**Khung đồ án tốt nghiệp**

Sinh viên: Nguyễn Doãn Nhân – D15AT

Tên đồ án: Nghiên cứu phát hiện tấn công TCP SYN Flood

Nội dung:

1. Tổng quan về tấn công DoS/DDoS và các biện pháp phòng chống
   1. Tổng quan về tấn công DoS/DDoS
      1. Khái quát về tấn công DoS/DDoS
      2. Các dạng tấn công DoS/DDoS
      3. Các phương thức liên lạc của mạng botnet phục vụ tấn công DDoS
      4. Các thách thức trong phát hiện và phòng chống tấn công DoS/DDoS
   2. Các biện pháp phòng chống tấn công DoS/DDoS
      1. Các biện pháp phòng chống ở lớp mạng
      2. Các biện pháp phòng chống lớp ứng dụng
      3. Các biện pháp phòng chống theo giai đoạn triển khai
   3. Kết chương
2. Tấn công TCP SYN Flood và mô hình phát hiện các gói tin giả mạo
   1. Khái quát về tấn công TCP SYN Flood
      1. Giới thiệu tấn công TCP SYN Flood
      2. Cơ chế tấn công TCP SYN Flood
      3. Các biện pháp phòng chống
   2. Phát hiện các gói tin giả mạo của tấn công TCP SYN Flood
      1. Đặc trưng của các gói tin IP được gửi đi từ cùng một máy nguồn
      2. Mô hình phát hiện các gói tin giả mạo của tấn công TCP SYN Flood
         * Giới thiệu mô hình
         * Thuật toán DBSCAN
         * Ứng dụng thuật toán DBSCAN trong phát hiện các gói tin giả mạo
   3. Kết chương
3. Cài đặt và thử nghiệm
   1. Thử nghiệm với tập dữ liệu offline
      1. Mô hình thử nghiệm
      2. Giới thiệu dữ liệu thử nghiệm
      3. Thử nghiệm và kết quả
   2. Thử nghiệm phát hiện online
      1. Mô hình thử nghiệm
      2. Thử nghiệm và kết quả
   3. Kết chương