BAB IV

PEMBAHASAN DAN HASIL

4.1 Pembahasan

4.1.1 Alur Penetrasi

1.Pengujian Buta (Blind Testing)

Dalam tes buta, seorang penguji hanya diberi nama seseorang yang menjadi target.

2. Perencanaan (Planning)

Pada tahap ini adalah ruang lingkup Pentest, rentang waktu, dokumen legal (kontrak), jumlah tim yang dibutuhkan. Termasuk apakah sampel diberitahukan terlebih dahulu atau tidak tentang adanya pentest.

3. Pengumpulan Informasi (Information Gathering)

Pada tahapan ini dikumpulkan semua informasi tentang sistem target. Kemudian dilakukan network survey untuk mengumpulkan informasi domain, server, layanan yang ada, IP adress, host, adanya firewall, dan sebagainya. Tools yang dapat digunakan.

4. Penilaian Kerentanan (Vulnerability Assessment)

Setelah mengetahui informasi tentang sistem, pencarian celah keamanan dilakukan secara manual atau otomatis, misalnya dengan tools SET.

5. Eksploitasi (Exploitation)

Pada proses ini dilakukan penentuan target, pemilihan tools dan exploit yang tepat.

6. Reporting

Pada tahapan pembuatan laporan ini biasanya dilaporkan tentang langkah kerja yang dilakukan, celah keamanan yang ditemukan serta usulan perbaikan.

4.1.2 Konfigurasi

Konfigurasi *Fsociety*

a. *sudo git clone https://github.com/Manisso/fsociety.git*

b. *cd fsociety*

c. *ls*

d. *usage: fsociety [-h] [-i] [-s]*

A Penetration Testing Framework

optional arguments:

-h, --help show this help message and exit

-i, --info gets fsociety info

-s, --suggest suggest a tool

Package Fsociety

a. *Menu*

- Pengumpulan Informasi
- Serangan Kata Sandi
- Pengujian Nirkabel
- Alat Eksploitasi
- Mengendus & Memalsukan
- Peretasan Web

- Peretasan Web Pribadi
- Pasca Eksploitasi
- Kontributor
- Memasang pembaharuan

b. *Information Gathering*

- Nmap
- Setoolkit
- Host Ke IP
- WPScan
- Pemindai CMS
- XSStrike
- Dork - Auditor Kerentanan Pasif Google Dorks
- Pindai Pengguna server
- Crips

c. *Passwords Aattacks*

- Cupp
- Ncrack

d. *Wireless Testing*

- Penculik
- Pixiewps
- Honeypot Bluetooth

e. *Exploitation Tools*

- ATSCAN

- sqlmap
- Shellnoob
- Commix
- Lewati Otomatis FTP
- Autopwn JBoss

f. *Sniffing & Spoofing*

- Setoolkit
- SSLtrip
- pyPISHER
- Mailer SMTP

g. *Web Hacking*

- Peretasan Drupal
- Inurlbr
- Pemindai Wordpress & Joomla
- Pemindai Bentuk Gravitasi
- Pemeriksa Unggahan File
- Pemindai Eksploitasi Wordpress
- Pemindai Plugin Wordpress
- Shell dan Pencari Direktori
- Joomla! 1.5 - 3.4.5 eksekusi kode jarak jauh
- Vbulletin 5.X eksekusi kode jarak jauh
- BruteX - Secara otomatis memaksa semua layanan berjalan pada target
- Arachni - Kerangka Pemindai Keamanan Aplikasi Web

h. *Private Web Hacking*

- Dapatkan semua situs web
- Dapatkan situs web joomla
- Dapatkan situs web wordpress
- Penemu Panel Kontrol
- Pencari File Zip
- Unggah Pencari File
- Dapatkan pengguna server
- Pemindai SQLi
- Pemindaian Port (rentang port)
- Pemindaian Port (port umum)
- Dapatkan Info server
- Lewati Cloudflare

i. *Post Exploitation*

- Pemeriksa Shell
- PENYAIR
- Weeman

Konfigurasi *Cewl*

a. sudo apt install cewl

b. root@kali:~# cewl -h

CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

Usage: cewl [OPTIONS] ... <url>

OPTIONS:

-h, --help: Show help.

-k, --keep: Keep the downloaded file.

-d <x>,--depth <x>: Depth to spider to, default 2.

-m, --min_word_length: Minimum word length, default 3.

-o, --offsite: Let the spider visit other sites.

--exclude: A file containing a list of paths to exclude

--allowed: A regex pattern that path must match to be followed

-w, --write: Write the output to the file.

-u, --ua <agent>: User agent to send.

-n, --no-words: Don't output the wordlist.

-g <x>, --groups <x>: Return groups of words as well

--lowercase: Lowercase all parsed words

--with-numbers: Accept words with numbers in as well as just letters

--convert-umlauts: Convert common ISO-8859-1 (Latin-1) umlauts (ä-ae, ö-oe, ü-ue, ß-ss)

-a, --meta: include meta data.

--meta_file file: Output file for meta data.

-e, --email: Include email addresses.

--email_file <file>: Output file for email addresses.

--meta-temp-dir <dir>: The temporary directory used by exiftool when parsing files, default /tmp.

-c, --count: Show the count for each word found.

-v, --verbose: Verbose.

--debug: Extra debug information.

Authentication

--auth_type: Digest or basic.

--auth_user: Authentication username.

--auth_pass: Authentication password.

Proxy Support

--proxy_host: Proxy host.

--proxy_port: Proxy port, default 8080.

--proxy_username: Username for proxy, if required.

--proxy_password: Password for proxy, if required.

Headers

--header, -H: In format name:value - can pass multiple.

<url>: The site to spider.

Konfigurasi *Phoneinfoga*

a. *curl -sSL*

   https://raw.githubusercontent.com/sundowndev/phoneinfoga/master/support/scripts/install | bash

b. *sudo install ./phoneinfoga /usr/local/bin/phoneinfoga*

c. *phoneinfoga -h*

PhoneInfoga is one of the most advanced tools to scan phone numbers using only free resources.

Usage:

phoneinfoga [command]

Examples:

phoneinfoga scan -n <number>

Available Commands:

Help	*Help about any command*
Scan	*Scan a phone number*
scanners	*Display list of loaded scanners*
serve	*Serve web client*
version	*Print current version of the tool*

Flags:

-h, --help help for phoneinfoga

Use "phoneinfoga [command] --help" for more information about a command.

Konfigurasi Social Analyzer

a. pip3 install social-analyzer

b. Qeeqbox/social-analyzer - API and Web App for analyzing & finding a person's profile across 900+ social media websites (Detections are updated regularly)

Arguments:

--username *E.g. johndoe, john_doe or johndoe9999*

--websites *A website or websites separated by space E.g. youtube, tiktok or tumblr*

--mode *Analysis mode E.g.fast -> FindUserProfilesFast, slow -> FindUserProfilesSlow or special -> FindUserProfilesSpecial*

--output *Show the output in the following format: json -> json output for integration or pretty -> prettify the output*

--options *Show the following when a profile is found: link, rate, title or text*

--method *find -> show detected profiles, get -> show all profiles regardless detected or not, all -> combine find & get*

--filter *Filter detected profiles by good, maybe or bad, you can do combine them with comma (good,bad) or use all*

--profiles *Filter profiles by detected, unknown or failed, you can do combine them with comma (detected,failed) or use all*

--countries *select websites by country or countries separated by space as: us brru*

