

**LAPORAN RESPONSI
UJIAN TENGAH SEMESTER GENAP
PRAKTIKUM KEAMANAN INFORMASI 1**



DISUSUN OLEH:

Nama : Yana Dayinta Nesthi
Kelas : RI4AA
NIM : 21/478358/SV/19272
Dosen : Anni Karimatul Fauziyyah, S.Kom., M.Eng.

**SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023**

RESPONSI UJIAN TENGAH SEMESTER GENAP

A. LATAR BELAKANG

Pengintaian/Reconnaissance mengacu pada pengumpulan informasi tentang target, yang merupakan langkah pertama dalam setiap serangan terhadap suatu sistem. Pengintaian membantu penyerang mempersempit ruang lingkup upaya mereka dan membantu dalam pemilihan senjata serangan. Penyerang menggunakan informasi yang dikumpulkan untuk membuat cetak biru, atau "jejak", dari organisasi, yang membantu mereka memilih strategi yang paling efektif untuk membahayakan sistem dan keamanan jaringan. Demikian pula, penilaian keamanan sistem atau jaringan dimulai dengan pengintaian dan pelacakan target. Penguji penetrasi (pen) harus mengumpulkan informasi yang cukup tentang target evaluasi sebelum memulai penilaian. Peretas etis harus mensimulasikan semua langkah yang biasanya diikuti penyerang untuk mendapatkan gambaran yang adil tentang postur keamanan organisasi target.

Dalam skenario ini, Anda bekerja sebagai peretas etis dengan organisasi besar. Organisasi Anda khawatir dengan berita tentang vektor serangan baru yang mengganggu organisasi besar di seluruh dunia. Selain itu, organisasi Anda pernah menjadi target pelanggaran keamanan besar di masa lalu saat data pribadi beberapa pelanggannya terekspos ke situs jejaring sosial. Anda telah diminta oleh manajer senior untuk melakukan penilaian keamanan proaktif terhadap perusahaan. Sebelum Anda dapat memulai penilaian apa pun, Anda harus mendiskusikan dan menentukan ruang lingkup dengan manajemen; ruang lingkup penilaian mengidentifikasi sistem, jaringan, kebijakan dan prosedur, sumber daya manusia, dan komponen lain dari sistem yang memerlukan evaluasi keamanan. Anda juga harus setuju dengan manajemen tentang aturan keterlibatan (RoE)—penilaian “apa yang boleh dan tidak boleh dilakukan”. Setelah Anda memiliki persetujuan yang diperlukan untuk melakukan peretasan etis, Anda harus mulai mengumpulkan informasi tentang organisasi target.

B. LANGKAH RESPONSI

Setelah Anda secara metodologis memulai proses footprinting, Anda akan mendapatkan cetak biru profil keamanan organisasi target. Istilah "cetak biru" mengacu pada profil sistem unik dari organisasi target sebagai hasil dari footprinting. Pada tugas ini Anda akan mengumpulkan berbagai informasi tentang organisasi target dari berbagai sumber terbuka atau yang dapat diakses publik OSINT.

C. TUGAS

1. Buatlah Dokumen yang berisi data pengintaian informasi tentang organisasi target yang mencakup, pada:
 - a. Informasi Organisasi
 - b. Informasi Network

Domain, sub-domain, blok jaringan, topologi jaringan, firewall, alamat IP dari sistem yang dapat dijangkau, catatan Whois, catatan DNS, dan informasi terkait lainnya

- c. Informasi Sistem operasi, OS server web, akun pengguna dan kata sandi, dll
2. Anda dapat mengikuti panduan atau menambahkan teknik pengintaian yang sudah dipelajari di pertemuan praktikum
3. Semakin lengkap isi dokumen blue print pengintaian meliputi bukti/langkah ekstrak informasi, analisa hasil

