BAB V
SIMPULAN, IMPLIKASI DAN REKOMENDASI

5.1 Simpulan

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan oleh penulis "Implementasi Honeypot Pada Server Untuk Mendeteksi Serangan DoS" dapat diambil kesimpulan sebagai berikut:

1. Implementasi Honeypot Dionaea berhasil menciptakan layanan tiruan dengan membuka port tertentu untuk menarik perhatian dan menjadi sasaran utama serangan.
2. Penelitian ini menganalisis kinerja Honeypot Dionaea dalam mendeteksi serangan siber. Hasilnya menunjukkan deteksi cepat pada IP private rata-rata kurang dari 1 detik dengan tingkat deteksi TCP Flood 5%, HTTP Flood 97%, Slow HTTP 89%, dan Slowloris 98%. Pada IP publik, waktu deteksi rata-rata lebih dari 1 detik dengan tingkat deteksi TCP Flood 6%, HTTP Flood 97%, Slow HTTP 95%, dan Slowloris 93%. Ketidaksempurnaan deteksi (kurang dari 100%) disebabkan oleh kombinasi faktor protokol, konfigurasi Dionaea, karakteristik jaringan, dan keterbatasan alat uji. Selain itu, server honeypot memiliki keterbatasan dalam menangani lalu lintas tinggi, sehingga serangan yang terlalu besar atau berlangsung terus-menerus dapat menyebabkan beberapa paket terlewat atau tidak tercatat.

5.2 Implikasi

Penelitian ini "Implementasi Honeypot pada server untuk mendeteksi serangan DoS" memiliki beberapa implikasi penting dalam penggunaan Honeypot sebagai alat deteksi dan analisis serangan. Honeypot memberikan pemahaman tentang metode yang digunakan oleh pelaku serangan, ini memungkinkan untuk menjadi pengembangan stategi pertahanan yang lebih kuat. Honeypot berfungsi sebagai langkah awal perlindungan terhadap data dan informasi sensitif, data yang didapatkan dari *log activity* yang terekam dalam Honeypot dapat menjadi dasar untuk riset keamanan yang lebih lanjut untuk menciptakan lingkungan yang siap menghadapi acaman serangan siber.

5.3 Rekomendasi

Berdasarkan hasil penelitian dan kesimpulan yang telah diambil, berikut adalah beberapa rekomendasi yang penulis sampaikan untuk pengembangan selanjutnya. Saran tersebut sebagai berikut:

1. Honeypot sebaiknya diintegrasikan dengan sistem keamanan yang lain untuk menciptakan lapisan pertahanan yang kuat.
2. Menggunakan alat analisis yang canggih guna mempercepat waktu respon terhadap ancaman. Contohnya seperti ELK Stack dll.
3. Mengimplementasikan Honeypot dalam server nyata untuk mengetahui seberapa efektif Honeypot dalam server nyata dalam mendeteksi serangan.
4. Histori log serangan ditampilkan dalam bentuk grafik atau gambar agar mudah dipahami.
5. Disarankan untuk melakukan penelitian lebih lanjut mengenai jenis serangan yang terdeteksi oleh Honeypot, serta dampak dari serangan tersebut kepada infrastruktur jaringan.