--type *Select websites by type (Adult, Music etc)*

--top *select top websites as 10, 50 etc...[--websites is not needed]*

--extract *Extract profiles, urls & patterns if possible*

--metadata *Extract metadata if possible (pypi QeeqBox OSINT)*

--trim *Trim long strings*

--gui *Reserved for a gui (Not implemented)*

--cli *Reserved for a cli (Not needed)*

--screenshots *Get screenshots from detected profiles (This needs --logs)*

--simplify *Print the detected profiles only (links)*

Listing websites & detections:

--list *List all available websites*

Setting:

--headers Headers as dict

--logs Turn logs on or off

--logs_dir Change logs directory

--timeout Change timeout between each request

--silent Disable output to screen

Konfigurasi *URLBuster*

a. python3

b. sudo pip3 instal urlbuster

c. urlbuster –help

d. usage: urlbuster [options] -w <str>/-W <file> BASE_URL

urlbuster -V, --version

urlbuster -h, --help

urlbuster: error: the following arguments are required: BASE_URL

Konfigurasi *Sherlock*

a. sudo apt install sherlock

b. root@kali:~# sherlock -h

usage: sherlock [-h] [--version] [--verbose] [--folderoutput FOLDEROUTPUT]

[--output OUTPUT] [--tor] [--unique-tor] [--csv] [--xlsx]

[--site SITE_NAME] [--proxy PROXY_URL] [--json JSON_FILE]

[--timeout TIMEOUT] [--print-all] [--print-found] [--no-color]

[--browse] [--local] [--nsfw]

USERNAMES [USERNAMES ...]

Sherlock: Find Usernames Across Social Networks (Version 0.14.2)

positional arguments:

USERNAMES One or more usernames to check with social networks. Check similar usernames using {%} (replace to '_', '-', '.').

options:

-h, --help show this help message and exit

--version Display version information and dependencies.

--verbose, -v, -d, --debug Display extra debugging information and metrics.

--folderoutput FOLDEROUTPUT, -fo FOLDEROUTPUT If using multiple usernames, the output of the results will be saved to this folder.

--output OUTPUT, -o OUTPUT If using single username, the output of the result will be saved to this file.

--tor, -t Make requests over Tor; increases runtime; requires Tor to be installed and in system path.

--unique-tor, -u Make requests over Tor with new Tor circuit after each Request; increases runtime; requires Tor to be installed and in system path.

--csv Create Comma-Separated Values (CSV) File.

--xlsx *Create the standard file for the modern Microsoft Excel spreadsheet (xslx).*

--site SITE_NAME *Limit analysis to just the listed sites. Add multiple options to specify more than one site.*

--proxy PROXY_URL, -p PROXY_URL

Make requests over a proxy. e.g. socks5://127.0.0.1:1080

--json JSON_FILE, -j JSON_FILE

Load data from a JSON file or an online, valid, JSONfile.

--timeout TIMEOUT *Time (in seconds) to wait for response to requests (Default: 60)*

--print-all *Output sites where the username was not found.*

--print-found *Output sites where the username was found.*

--no-color *Don't color terminal output*

--browse, -b *Browse to all results on default browser.*

--local, -l *Force the use of the local data.json file.*

--nsfw *Include checking of NSFW sites from default list.*

Rekayasa sosial.

Pengujian Rekayasa Sosial

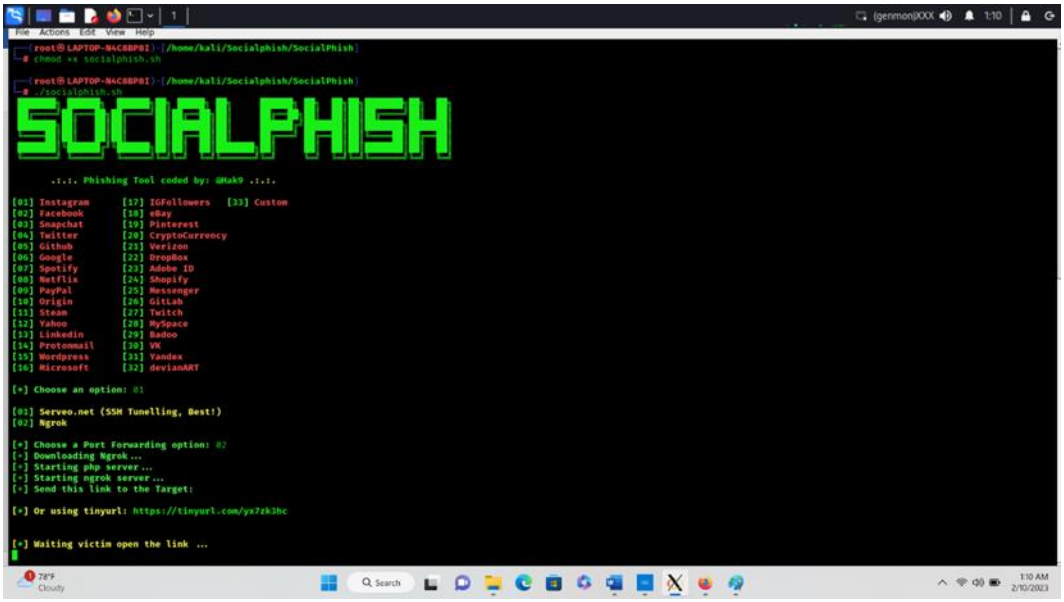
social-analyzer --username "raihantinoalbaihaqi --metadata --top 100

Pengelabuan. Penyerang dapat menggunakan informasi media sosial yang dikumpulkan untuk menipu pengirim pesan email dan mengelabui pengguna agar mengklik tautan atau mengirimkan data pribadi penyerang. Alamat email karyawan tingkat tinggi dapat dipalsukan dengan pesan yang menginstruksikan penerima

untuk mengirim uang, mengeklik tautan berbahaya, atau membalas dengan data sensitive.

```
┌──(kali㉿LAPTOP-N4C8BP8I)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿LAPTOP-N4C8BP8I)-[/home/kali]
└─# cd Socialphish
bash: cd: Socialphish: No such file or directory

┌──(root㉿LAPTOP-N4C8BP8I)-[/home/kali]
└─# mkdir Socialphish

┌──(root㉿LAPTOP-N4C8BP8I)-[/home/kali]
└─# cd SOcialphish
bash: cd: SOcialphish: No such file or directory

┌──(root㉿LAPTOP-N4C8BP8I)-[/home/kali]
└─# cd Socialphish

┌──(root㉿LAPTOP-N4C8BP8I)-[/home/kali/Socialphish]
└─# git clone https://github.com/xHak9x/SocialPhish.git
Cloning into 'SocialPhish'...
remote: Enumerating objects: 392, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 392 (delta 0), reused 2 (delta 0), pack-reused 389
Receiving objects: 100% (392/392), 7.92 MiB | 5.27 MiB/s, done.
Resolving deltas: 100% (121/121), done.

┌──(root㉿LAPTOP-N4C8BP8I)-[/home/kali/Socialphish]
└─# ls
SocialPhish

┌──(root㉿LAPTOP-N4C8BP8I)-[/home/kali/Socialphish]
└─# cd SocialPhish

┌──(root㉿LAPTOP-N4C8BP8I)-[/home/kali/Socialphish/SocialPhish]
└─# ls
LICENSE  README.md  sites  socialphish.sh
```

```
┌──(root㉿LAPTOP-N4C8BP8I)-[/home/kali/Socialphish/SocialPhish]
└─# chmod +x socialphish.sh

┌──(root㉿LAPTOP-N4C8BP8I)-[/home/kali/Socialphish/SocialPhish]
└─# ./socialphish.sh
```

