ĐỀ TÀI: XÂY DỰNG HỆ THỐNG PHÁT HIỆN XÂM NHẬP IDS – SNORT

CHƯƠNG I: TỔNG QUAN VỀ BẢO MẬT

1.1. GIỚI THIỆU VỀ BẢO MẬT

1.1.1. Khái niệm

1.1.2. Tính an toàn của hệ thống mạng

1.2. CÁC PHƯƠNG PHÁP XÂM NHẬP HỆ THỐNG PHỔ BIẾN – BIỆN PHÁP PHÁT HIỆN VÀ NGĂN NGỪA

1.2.1. Phương thức ăn cắp thông tin bằng Packet Sniffer

1.2.2. Phương thức tấn công mật khẩu Password attack

1.2.3. Phương thức tấn công bằng Mail Relay

1.2.4. Phương thức tấn công hệ thống DNS

1.2.5. Phương thức tấn công Man-in-the-middle attack

1.3. CÁC GIẢI PHÁP BẢO MẬT AN TOÀN CHO HỆ THỐNG

1.3.1. Bảo mật VPN (Virtual Private Network)

1.3.2. Firewall

1.3.3. Bảo mật bằng IDS (Hệ thống dò tìm và phát hiện xâm nhập)

CHƯƠNG II: HỆ THỐNG PHÁT HIỆN XÂM NHẬP IDS

2.1. GIỚI THIỆU VỀ IDS

2.1.1. Định nghĩa về IDS

2.1.2 Kiến Trúc và nguyên lý hoạt động IDS

2.2. PHÂN LOẠI IDS

2.2.1. Network based IDS – NIDS

2.2.2. Host based IDS – HIDS

2.3. CƠ CHẾ HOẠT ĐỘNG CỦA IDS

2.3.1. Mô hình phát hiện sự lạm dụng

2.3.2. Mô hình phát hiện sự bất thường

2.3.3. So sánh giữa hai mô hình

2.4. CÁCH PHÁT HIỆN KIỂU TẤN CÔNG THÔNG DỤNG CỦA IDS

2.4.1. Tấn công từ chối dịch vụ (Denial of Service attack)

2.4.2. Quét và thăm dò (Scanning và Probe)

2.4.3. Tấn công vào mật mã (Password attack)

2.4.4. Chiếm đặc quyền (Privilege-grabbing)

2.4.5. Cài đặt mã nguy hiểm (Hostile code insertion)

2.4.6. Hành động phá hoại trên máy móc (Cyber vandalism)

2.4.7. Tấn công hạ tầng bảo mật (Security infrastructure attack)

CHƯƠNG III: TRIỂN KHAI ỨNG DỤNG DÒ TÌM XÂM NHẬP TRÊN HỆ THỐNG DỰA TRÊN SNORT

3.1. GIỚI THIỆU VỀ SNORT

3.2. KIẾN TRÚC SNORT

3.3. THÀNH PHẦN VÀ CHỨC NĂNG CỦA SNORT

3.3.1. Module giải mã gói tin (Packet Decoder)

3.3.2. Module tiền xử lý (Preprocessor)

3.3.3. Module phát hiện (Detection Engine)

3.3.4. Module log và cảnh báo (Logging and Alerting system)

3.3.5. Module kết xuất thông tin (output module)

3.4. BỘ LUẬT CỦA SNORT

3.4.1. Giới thiệu về bộ luật

3.4.2. Cấu trúc luật của Snort

3.5. CÁC CƠ CHẾ HOẠT ĐỘNG CỦA SNORT

CHƯƠNG IV: DEMO

4.1 Demo tấn công

4.2 Demo phát hiện

CHƯƠNG V : KẾT LUẬN