

**LAPORAN TUGAS BESAR
PASSIVE DAN ACTIVE RECONNAISSANCE**



OLEH:

NAMA : ANDINI FEBRIANTI
KELAS : 5A JK
NIM : 105841113223

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MAKASSAR
2025**

SKENARIO OPERASIONAL

Di tengah dunia digital yang penuh risiko, Anda ditunjuk sebagai Konsultan Keamanan Siber dengan misi krusial: mengidentifikasi setiap potensi titik lemah pada sistem target sebelum serangan yang sesungguhnya terjadi. Misi ini dimulai dari fase *Reconnaissance*, tahap pengumpulan intelijen yang senyap dan metodis.

Misi dibagi menjadi dua operasi berbeda. Operasi pertama berfokus pada observasi eksternal (Pasif) terhadap target publik, yaitu Portal Web Resmi Pemerintah Kabupaten Maros (maroskab.go.id). Di sini, aturan etika sangat ketat: tidak ada interaksi langsung, hanya pengumpulan informasi dari sumber terbuka (OSINT) untuk memetakan wajah publik organisasi tersebut.

Operasi kedua bergeser ke lingkungan yang terkendali, sebuah Mesin Virtual Lab Rentan dengan IP 172.20.10.4. Di sinilah aktivitas pemindaian intensif (*Active Reconnaissance*) diizinkan. Dengan *platform* Kali Linux dan *tools* canggih seperti Nmap dan Wireshark, tujuan adalah mengungkap setiap *port* yang terbuka, mengidentifikasi layanan yang usang, hingga memastikan jenis sistem operasi target.

Hasil dari kedua operasi ini akan menjadi peta harta karun bagi *hacker*—peta yang menunjukkan jalur masuk paling mudah (*entry point*) dan menetapkan target mana yang akan dieksloitasi di fase berikutnya.

1. PENDAHULUAN

Transisi menuju ekosistem digital telah menempatkan keamanan informasi sebagai pilar utama dalam menjamin keberlangsungan operasional dan menjaga kepercayaan publik. Setiap entitas, baik pemerintah maupun swasta, diwajibkan untuk secara proaktif melindungi aset digital mereka dari berbagai ancaman siber yang terus berkembang. Dalam kerangka kerja *Penetration Testing* (Pentest), fase awal dan paling krusial adalah tahap *Reconnaissance* (*pengintaian* atau *pengumpulan informasi*).

Tahap ini bertujuan untuk membangun peta rinci mengenai target, mengidentifikasi arsitektur jaringan, *host* yang aktif, dan potensi permukaan serangan (*attack surface*) yang dapat dieksloitasi di masa mendatang. Pengumpulan informasi ini secara fundamental memberikan landasan analitis sebelum tindakan intervensi teknis (seperti eksloitasi) dilakukan.

2. RUANG LINGKUP & SKENARIO PENGUJIAN

a. Peran dan Tujuan

- **Peran :** Konsultan Keamanan Siber
- **Tujuan :** Mengumpulkan informasi terkait infrastruktur target dan menemukan potensi titik masuk (entry point)

b. Target Pengujian

- **Passive Reconnaissance**

Target : Website Pemerintah Kabupaten Maros (maroskab.go.id)

- **Active Reconnaissance**

Target : VM Lab Rentan – IP: 172.20.10.4

c. Rules of Engagement

Penting untuk dicatat bahwa semua pemindaian aktif, seperti *port scanning* dan analisis trafik, hanya kami lakukan pada mesin yang ada di lab (IP 172.20.10.4). Sementara itu, saat mengamati *website* publik, kami hanya melakukan pengintaian pasif. Ini berarti tidak ada interaksi langsung atau aktivitas yang berpotensi merusak kami lakukan pada target publik, sehingga proses pengumpulan informasi tetap aman dan sesuai etika.

