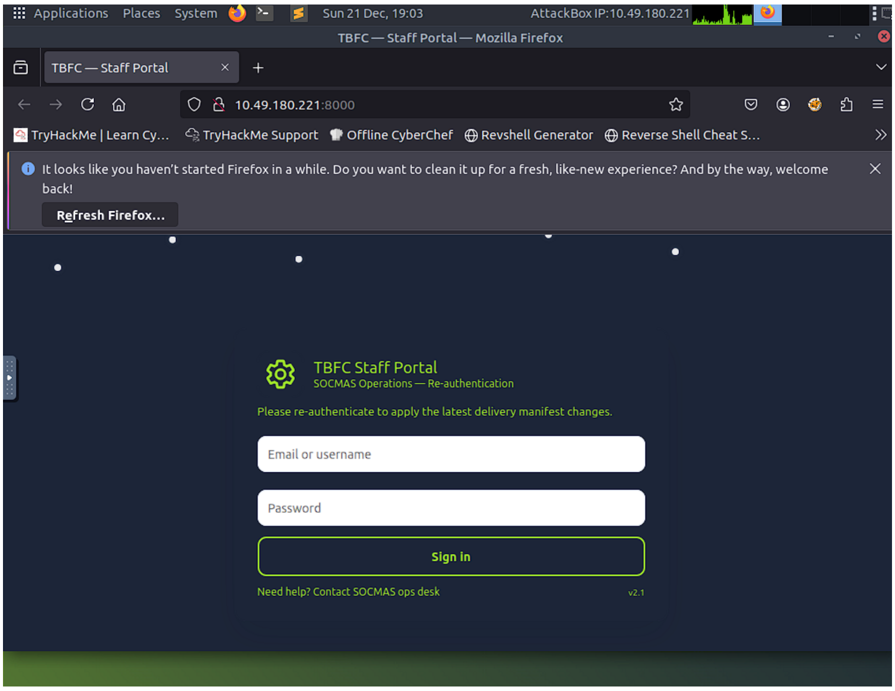
Attacker machine

Status: Connected via Attackbox

Target machine

Status: On

Figure 1: Setup machine



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

TBFC Staff Portal

SOCMAS Operations — Re-authentication

Please re-authenticate to apply the latest delivery manifest changes.

