BAB V
PENUTUP

5.1 Kesimpulan

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

a. Analisis berhasil dilakukan pada file pdf yang teriferksi malware menggunakan metode *static analysis* dengan melakukan scan melalui VirusTotal dan Any Run, untuk melihat malware dan anti-malware yang dapat mendeteksi file pdf yang sudah terinfeksi malware.
b. Document yang berformat pdf dapat disisipkan malware menggunakan teknik repackaging attack yang dilakukan dengan menyisipkan malware pada file berformat PDF. Malware berhasil dibuat mengunakan tools metasploit yang terdapat pada OS kali linux.
c. Deteksi berhasil dilakukan dengan hasil rasio deteksi pada VirusTotal dan AnyRun yaitu 41 dari 63 anti-malware berhasil melakukan deteksi. Ditemukan juga perbedaan ukuran file sebelum dilakukan infksi malware yaitu 174.35 KB dan setelah infeksi malware menjadi 289.40 KB.
d. Dengan berhasil dilakukannya injeksi malware pada file PDF, maka terbukti file PDF memiliki ancaman serangan dengan tujuan tertentu, sehingga agar pengguna komputer khususnya dengan sistem operasi windows dapat lebih berhati hati dalam mengunduh file PDF.

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 dijadikan rujukan untuk di lakukan perbandingan dengan metode dinamis dan menjadi metode hybrid.