https://bit.ly/37y5Jog

There should be a Kali VM available in /virtual/csc427/

Task 1: Girl Scouts Cookies

Anthony loves cookies. He was once visited by a girl scout and was asked if he would like to buy a box of cookies. He responded that he would love to, and he received a box full of delicious cookies. These were not the cookies Anthony desired and so he set out to create a malicious application that, when run, would steal the victim's cookies. Unfortunately for Anthony, he isn't very good with social engineering, so he was unable to get any girl scouts to run his application. He hired, you, an expert in social engineering to write a phishing email for him.

Your task is to write a phishing email to get the girl scouts to run the application. Things to include are the fake email that you will use, the subject line, and the body of the email. Be creative! YOU DO NOT NEED TO USE SET for this question.

Task 2: Credential Farming

Anthony still felt bitter about the sweet, sweet cookies he got from the Girl Scouts and your excellent phishing email. To satiate his hunger, he requested you to get the Facebook.com credentials of Girl Scouts so that he may exact his revenge.

Your task is to use Social Engineering Toolkit (SET) to CLONE facebook.com to HARVEST the Girl Scouts' credentials. To convince Anthony that it works, send him the Report that the Credential Harvester method creates. Anthony also wants to know how to do it himself (since he saw you do it in five minutes). Give the commands you used in SET to clone Facebook in a steps.txt file (ex.

9
2
3
x.com
…).

If you did not see this, you did not do it correctly:

Copy and paste **[*] We got a hit (printing the output)** to **[*] Hit Control-C to generate the report** into report.txt. It should be the blurb that includes the username and password field.

Task 3: Analyst

Anthony is impressed by your social engineering skills, but is afraid that you might try to socially engineer an attack on him. For his own safety, he asks you to provide him a list of three things that he can do to not fall for your malicious tricks.

Your task is to provide a list of three things that can help Anthony avoid being affected by a social engineering attack. YOU DO NOT NEED TO USE SET for this question.

SUBMIT:
email.txt
report.txt
steps.txt
Analysis.txt

SET Complex Attack Vector:

Using a backdoor trojan to take a picture of your victim with SET:

Run SET as root.
Choose Social Engineering Attacks (option 1).
Create a payload and listener
Enter the IP address for the payload. You can find this by running ifconfig.
Select the payload you want to generate. The Windows Reverse_TCP Meterpreter is a good one.

Then select Backdoored Executable.
Input the port of the listener.
If the Windows Reverse_TCP Meterpreter payload was selected, you should have generated a file called payload.exe. Rename the file to a name that a victim is likely to click on.

Now, to deliver it to them, go back to SET and this time select the Spear-Phishing Attack Vector. From their, choose to perform a mass email attack. Then choose the payload you want to use. We want to use our custom payload, so we will select option 1, input our IP address for the payload and then we will choose option 7 and specify the path to the backdoor executable. Choose the port for the listener and then continue and let SET send the emails.

Once you have caught a fish (victim), we can then migrate their windows explorer to our file explorer. This will ensure that any newly saved files on the victim's computer will also be saved on your filesystem as well. We used the command 'migrate PID', where PID is the PID of the file explorer in windows. Since the PID is variable, set it as necessary. Assuming that the victim has a webcam setup, we can use the command 'webcam_snap' to get a picture of what the webcam sees. SET will inform us of the location the picture is saved on our filesystem. We can follow the path and open the image to get a good look at our victim.