BAB V
PENUTUP

5.1 Kesimpulan

Setelah penelitian dilakukan menggunakan *tool* VirusTotal dan *framework* MobSF dengan sampel *file* apk aplikasi COVID_19 yang dilakukan *repackaging attack* untuk disusupkan *payload* yang bekerja dalam melakukan *exploit*, maka dapat ditarik beberapa kesimpulan sebagai berikut :

a. Berhasil dalam membangun lingkungan penelitian yang digunakan dalam mesin *linux* pada sistem operasi Kali *Linux* 2020.3. *Framework* MobSF dan Metasploit *framework* dapat diinstal serta menjalankan analisis dan implementasi dengan baik .
b. Berhasil dalam mengimplementasikan teknik analisis statis menggunakan VirusTotal dengan hasil aplikasi COVID_19 dapat dideteksi oleh 19 dari 60 *anti-malware*. Hasil analisis dengan *framework* MobSF juga menemukan 15 *permission* yang dapat dikategorikan berbahaya.
c. Berhasil dalam mengimplementasikan teknik analisis dinamis dengan uji hasil kerja *malware* yang dibuat dalam *framework* Metasploit, yaitu berhasil menjalankan 7 perintah *exploit* seperti call log dump, location, screenshot, messages (sms) dump, send sms, check_root, sysinfo.
d. Hasil perbandingan analisis *file* apk COVID_19 yang telah disusupkan *malware* adalah sebagai berikut :
    1. Dari analisis statis menggunakan VirusTotal dan *framework* MobSF dapat ditemukan adanya perbedaan ukuran *file* pada aplikasi COVID_19. Di mana setelah dilakukan *repackaging attack*, ukuran *file* pada apk COVID_19 adalah 20.80 yang sebelumnya adalah 20.82. Tentunya diikuti juga dengan perubahan SHA256 setelah dilakukan *repackaging attack*.
    2. *Framework* MobSF menemukan adanya perubahan pada *permission* yang sebelumnya hanya ada 3 *permission* yang diminta oleh aplikasi COVID_19, namun setelah *repackaging attack* total *permission* yang ditemukan menjadi 22 dan 15 diantaranya dikategorikan sebagai berbahaya oleh *framework* MobSF.

3. Dari analisis dinamis yang dilakukan pada *device android* Mi9T terdapat perbedaan pada saat proses instalasi aplikasi COVID_19, di mana aplikasi COVID_19 yang telah dilakukan *repackaging attack* diblokir oleh *Google Play Protect*.

e. Dengan berhasil dilakukan repackaging attack pada sampel aplikasi Android dengan tema COVID-19, maka terbukti modifikasi aplikasi third-party dapat dilakukan dengan tujuan tertentu. Sehingga agar pengguna smartphone khususnya dengan platform android lebih berhati-hati dalam mengunduh aplikasi dari internet.

f. Dengan tren *Coronavirus* yang terus meningkat hingga saat penelitian ini dilakukan maka diharapkan agar pengguna *smartphone* khususnya dengan platform *android* agar lebih selektif dan berhati-hati dalam menggunakan ataupun mengunduh aplikasi COVID-19 yang tersebar di internet.

5.2 Saran

Penelitian yang dilakukan ini masih ada banyak kekurangan, serta membutuhkan pemahaman yang lebih baik dalam menghasilkan laporan dari analisis yang telah dilakukan agar lebih dimengerti orang awam. Sehingga penulis memberikan saran-saran yang dapat dilakukan baik untuk pengguna *smartphone* dengan platform *android* dan penelitian kedepannya, diantaranya adalah:

a. Bagi pengguna smartphone dengan platform *android*, diharapkan untuk tidak lengah dan selalu waspada dalam mengunduh aplikasi khususnya dengan tema COVID-19, dan dapat mengunggah file ataupun aplikasi pada VirusTotal untuk mendeteksi malware sebelum melakukan instalasi pada smartphone *android*.

b. Lebih banyak melakukan eksplorasi dalam menggunakan tools analisis malware.

c. Mengikuti perkembangan dan *trend malware* yang sedang terjadi karena perkembangan dalam kejahatan siber semakin canggih.

d. Mempelajari lebih banyak fitur dan fungsi dari kegunaan *framework* Metasploit, karena diperlukan pemahaman yang mendalam dalam melakukan *penetration-testing* agar lebih maksimal.