BAB V

PENUTUP

5.1 Kesimpulan

Dari hasil penelitian dan ujicoba yang telah dilakukan terhadap "Implementasi Analisa Serangan *Denial of Service* (DOS) berbasis *Brute Force* menggunakan Wireshark", maka ditarik kesimpulan sebagai berikut:

1) Serangan *Denial of Service* berbasis *brute force* dapat dicegah menggunakan Wireshark dengan cara menfilter pada *port* yang sering menjadi target a*ttacker* (*port* 443, *port* 445, *port* 80) dan mengecek jika terdapat aktivitas mencurigakan.
2) Analisa *Traffic Capture*: *Traffic capture* dapat dianalisa untuk mengidentifikasi pola serangan *brute force*. Fungsi *filter* pada Wireshark memudahkan *cyber blue team* (*defender*) untuk mendeteksi dan memahami karakteristik dan menganalisa sedang berlangsung atau yang telah terjadi pada *port-port* tertentu. p
3) *Lateral Movement* dan *Pivoting:* Wireshark dapat digunakan untuk mendeteksi aktivitas *lateral movement* dan *pivoting* yang dilakukan oleh *attacker* setelah berhasil masuk ke dalam jaringan. Serangan yang berusaha menyebar ke bagian lain dari jaringan dapat diidentifikasi melalui analisa paket data yang mencurigakan. *Cyber blue team* dapat mengidentifikasi dan mencegah penyebaran serangan lebih lanjut.
4) Penggunaan *Network Share*: Serangan terhadap *network share* dapat diidentifikasi melalui analisa paket yang berhubungan dengan akses *file*

atau *folder* pada Wireshark. Dapat berupa aktivitas mencurigakan seperti upaya pengaksesan tidak sah dapat dideteksi.

5.2 Saran

Berdasarkan hasil penelitian dan kesimpulan yang telah diuraikan, berikut adalah beberapa saran untuk pengembangan lebih lanjut serta implikasi praktis dari penelitian ini :

1) Analisa pada *Port* lain: Analisa serangan DOS berbasis *brute force* ini hanya berfokus pada *port* 443. Penelitian ini akan bisa dikembangkan lagi dengan mengimplementasi *port* lain.
2) Penggunaan Alat Analisis Tambahan: Selain Wireshark, IDS/IPS (*Intrusion Detection System/Intrusion Prevention System*) yang dapat bekerja secara bersamaan dengan Wireshark untuk memberikan perlindungan yang lebih komprehensif. Integrasi ini akan memperkuat kemampuan deteksi dan respon terhadap serangan.
3) Pelatihan terhadap Penggunaan *Sniffing Tools*: Pelatihan mendalam terhadap *cyver blue team* mengenai penggunaan Wireshark dan *sniffing tools* lainnya untuk memastikan mereka memiliki keterampilan yang diperlukan untuk mendeteksi dan menganalisa serangan secara efektif.