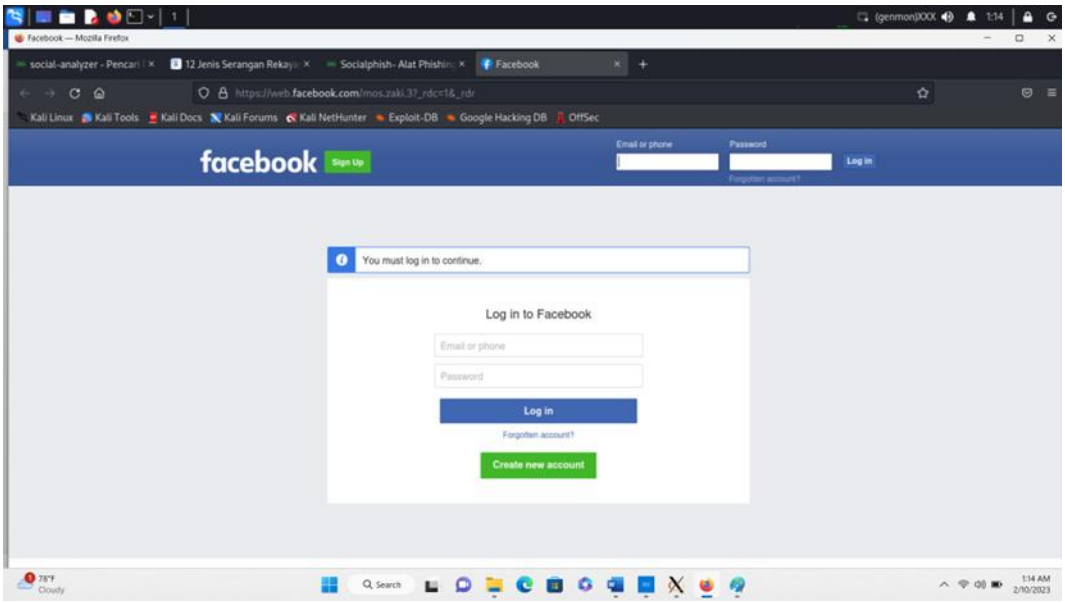


Gambar 4.1 Terminal Socialphish

https://tinyurl.com/yx7zk3hc

Gambar 4.2 Link Phish

Tautan tersebut telah dibuat oleh alat yang merupakan halaman web phishing Instagram/Facebook. Kirim tautan ini ke korban. Begitu dia membuka tautan, dia akan mendapatkan halaman web asli Instagram yang mirip dan begitu dia mengisi detail di halaman web. Ini akan disorot di terminal Socialphish.



Gambar 4.3 Formulir Phish

Formulir phising Facebook, Ketika pengguna membuka tautan akun dan mengisi formulir tersebut semua detail akan ditampilkan di terminal socialphish.

Tabel Penetrasi 4.1

Pengujian Buta (*Blind Testing*)	*a.radxxx*
Perencanaan (*Planning*)	*Melakukan Penetrasi sampai dengan selesai membutuhkan waktu paling lambat 5 jam bergantung pada tujuan penetrasi – Sampel Mengetahui – Jumlah Tim 1*
Pengumpulan Informasi (*Information Gathering*)	*Manual*
Penilaian Kerentanan (*Vulnerability Assessment*)	*Manual*
Eksploitasi (*Exploitation*)	*Fsociety Package, Cewl, Phoninfoga, URLBuster*

Tabel 4.2 Tabel Ancaman

Platform	Rekayasa Sosial	Eksploitasi Data	Phising	Pelanggaran Data	Malware
Instagram	√	√	√	√	√
Facebook	√	√	√	√	√
WhatsApp	√	√	√	√	√

Tabel 4.3 Klasifikasi Malware

Klasifikasi Malware	Instagram	Facebook	WhatsApp
Keylogger	0	0	0
Worm	0	0	0
Trojan	0	0	0
Rootkit	0	0	0
Ransomware	0	0	0
Adware	0	0	0
Spyware	1	1	1
Botnet	0	0	1

Keylogger

Keylogger atau perekam keyboard merupakan tindakan merekam aktivitas pengetikan di keyboard tanpa sepengetahuan user. Hasil record yang terekam akan dikirimkan ke pelaku keylogger.

Worm

Worm memiliki cara kerja yang sama seperti virus, yakni menduplikasi dirinya sendiri dan menyebar ke seluruh komputer. Bedanya, worm lebih efektif dan bisa berjalan sendiri tanpa bantuan Anda, sementara virus biasanya bekerja apabila mengeklik file yang telah terinfeksi.

Efektivitas worm membuat jenis malware ini digunakan untuk menyerang server website, e-mail, dan database. Worm bisa pula menyebar cepat melalui internet dan jaringan komputer setelah berhasil menginfeksi suatu server.

Trojan

Trojan Horse merupakan malware yang menyamar menjadi program yang sah atau valid untuk mengelabui. Trojan akan terus bersembunyi di komputer sampai user membuka program tersebut.

Program Trojan yang terbuka digunakan oleh pelaku untuk mengintai aktivitas., mencuri data sensitif, bahkan bisa mengakses sistem computer. Trojan berasal dari aktivitas phising yang dilakukan melalui e-mail atau website yang di kunjungi.

Rootkit

Rootkit merupakan sekumpulan malware yang dibuat oleh pelaku untuk menahan perintah dan kontrol terhadap komputer tanpa diketahui oleh pengguna. alhasil, komputer akan dikontrol secara penuh oleh pelaku setelah terinfeksi rootkit. Pelaku akan mengintai penggunaan komputer mengambil file serta mengubah pengaturan sistem secara jarak jauh. Rata-rata software antivirus sulit menghapus rootkit sehingga pengguna harus membangun ulang sistem komputer yang telah disusupi.

Ransomware

Ransom berarti tebusan. Artinya, malware ini akan menolak akses ke data atau sistem komputer sampai korban membayar uang tebusan. Selama tebusannya belum dibayarkan, pelaku akan berusaha untuk mencuri data atau menyebarkan virus ke komputer.

Adware

Jenis malware ini tidak cukup berbahaya, tetapi sangat mengganggu kenyamanan saat browsing. Adware akan memunculkan pop-up iklan secara terus-menerus di layar ketika pengguna mengunjungi sebuah website, adware merupakan taktik pelaku untuk mengelabui pengguna. Adware mendukung program lain sehingga ada file atau software yang terinstal di perangkat tanpa pengguna sadari.

Spyware

Spyware merupakan jenis malware yang bisa memperoleh akses atau informasi rahasia mengenai perusahaan. Malware ini akan berusaha untuk mencuri informasi penggunaan internet, keuangan, atau bahkan karyawan.

Spyware mengintai kebiasaan saat mengakses internet dan riwayat penelusuran. Data yang didapat dari malware kemudian dijual kepada oknum yang tidak bertanggung jawab.

Botnet

Robot network alias botnet merupakan kumpulan bot yang dikendalikan dari jarak jauh. Botnet akan menyusup ke suatu jaringan keamanan yang terhubung pada sistem komputer. Botnet lebih berbahaya karena bisa menyebar ke peralatan lain yang memerlukan internet (internet of things) seperti printer dan mesin cnc. Botnet juga menyerang website melalui serangan DDoS sehingga website tidak bisa diakses untuk sementara.