3. TOOLS & LINGKUNGAN PENGUJIAN

a. Alat (Tools) dan Fungsinya

- **Kali Linux :** digunakan sebagai lingkungan dasar untuk pengujian keamanan siber.
- **Netdiscover :** Digunakan untuk host discovery (penemuan host aktif) pada jaringan lokal melalui permintaan ARP.
- **Nmap :** Melaksanakan pemindaian port, identifikasi layanan (service), dan deteksi sistem operasi (OS fingerprinting).
- **Wireshark :** Berfungsi sebagai packet sniffer untuk analisis mendalam terhadap protokol dan lalu lintas jaringan (network traffic analysis).
- **Crt.sh :** Digunakan untuk pemetaan subdomain dan pengumpulan informasi melalui catatan Certificate Transparency.
- **Builtwith :** Melakukan identifikasi teknologi yang digunakan oleh situs web target, seperti frameworks dan web server.

- **Github Server** : Dioptimalkan untuk pencarian informasi sensitif yang terekspos dalam kode publik (code repositories).

4. METODOLOGI RECONNAISSANCE

Tahapan yang digunakan

a. Passive reconnaissance

- **Pengumpulan Data OSINT (Open Source Intelligence):**

Tahap ini bertujuan untuk mengumpulkan informasi relevan mengenai target dari sumber-sumber yang tersedia secara publik (misalnya, melalui *tools* seperti crt.sh dan GitHub Search).

- **Non-Interaksi dengan Server:**

Seluruh aktivitas dalam fase ini dilakukan tanpa *melibatkan* komunikasi langsung atau pengiriman paket data ke server target.

b. Active Reconnaissance

- **Pemindaian Port dan Layanan (Service Enumeration):**

Melakukan pemindaian langsung (misalnya, menggunakan Nmap) terhadap alamat host target di lingkungan lab untuk mengidentifikasi port TCP/UDP yang terbuka dan layanan (service) yang berjalan pada port tersebut.

- **Identifikasi Sistem dan Protokol Jaringan:**

Menganalisis respons dari *host* target untuk mengidentifikasi Sistem Operasi (*OS Fingerprinting*) dan memastikan protokol jaringan yang digunakan untuk komunikasi (misalnya, melalui Wireshark).

5. PASSIVE RECONNAISSANCE (HASIL & ANALISIS)

Kategori Informasi	Informasi yang ditemukan	Alat / website	Alasan relevansi
Pencarian Sub-Domain	http://bkpsdm.maroskab.go.id http://mpp.maroskab.go.id http://mattampapoledesa.maroskab.go.id http://server.maroskab.go.id	Crt.sh crt.sh %.maroskab.go.id	Menunjukkan permukaan serangan (attack surface) yang lebih luas.

	http://lpse.maroskab.go.id		
Informasi Karyawan	Muhammad Taufan (Kabid Dinas Komunikasi dan Informatika) Ihsan Najamuddin (Kabid Diseminasi Komunikasi dan Informasi Publik) Sumartini (Kabid Pengelolaan Data dan Layanan Publik)	PDF	Untuk memahami struktur organisasi dan pihak yang relevan.
Format Email	info@maroskab.go.id	https://maroskab.go.id/	Digunakan untuk validasi pola email dalam simulasi keamanan.
Teknologi Website	Cloudflare React Cloudflare Web Analytics	BuiltWith https://builtwith.com/%20maroskab.go.id/	Menunjukkan penggunaan WAF dan potensi analisis keamanan sisi klien.
Informasi Sensitif Terpapar	Tidak ditemukan adanya informasi sensitif yang terekspos langsung ke publik (seperti <i>key API</i> atau <i>kredensial</i> yang <i>hardcoded</i>).	GitHub Search (OSINT)	Tidak ditemukan informasi sensitif yang terekspos secara publik mengindikasikan bahwa target (situs <i>website</i> publik) telamenerapkan praktik keamanan yang baik dalam manajemen kodennya.