Panduan Pengintaian

- a. Footprinting dengan search engine
Memasukkan di kolom pencarian target www.eccouncil.org
 - o intitle:password site:www.eccouncil.org
 - o EC-Council filetype:pdf
- b. Footprinting dengan social media melalui youtube
 - o Ambil link salah satu video ec-council copy ke url <https://citizenevidence.amnestyusa.org/>.
- c. Menemukan Domains and Sub-domains dengan Netcraft
 - o Masuk ke url <https://www.netcraft.com>
 - o Klik pada Resources tab pada menu bar dan klik Site Report link di bawah menu Tools
 - o Pada tampilan search masukkan alamat www.eccouncil.org
- d. Gather data orang melalui peekyou
 - o Akses <https://www.peakyou.com>. Pada First Name dan Last Name, masukkan nama Satya dan Nadella. Pada Location drop-down box, pilih Washington, DC.
- e. Gather Email List dengan theHarvester

- Akses terminal kali linux masuk ke root

```
(root@kali)-[/home/kali]
# theHarvester -d microsoft.com -l 200 -b baidu
```

- e. Informasi OS

- Masuk ke <https://censys.io/domain?q=>. inputkan target url misal www.eccouncil.org

f. Gather social media dengan theHarvester

- Akses terminal kali linux masuk ke root

- Ketikan : theHarvester -d eccouncil -l 200 -b linkedin

- theHarvester -d www.eccouncil.org -l 500 -b google

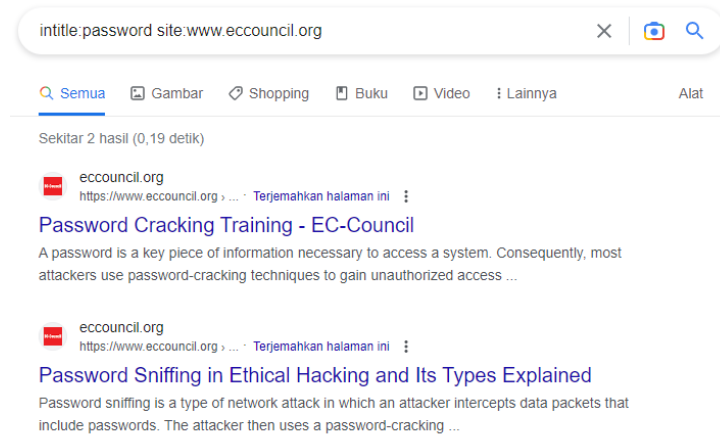
- theHarvester -d www.eccouncil.org -l 500 -b all

