BAB V
PENUTUP

5.1 Kesimpulan

Setelah penelitian dilakukan dengan analisis statis dan dinamis pada sample malware yang telah dibuat, maka dapat ditarik kesimpulan sebagai berikut:

a) VirusTotal dapat dipakai untuk menentukan antivirus yang dapat mengatasi file malware Curriculum Vitae.docm. Berikut adalah 36 antivirus yang dapat melakukan pendeteksian pada malware Curriculum Vitae.docm. Adapun antivirus yang dapat mendeteksi malware tersebut, diantaranya: *Ad-Aware, Avast, Avira (no cloud), BitDefender, ClamAV, Cyren, Emsisoft, ESET-NOD32, Arcabit, AVG, Baidu, CAT-QuickHeal, Cynet, DrWeb, eScan, F-Secure, FireEye, GData, Jiangmin, MAX, McAfee-GW-Edition, NANO-Antivirus, Rising, SentinelOne (Static ML), Symantec, Tencent, Fortinet, Ikarus, Kaspersky, McAfee, Microsoft, Qihoo-360, Sangfor Engine Zero, Sophos, TACHYON, ZoneAlarm by Check Point.*

b) CMD dapat digunakan untuk menemukan IP penyerang yang terhubung pada perangkat korban. Adapun perintah yang digunakan untuk pendeteksian IP tersebut yaitu *netstat –n* dan *netstat -ano*.

c) CMD dan Task Manager dapat digunakan untuk melakukan pendeteksian saat membuka file asing. Adapun cara yang dilakukan adalah dengan penggunaan CMD dan penulisan perintah *netstat –n* untuk pengecekan IP yang terhubung, kemudian penggunaan *task manager* untuk pengecekan aplikasi asing yang berjalan di bagian *processes*.

d) Analisis menggunakan VirusTotal membuktikan bahwa file malware Curriculum Vitae.docm mengandung malware, hal ini terbukti pada 36 dari 64 antivirus yang telah mendeteksi adanya malware di Curriculum Vitae.docm.

e) Analisis menggunakan AnyRun dapat digunakan untuk pembuktian bahwa malware bisa dijalankan di komputer lain selain virtual computer. Pembuktian tersebut dilakukan dengan pengunggahan file malware ke AnyRun, kemudian menjalankan malware tersebut.

f) Untuk pemutusan koneksi dengan penyerang saat telah terinfeksi malware macro Curriculum Vitae.docm, cukup dengan melakukan kill process pada aplikasi asing yang berjalan di task manager dan selanjutnya menghapus aplikasi malware tersebut.

5.2 Saran

Sebagai penutup, penulis berharap semoga penelitian ini memberikan manfaat bagi pembaca, penulis dan pengguna Microsoft office word. Pada penelitian ini masih terdapat beberapa kekurangan dan masih bisa dikembangkan. Berikut beberapa saran dari penulis untuk penelitian selanjutnya:

a) Perkembangan malware dan sistem keamanan harus diikuti. Karena setiap hari kejahatan siber maupun sistem keamanan semakin canggih

b) Agar penetration testing yang dilakukan bisa lebih maksimal, diperlukannya pembelajaran lebih banyak dari fitur dan fungsi Metasploit framework.

c) Pengkodean dalam pembuatan malware macro masih dapat ditingkatkan, karena masih bisa dideteksi dengan cmd dan task manager.

d) Pengguna Microsoft word harus waspada jika file yang diterima, perlu pengaktifan macro. Karena hal ini menjadi penyebab terinfeksinya komputer yang dimiliki.

e) Untuk penelitian selanjutnya, dapat difokuskan pada pembuatan antivirus sederhana berdasarkan antivirus yang berhasil mendeteksi malware di VirusTotal. Hal ini dilakukan untuk mengatasi malware macro ini.