a. Bukti dokumentasi

1. Pencarian Domain dan Sub-domain

Certificates	<u>crt.sh ID</u>	<u>Logged At</u>	<u>Not Before</u>	<u>Not After</u>	<u>Common Name</u>	<u>Matching Identities</u>	<u>Issuer Name</u>
	2274715812	2025-11-25	2025-11-25	2026-02-23	mpp.maroskab.go.id	mpp.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
	2274717022	2025-11-25	2025-11-25	2026-02-23	maroskab.go.id	mpp.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
	2266262531	2025-11-22	2025-11-22	2026-02-20	webmail.maroskab.go.id	mail.maroskab.go.id webmail.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
	2265416066	2025-11-22	2025-11-22	2026-02-20	webmail.maroskab.go.id	mail.maroskab.go.id webmail.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
	22695659201	2025-11-22	2025-11-22	2026-02-20	mattampapoleida.maroskab.go.id	mattampapoleida.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
	22653081596	2025-11-22	2025-11-22	2026-02-20	mattampapoleida.maroskab.go.id	mattampapoleida.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
	22717062750	2025-11-07	2025-11-07	2026-02-05	maroskab.go.id	* maroskab.go.id maroskab.go.id * maroskab.go.id maroskab.go.id * maroskab.go.id maroskab.go.id	C=US, O=Securing, Limited, CN=Securing Public Server Authentication CA DV E36
	22717058682	2025-11-07	2025-11-07	2026-02-05	maroskab.go.id	* maroskab.go.id maroskab.go.id * maroskab.go.id maroskab.go.id	C=US, O=Securing, Limited, CN=Securing Public Server Authentication CA DV E36
	22238384639	2025-11-05	2025-10-25	2026-01-23	maroskab.go.id	maroskab.go.id	C=US, O=Google Trust Services, CN=WE1
	22122801605	2025-10-31	2025-10-31	2026-01-29	bkpsdm.maroskab.go.id	bkpsdm.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
	22122774904	2025-10-31	2025-10-31	2026-01-29	bkpsdm.maroskab.go.id	bkpsdm.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
	22103704210	2025-10-30	2025-10-30	2026-01-28	sambujeada.maroskab.go.id	sambujeada.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
	22103690863	2025-10-30	2025-10-30	2026-01-28	sambujeada.maroskab.go.id	sambujeada.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
	22094513448	2025-10-30	2025-10-30	2026-01-28	ppid.maroskab.go.id	ppid.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
	2209449488	2025-10-30	2025-10-30	2026-01-28	ppid.maroskab.go.id	ppid.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
	22083182908	2025-10-29	2025-10-29	2026-01-27	sidasateru.maroskab.go.id	sidasateru.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
	22083159768	2025-10-29	2025-10-29	2026-01-27	sidasateru.maroskab.go.id	sidasateru.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
	21996705325	2025-10-25	2025-10-25	2026-01-23	dmpmsr.maroskab.go.id	dmpmsr.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
	21996705943	2025-10-25	2025-10-25	2026-01-23	dmpmsr.maroskab.go.id	dmpmsr.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
	21983861168	2025-10-25	2025-10-25	2026-01-23	maroskab.go.id	maroskab.go.id	C=US, O=Google Trust Services, CN=WE1
	21819450783	2025-10-19	2025-10-19	2026-01-17	server.maroskab.go.id	server.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
	21819449936	2025-10-19	2025-10-19	2026-01-17	server.maroskab.go.id	server.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
	21808196303	2025-10-18	2025-08-27	2025-11-25	maroskab.go.id	* maroskab.go.id maroskab.go.id	C=US, O=Google Trust Services, CN=WE1
	21804355920	2025-10-18	2025-10-18	2026-01-16	kelurahan.maroskab.go.id	kelurahan.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
	21804325510	2025-10-18	2025-10-18	2026-01-16	kelurahan.maroskab.go.id	kelurahan.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
	21298691363	2025-09-26	2025-09-26	2025-12-25	mpp.maroskab.go.id	mpp.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
	21209680315	2025-09-26	2025-09-26	2025-12-25	mann.maroskab.no.id	mann.maroskab.no.id	C=US, O=Let's Encrypt, CN=R13

Menampilkan daftar subdomain yang terdaftar pada sertifikat SSL, memperluas attack surface.

2. Informasi dan Email karyawan

- Informasi email

Google search results for "email maroskab". The top result is a snippet from a page about government email addresses in Maros, listing several official email domains such as info@maroskab.go.id, kominfo@maroskab.go.id, sekda@maroskab.go.id, and pariwisata@maroskab.go.id.

Penemuan alamat email generik (info@maroskab.go.id) yang memvalidasi format domain email organisasi.