Tabel 4.4 Klasifikasi Rekayasa Sosial

Klasifikasi Rekayasa Sosial	Instagram	Facebook	WhatsApp
Baiting	0	0	0
Spear phishing	1	1	1
Pretexting	1	1	1

Tabel 4.5 Klasifikasi Eksploitasi Data

Klasifikasi Data Eksploitasi	Instagram	Facebook	WhatsApp
Any	1	1	1

Tabel 4.6 Klasifikasi Pelanggaran Data

Klasifikasi Pelanggaran Data	Instagram	Facebook	WhatsApp
Any	1	1	1

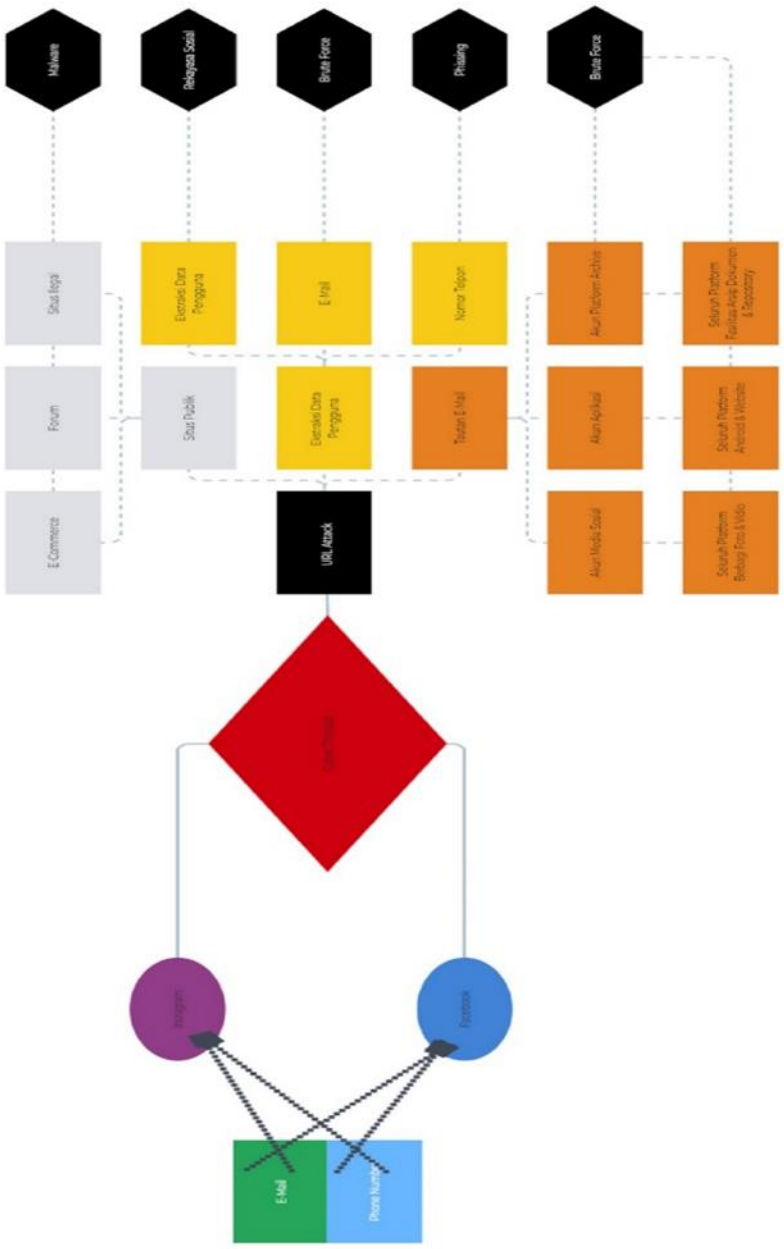
Tabel 4.7 Klasifikasi *Phising*

Klasifikasi Phising	Instagram	Facebook	WhatsApp
Whaling	1	1	1
Media Social Phising	1	1	1
Business email compromise	1	1	1

Tabel 4.8 Variabel

Variabel Ancaman	Instagram	Facebook	WhatsApp	
16	7	7	7	Skor

4.2 Hasil



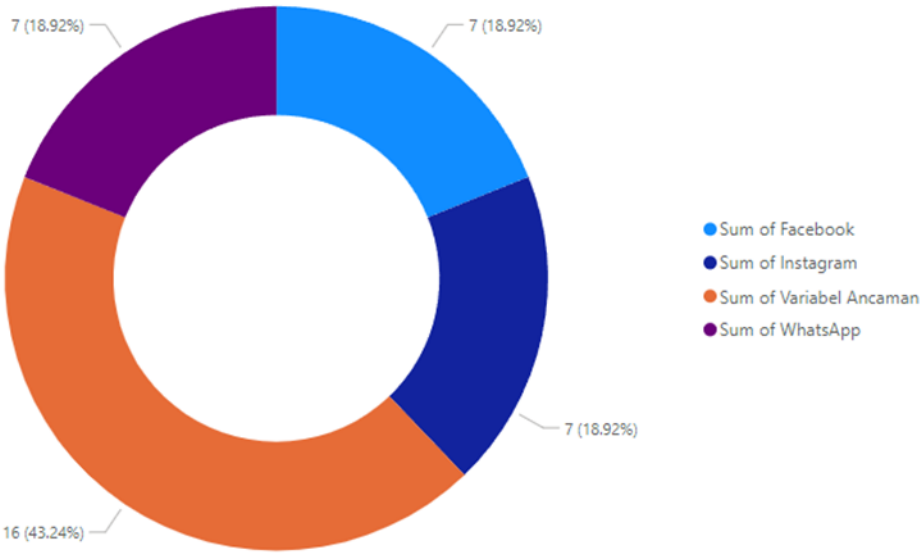
Gambar 4.4 *Brainstroming*

Struktur *Brainstroming*

Brainstorm yang digunakan untuk memetakan ide, kata, gambar, dan konsep terkait secara bersamaan. Brainstorms merupakan alat dan metode untuk menghasilkan ide, menemukan asosiasi, mengklasifikasikan ide,

mengatur informasi dan memvisualisasikan struktur. Brainstorm sering digunakan pada tahap awal proyek dan berfungsi sebagai bentuk pencatatan.

Visualisasi Chart Donuts



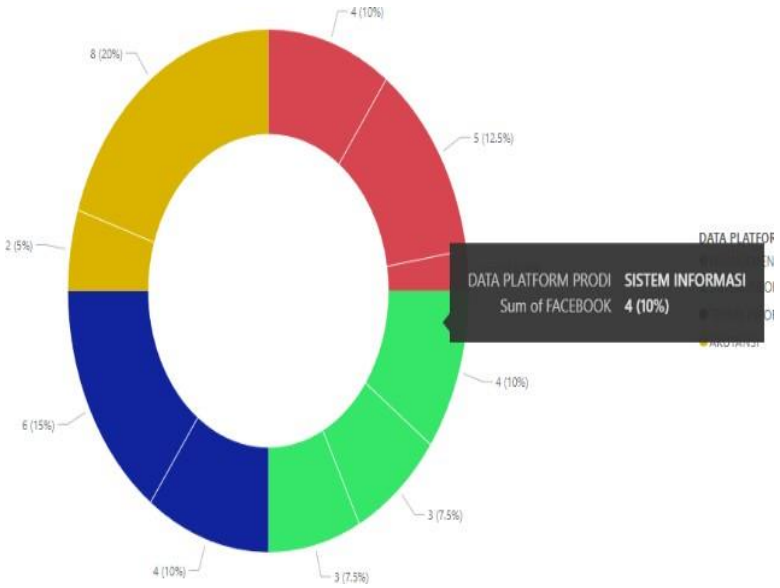
Gambar 4.5 *Chart Donuts*

Struktur Visualisasi *Chart Donuts*

Struktur Chart Donuts bekerja pada dua dimensi, dan oleh karena itu, diperlukan dua kumpulan informasi dengan hubungan yang sama. Dimensi pertama mewakili atribut, dan dimensi kedua mewakili nilainya, dalam penelitian ini ancaman siber terdiri dari 16 ancaman yang terdiri dari phising, malware rekayasa sosial, eksploitasi data serta pelanggaran data dan perilaku pengguna media sosial memiliki 18.92% ancaman berdasarkan pengujian penetrasi terhadap pengujian buta.

