



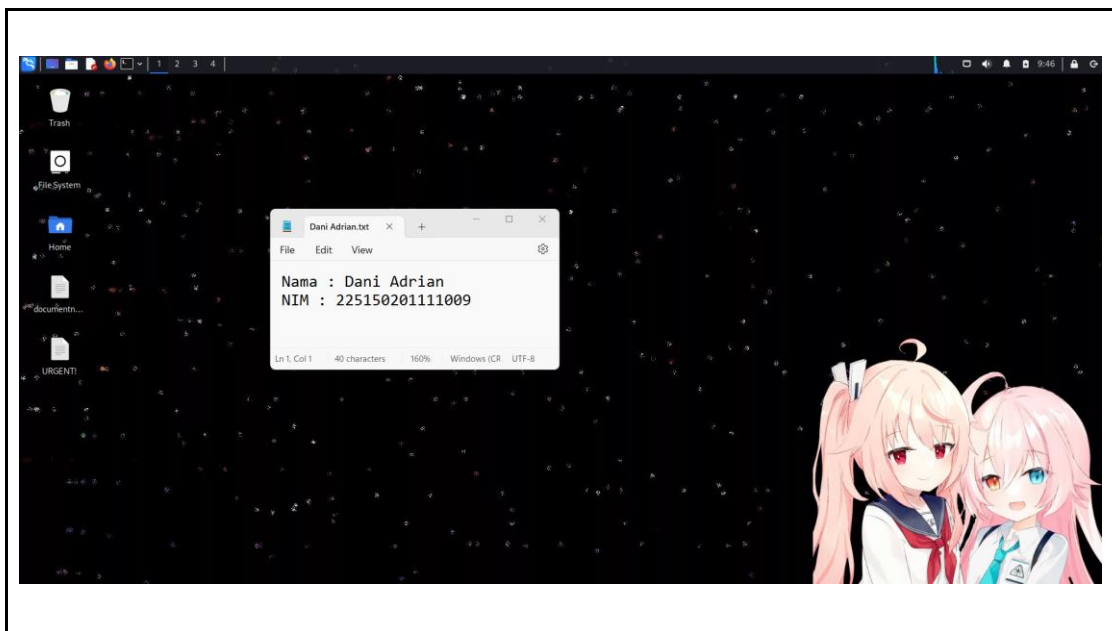
**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA**

BAB : Kode dan Aktivitas Mencurigakan
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 16/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Langkah Praktikum

A. Eksekusi Malware

1. Jalankan sistem operasi Linux (Desktop/Server) pada aplikasi Virtual Machine (VM)



2. Jalankan command berikut pada VM Terminal Anda:

```
sudo apt update && sudo apt install jd-gui # Debian paru  
-Sy --aur --noconfirm jd-gui-bin # ArchLinux
```

Note: jika tidak memiliki perintah `paru` didalam sistem, install menggunakan langkah berikut: <https://github.com/Morganamilo/paru#installation>



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : Kode dan Aktivitas Mencurigakan
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 16/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
File Actions Edit View Help
(user@kali)~$ sudo apt update && sudo apt install jd-gui
[sudo] password for user:
Hit:1 http://deb.debian.org/debian bullseye InRelease
Get:2 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Packages [19.9 MB]
Hit:4 https://deb.parrot.sh/parrot lts InRelease
Get:5 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [46.5 MB]
Get:6 http://kali.download/kali kali-rolling/contrib amd64 Packages [115 kB]
Get:7 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [257 kB]
Get:8 http://kali.download/kali kali-rolling/non-free amd64 Packages [193 kB]
Get:9 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [864 kB]
Get:10 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [33.1 kB]
Get:11 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.9 kB]
Fetched 67.9 MB in 1min 34s (725 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1105 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://deb.parrot.sh/parrot/dists/lts/InRelease: Key is stored in legacy trusted.gpg keyri
ng (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  kali-desktop-base libabsl20220623 libaio1 libdaq2 python3-pyppeteer python3-pyrsistent
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  jd-gui
0 upgraded, 1 newly installed, 0 to remove and 1105 not upgraded.
Need to get 1287 kB of archives.
```

Penjelasan :
Command diatas bertujuan memperbarui daftar paket dan menginstall JD-GUI (Decompiler Java).

`sudo apt install jd-gui` : untuk menginstall JD-GUI pada sistem

3. Kemudian buatlah folder baru:

