**ĐẠI HỌC ĐÀ NẴNG**

**TRƯỜNG ĐẠI HỌC BÁCH KHOA**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO ĐỒ ÁN**

**CHUYÊN NGÀNH MẠNG**

**ĐỀ TÀI :**

**Ứng dụng các công cụ của Security Onion nhằm phân tích và phát hiện một cuộc tấn công (Web, Database,…)**

**SINH VIÊN : Trương Quang Hùng**

**MÃ SINH VIÊN : 102170022**

**LỚP : 17T1**

**GVHD : PGS.TS. Nguyễn Tấn Khôi**

**Đà Nẵng, 04/2021**

**TÓM TẮT**

Tên đề tài: Ứng dụng các công cụ của Security Onion nhằm phân tích và phát hiện một cuộc tấn công (Web, Database,…)

Sinh viên thực hiện: Trương Quang Hùng

Số thẻ SV: 102170022

Lớp: 17T1

1. Giới thiệu:

Dưới sự phát triển của cuộc cách mạng công nghiệp 4.0 vai trò của mạng ngày càng thể hiện rõ rệt. Tuy nhiên việc tham gia vào môi trường mạng khiến người sử dụng luôn phải đối mặt với nhiều nguy cơ khác nhau: từ việc bị thăm dò, khai thác dữ liệu đến khả năng gặp phải các cuộc tấn công về Web, Database,…

Security Onion là một bản phân phối mã nguồn mở của Linux với nhiều công cụ hữu dụng có thể phân tích, phát hiện các mối nguy hại trong môi trường mạng dựa vào việc phân tích các gói tin gửi đi trong mạng. Bằng cách cài đặt và cấu hình phù hợp, Security Onion có thể đóng vai trò như một hệ thống phát hiện xâm nhập mạng (NIDS – Network Intrusion Detection System) giúp người dùng có thể dễ dàng phát hiện các mối nguy hại đến các máy trong mạng.

1. Các bước thực hiện đề tài:

* Tìm hiểu đề tài, phân tích các yêu cầu cần thiết để xây dựng hệ thống.
* Tiến hành thiết kế mô hình mạng, cài đặt môi trường mạng trên GNS3.
* Tải, cài đặt các máy ảo cần dùng: Kali linux, Security Onion, Fedora 14.
* Mô phỏng sử dụng Security Onion để phân tích và phát hiện các hành động thăm dò, tấn công Fedora 14 của Kali linux.

1. Kết quả đạt được:

Nắm bắt được cách thực hoạt động của Security Onion khi thực hiện phân tích các gói tin để phát hiện nguy cơ tấn công trong môi trường mạng. Hiểu cấu trúc của bộ luật sử dụng trong Security Onion từ đó có thể bổ sung giúp tăng khả năng phát hiện xâm nhập của hệ thống. Nâng cao kiến thức, kinh nghiệm của bản thân khi làm việc trong môi trường mạng.

**LỜI CẢM ƠN**

Trong lời đầu tiên của bản báo cáo đồ án chuyên nhành Mạng này, em mong muốn  
gửi lời cảm ơn và biết ơn chân thành nhất của mình tới tất cả những người đã hỗ trợ,   
giúp đỡ chúng em về kiến thức và tinh thần trong quá trình thực hiện làm đồ án.

Trước hết, em xin chân thành cảm ơn thầy - PGS.TS. Nguyễn Tấn Khôi, giảng viên khoa Công nghệ thông tin, trường đại học Bách Khoa – Đại học Đà Nẵng, người đã trực tiếp hướng dẫn, nhận xét, giúp đỡ em trong suốt quá trình thực hiện đồ án này. Em xin chân thành cảm ơn Ban giám hiệu nhà trường, các thầy cô trong khoa Công nghệ thông tin và các phòng ban nhà trường đã tạo điều kiện tốt nhất cho em cũng như các bạn sinh viên khác trong suốt quá trình học tập và làm đồ án.

Do thời gian thực hiện có hạn, kiến thức còn nhiều hạn chế nên đồ án chuyên ngành Mạng chắc chắn không tránh khỏi những thiếu sót nhất định. Em rất mong nhận được ý kiến đóng góp của các thầy cô giáo và các bạn để em có thêm kinh nghiệm, hoàn thiện và phát triển đề tài hay đồ án trong tương lai.

Em xin chân thành cảm ơn!