Indikator Facebook Prodi Sistem Informasi

Indikator pengguna platform facebook pada prodi sistem informasi

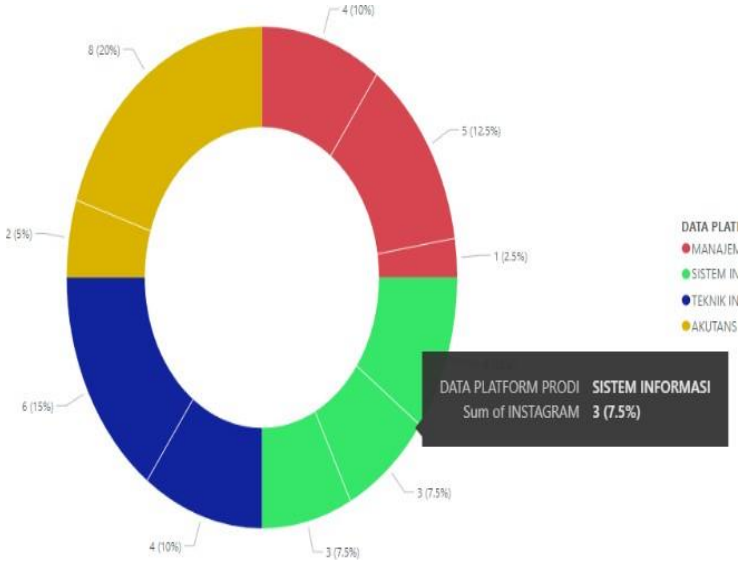


Gambar 4.6 *Donut chart* Facebook SI

Pada gambar 4.6 dijelaskan bahwa tampilan pengguna facebook pada prodi sistem informasi terdapat nilai rasio 10% dari masing-masing pengguna platform facebook dari setiap prodi yaitu Sistem informasi, Teknik informatika, Manajemen dan Akutansi.

Indikator Instagram Prodi Sistem Informasi

Indikator pengguna platform instagram pada prodi sistem informasi

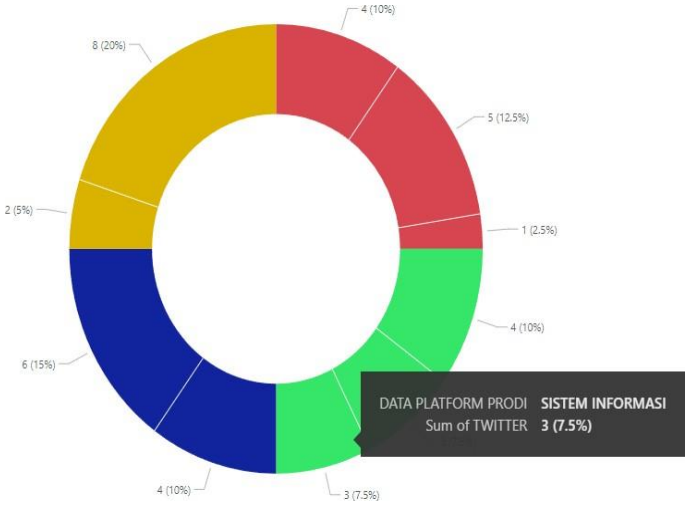


Gambar 4.7 *Donut Chart* Instagram SI

Pada gambar 4.7 dijelaskan bahwa tampilan pengguna facebook pada prodi sistem informasi terdapat nilai rasio 7,5% dari masing-masing pengguna platform Instagram dari setiap prodi yaitu Sistem informasi, Teknik informatika, Manajemen dan Akutansi.

Indikator Pengguna Twitter Prodi Sistem Informasi

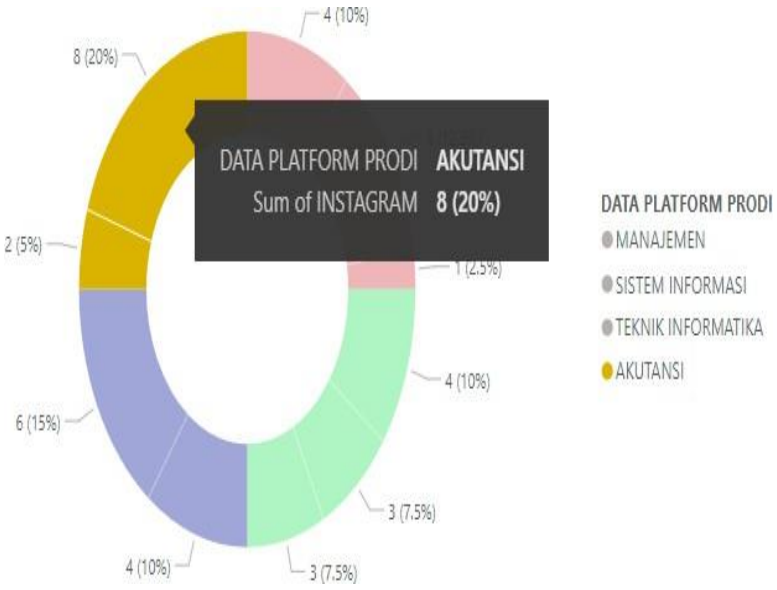
Indikator pengguna platform instagram pada prodi sistem informasi



Gambar 4.8 *Donut Chart* Twitter SI

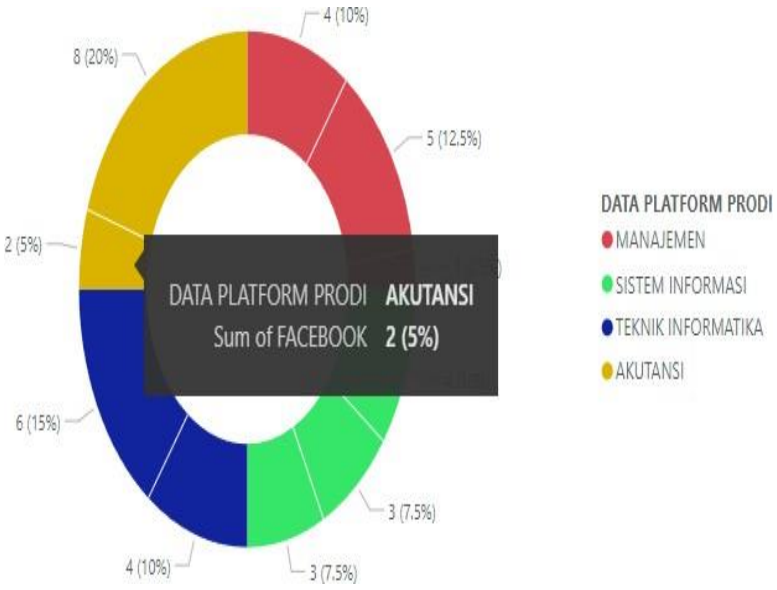
Pada gambar 4.8 dijelaskan bahwa tampilan pengguna twitter pada prodi sistem informasi terdapat nilai rasio 7,5% dari masing-masing pengguna platform twitter dari setiap prodi yaitu Sistem informasi, Teknik informatika, Manajemen dan Akutansi.