- Karyawan diskominfo

No.	Nama	NIP	Jabatan-Unit Kerja-Subunit Kerja	NHK	Status Akun WL	Tahun WL	Jenis Laporan	Status Pelapora
29	SUMARTINI	'196911151989032004	KEPALA BIDANG PENGELOLAAN DATA DAN LAYANAN PUBLIK - DINAS KOMUNIKASI DAN INFORMATIKA - BIDANG PENGELOLAAN DATA DAN LAYANAN PUBLIK	441042	Online	2020	Periodik	Sudah Lapor
156	MUHAMMAD TAUFAN	'198407312003121001	KEPALA BIDANG - DINAS KOMUNIKASI DAN INFORMATIKA - BIDANG LAYANAN E-GOVERNMENT	719444	Online	2020	Periodik	Sudah Lapor
82	IHSAN NADJAMUDDIN	'197208082001121005	KEPALA BIDANG DISEMINASI KOMUNIKASI DAN INFORMASI PUBLIK - DINAS KOMUNIKASI DAN INFORMATIKA - BIDANG DISEMINASI KOMUNIKASI DAN INFORMASI PUBLIK	144339	Online	2020	Periodik	Sudah Lapor

Pengumpulan data personel kunci (High-Value Targets) melalui halaman profil publik untuk pemetaan struktur organisasi.

3. Teknologi yang digunakan

The screenshot shows a web browser window with several tabs open, displaying data from different sources:

- Widgets**: A section with links to "CrUX Dataset", "CrUX Top 5m", "CrUX Top 10m", "Common Crawl", "CommonCrawl Top 5m", and "Google Font API".
- Global Trends**: A section showing "CrUX Dataset" statistics, which states it is a data collection system that gathers information about how real users interact with websites, included in the user experiences data gathered from Google Chrome and thus considered sufficiently popular on the Internet.
- CrUX Dataset**: A link to "CrUX Dataset Usage Statistics - Download List of All Websites using CrUX Dataset". It describes CrUX as a data collection system that gathers information about how real users interact with websites, included in the user experiences data gathered from Google Chrome and thus considered sufficiently popular on the Internet.
- CrUX Top 5m**: A link to "CrUX Top 5m Usage Statistics - Download List of All Websites using CrUX Top 5m". It defines it as a relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 5 million.
- CrUX Top 10m**: A link to "CrUX Top 10m Usage Statistics - Download List of All Websites using CrUX Top 10m". It defines it as a relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 10 million.
- Common Crawl**: A link to "Common Crawl Usage Statistics - Download List of All Websites using Common Crawl". It states that this website was found in the Common Crawl dataset. Data from this site was probably used to train AI LMs.
- CommonCrawl Top 5m**: A link to "CommonCrawl Top 5m Usage Statistics - Download List of All Websites using CommonCrawl Top 5m". It states that this website appears in the Common Crawl Page Rank top 5m websites.
- Google Font API**: A link to "Google Font API Usage Statistics - Download List of All Websites using Google Font API". It explains that the Google Font API helps you add web fonts to any web page.

Mobile

- ◆ iPhone / Mobile Compatible

[iPhone / Mobile Compatible Usage Statistics](#) · [Download List of All Websites using iPhone / Mobile Compatible](#)
The website contains code that allows the page to support iPhone / Mobile Content.
- ◆ Viewport Meta

[Viewport Meta Usage Statistics](#) · [Download List of All Websites using Viewport Meta](#)
This page uses the viewport meta tag which means the content may be optimized for mobile content.

Content Delivery Network

- ◆ Cloudflare

[Cloudflare Usage Statistics](#) · [Download List of All Websites using Cloudflare](#)
Automatically optimizes the delivery of your web pages so your visitors get the fastest page load times and best performance.
- ◆ Cloudflare Challenge

[Cloudflare Challenge Usage Statistics](#) · [Download List of All Websites using Cloudflare Challenge](#)
The website challenges the user to identify themselves as a human being.
- ◆ Cloudflare Automatic Challenge

[Cloudflare Automatic Challenge Usage Statistics](#) · [Download List of All Websites using Cloudflare Automatic Challenge](#)
The website automatically redirects the user if it was detected not to be a bot.

Deteksi penggunaan Cloudflare dan daftar pejabat terkait yang rentan terhadap serangan Social Engineering.