- theHarvester -d www.eccouncil.org -l 100 -b all -f test.html

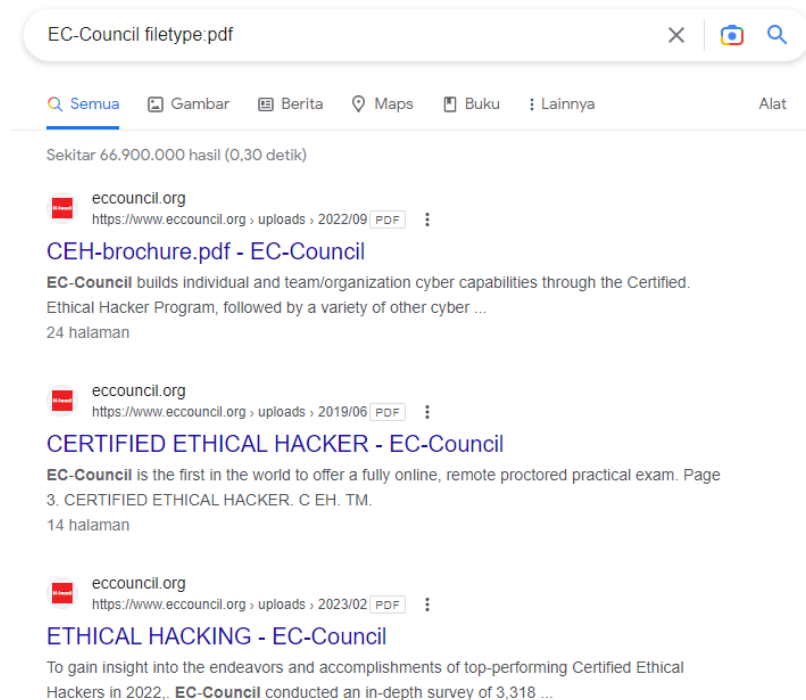
D. HASIL

a. Footprinting dengan search engine

- Memasukkan di kolom pencarian target www.eccouncil.org
- intitle:password site:www.eccouncil.org

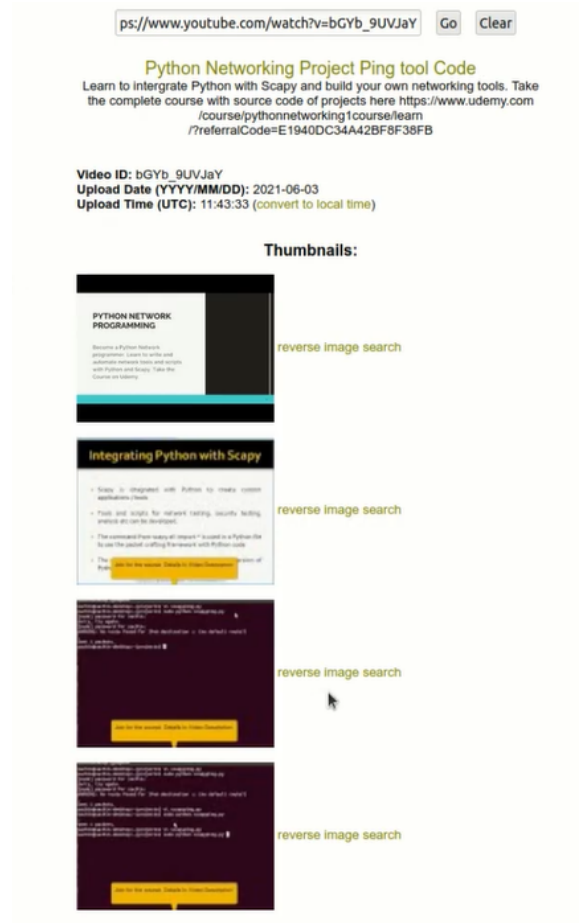


- EC-Council filetype:pdf




b. Footprinting dengan social media melalui youtube

- Ambil link salah satu video ec-council copy ke url <https://citizenevidence.amnestyusa.org/>



- c. Menemukan Domains and Sub-domains dengan Netcraft
- Masuk ke url <https://www.netcraft.com>
 - Klik pada Resources tab pada menu bar dan klik Site Report link di bawah menu Tools
 - Pada tampilan search masukkan alamat www.eccouncil.org

DOMAIN (pada bagian network)



[Services](#)
[Solutions](#)
[News](#)
[Company](#)
[Resources](#)
[Q](#)
[Discover More](#)
[Report Fraud](#)

Background

Site title	EC-Council Certifications Best Cybersecurity Courses & Training		Date first seen	February 2002
Site rank	1554	Netcraft Risk Rating	0/10	
Description	Get certified from EC-Council for the best cyber security courses & training online. Enroll now to boost your career with cybersecurity courses & Get started now!		Primary language	English

Network

Site	http://www.eccouncil.org	Domain	eccouncil.org	
Netblock Owner	Cloudflare, Inc.	Nameserver	henry.ns.cloudflare.com	
Hosting company	Cloudflare	Domain registrar	pir.org	
Hosting country	US	Nameserver organisation	whois.cloudflare.com	
IPv4 address	104.18.9.180 (VirusTotal)	Organisation	REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, US	
IPv4 autonomous systems	AS13335	DNS admin	dns@cloudflare.com	
IPv6 address	2006:4700:0:0:0:0:6812:8b4	Top Level Domain	Organization entities (.org)	
IPv6 autonomous systems	AS13335	DNS Security Extensions	Enabled	
Reverse DNS	unknown			

IP delegation

IPv4 address (104.18.9.180)

IP range	Country	Name	Description
::ffff:0:0:0:0/96	United States	IANA-IPv4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
↳ 104.16.0.0-104.31.255.255	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 104.18.9.180	United States	CLOUDFLARENET	Cloudflare, Inc.