```
mkdir ~/victim_NIManda
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : Kode dan Aktivitas Mencurigakan
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 16/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)-[~]  
$ mkdir ~/victim_225150201111009
```

Dani Adrian.txt

File Edit View

Nama : Dani Adrian
NIM : 225150201111009

4. Berikutnya, unduh file yang kita butuhkan, dan masukkan ke dalam folder yang telah kita buat sebelumnya, tautan *resource*, (**unduh file MyApp.jar**):
https://drive.google.com/drive/u/4/folders/1fcDWz_HVJpQvRnTWRGsDgF-egtlrOx4C



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : Kode dan Aktivitas Mencurigakan
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 16/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Dibagikan kepada saya > Innocent App ▾

Jenis ▾ Orang ▾ Dimodifikasi ▾

Nama	Pemilik	Terakhir diubah ▾ ↓	Ukuran file
decryptor	noverdy123	28 Mei 2023 noverdy123	—
Very Important Document.pdf.dokb	noverdy123	3 Jun 2023 noverdy123	114 KB
MyApp.jar	noverdy123	27 Mei 2023 noverdy123	8 KB

Dani Adr × + − □ ×

File Edit View

Nama : Dani Adrian
NIM : 225150201111009

Ln 1, Col 12 40 characters 130% Window UTF-8

```
(user@kali)-[~]  
$ mv ~/Downloads/MyApp.jar ~/victim_225150201111009/  
  
(user@kali)-[~]  
$ cd victim_225150201111009  
  
(user@kali)-[~/victim_225150201111009]  
$ ls  
MyApp.jar
```

Dani Adr × + − □ ×

File Edit View

Nama : Dani Adrian
NIM : 225150201111009

Ln 1, Col 12 40 characters 130% Window UTF-8

Penjelasan :

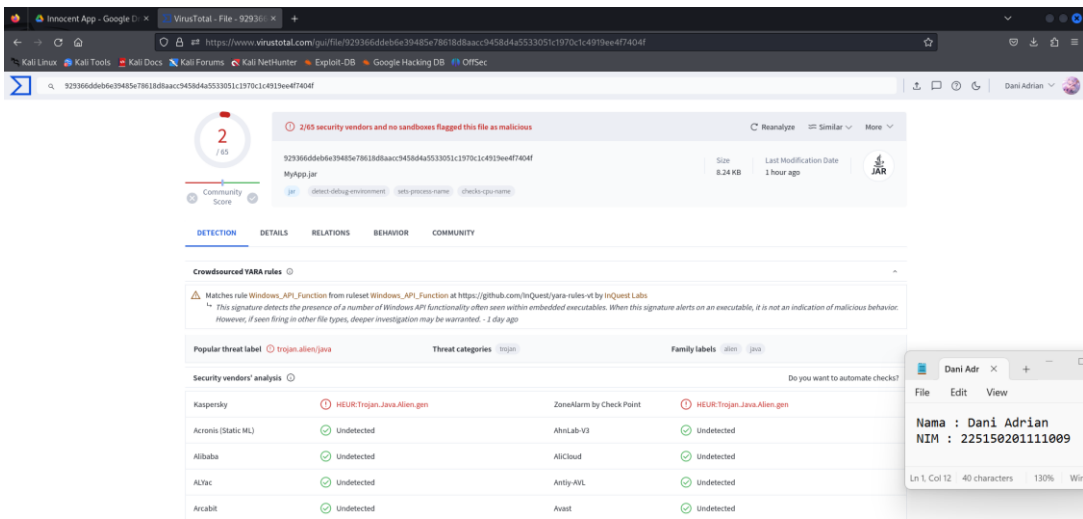
mv ~/Downloads/MyApp.jar ~/victim_225150201111009/ :
Command untuk memindahkan file dari downloads ke
~/victim_225150201111009

5. Masuk ke laman virustotal.com, kemudian upload file MyApp.jar ke dalam laman tersebut. **Jelaskan hasil yang diberikan dari virustotal tersebut.**



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : Kode dan Aktivitas Mencurigakan
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 16/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas



Penjelasan :

Laporan VirusTotal untuk file "MyApp.jar" menunjukkan bahwa 2 dari 65 vendor keamanan menandai file ini sebagai mungkin berbahaya. Secara spesifik, Kaspersky dan ZoneAlarm oleh Check Point mengidentifikasi file tersebut dengan label HEUR:Trojan.Java.Alien.gen, menunjukkan deteksi heuristik dari kemungkinan trojan berbasis Java.

Analisis Vendor Keamanan:

Ditandai: Kaspersky dan ZoneAlarm oleh Check Point.

Tidak Terdeteksi: 63 vendor lainnya termasuk nama-nama terkenal seperti Avast, Acronis, Alibaba, ALYac, dan lainnya.

6. Kemudian, buka terminal anda dan masuk ke dalam path direktori tempat file MyApp.jar



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : Kode dan Aktivitas Mencurigakan
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 16/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
cd ~/victim_NIManda
```