6. ACTIVE RECONNAISSANCE (HASIL & ANALISIS)

```
(kali㉿Andini) ~
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.10.3 brd 255.255.255.255 broadcast 172.20.10.15
        netmask 255.255.255.240 scopeid 0x20<link>
        inet6 fe80::f239:dbd0:f5ef:97e0 brd ff02::1 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a0:93:e4 txqueuelen 1000 (Ethernet)
    RX packets 1048 bytes 10905 (11.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 314 bytes 21048 (20.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 brd 127.0.0.1 netmask 255.0.0.0
        loop txqueuelen 1000 (Local Loopback)
    RX packets 10 bytes 580 (580.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10 bytes 580 (580.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Sebelum melanjutkan ke tahap pemindaian aktif (Active Reconnaissance), verifikasi konfigurasi jaringan pada mesin penyerang (Kali Linux) dilakukan menggunakan perintah ip a dan ifconfig. Output dari perintah tersebut mengidentifikasi bahwa interface eth0

memiliki alamat IP 172.20.10.4 dengan netmask 255.255.255.240. Konfigurasi ini secara kritis mengonfirmasi bahwa host penyerang berada dalam satu segmen jaringan (subnet) yang sama dengan target pengujian. Kesamaan segmen jaringan ini memvalidasi skenario Internal Network Attack, memastikan konektivitas pada Layer 2 (Data Link) dan memungkinkan efektivitas teknik ARP Scanning. Selain itu, berada pada subnet yang sama menjamin bahwa paket probe dari tools seperti Nmap dapat mencapai target secara langsung tanpa perlu melintasi Network Firewall atau perangkat router eksternal yang berpotensi menghalangi proses scanning.

a. Host Discovery dan Port Scanning

Tugas	Command	Hasil	Potensi Dampak
Host Discovery	sudo netdiscover -r 172.20.10.0/24	Target ditemukan: 172.20.10.4	Memastikan host aktif di jaringan.
TCP SYN Scan	sudo nmap -sS 172.20.10.4	Port terbuka: 22, 80, 6667	Permukaan serangan layanan aktif.
UDP Scan	sudo nmap -sU --top ports 20 172.20.10.4	Open/Filtered: 53, 67,68	DNS dan DHCP berpotensi menjadi target analisis.

- Dokumentasi

- Host discovery

```

Session Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
14 Captured ARP Req/Rep packets, from 3 hosts. Total size: 840
IP At MAC Address Count Len MAC Vendor / Hostname
172.20.10.2 d4:e9:8a:32:bf:a4 11 660 Intel Corporate
172.20.10.1 16:f2:87:de:a5:64 2 120 Unknown vendor
172.20.10.4 00:0c:29:93:5c:58 1 60 VMware, Inc.

```

Mengidentifikasi host yang aktif. Target 172.20.10.4 teridentifikasi menggunakan vendor VMware (volunsOS)

- TCP SYN scan

```
(kali㉿Andini) [~]
└─$ sudo nmap -sV -o 172.20.10.4
sudo: unable to resolve host Andini: Name or service not known
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 08:50 EST
Nmap scan report for 172.20.10.4
Host is up (0.0032s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http  Apache httpd 2.4.7 ((Ubuntu))
6667/tcp  open  irc   ngircd
MAC Address: 00:0C:29:93:5C:58 (VMware)
Device type: general purpose
Running: Linux 3.X!4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.90 seconds

(kali㉿Andini) [~]
└─$ sudo nmap -sV -o 172.20.10.4
```

Menemukan port TCP terbuka (22, 80, 6667) tanpa menyelesaikan 3-way handshake

- UDP scn

```
(kali㉿Andini) [~]
└─$ sudo nmap -sU -top-ports 20 172.20.10.4
sudo: unable to resolve host Andini: Name or service not known
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 08:46 EST
Nmap scan report for 172.20.10.4
Host is up (0.0022s latency).