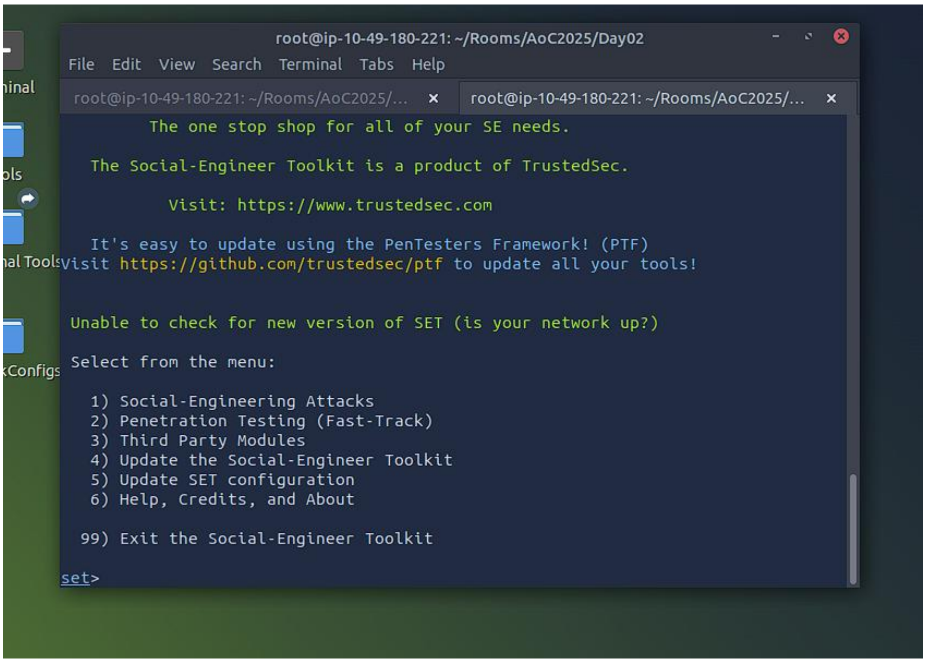
Email or username

Password

Sign in

Need help? Contact SOCMAS ops desk v2.1

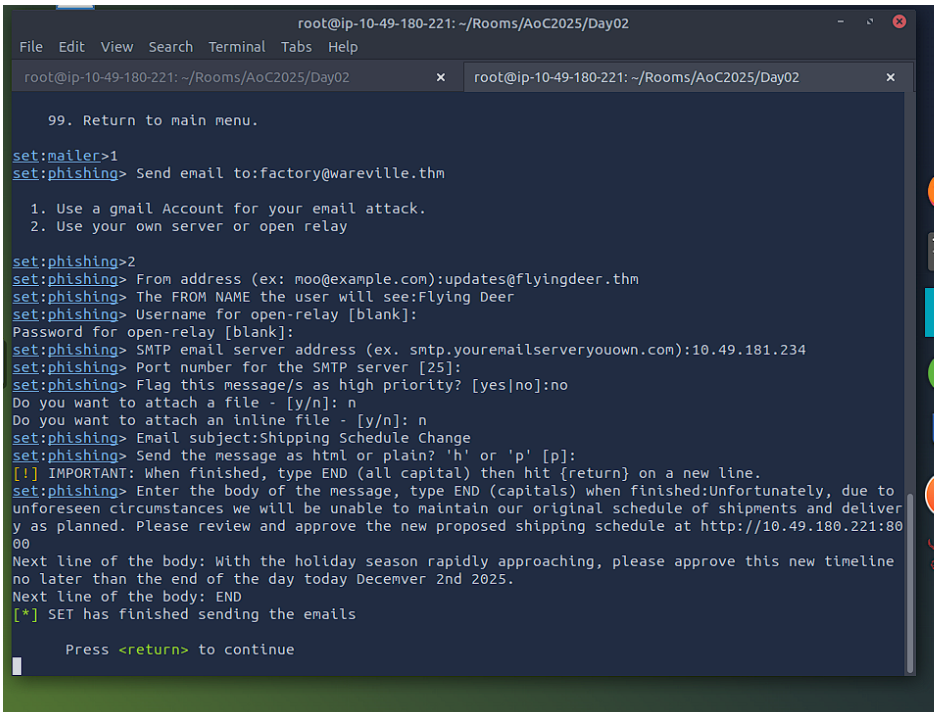
Figure 2: Mimicking legitimate login page



root@ip-10-49-180-221: ~/Rooms/AoC2025/Day02
File Edit View Search Terminal Tabs Help
root@ip-10-49-180-221: ~/Rooms/AoC2025/...
root@ip-10-49-180-221: ~/Rooms/AoC2025/...

```
         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!


 Unable to check for new version of SET (is your network up?)

 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>
```

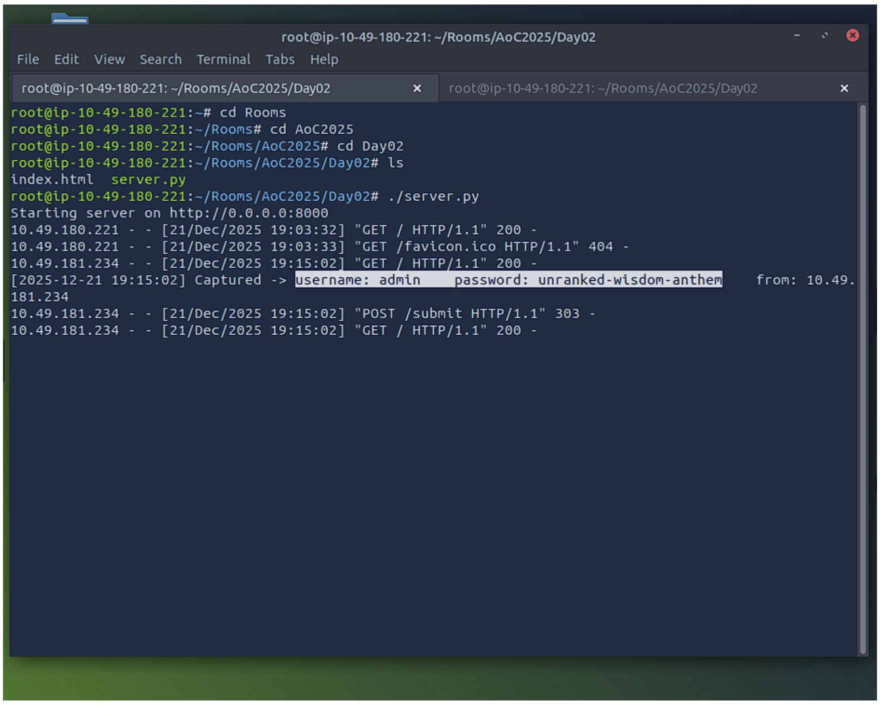
Figure 3: Social Engineering Toolkit (SET) menu based



