BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan data yang diperoleh dari penelitian yang sudah dilakukan dapat disimpulkan bahwa :

1. Penggunaan *Collective Intelligence Framework* (CIF) dapat meningkatkan kemampuan *honeypot* dalam mendeteksi *malware* dilihat dari data hasil pengujian aplikasi yang menunjukkan terdeteksinya *ip address* pengirim *malware* meskipun dalam persentase yang kecil. Sedangkan *hash* dan *url* tidak terdeteksi karena data dari penyedia *threat intelligence* yang masih minim pada saat penelitian ini dilakukan.
2. Serangan terhadap perangkat yang terhubung pada jaringan publik sangatlah besar. Data dari penelitian ini membuktikan bahwa selama bulan Oktober 2017 hingga Januari 2018 terjadi 329.831 serangan jaringan dari 18.949 penyerang dan 1120 serangan diantaranya merupakan serangan *malware*.
3. Serangan *malware* terjadi pada port 445 (SMB) dan 3306 (MySQL). Port 445 adalah port yang digunakan oleh layanan *server message block (SMB)* untuk berbagi *file*. Terdapat kelemahan pada layanan tersebut yang dimanfaatkan untuk mengirimkan *ransomware* pada penelitian ini ditemukan sebanyak 943 *malware* yang dikirimkan melalui *port* 445 yang menandakan bahwa *port* tersebut masih

4. digunakan untuk mendistribusikan *malware* terutama ransomware. Selain itu ditemukan 177 *malware* yang dikirimkan melalui *port* 3306 yang biasa digunakan untuk mengirimkan *malware* berjenis trojan.
5. Implementasi *collective intelligence framework (CIF)* untuk mendeteksi *malware* belum efektif melihat tidak terdeteksinya *hash* dan *url*. Namun hasil deteksi terhadap *host (ip address)* cukup tinggi dan semakin meningkat dari waktu ke waktu karena *threat intelligence* yang digunakan berasal dari perusahaan dan kumunitas yang aktif.
6. *Honeypot* dan *server CIF* membutuhkan *processor* dengan spesifikasi tinggi untuk dapat berjalan secara efektif.
7. Hasil pengujian rule membuktikan bahwa *host (ip address)* yang menyerang *honeypot* juga menyerang perangkat jaringan lain.

5.2 Saran

Saran peneliti untuk penelitian dan pengembangan aplikasi selanjutnya adalah sebagai berikut :

1. Perlu ditambahkan *threat intelligence* pada *server* CIF terutama yang berasal dari Asia dan Indonesia agar kemungkinan serangan dapat dideteksi oleh CIF menjadi lebih besar.
2. Perlu adanya peningkatan performa aplikasi dengan cara meningkatkan spesifikasi perangkat yang digunakan dan membuat kode program yang lebih efisien untuk berjalan pada *server*.

3. *Honeypot* sebaiknya dijalankan pada beberapa jaringan dan lokasi yang berbeda agar dapat mengetahui variasi serangan antara satu jaringan dengan jaringan lainnya.