PORT      STATE SERVICE
53/udp    closed  domain
67/udp    closed  dhcps
68/udp    open   filtered dhpc
69/udp    closed  tftp
123/udp   closed  ntpt
137/udp   closed  netbios-ns
138/udp   closed  netbios-dgm
139/udp   closed  netbios-ssn
161/udp   closed  snmp
162/udp   closed  snmptrap
445/udp   closed  microsoft-ds
500/udp   closed  isakmp
514/udp   closed  syslog
592/udp   closed  rrdt
631/udp   closed  ipp
1434/udp  closed  ms-sql-m
1900/udp  closed  upnp
4500/udp  closed  nat-t-ike
49152/udp closed  unknown
MAC Address: 00:0C:29:93:5C:58 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 19.45 seconds

(kali㉿Andini) [~]
```

Identifikasi layanan berbasis UDP seperti DNS (53) dan DHCP (67) yang berstatus open/filtered

b. Service and Version Detection

`sudo nmap -sV 172.20.10.4`

Port	Service	Version	Analisis Risiko
22	SSH	OpenSSH 6.6.1p1	Versi lama SSH (rilis tahun 2014) berpotensi memiliki celah keamanan yang sudah dipublikasikan. Risiko utama meliputi potensi <i>brute force</i> , <i>enumeration</i> nama pengguna, atau

			serangan yang menargetkan <i>bug</i> spesifik pada versi 6.6.1p1.
80	HTTP	Apache 2.4.7	Banyak CVE publik untuk versi lama.
6667	IRC	Ngircd	Ditemukannya Port 6667 dengan layanan ngircd merupakan anomali signifikan untuk server yang diasumsikan sebagai <i>server</i> umum. Port ini sering dikaitkan dengan <i>backdoor</i> , <i>botnet</i> untuk <i>Command & Control</i> (C2), atau <i>vulnerability</i> pada implementasi IRC. Ini menjadi prioritas utama untuk tahap eksloitasi selanjutnya

- **Bukti service detection**

```
(kali㉿Andini)-[~]
└─$ sudo nmap -sV -O 172.20.10.4
sudo: unable to resolve host Andini: Name or service not known
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 08:50 EST
Nmap scan report for 172.20.10.4
Host is up (0.0032s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http  Apache httpd 2.4.7 ((Ubuntu))
6667/tcp  open  irc   ngircd
MAC Address: 00:0C:29:93:5C:58 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.90 seconds
```

Target teridentifikasi menggunakan Ubuntu Linux lawas dengan layanan OpenSSH 6.6.1p1 dan Apache 2.4.7.

c. OS Fingerprinting

Hasil	Detail OS	Analisis
OS Terdeteksi	Linux Kernel 3.x – 4.x	Berdasarkan hasil pemindaian, Nmap memprediksi bahwa sistem operasi target berjalan di atas Kernel Linux versi 3.2 – 4.14. Temuan ini sangat kritis karena kernel versi

		<p>lawas tersebut umumnya diasosiasikan dengan distribusi Linux lama (seperti Ubuntu 14.04 Trusty Tahr). Sistem operasi yang sudah mencapai status <i>End-of-Life (EOL)</i> tidak lagi menerima pembaruan keamanan, sehingga sangat rentan terhadap serangan <i>Kernel Exploit</i> lokal (misalnya kerentanan <i>Dirty COW</i> - CVE-2016-5195) yang memungkinkan penyerang menaikkan hak akses (<i>Privilege Escalation</i>) menjadi <i>root</i>.</p>
--	--	--

- **Bukti Dokumentasi**

```
(kali㉿Andini)-[~]
└─$ sudo nmap -sV -O 172.20.10.4
sudo: unable to resolve host Andini: Name or service not known
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 08:50 EST
Nmap scan report for 172.20.10.4
Host is up (0.0032s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http   Apache httpd 2.4.7 ((Ubuntu))
6667/tcp  open  irc    ngircd
MAC Address: 00:0C:29:93:5C:58 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.90 seconds