The screenshot shows a terminal window on a Kali Linux system. The user is in the directory `~/victim_225150201111009/`. They execute the command `mv ~/Downloads/MyApp.jar ~/victim_225150201111009/` to move a file. Then they run `cd victim_225150201111009` and `ls`, which lists the file `MyApp.jar`. To the right, a text editor window titled 'Dani Adr' displays the user's name and NIM: 'Nama : Dani Adrian' and 'NIM : 225150201111009'.

7. Tambahkan beberapa file (bebas) ke dalam folder tersebut.

The screenshot shows the terminal and a file manager window. In the terminal, the user runs `ls` in the directory `~/victim_225150201111009`, and the output lists three files: `'Modul 9 - Kode dan Aktivitas Mencurigakan.pdf'`, `MyApp.jar`, and `azusa.jpg`. The file manager window, titled 'victim_225150201111009 - Thunar', shows these three files in a graphical view: `azusa.jpg` (an anime-style image), `Modul 9 - Kode dan Aktivitas Mencurigakan.pdf` (a document icon), and `MyApp.jar` (a jar icon). The status bar at the bottom indicates '3 files: 455.0 KiB (465891 bytes) | Free space: 3.8 GiB'.

8. Jalankan file MyApp.jar dengan perintah berikut:

```
java -jar MyApp.jar
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : Kode dan Aktivitas Mencurigakan
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 16/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

Jelaskan apa yang terjadi pada file lainnya setelah program tersebut dijalankan.

```
(user@kali)~/victim_225150201111009
$ java -jar MyApp.jar
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Hello World!

(user@kali)~/victim_225150201111009
$ ls -l ~/victim_225150201111009
total 460
-rw-r--r-- 1 user user 260976 May 24 15:17 'Modul 9 - Kode dan Aktivitas Mencurigakan.pdf.dokb'
-rw-r--r-- 1 user user 8435 May 24 13:37 MyApp.jar
-rw-r--r-- 1 user user 196496 May 24 15:17 azusa.jpg.dokb

