Đề tài:

Tìm hiểu và triển khai hệ thống phát hiện xâm nhập mạng (Snort)

1.Thành viên và công việc

Họ và tên	MSSV	Công việc	Tiến độ
Hoàng Sơn	1651060882	-Cài đặt phần mềm phát hiện xâm nhập Snort -Cài đặt các gói phần mềm bổ trợ -Cài đặt Snort -Cấu hình Snort chạy ở chế độ phát hiện xâm nhập mạng -Kiểm tra sự hoạt động của Snort Các bước phát hiện tấn công dò quét -Sử dụng phanf mềm Nmap dò quét các máy tính đang chạy -Phát hiện tấn công -Kết quả tấn công -Hiện ra giao diện thống kê của Snort	-Cài đặt UbuntuServer -Tìm hiểu và cài đặt các gói phần mềm bổ trợ

2. Nội dung nghiên cứu

Tổng quan về Snort:

Snort là một ứng dụng bảo mật mới với 3 chức năng chính là: đánh hơi gói tin, theo dõi gói tin và sử dụng như một NIDS. Ngoài ra còn có nhiều chương trình thêm vào để cung cấp những cách khác nhau nhằm mục đích ghi dấu và quản lý logfile của Snort, thêm và bảo trì tập luật, thông báo cho người quản trị hệ thống khi có những traffic gây hại được nhận ra…Có nhiều cách để sử dụng. Snort trong thiết kế bảo mật của công ty.

Thông thường Snort chỉ sử dụng TCP/IP nhưng những phần thêm vào có thể mở rộng khả năng cung cấp các loại ngôn ngữ khác như Novell'IPX...

Snort có 5 thành phần chính như sau:

1. Bộ giải mã gói tin - Packet Decoder
2. Các bộ tiền xử lý - PreProcessers
3. Máy phát hiện - Detection Engine
4. Hệ thống cảnh báo và ghi dấu - Logging and Alerting System
5. Môđun xuất - Output Modules

Sơ đồ sau biểu diễn quan hệ giữa các thành phần của Snort. Tại đó các gói dữ liệu giao tiếp từ mạng Internet vào trong hệ thống được đi qua Packet decoder. Tại mỗi thành phần các gói tin được xử lý rồi truyền kết quả cho thành phần kế tiếp trong hệ thống. Output modul sẽ loại bỏ các gói tin, ghi log hay sinh ra cảnh báo.

Snort có 4 chế độ hoạt động như sau:

1. Sniffer mode: ở chế độ này snort sẽ lắng nghe và đọc các gói tin trên mạng sau đó sẽ trình bày kết quả trên giao diện hiển thị.
2. Packet Logger mode: lưu trữ các gói tin trong các tập tin log.
3. Network instruction detect system (NIDS) : đây là chế dộ hoạt động mạnh mẽ và được áp dụng nhiều nhất, khi hoạt động ở NIDS mode Snort sẽ phân tích các gói tin luân chuyển trên mạng và so sánh với các thông tin được định

nghĩa của người dùng để từ đó có những hành động tương ứng như thông báo cho quản trị mạng khi xảy ra tình huống quét lỗi do các hacker /attacker tiến hành hay cảnh báo virus..

4. Inline mode: khi triển khai snort trên linux thì chúng ta có thể cấu hình snort để phân tích các gói tin từ iptables thay vì libpcap do đó iptable có thể drop hoặc pass các gói tin theo snort rule.

Bộ giải mã gói tin

Thông qua Card mạng và dây dẫn, bộ giải mã gói tin xác định giao thức nào đang dùng và kết nối dữ liệu dựa trên những hành vi cho phép của các gói tin. Nó giải mã các gói tin từ nhiều dạng khác nhau của mạng (Ethernet, SLIP, PPP....) để chuẩn bị cho giai đoạn tiền xử lý. Packet Decoder có thể tạo ra những cảnh báo dựa trên sự phát hiện những giao thức khác lạ, những gói tin quá dài,

những tùy chọn TCP lạ hoặc những hành động khác