(kali㉿Andini)-[~]
└─$ sudo nmap -sV -O 172.20.10.4
```

Deteksi kernel Linux versi 3.x - 4.x menggunakan opsi -O pada Nmap, mengindikasikan target menggunakan sistem operasi yang sudah usang (End-of-Life).

d. Network Protocol Analysis

Tools : wireshark

Melalui pemeriksaan mendalam pada tangkapan lalu lintas (packet capture) Wireshark, teramati adanya pola anomali dalam proses pembentukan koneksi TCP Three-Way Handshake. Urutan komunikasi standar (SYN → SYN-ACK → ACK) tidak diselesaikan secara normal.

Secara spesifik, pola yang terekam adalah sebagai berikut:

1. Host Penyerang mengirim paket SYN (Synchronize) ke port target.

2. Host Target merespons dengan paket SYN-ACK (Synchronize-Acknowledge), yang mengindikasikan bahwa port tersebut berstatus Open (terbuka) dan siap untuk handshake penuh.
3. Alih-alih menyelesaikan koneksi dengan paket ACK, Host Penyerang justru menghentikan proses dengan mengirim paket RST (Reset).

Pola pemutusan tiba-tiba ini secara teknis memvalidasi penggunaan metode TCP SYN Scan (Stealth Scan) yang diaktifkan oleh opsi -sS pada tool Nmap. Teknik ini dikenal sebagai Half-Open Scanning karena koneksi TCP tidak pernah dibentuk secara lengkap. Tujuan utama dari metode Stealth Scan ini adalah untuk mendeteksi port terbuka sambil meminimalkan jejak kaki, khususnya untuk menghindari pencatatan (logging) pada lapisan aplikasi web server target, yang umumnya hanya mencatat sesi yang berhasil dibuat sepenuhnya.

- **Bukti dokumentasi**

No.	Time	Source	Destination	Protocol	Length	Info
5799	942.578369535	172.29.19.4	172.28.19.3	HTTP	66.89	33358 [ACK] Seq=1 Ack=409 Win=38080 Len=0 Tsvl=425243 Tscr=4113988111
5799	942.578369535	172.29.19.4	172.28.19.3	HTTP	66.89	33358 [ACK] Seq=1 Ack=409 Win=38080 Len=0 Tsvl=425243 Tscr=4113988111
5800	942.578369535	172.29.19.4	172.28.19.3	HTTP	66.89	33358 [ACK] Seq=1 Ack=409 Win=38080 Len=0 Tsvl=425243 Tscr=4113988111
5801	942.578388879	172.29.19.3	172.28.19.4	HTTP	66.33349	88 [ACK] Seq=174 Ack=478 Win=64128 Len=0 Tsvl=4113988111 Tscr=425243
5802	942.578388879	172.29.19.3	172.28.19.4	HTTP	1385	HTTP/1.1 200 OK (text/html)
5803	942.578388879	172.29.19.3	172.28.19.4	HTTP	66.89	33358 [ACK] Seq=19 Win=38080 Len=0 Tsvl=425243 Tscr=4113988111
5804	942.572645088	172.29.19.3	172.28.19.4	HTTP	66.33349	88 [ACK] Seq=19 Ack=42408 Win=67298 Len=0 Tsvl=4113988112 Tscr=425243
5805	942.574662413	172.29.19.3	172.28.19.4	HTTP	66.89	33358 [ACK] Seq=19 Ack=42408 Win=67298 Len=0 Tsvl=425243 Tscr=4113988111
5806	942.574662413	172.29.19.3	172.28.19.4	HTTP	66.89	33358 [ACK] Seq=19 Ack=42408 Win=67298 Len=0 Tsvl=425243 Tscr=4113988111
5807	942.574671567	172.29.19.3	172.28.19.4	HTTP	66.33358	88 [ACK] Seq=16 Ack=457 Win=64128 Len=0 Tsvl=4113988112 Tscr=425243
5808	942.574671567	172.29.19.3	172.28.19.4	HTTP	66.33349	88 [FIN, ACK] Seq=174 Ack=479 Win=64128 Len=0 Tsvl=4113988113 Tscr=425243
5809	942.574671567	172.29.19.3	172.28.19.4	HTTP	74	HTTP/1.1 200 OK (text/html)
5810	942.574688922	172.29.19.3	172.28.19.4	HTTP	66.33342	88 [FIN, ACK] Seq=19 Ack=1241 Win=7298 Len=0 Tsvl=4113988113 Tscr=425243
5811	942.574688922	172.29.19.3	172.28.19.4	HTTP	66.33342	88 [FIN, ACK] Seq=19 Ack=1241 Win=7298 Len=0 Tsvl=4113988113 Tscr=425243
5812	942.574688922	172.29.19.3	172.28.19.4	HTTP	66.89	33358 [ACK] Seq=19 Ack=175 Win=38080 Len=0 Tsvl=425243 Tscr=4113988113
5813	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.89	33372 [SYN, ACK] Seq=1 Ack=29969 Len=0 MSS=1469 SACK_PERM Tsvl=425243 Tscr=4113988113 WS=128
5814	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.89	33372 [SYN, ACK] Seq=1 Ack=29969 Len=0 MSS=1469 SACK_PERM Tsvl=425243 Tscr=4113988113
5815	942.574688926	172.29.19.4	172.28.19.3	HTTP	66.89	33358 [ACK] Seq=458 Ack=617 Min=38028 Len=0 Tsvl=425243 Tscr=4113988113
5816	942.574688926	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425243
5817	942.574688926	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425243
5818	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425243
5819	942.574688927	172.29.19.4	172.28.19.3	HTTP	229	GET /NMAP1 HTTP/1.1
5820	942.574688927	172.29.19.4	172.28.19.3	HTTP	74	88 - 33378 [SYN, ACK] Seq=1 Ack=14469 Len=0 MSS=1469 SACK_PERM Tsvl=425244 Tscr=4113988114 WS=128