(user@kali)~/victim_225150201111009
$
```

Penjelasan :

Program MyApp.jar hanya menampilkan pesan "Hello World!" tanpa melakukan tindakan mencurigakan terhadap file lain di dalam direktori victim_225150201111009. Semua file tetap ada.

Namun ada penambahan ekstensi ".dokb" pada nama file Modul 9 - Kode dan Aktivitas Mencurigakan.pdf dan azusa.jpg. Ini adalah tanda adanya tindakan yang mencurigakan kedua telah dimodifikasi atau terenkripsi.

B. Analisa Malware

- Berikutnya, kita jalankan decompiler tools yang telah kita install (jd-gui) melalui terminal dengan perintah:

Jd-gui

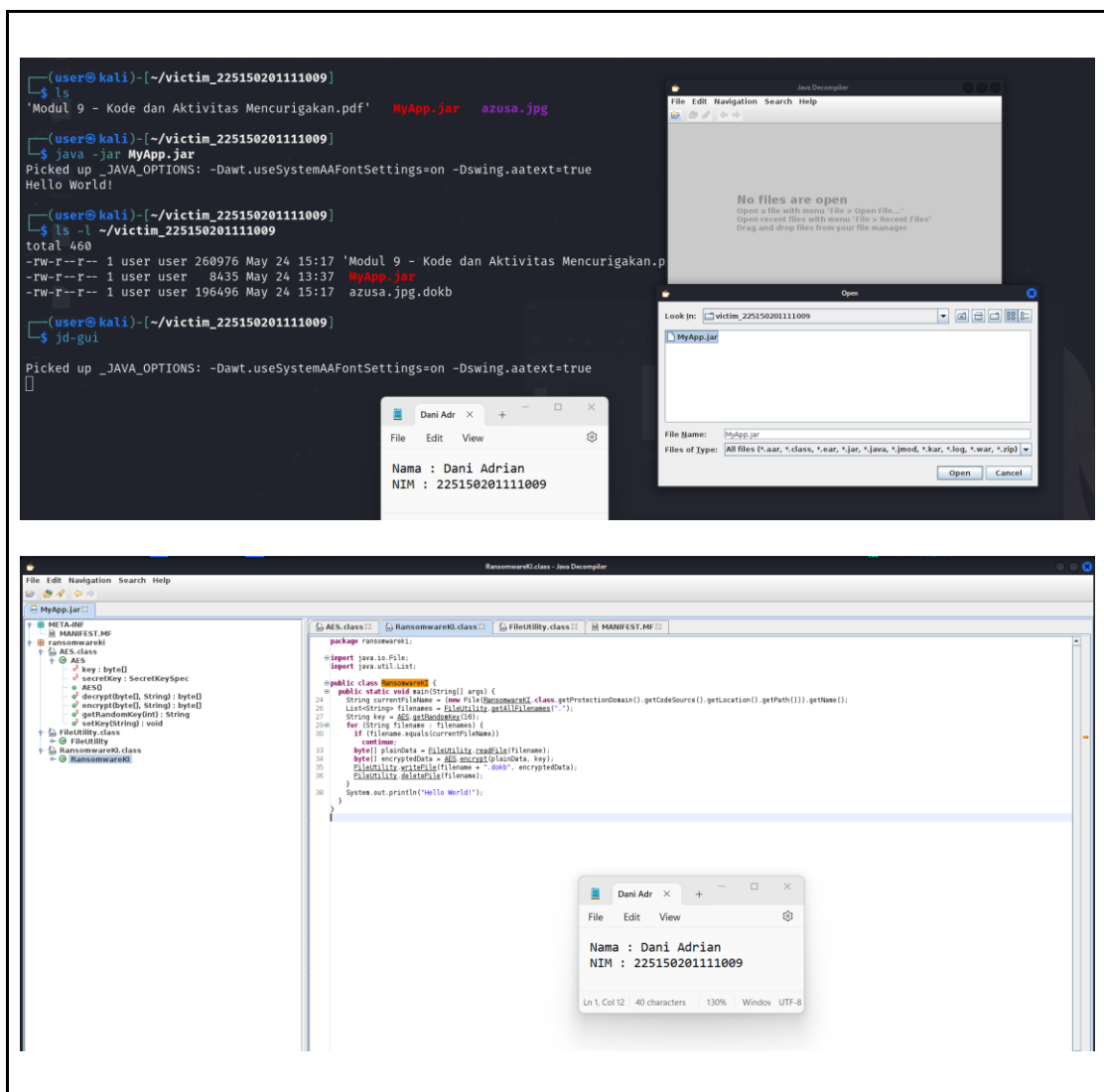


LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : Kode dan Aktivitas Mencurigakan
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 16/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

10. Setelah jd-gui berhasil dijalankan masuk ke bagian file -> open file, kemudian pilih file MyApp.jar

11. Setelah jd-gui berhasil dijalankan masuk ke bagian file -> open file, kemudian pilih file MyApp.jar





LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB	: Kode dan Aktivitas Mencurigakan
NAMA	: DANI ADRIAN
NIM	: 225150201111009
TANGGAL	: 16/05/2024
ASISTEN	: Bernas Cakra Sakti Harisna Mohammad Seto Aji Pamungkas

Penjelasan : :

Program tersebut adalah kode ransomware yang menggunakan enkripsi AES untuk mengenkripsi file-file dalam sebuah direktori.

Saat program dijalankan, program akan mengenkripsi file-file dalam direktori tempat program dijalankan menggunakan kunci acak yang dihasilkan oleh `AES.getRandomKey(16)`. Setelah mengenkripsi file, program akan mencetak "Hello World!" sebagai penanda bahwa proses enkripsi telah selesai.

12. Kemudian, kita lakukan analisa melalui jd-gui tersebut.
File .class apa saja yang terdapat dalam file malware tersebut ?

- AES.class
- FileUtility.class
- RansomwareKI.class

13. Apa yang dilakukan FileUtility.class dalam file malware tersebut?

`FileUtility.java`: Kelas ini berisi utilitas untuk membaca, menulis, dan menghapus file. Metode `readFile` digunakan untuk membaca isi file ke dalam byte array, `writeFile` untuk menulis byte array ke dalam file, dan `deleteFile` untuk menghapus file. Metode `getAllFileNames` digunakan untuk mendapatkan semua nama file dalam sebuah direktori.



**LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA**

BAB	: Kode dan Aktivitas Mencurigakan
NAMA	: DANI ADRIAN
NIM	: 225150201111009
TANGGAL	: 16/05/2024
ASISTEN	: Bernas Cakra Sakti Harisna Mohammad Seto Aji Pamungkas