IPv6 address (2006:4700:0:0:0:0:6812:8b4)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inetStnum object
↳ 2006::/12	United States	NET6-2000	American Registry for Internet Numbers
↳ 2006:4700::/32	United States	CLOUDFLARENET	Cloudflare, Inc.
↳ 2006:4700:0:0:0:0:6812:8b4	United States	CLOUDFLARENET	Cloudflare, Inc.

SUB DOMAIN:

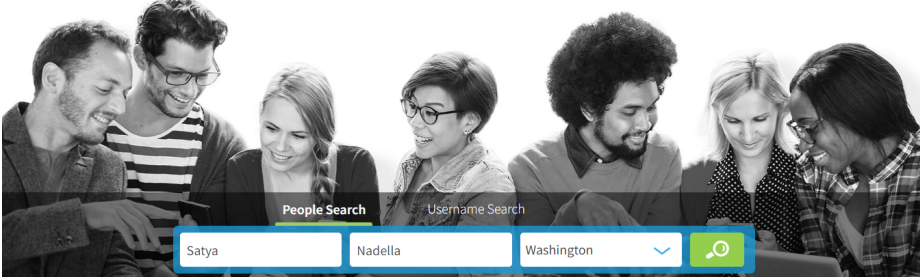
Rank	Site	First seen	Netblock	OS	Site Report
583	aspen.eccouncil.org	June 2010	Cloudflare, Inc.	Linux	
665	codeded.eccouncil.org	January 2020	Cloudflare, Inc.	Linux	
921	cyberq.eccouncil.org	October 2018	Cloudflare, Inc.	Linux	
1013	iclass.eccouncil.org	October 2009	Cloudflare, Inc.	Linux	
1554	www.eccouncil.org	February 2002	Cloudflare, Inc.	Linux	
7630	cert.eccouncil.org	March 2012	Cloudflare, Inc.	Linux	
10184	store.eccouncil.org	July 2013	Cloudflare, Inc.	Linux	

- d. Gather data orang melalui peekyou
- Akses <https://www.peekyou.com>. Pada First Name dan Last Name , masukkan nama Satya dan Nadella. Pada Location drop-down box, pilih Washington, DC.



Fast People Search Made Easy


Find friends, relatives and colleagues across the Web.



People Search

Username Search

People Search > Nadella > Satya Nadella > Florida > Marco Island > Satya Nadella



Satya Nadella, Age 53

Current Address:

S Collier Blvd, Marco Island, FL

Past Addresses:

See available information

Phone Number:

(239) 394-XXXX

Email Address:

See available information

UNLOCK PROFILE

Phone & Email (1)

All Addresses (1)

Family

Social


Court

And More

PHONE & EMAIL (1)

We found 1 phone number and email address.

See Satya's contact info now >



(239) 394-XXXX

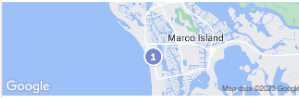
Marco Island, FL • CenturyLink

SEE CONTACT DETAILS >

ADDRESS HISTORY (1)

We found 1 address for Satya.

See where Satya has lived >



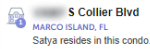
Address information for Satya may include:

Current Address

Past Addresses

Property Owner

Home Value



S Collier Blvd

MARCO ISLAND, FL


Satya resides in this condo.