Indikator Pengguna Instagram Prodi Akuntansi



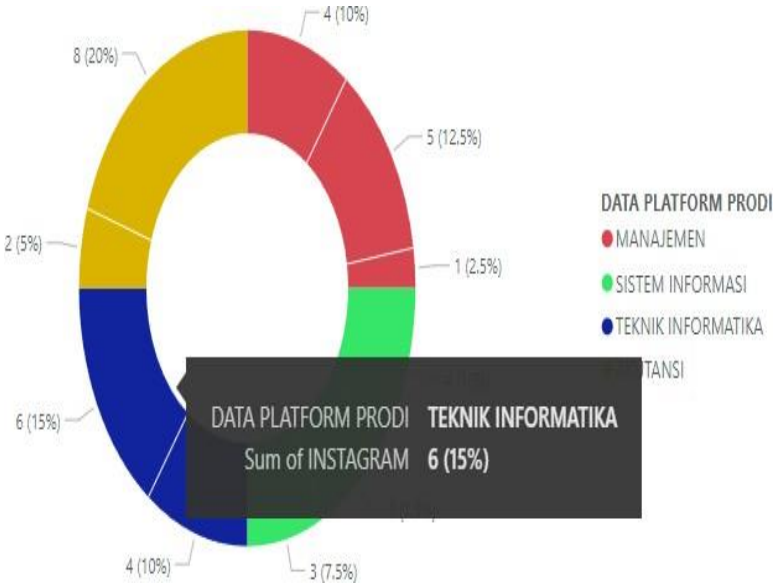
Gambar 4.9 *Donut Chart* Instagram AK

Indikator Pengguna Facebook Prodi Akuntansi



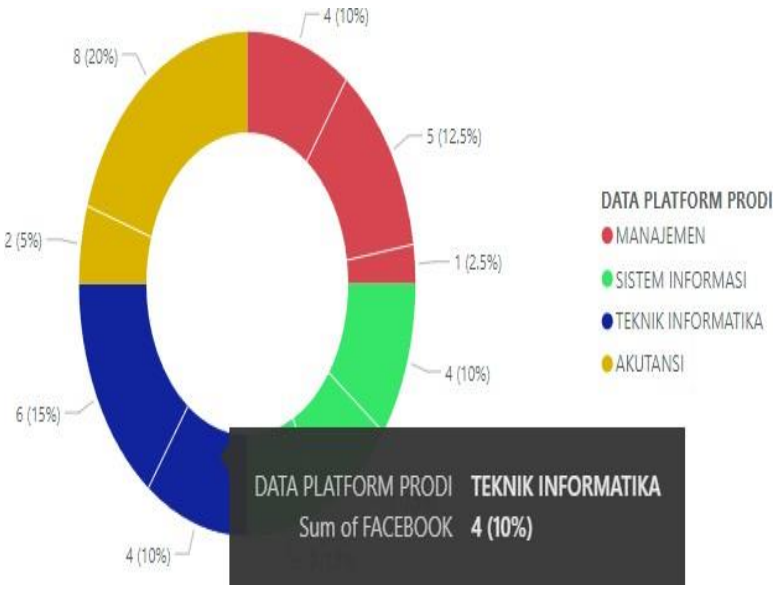
Gambar 4.10 *Donut Chart* Facebook AK

Indikator Instagram Teknik Informatika



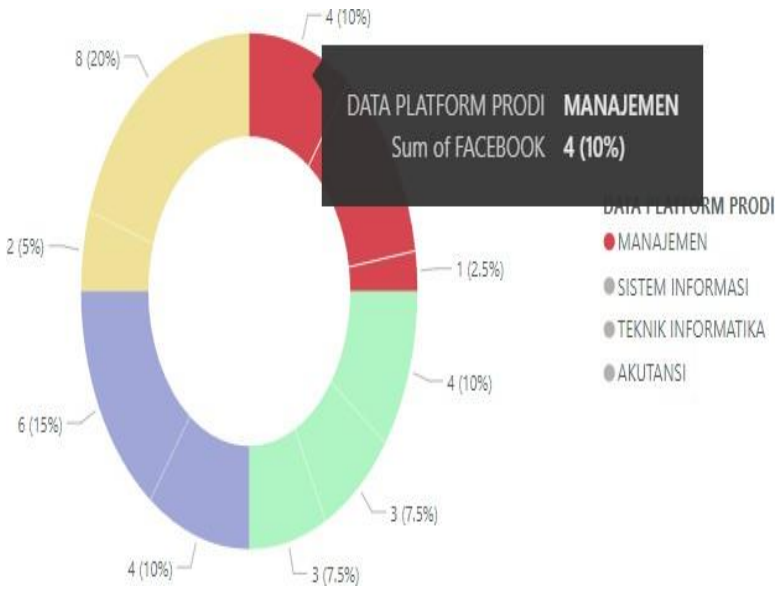
Gambar 4.11 *Donut Chart* Instagram TI

Indikator Facebook Teknik Informatika



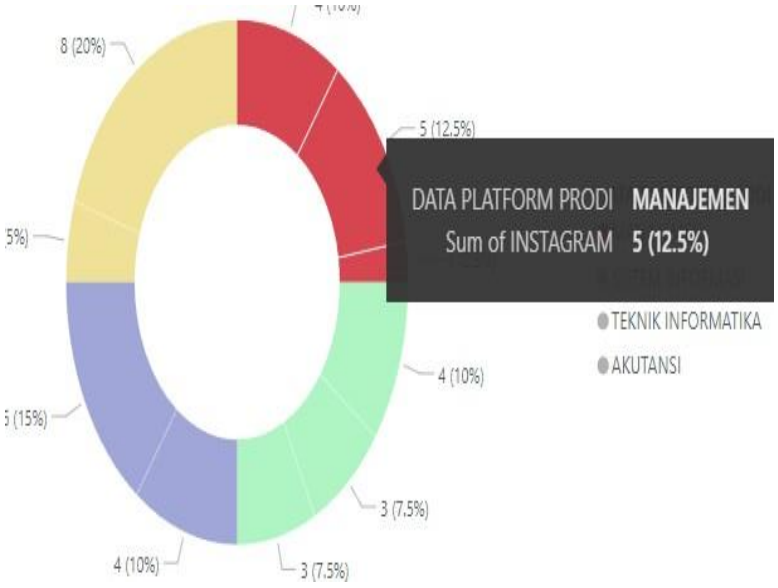
Gambar 4.12 *Donut Chart* Facebook TI

Indikator Facebook Manajemen



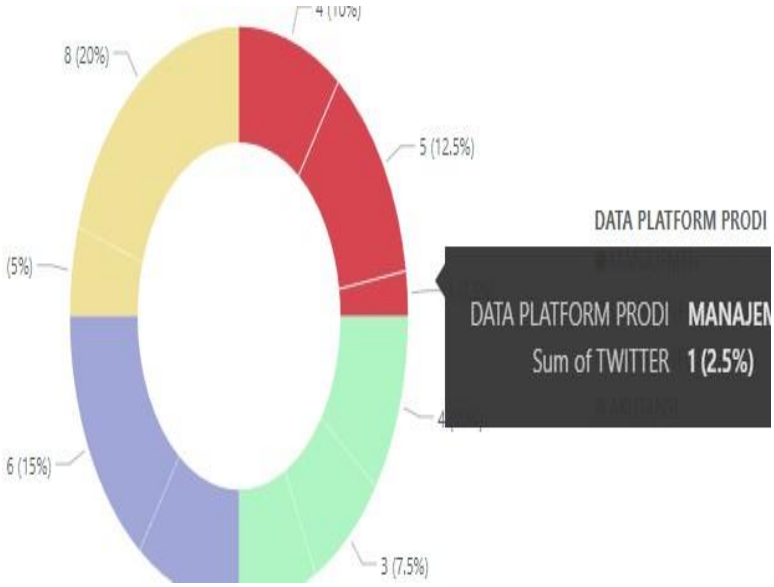
Gambar 4.13 *Donut Chart* Facebook MAN

Indikator Instagram Manajemen



Gambar 4.14 *Donut Chart* Instagram MAN

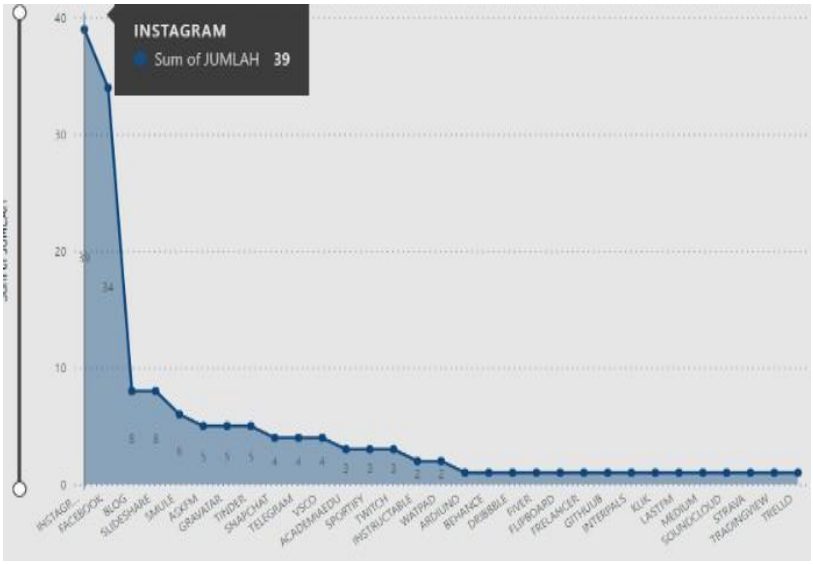
Indikator Pengguna Twitter Prodi Manajemen



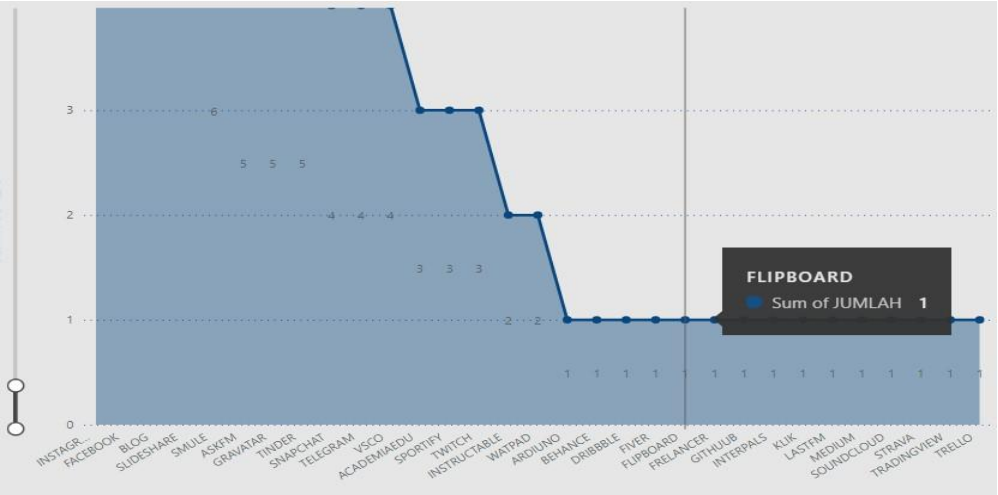
Gambar 4.15 *Donut Chart* Twitter MAN

4.3 Area Chart

Area chart menggambarkan suatu keseluruhan pengguna platform tertinggi samapaiplatform dengan pengguna terendah berdasarkan seluruh data dari setiap program studi Sistem informasi, Teknik informatika, Manajemen dan Akutansi.