14. Apa yang dilakukan AES.class dalam file malware tersebut, algoritma kriptografi apa saja yang digunakan dalam malware tersebut?

AES.java: Kelas ini digunakan untuk mengenkripsi dan mendekripsi data menggunakan algoritma AES. Metode `setKey` digunakan untuk menginisialisasi kunci enkripsi. Metode `encrypt` digunakan untuk mengenkripsi data, sedangkan metode `decrypt` digunakan untuk mendekripsi data.

15. Apa yang dilakukan RansomwareKI.class dalam file malware tersebut?

RansomwareKI.java: Kelas utama yang digunakan untuk menjalankan ransomware. Pada metode `main`, program akan mengenkripsi semua file dalam direktori kerja kecuali file ransomware itu sendiri. Setelah mengenkripsi, program akan menambahkan ekstensi `".dokb"` pada nama file yang terenkripsi dan menghapus file aslinya.

C. Mitigasi dan Pemulihan dari Malware

16. Setelah kita melakukan analisa pada malware tersebut, kita dapat melakukan pemulihan kembali pada file kita yang terenkripsi.
17. **Unduh file 'Very Important Document.pdf.dokb'** dan masukkan ke dalam folder `~/victim_NIM` dari tautan Drive sebelumnya pada nomor 4.



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : Kode dan Aktivitas Mencurigakan
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 16/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

The screenshot displays a file manager interface with a table of files and a text editor window. The table lists files with columns for Name, Owner, Last Modified, and Size. The text editor window shows a text file with the name 'Dani Adr' and the content 'Nama : Dani Adrian' and 'NIM : 225150201111009'.

Nama	Pemilik	Terakhir diubah	Ukuran file
decryptor	noverdy123	28 Mei 2023 noverdy123	—
Very Important Document.pdf.dokb	noverdy123	3 Jun 2023 noverdy123	114 KB
MyApp.jar	noverdy123	27 Mei 2023 noverdy123	8 KB

File Editor View

Nama : Dani Adrian
NIM : 225150201111009

Ln 1, Col 12 | 40 characters | 130% | Window | UTF-8

File Editor View

Nama : Dani Adrian
NIM : 225150201111009

Ln 1, Col 12 | 40 characters | 130% | Window | UTF-8

18. Buatlah folder dengan nama 'result' di dalam folder ~/victim_NIManda.



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : Kode dan Aktivitas Mencurigakan
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 16/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
user@kali: ~/victim_225150201111009
(user@kali)~[~/victim_225150201111009]
$ mkdir result
(user@kali)~[~/victim_225150201111009]
$ ls
'Modul 9 - Kode dan Aktivitas Mencurigakan.pdf.dokb'  MyApp.jar  'Very Important Document.pdf.dokb'  azusa.jpg.dokb  result
(user@kali)~[~/victim_225150201111009]
$
```

