# BAB V
# PENUTUP

## 5.1 Kesimpulan

Setelah penelitian dilakukan menggunakan tool VirusTotal dan anyrun dengan sampel file pdf yang dilakukan repackaging attack untuk disusupkan payload yang bekerja dalam melakukan exploit, maka dapat ditarik beberapa kesimpulan sebagai berikut :

a) Penggunaan Bahwa file pdf yang terifeksi malware bisa di scan melalui VirusTotal, untuk melihat malware dan anti-malware yang terdapat pada file pdf yang sudah terinfeksi malware.
b) Document yang berformat pdf masih dapat disisipkan malware, pengemasan backdor dilakukan dengan menyisipkanya pada file berformat PDF, mengunakan tools metasploit yang terdapat pada OS kali linux.
c) Berhasil dalam mengimplementasikan teknik analisis statis menggunakan VirusTotal dengan hasil dapat dideteksi oleh 19 dari 60 anti-malware. Hasil analisis dinamis dengan any run juga menemukan 15 permission yang dapat dikategorikan berbahaya.
d) Berdasarkan hasil analisa kedua metode dapat disimpulkan bahwa malware jenis ini masih terbilang sangat ringan dan masih dapat dengan mudah di antisipasi pada sistem, dengan memasang anti virus yang selalu terupdate.

## 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 untuk penelitian kedepannya, diantaranya adalah:

a) Lebih banyak melakukan eksplorasi dalam menggunakan tools analisis malware.

b) Lebih sering untuk mengupdate anti-virus yang ada pada device, karena perkembangan malware yang semakin canggih akan semakin mudah masuk, apabila tidak adanya pembaharuan terbaru pada anti-virus.
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.
e) Penelitian ini bisa menjadi rujukan untuk penelitian selanjutnya yang membahas tentang analisi malware.
f) Bisa rujukan untuk di lakukan perbandingan dengan metode dinamis dan menjadi metode hybrid.