root@ip-10-49-180-221: ~/Rooms/AoC2025/Day02
File Edit View Search Terminal Tabs Help
root@ip-10-49-180-221: ~/Rooms/AoC2025/Day02
root@ip-10-49-180-221: ~/Rooms/AoC2025/Day02

```
    99. Return to main menu.

set:mailer>1
set:phishing> Send email to:factory@wareville.thm

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):updates@flyingdeer.thm
set:phishing> The FROM NAME the user will see:Flying Deer
set:phishing> Username for open-relay [blank]:
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):10.49.181.234
set:phishing> Port number for the SMTP server [25]:
set:phishing> Flag this message/s as high priority? [yes|no]:no
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Shipping Schedule Change
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new line.
set:phishing> Enter the body of the message, type END (capitals) when finished:Unfortunately, due to
unforeseen circumstances we will be unable to maintain our original schedule of shipments and deliver
y as planned. Please review and approve the new proposed shipping schedule at http://10.49.180.221:80
00
Next line of the body: With the holiday season rapidly approaching, please approve this new timeline
no later than the end of the day today Decemver 2nd 2025.
Next line of the body: END
[*] SET has finished sending the emails

      Press <return> to continue
```

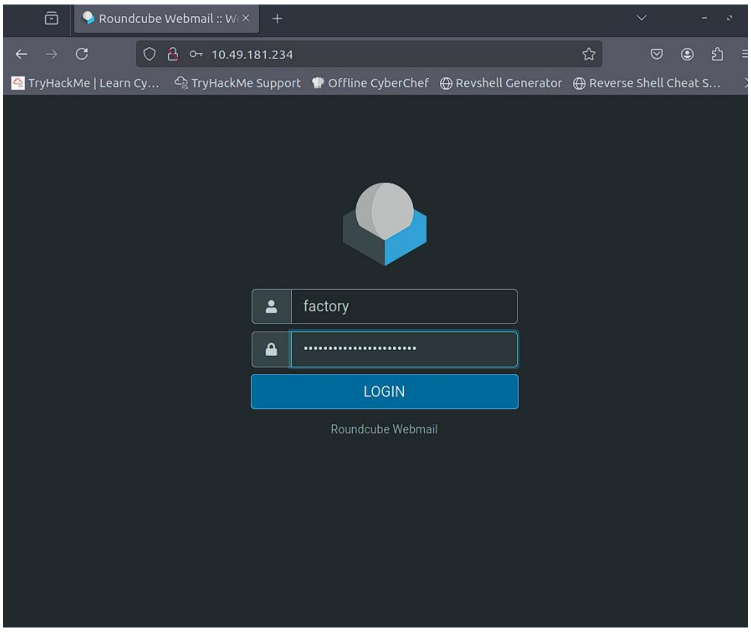
Figure 4: Create phishing email using SET



root@ip-10-49-180-221: ~/Rooms/AoC2025/Day02
File Edit View Search Terminal Tabs Help
root@ip-10-49-180-221: ~/Rooms/AoC2025/Day02
root@ip-10-49-180-221: ~/Rooms/AoC2025/Day02

```
root@ip-10-49-180-221:~# cd Rooms
root@ip-10-49-180-221:~/Rooms# cd AoC2025
root@ip-10-49-180-221:~/Rooms/AoC2025# cd Day02
root@ip-10-49-180-221:~/Rooms/AoC2025/Day02# ls
index.html  server.py
root@ip-10-49-180-221:~/Rooms/AoC2025/Day02# ./server.py
Starting server on http://0.0.0.0:8000
10.49.180.221 - - [21/Dec/2025 19:03:32] "GET / HTTP/1.1" 200 -
10.49.180.221 - - [21/Dec/2025 19:03:33] "GET /favicon.ico HTTP/1.1" 404 -
10.49.181.234 - - [21/Dec/2025 19:15:02] "GET / HTTP/1.1" 200 -
[2025-12-21 19:15:02] Captured -> username: admin    password: unranked-wisdom-anthem    from: 10.49.
181.234
10.49.181.234 - - [21/Dec/2025 19:15:02] "POST /submit HTTP/1.1" 303 -
10.49.181.234 - - [21/Dec/2025 19:15:02] "GET / HTTP/1.1" 200 -
```