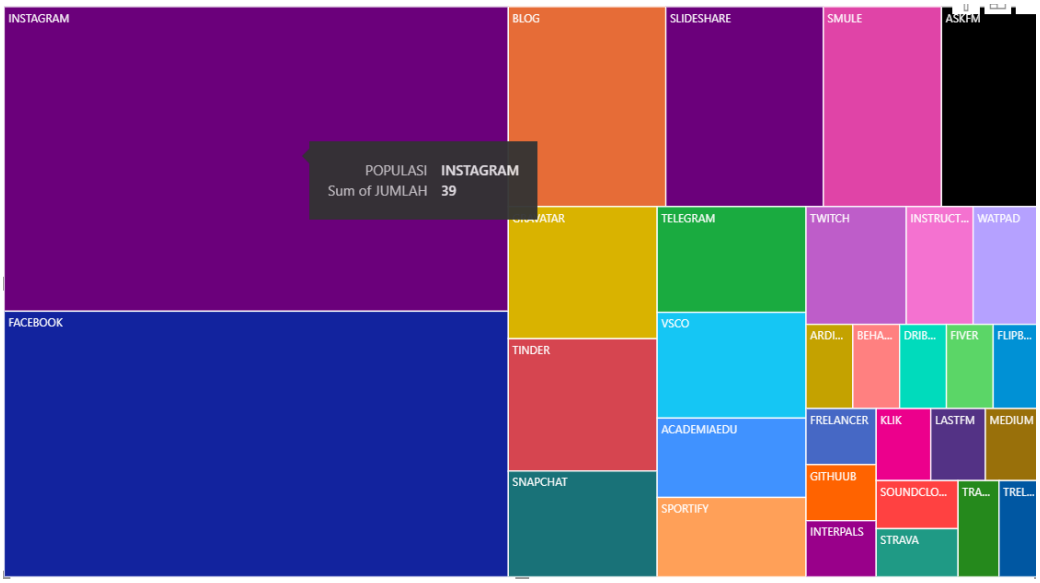
Gambar4.16 *Area Chart* 1



Gambar 4.17 *Area Chart* 2

4.4 Tree Map

TreeMap menggambarkan suatu populasi dengan menampilkan data untuk menggambarkan kondisi dengan block besar untuk nilai value tinggi dan kecil denganvalue rendah.



Gambar 4.18 *TreeMap*

TreeMap terdiri beberapa platform dengan jumlah pengguna tertentu

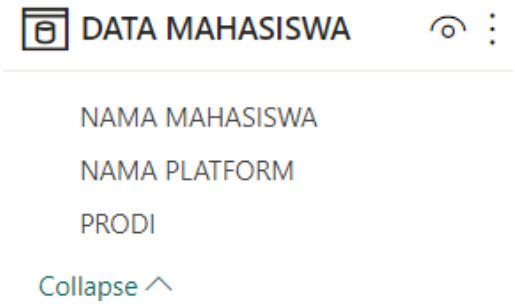
INSTAGRAM	=	39	(26 %)
FACEBOOK	=	34	(22.67%)
SNAPCHAT	=	4	(2.67%)
TINDER	=	5	(3.33%)
ASKFM	=	5	(3.33%
VSCO	=	4	(2.67)
GITHUUB	=	1	(0.67%)
SLIDESHARE	=	8	(5.33%)
ACADEMIAEDU	=	3	(2%)
BLOG	=	8	(5.33%)
TWITCH	=	3	(2%)
INSTRUCTABLE	=	2	(1.33%)
SMULE	=	6	(4%)
SPORTIFY	=	3	(2%)
WATPAD	=	2	(1.33%)
FIVER	=	1	(0.67%)
FLIPBOARD	=	1	(0.67%)
FRELANCER	=	1	(0.67%)
ARDIUNO	=	1	(0.67%)
MEDIUM	=	1	(0.67%)
INTERPALS	=	1	(0.67%)
TELEGRAM	=	4	(2.67%)
STRAVA	=	1	(0.67%)
GRAVATAR	=	5	(3.33%)
BEHANCE	=	1	(0.67%)
LASTFM	=	1	(0.67%)
TRADINGVIEW	=	1	(0.67%)
TRELLO	=	1	(0.67%)
DRIBBBLE	=	1	(0.67%)
KLIK	=	1	(0.67%)
SOUNDCLOUD	=	1	(0.67%)

