

BAB 5

KESIMPULAN DAN SARAN

5.1 KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, penelitian ini menggunakan DynamiteLab untuk menganalisis trafik jaringan di Kampus 1 UNJAYA dengan kesimpulan sebagai berikut:

1. Aktivitas mencurigakan teridentifikasi, terutama yang terkait dengan protokol *P2P ThunderNetwork* dan jaringan *Tor*. Protokol TCP dan UDP merupakan sumber utama peringatan. TCP menyumbang lebih dari 66% dari total peringatan, sementara UDP menyumbang 44%. TCP, meskipun andal, rentan terhadap serangan berbasis koneksi seperti DoS, sementara UDP, dengan karakteristik tanpa koneksi, menunjukkan potensi ancaman melalui transfer data yang cepat namun kurang terlindungi.
2. Peringatan utama yang terdeteksi adalah *Misc Attack* dan *Potential Corporate Privacy Violation*, yang menunjukkan adanya ancaman serangan serta pelanggaran privasi yang signifikan.
3. Host internal (172.16.11.32) dan eksternal (108.137.182.98) menjadi titik perhatian, dengan host internal menghasilkan jumlah peringatan terbanyak.

5.2 SARAN

Penelitian ini merekomendasikan evaluasi dan penguatan kebijakan keamanan jaringan di Kampus 1 UNJAYA. Penting untuk terus memantau protokol utama seperti TCP dan UDP serta aktivitas dari host internal dan eksternal. Untuk efektivitas deteksi ancaman, sebaiknya menggunakan berbagai alat analisis dan pemantauan yang lebih ketat. Pengembangan sistem keamanan yang canggih juga dianjurkan untuk mengatasi potensi ancaman di masa depan.