**LỜI CAM ĐOAN**

Tôi xin cam đoan:

1. Nội dung trong đồ án này là do tôi thực hiện dưới sự hướng dẫn trực tiếp của PGS.TS. Nguyễn Tấn Khôi.

2. Các tham khảo dùng trong đồ án đều được trích dẫn rõ ràng tên tác giả, tên công trình, thời gian , địa điểm công bố.

3. Nếu có những sao chép không hợp lệ, vi phạm, tôi xin chịu hoàn toàn trách nhiệm.

Sinh viên thực hiện

**Trương Quang Hùng – 17T1**

**MỞ ĐẦU**

1. **Tổng quan về đề tài**

Security Onion là một bản phân phối mã nguồn mở của Linux với nhiều công cụ hữu dụng có thể phân tích, phát hiện các mối nguy hại trong môi trường mạng dựa vào việc phân tích các gói tin gửi đi trong mạng. Bằng cách cài đặt và cấu hình phù hợp, Security Onion có thể đóng vai trò như một hệ thống phát hiện xâm nhập mạng (NIDS – Network Intrusion Detection System).

1. **Mục đích và ý nghĩa của đề tài**
   1. ***Mục đích***

Môi trường mạng luôn tồn lại nhiều nguy cơ bị tấn công, xâm nhập vì vậy việc cài đặt một hệ thống phát hiện các nguy cơ đó một cách nhanh chóng, dễ dàng và chính xác là điều vô cùng cần thiết.

* 1. ***Ý nghĩa***

Thực hiện các kế hoạch để phát hiện sớm những rủi ro, xâm nhập nhằm bảo vệ mạng lưới mạng khỏi Hacker.

1. **Phương pháp thực hiện**

Thực hiện theo các bước sau:

* Tìm hiểu đề tài và phân tích yêu cầu.
* Xây dựng mô hình hệ thống.
* Triển khai phân tích và phát hiện các cuộc tấn công.

1. **Bố cục của đồ án**

Đồ án bao gồm các nội dung sau:

*Mở đầu*

*Chương 1: Trình bày về cơ sở lý thuyết*

*Chương 2: Trình bày về phân tích và thiết kế hệ thống*

*Chương 3: Trình bày về triển khai phát hiện xâm nhập hệ thống*

*Kết luận và hướng phát triển*

**Chương 1: TỔNG QUAN VỀ ĐỀ TÀI**

* 1. **Tổng quan về Security Onion**
     1. ***Định nghĩa***
     2. ***Chức năng***
     3. ***Ưu điểm***
     4. ***Nhược điểm***
  2. **Công nghệ phát triển**
     1. ***Hệ điều hành mã nguồn mở Linux***
     2. ***Hệ thống phát hiện xâm nhập mạng***
     3. ***Kiến trúc***
     4. ***Công cụ Snort***
     5. ***Công cụ Sguil***
     6. ***Công cụ Squert***
     7. ***Bộ luật của Security Onion***
  3. **Các kiểu xâm nhập cơ bản**
     1. ***Thăm dò thông tin sử dụng Nmap***
     2. ***Tấn công Cross-Site Scripting (XSS)***
     3. ***Tấn công SQL injection***
  4. **Mô hình hệ thống phát hiện xâm nhập mạng**
     1. ***Chương trình mô phỏng GNS3***
     2. ***Hệ điều hành Kali Linux***
     3. ***Ứng dụng web Damn vulnerable web application***

**Kết chương**

**Chương 2: PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG**

* 1. **Phân tích yêu cầu**
     1. ***Mục tiêu đề tài***
  2. **Thiết kế hệ thống**
     1. ***Sơ đồ kiến trúc hệ thống***
     2. ***Phân tích hệ thống***

**Kết chương**

**Chương 3: XÂY DỰNG VÀ MÔ PHỎNG HỆ THỐNG**

* 1. **Xây dựng mạng lưới Mạng bằng GNS3**
     1. ***Cài đặt GNS3 và Router Cisco***
     2. ***Cấu hình Router Cisco***
  2. **Xây dựng mô hình hệ thống phát hiện xâm nhập mạng**
     1. ***Cài đặt Security Onion***
     2. ***Cài đặt Kali linux***
     3. ***Cài đặt DVWA trên Fedora 14***
  3. **Mô phỏng hệ thống phát hiện xâm nhập**
     1. ***Cấu hình Security Onion***
     2. ***Chức năng phát hiện thăm dò dữ liệu bằng nmap***
     3. ***Chức năng phát hiện tấn công XSS***
     4. ***Chức năng phát hiện SQL injection***
     5. ***Thêm luật giúp nâng cao khả năng phát hiện xâm nhập của hệ thống***

**Kết chương**

**KẾT LUẬN**

**Kết quả đạt được**

**Hướng phát triển**

**TÀI LIỆU THAM KHẢO**