View more

FAMILY MEMBERS

Locate relatives by name and age

Search for Satya's family members >



Family member details may include:

Name & Age

Contact Info

Demographics

Location

Historical Records*

3.9 BILLION RECORDS


Search for birth, death, marriage, divorce, US Census, and military records.

View more

SOCIAL PROFILES

Search for profiles by email and username.

Uncover Satya's photos, videos, and more >



Social information for Satya may include:

Online Aliases

Photos and Videos

Dating Sites

Posts and Wish Lists

Online Social Data

120+ SOCIAL NETWORKS


Powerful social search locates profiles on social networks, dating sites, online shopping, web forums, music platforms, etc.

View more

COURT RECORDS*

Spokeo accesses over 620 million court records.

Search for criminal records now >



Court record search results may include:

Arrests

Sex Offenders

Traffic Violations

Felonies

Nationwide & State Records

UPDATED MONTHLY

Spokeo searches nationwide and local databases for court records, including available offense details, dates, and convictions.

View more

ADDITIONAL DETAILS

Personal details for Satya may include >

Personal Information

VITAL INFO & HISTORICAL RECORDS

Uncover details about birth, marriage, and divorce. Find census, military, and other historical records.*

Wealth

PROPERTY, HOUSEHOLD INCOME, & MORE

View property details and household demographic information related to income, investments, and interests.

Work

EMPLOYMENT HISTORY

Discover work experience, company details, and more.

e. Gather Email List dengan theHarvester

```
(root@kali)-[/home/kali]
# cd

(root@kali)-[~]
# theHarvester -d microsoft.com -l 200 -b baidu

[*] Searching Baidu.

[*] No IPs found.

[*] Emails found: 1
-----
yuwa@microsoft.com

[*] Hosts found: 3
-----
mcp.microsoft.com:168.61.188.172
support.microsoft.com:23.195.240.116
www.microsoft.com:23.195.241.152
```

f. Informasi OS

Masuk ke <http://censys.io/domain?q=www.eccouncil.org> inputkan target url misal

Full Text Searches

When no field is specified, Censys attempts a full-text search over all fields.

For example, searching for `Dell` will return hosts whose `location.city` is "Dell Rapids" in addition to hosts whose `services.software.vendor` is "Dell." If you're interested in Dell-manufactured devices, you'd want to specify fields where that information is stored.

Specifying Fields and Values

Effective searches will specify the field where an attribute is stored. For this, you'll need to know the fields in the dataset you're searching.

See a full list of fields and their value types under the **Data Definitions** tab or choose to view **Raw Data** on a details page, such as the [table view of the host](#) for Google Public DNS.

A typical search provides at least one field—which reflects the nesting of the JSON schema using dot notation (e.g., `services.http.response.headers.server.headers`)—and a value. If the value type is text, a fuzzy match would be returned as a result; if the value type is keyword, only an exact match would be returned.

For example, you can search for all hosts with an HTTP service returning an HTTP status code by specifying the field and value: `services.http.response.status_code: 500`.

Wildcards

By default, Censys searches for complete values. For example, the search `Dell` will not return records that contain the word `Dell`. Wildcards can be used to expand a search to include partial matches in the results.

There are two wildcards:

- `?` — This wildcard indicates a single character.
- `*` — This wildcard indicates zero or more characters.

Combining wildcards can be extremely useful as well.

The query below leverages knowledge of the CPE software format and searches for services running Microsoft IIS web servers with a major version <10 (because the `?` represent only a single character) and a minor version identified (because of the presence of the period). The `*` wildcard accounts for the rest of the CPE format:

```
services.software.uniform_resource_identifier: "cpe:2.3:a:microsoft:iis:?.*"
```

Networks, Protocols, and Ports

Search for blocks of IP addresses using CIDR notation (e.g., `ip: 23.20.0.0/14`) or by providing a range: `ip: [23.20.0.0 to 23.20.5.34]`. Search for hosts running a particular protocol by searching the service name field: `services.service_name: ST`. Search for hosts with specific ports by searching the port field: `services.port: 3389`.