The nano editor window shows the following text:

```
Nama : Dani Adrian
NIM : 225150201111009
```

19. Jalankan script code yang dapat membantu kita memulihkan salah satu file penting berjudul “Very Important Document.pdf.dokb” kembali menjadi file .pdf

```
(user@kali)~[~/victim_225150201111009]
$ nano decrypt_aes.py
```

The nano editor window shows the following text:

```
Nama : Dani Adrian
NIM : 225150201111009
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : Kode dan Aktivitas Mencurigakan
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 16/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

The screenshot shows a Kali Linux terminal window with the following commands and output:

```
(user@kali)-[~/victim_225150201111009]
$ pip install pycryptodome
Defaulting to user installation because normal site-packages is not writeable
Collecting pycryptodome
  Downloading pycryptodome-3.20.0-cp35-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (3.4 kB)
  Downloading pycryptodome-3.20.0-cp35-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (2.1 MB)
    2.1/2.1 MB 1.3 MB/s eta 0:00:00
Installing collected packages: pycryptodome
Successfully installed pycryptodome-3.20.0

(user@kali)-[~/victim_225150201111009]
$ python3 decrypt_aes.py
```

The nano editor shows the following Python code in `decrypt_aes.py`:

```
from hashlib import sha1 # Import library kriptografi sha1
from Crypto.Cipher import AES # Import library kriptografi AES
import string # Bantuan lib string untuk loop lowercase text

# Mengakses/membuka file yang terenkripsi
encryptedfile = open('Very Important Document.pdf.dokb', 'rb').read()

for i in string.ascii_lowercase:
    # Generate kunci dari tiap karakter a-z
    key = i * 16 # Pasti tiap karakter akan digandakan sebanyak 16 misal 'aaaaaaaaaaaaaaaa'
    key = sha1(key.encode()).digest()[:16] # Mengambil 16 bytes pertama dari hasil SHA-1 digest bytes 0 sampai 15

    aes = AES.new(key, AES.MODE_ECB) # Membuat AES cipher dari key yang didapat dari SHA-1 digest sebelumnya menggunakan mode ECB
    result = aes.decrypt(encryptedfile) # Melakukan dekripsi file dengan algoritma kriptografi AES yang telah didefinisikan sebelumnya

    # Pastikan terdapat direktori result
    # Write file baru hasil proses dekripsi, seharusnya ada 26 file baru dan hanya ada 1 file yang dapat diakses.
    open(f'result/Very Important Document_Char_{i}.pdf', 'wb').write(result)
```

The terminal output shows the decrypted file content in a text editor window:

```
Nama : Dani Adrian
NIM : 225150201111009
```



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : Kode dan Aktivitas Mencurigakan
NAMA : DANI ADRIAN
NIM : 225150201111009
TANGGAL : 16/05/2024
ASISTEN : Bernas Cakra Sakti Harisna
Mohammad Seto Aji Pamungkas

