BAB V
PENUTUP

5.1 Kesimpulan

Setelah penelitian dilakukan menggunakan Remnux dan proses explorer dengan sampel malware file ridhomalware.mkv yang disusupkan payload yang berjalan dalam melakukan exploitasi, maka dapat di tarik kesimpulan sebagai berikut:

a. Analisis menggunakan Remnux membuktikan bahwa File RidhoMalware.mkv mengandung malware yang terenkripsi, ini terbukti dengan string dan nilai hex yang tidak dapat di baca.
b. Menghitung *Checksum* (*hashing)* aplikasi. Didapatkan nilai hashing yang sama ketika dipindahkan antar oprasi system dan di uji dengan ssedep bahwa memiliki 100% tingkat kecocokan, ini membuktikan bahwa malware tidak mengalami perubahan ukuran ketika prosess transfer file, Sehingga ukuran tetap sama yaitu 1GB.
c. Dari Analisis dinamis di dapatkannya *PID* 5368, IP address penyerang 192.168.56.10, dan *port* yang terbuka yaitu *port* 4444, dari file RidhoMalware.mkv yang sudah dilakukan analisis menggunakan *tools netstat.*
d. Analisa dinamis yang dilakukan dengan menggunakan *tools proses explorer* setelah malware dijalankan membuktikan bahwa terdapat 4 *system* aplikasi yang terbuka atau berjalan di latar belakang diantaranya *cmd.exe, conhost.exe, vlc.exe dan werfault.exe.* Selain itu file file yang berjalan di latar belakang langsung terhubung dengan malware RidhoMalware.mkv ini terbukti dari nilai parent yang langsung menuju ke PID 5368 dari malware itu sendiri.
e. Dari analisis dinamis dengan menggunakan tools prosess explorer dapat membaca string dari masing masing file yang terbuka di latar belakang. Selain itu analisis string yang di lakukan terhadap aplikasi vlc.exe dengan pid 5472 yang bertype string memory tidak terdapat string atau kosong.

f. Dalam analisis string file *cmd.exe, conhost.exe, vlc.exe dan werfault.exe,* terdapat kesamaan string salah satunya adalah "*!This program cannot be run in DOS mode.*" Yang menunjukan bahwa malware Ridho.Malware.mkv tidak dapat berjalan ketika korban berada di mode *DOS.*

g. Analisa string yang di lakukan ketika *attaker* menjalankan perintah untuk menyerang *client,* dapat di baca dan di simpan oleh string bertype m*emory* yang berada di aplikasi cmd.exe.

h. cmd.exe sudah terinfeksi oleh malware dangan adanya thread dan process yang sedang berjalan denagan name <non-existent Prosess>(4424)

i. malware *Ridhomalware.mkv* ini bersembunyi di balik cmd.exe dengan pid 3672

j. Analisa yang dilakukan dengan menggunakan Antivirus avira hanya memperingatkan tentang pembaruan terhadap vlc player

k. Antivirus avira tidak mengeluarkan peringatan ketika malware di jalankan dan malware berjalan lancar di sisitem oprasi windows 10

5.2 Saran

Sebagai penutup penelitian skripsi ini, penulis berharap semoga apa yang penulis sajikan dapat memberikan banyak manfaat bagi pembaca, penulis dan pengguna aplikasi vlc player. 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. Mengikuti perkembangan dan trend malware yang sedang terjadi karena perkembangan dalam kejahatan siber semakin canggih.

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

d. Untuk penelitian selanjutnya, dapat dititik fokuskan dalam pembuatan antivirus sederhana dalam mencegah malware bertipe video ini
e. Malware dengan topik file video ini masih jarang di temui dan sedikitnya reffrensi yang benar benar membahas tentang malware bertipe video ini. Untuk penelitian selanjutnya di harapkan dapat menganalisa tipe file lain seperti mp4, avi, wmv dan masih banyak lagi.