5821	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5822	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5823	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5824	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5825	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5826	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5827	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5828	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5829	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5830	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5831	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5832	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5833	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5834	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5835	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5836	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5837	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5838	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5839	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5840	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5841	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5842	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5843	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5844	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5845	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5846	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5847	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5848	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5849	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5850	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5851	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5852	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5853	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5854	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5855	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5856	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5857	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5858	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5859	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5860	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5861	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5862	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5863	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5864	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5865	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5866	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5867	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5868	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5869	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5870	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5871	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5872	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5873	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5874	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5875	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5876	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5877	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5878	942.574688927	172.29.19.4	172.28.19.3	HTTP	66.33372	88 [ACK] Seq=1 Ack=1 Win=64256 Len=0 Tsvl=4113988113 Tscr=425244
5879	942.574688927	172.29.19.4	172.28.19.3			

- Eksposur Data Personel: Terkumpulnya data mengenai personel kunci dan format email meningkatkan risiko Social Engineering terhadap organisasi.
 - Keamanan Kode Efektif: Tidak ditemukan kebocoran informasi sensitif (seperti key API atau kredensial hardcoded) di ranah publik, mengindikasikan implementasi praktik secure coding yang baik.
2. Active Reconnaissance (VM Lab 172.20.10.4):
 - Anomali Pemindaian: Analisis protokol mengonfirmasi bahwa port scanning dilakukan secara sembunyi-sembunyi (Stealth Scan / Half-Open Scanning) menggunakan paket RST untuk menghindari logging.
 - Kerentanan Kritis OS: Sistem operasi target teridentifikasi menggunakan Linux Kernel versi 3.x–4.x , yang telah mencapai status End-of-Life (EOL). Kerentanan ini menyebabkan host sangat rentan terhadap serangan Kernel Exploit lokal (misalnya Dirty COW - CVE-2016-5195) yang memungkinkan Privilege Escalation ke tingkat root.
 - Layanan Rentan: Tiga port terbuka (22, 80, 6667) menjalankan layanan dengan versi lama dan berisiko, terutama:
 - OpenSSH 6.6.1p1 dan Apache 2.4.7 memiliki banyak CVE publik.
 - Layanan Ngircd pada Port 6667 merupakan anomali signifikan yang menjadi prioritas utama sebagai potensi backdoor atau botnet C2.

b. Saran

Berdasarkan temuan kritis tersebut, direkomendasikan tindakan perbaikan segera (remediation) sebagai berikut:

1. Perbarui dan Migrasi OS (Penting Sekali):
 - Lakukan patch atau migrasi sistem operasi target dari Kernel Linux 3.x–4.x ke versi yang didukung dan terbaru untuk menghilangkan risiko serangan Kernel Exploit.
2. Perbarui Layanan Publik:
 - Tingkatkan versi OpenSSH (22) dan Apache HTTPD (80) ke versi terbaru untuk mengurangi paparan terhadap CVE yang sudah diketahui.
3. Audit dan Nonaktifkan Layanan Anomali:

- Lakukan audit keamanan mendalam terhadap layanan ngircd pada Port 6667. Jika layanan ini tidak diperlukan untuk fungsi bisnis, segera nonaktifkan (disable) dan filter port ini melalui firewall.

4. Tingkatkan Kontrol Data Publik:

- Tinjau kembali kebijakan publikasi data personel untuk meminimalkan eksposur informasi kunci, sehingga mengurangi risiko keberhasilan serangan Social Engineering