```
(user@kali)~/victim_225150201111009
$ cd result

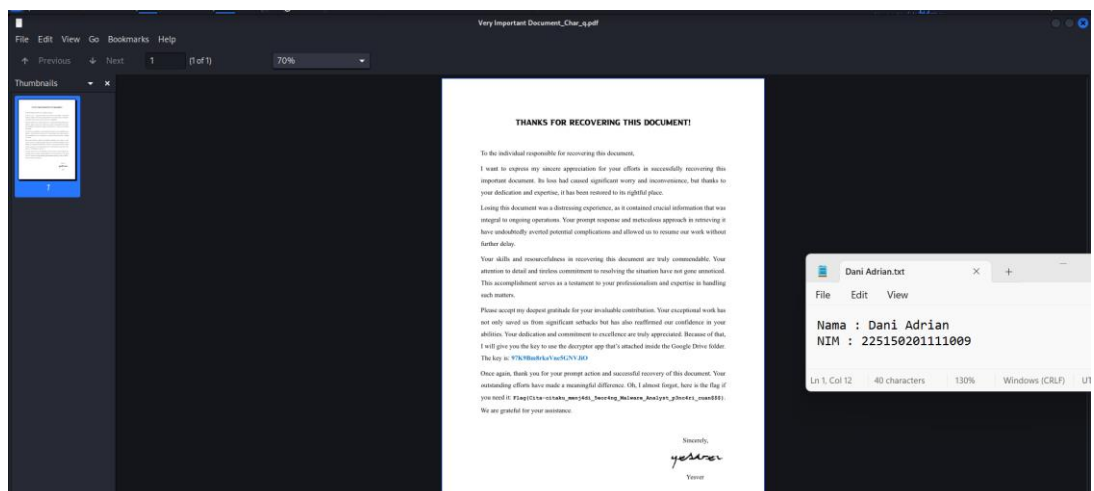
(user@kali)~/victim_225150201111009/result
$ ls
'Very Important Document_Char_a.pdf' 'Very Important Document_Char_j.pdf' 'Very Important Document_Char_s.pdf'
'Very Important Document_Char_b.pdf' 'Very Important Document_Char_k.pdf' 'Very Important Document_Char_t.pdf'
'Very Important Document_Char_c.pdf' 'Very Important Document_Char_l.pdf' 'Very Important Document_Char_u.pdf'
'Very Important Document_Char_d.pdf' 'Very Important Document_Char_m.pdf' 'Very Important Document_Char_v.pdf'
'Very Important Document_Char_e.pdf' 'Very Important Document_Char_n.pdf' 'Very Important Document_Char_w.pdf'
'Very Important Document_Char_f.pdf' 'Very Important Document_Char_o.pdf' 'Very Important Document_Char_x.pdf'
'Very Important Document_Char_g.pdf' 'Very Important Document_Char_p.pdf' 'Very Important Document_Char_y.pdf'
'Very Important Document_Char_h.pdf' 'Very Important Document_Char_q.pdf' 'Very Important Document_Char_z.pdf'
'Very Important Document_Char_i.pdf' 'Very Important Document_Char_r.pdf'
```

Penjelasan :

Program `decrypt_aes.py` adalah skrip Python yang digunakan untuk mencoba mendekripsi file `Very Important Document.pdf.dokb` yang terenkripsi menggunakan algoritma AES dengan mode ECB.

20. Jalankan kode yang telah anda buat, dan bukalah dokumen yang berhasil dipulihkan.

Screenshoot :





LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB	: Kode dan Aktivitas Mencurigakan
NAMA	: DANI ADRIAN
NIM	: 225150201111009
TANGGAL	: 16/05/2024
ASISTEN	: Bernas Cakra Sakti Harisna Mohammad Seto Aji Pamungkas

Flag : Flag{Cita-citaku_menj4di_5eor4ng_Malware_Analyst_p3nc4ri_cuan\$\$\$}

Dalam file tersebut, anda akan menemukan sebuah password juga. Password ini dapat kalian gunakan untuk menjalankan decryptor yang tersedia pada drive google yang ada pada nomor 5, apabila terjadi hal yang tidak diinginkan akibat malware tersebut.

Evaluasi

1. Malware jenis apa yang kita jalankan pada praktikum ini, dan jelaskan secara singkat bagaimana proses malware tersebut bekerja.

Malware yang dijalankan pada praktikum ini adalah Ransomware. Ransomware adalah jenis malware yang mengenkripsi file-file pada sistem korban, sehingga tidak dapat diakses oleh pengguna. Proses kerjanya adalah:

- Mengumpulkan semua nama file dalam direktori kerja kecuali file program itu sendiri.
- Menghasilkan kunci acak untuk enkripsi.
- Membaca setiap file, mengenkripsi kontennya menggunakan algoritma AES dengan kunci acak, dan menyimpan hasil enkripsi dalam file baru dengan ekstensi `.dokb`.
- Menghapus file asli setelah konten terenkripsi disimpan.
- Mencetak pesan "Hello World!" sebagai indikasi proses enkripsi selesai.

2. Jelaskan bagaimana cara kerja kode script yang ada pada nomor 18, dalam men-dekripsi dan memulihkan file dari malware tersebut.



LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB	: Kode dan Aktivitas Mencurigakan
NAMA	: DANI ADRIAN
NIM	: 225150201111009
TANGGAL	: 16/05/2024
ASISTEN	: Bernas Cakra Sakti Harisna Mohammad Seto Aji Pamungkas

Kode script pada nomor 18 menggunakan pendekatan brute force untuk mendekripsi file "Very Important Document.pdf.dokb" yang terenkripsi oleh ransomware. Script ini mencoba semua kemungkinan kunci enkripsi dengan panjang 16 karakter (hanya terdiri dari huruf kecil) secara berurutan. Untuk setiap kunci yang dicoba, script akan mencoba mendekripsi file menggunakan kunci tersebut dengan algoritma AES dalam mode ECB dan padding PKCS5. Jika hasil dekripsi valid (dalam hal ini, jika awalan file setelah didekripsi sesuai dengan header PDF), maka file hasil dekripsi akan disimpan dengan ekstensi `.pdf`.

3. Hal-hal apa saja yang kita perlu lakukan agar terhindar dari serangan malware

Beberapa hal yang dapat dilakukan untuk terhindar dari serangan malware:

- Menggunakan antivirus dan firewall yang selalu diperbarui.
- Tidak membuka atau mengunduh file dari sumber yang tidak dipercaya.
- Membuat cadangan data secara teratur.
- Menggunakan email filtering untuk mencegah phishing.
- Menjaga semua perangkat lunak selalu diperbarui dengan patch keamanan terbaru.
- Menggunakan enkripsi untuk data penting.
- Meningkatkan kesadaran keamanan dengan pelatihan bagi karyawan.
- Menggunakan prinsip akses minimum yang diperlukan untuk mencegah penyebaran malware.