Presentase data dengan nilai tertinggi dan terendah sebagai berikut : (Instagram 26%),

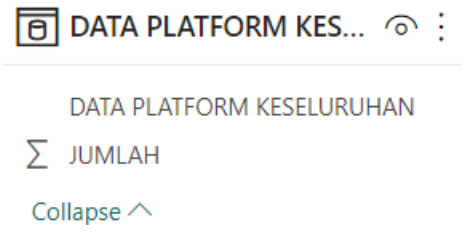
(Soundcloud,Klik,Dribble,Trello,Tradingview,Lastfm,Behance,Strava,Interpals,Medi

um,Ardiuno,Frelancer,Flipboard,Fiver,Instructable,Github 0.67%)

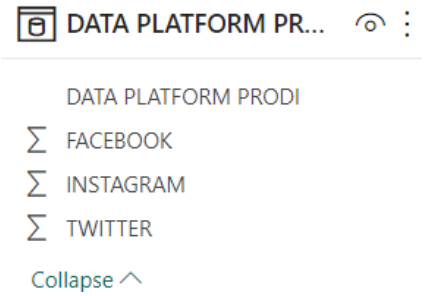
4.5 Tabel Data



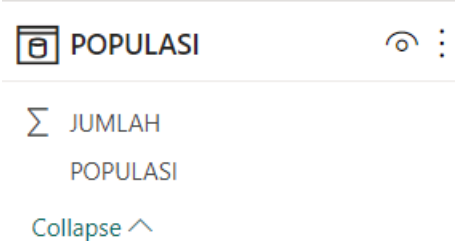
Gambar 4.19 Tabel Data Mahasiswa



Gambar 4.20 Tabel Data Platform

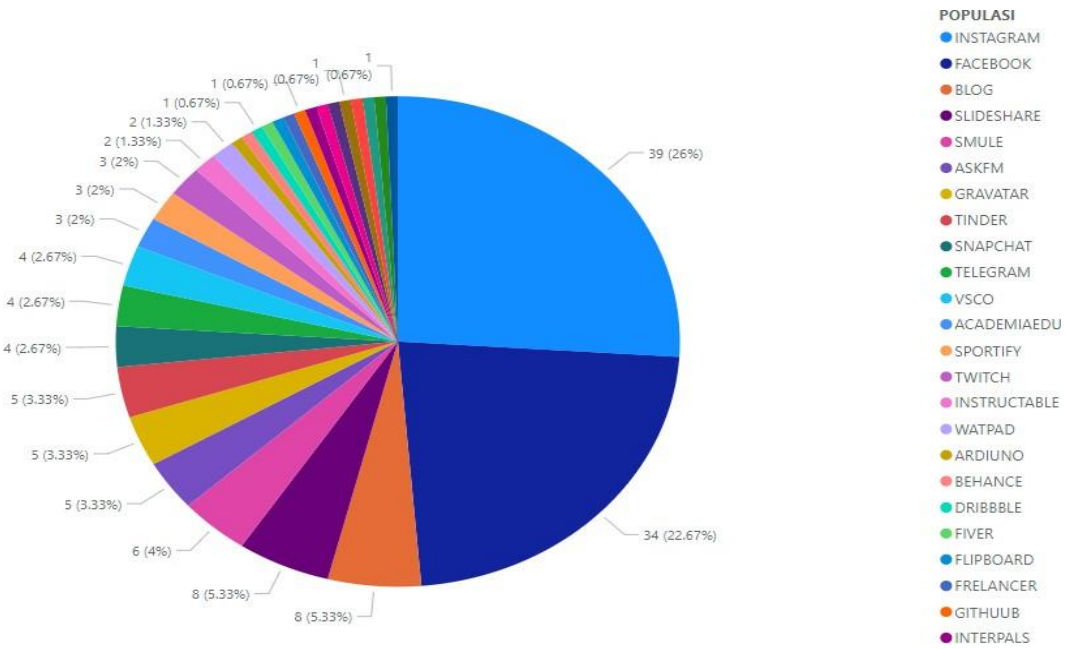


Gambar 4.21 Tabel Data Prodi



Gambar 4.22 Tabel Data Populasi

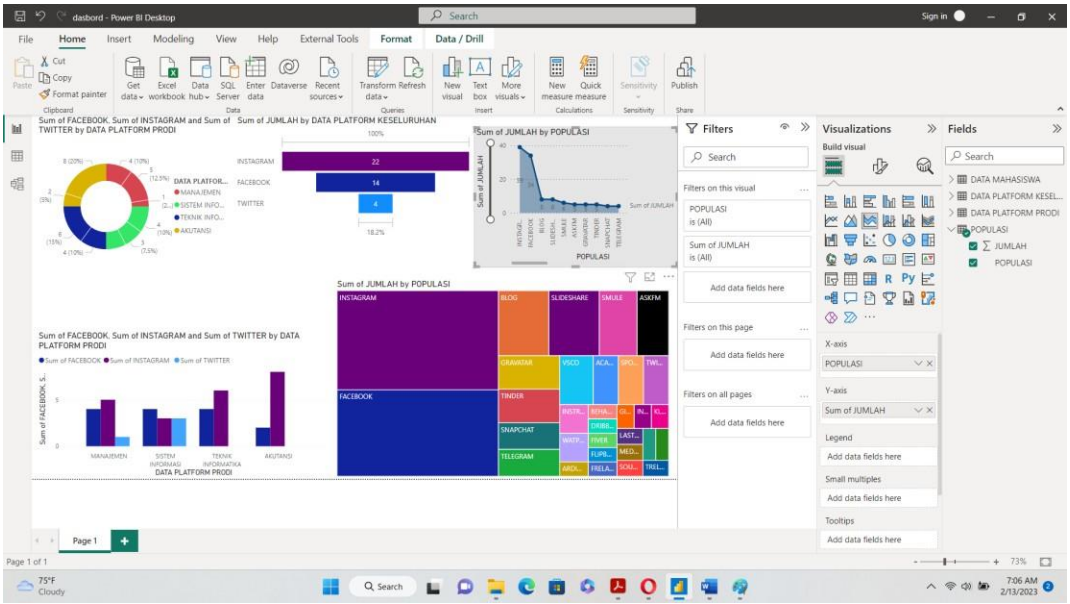
4.5 Hasil Gafik *Pie*



Gambar 4.23 Grafik *Pie*

Grafik Pie menggambarkan rasio penggunaan platform media sosial pada seluruhpopulasi mahasiswa pada program studi yang berbeda.

4.6 Dashboard



Gambar 4.24 *Dashboard*

Visualisasi pada dashboard sistem informasi merupakan visualisasi data statistik yang bertujuan untuk memudahkan pengguna membaca data statistik dalam bentuk visual. Terdapat beberapa jenis visualisasi dalam dashboard ini berikut diantaranya : *Donut Chart, Funnel, Stacked Area Chart, Line and clustered, Treemaps.*