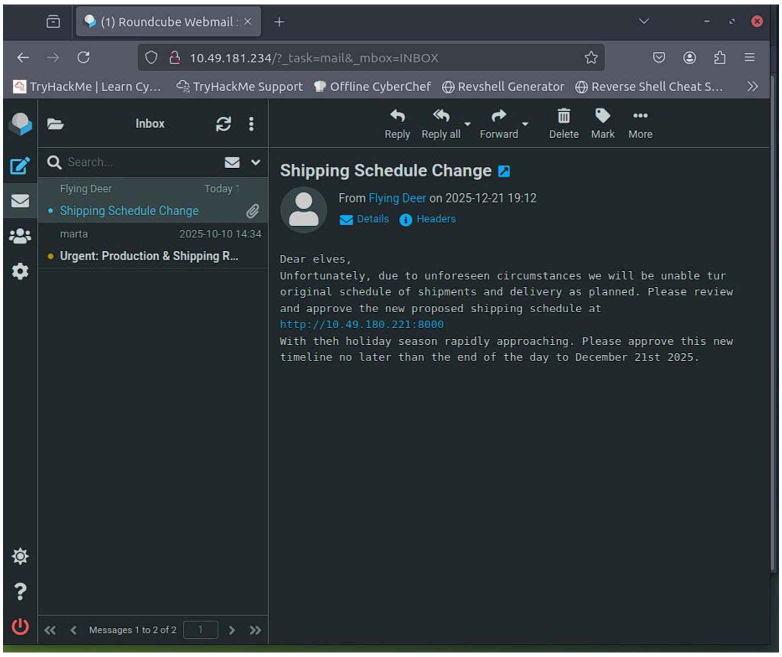
Figure 5: Capture user's username and password



factory

•••••••••••••••••••••••

Figure 6: Access Roundcube Webmail to access user's inbox using user's password



Flying Deer	Today
Shipping Schedule Change	
marta	2025-10-10 14:34
Urgent: Production & Shipping R...	

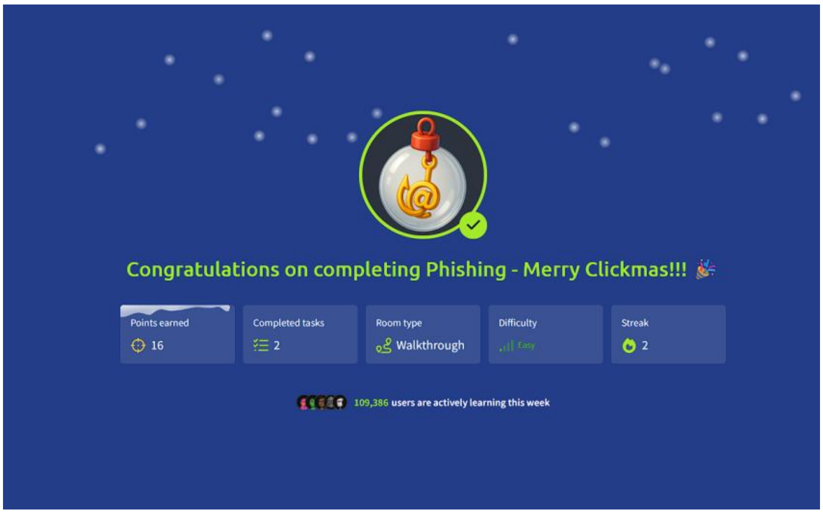
Shipping Schedule Change

From Flying Deer on 2025-12-21 19:12

Details Headers

```
Dear elves,
Unfortunately, due to unforeseen circumstances we will be unable tur
original schedule of shipments and delivery as planned. Please review
and approve the new proposed shipping schedule at
http://10.49.180.221:8000
With theh holiday season rapidly approaching. Please approve this new
timeline no later than the end of the day to December 21st 2025.
```

Figure 7: In target user's inbox and show our email we sent



Congratulations on completing Phishing - Merry Clickmas!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
16	2	Walkthrough	Easy	2

109,386 users are actively learning this week

Figure 8: Complete task