# BAB V
# PENUTUP

## 5.1 Kesimpulan

Berdasarkan hasil analisis yang telah dilakukan mengenai analisis dampak Trojan Emotet pada sistem operasi Windows menggunakan *packet analysis* dan tool Wireshark, diperoleh Kesimpulan sebagai berikut:

1. Aktivitas atau trafik Trojan Emotet pada sistem operasi Windows dapat dideteksi melalui packet analysis menggunakan Wireshark dengan mengamati alamat IP sumber dan tujuan, port komunikasi, protokol jaringan, *session* komunikasi, *payload*, serta pola *beaconing*. Hasil analisis menunjukkan adanya komunikasi berulang menuju beberapa alamat IP eksternal menggunakan protokol TCP, HTTP, dan HTTPS pada port 80 dan 443. Selain itu, teridentifikasi lalu lintas sebanyak 11.130 paket dengan volume data sekitar 8 MB serta frekuensi koneksi yang tinggi menuju beberapa alamat IP eksternal, yang menunjukkan karakteristi komunikasi jaringan Trojan Emotet berupa komunikasi berulang dan berkelanjutan menuju beberapa IP eksternal.

2. Aktivias lalu lintas jaringan yang dihasilkan Trojan Emotet menunjukkan beberapa *Indicator of Compromise (IoC)*, seperti komunikasi menuju banyak IP eksternal (*multi-destination IP*), komunikasi berulang (*beaconing*), *payload* terenkripsi, dan *session* komunikasi aktif yang mengarah pada indikasi aktivitas *Command and Control* (C2). Berdasarkan analisi aspek *Confidentiality, Integrity,* dan *Availability* (CIA), aktivitas tersebut berpotensi memengaruhi keamanan sistem operasi Windows melalui potensi pengiriman data ke server eksternal, penerimaan perintah dari server pengendali, serta peningkatan beban jaringan akibat komunikasi yang berlangsung secara terus-menerus.

## 5.2 Saran

1. Penelitian selanjutnya disarankan untuk menggunakan sandbox *analysis* dalam mengamati perilaku malware.
2. Penelitian berikutnya disarankan untuk mengintegrasikan analisis jaringan dengan sistem IDS atau *threat intelligence*.
3. Penelitian selanjutnya disarankan untuk menerapkan *machine learning* dalam mendeteksi pola *beaconing* malware.
4. Penelitian berikutnya disarankan untuk melakukan *memory forensics* guna memperoleh artefak digital tambahan.