Combining Search Criteria with Boolean Logic

Combine multiple search criteria using `and`, `or`, `not`, and parentheses. Booleans are case insensitive.

By default, criteria combined by boolean expressions are evaluated against a host as a whole.

AND

Searching for `services.port: 8880 and services.service_name: HTTP` will return hosts that have port 8880 open (with ANY service running on it) and a HTTP service running on ANY port.

To search for HTTP services running on port 8880, use the `same_service()` function: `same_service(services.port: 8880 and services.service_name: HTTP)`.

OR

Searching for `services.port: 21 or services.service_name: FTP` will return any hosts that have either port 21 open (with ANY service running on it) and an FTP service running on ANY port.

NOT

Searching for `not same_service(service_name: HTTP and port: 443)` would return hosts that do not have HTTP running on 443.

Searching for `same_service(service_name: "HTTP" and not port:443)` would return any host that has an HTTP service that is not running on port 443. This could include hosts that have HTTP on 443, as long as there is one other HTTP service on a different port number.

Ranges

Search for ranges of numbers using `[` and `]` for inclusive ranges and `{` and `}` for exclusive ranges. For example, `services.http.response.status_code: [500 to 503]`. Dates should be formatted using the following syntax: `[2012-01-01 to 2012-12-31]`. One-sided limits can also be specified: `[2012-01-01 to *]`. The `to` operator is case insensitive.

Regular Expressions

Regexes are restricted to paid customers. The full regex syntax is [available here](#).

NOTE Censys regex searches are case-insensitive except when the exact match operator `=` is used.

For example, `services.software.vendor:/De[1]+/` will return results where the word is either capitalized or lowercase, while `services.software.vendor=/De[1]+/` will only return results for the capitalized word.

- g. Gather social media dengan theHarvester

Akses terminal kali linux, masuk ke root

Ketikkan: theHarvester -d eccouncil -l 200 -b linkedin

```
[~](kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌─(root㉿kali)-[/home/kali]
└─# theHarvester -d eccouncil -l 200 -b linkedin

*****
 *                               *
 * | _ | |_ / \ ^ / \ . _ / \ x = | _ |   *
 * | _ | | | \ / \ C | | _ V \ \ X ||_ |   *
 *                                         *
 *                                     *
 * theHarvester 3.2.3                  *
 * Coded by Christian Martorella       *
 * Edge-Security Research              *
 * cmartorella@edge-security.com      *
 *                                   *
 *****

[*] Target: eccouncil

        Searching 100 results.
        Searching 200 results.

[*] Searching LinkedIn.

[*] No users found.

[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

```
theHarvester -d www.eccouncil.org -l 500 -b google
```

```
[*] Target: 222.eccouncil.org

    Searching 0 results.
    Searching 100 results.
    Searching 200 results.
    Searching 300 results.
    Searching 400 results.
    Searching 500 results.

[*] Searching Google.

[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

theHarvester -d www.eccouncil.com -l 500 -b all

```

[*] Target: www.eccouncil.com

[!] Missing API key for Securitytrail.
[!] Missing API key for PentestTools.
[!] Missing API key for Hunter.
[!] Missing API key for Intelx.
[!] Missing API key for Spyse.
No module named 'censys'
sys:1: RuntimeWarning: coroutine 'start.<locals>.store' was never awaited
RuntimeWarning: Enable tracemalloc to get the object allocation traceback

```

theHarvester -d www.eccouncil.org -l 100 -b all -f test.html

```

[*] Target: www.eccouncil.org

[!] Missing API key for Intelx.
[!] Missing API key for Spyse.
[!] Missing API key for Github.
No module named 'censys'
sys:1: RuntimeWarning: coroutine 'start.<locals>.store' was never awaited
RuntimeWarning: Enable tracemalloc to get the object allocation traceback

```