|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  Logo HvKTMM  ĐỒ ÁN MÔN HỌC  **CHUYÊN ĐỀ CƠ SỞ/ THỰC TẬP CHUYÊN ĐỀ**  **Đề tài:**  **NGHIÊN CỨU HỆ THỐNG PHÁT HIỆN XÂM NHẬP MẠNG SECURITY ONION**  *Sinh viên thực hiện:* **Phạm Minh Sơn – CT401020**  **Nguyễn Văn Thành – CT400446**  **Nguyễn Đình Thành – CT400447**  **Nhóm 6**  *Giảng viên hướng dẫn:* **TS. Nguyễn Đào Trường**    Hà Nội, 9-2023 |

**1. LỜI MỞ ĐẦU**

1.1. Tính cấp thiết của đề tài

1.2. Mục tiêu đạt được khi thực hiện báo cáo

1.3. Phương pháp, đối tượng nghiên cứu

**2. CÁC CHƯƠNG, MỤC DỰ KIẾN**

Nội dung báo cáo gồm 4 chương:

**CHƯƠNG 1. TỔNG QUAN VỀ HỆ THỐNG PHÁT HIỆN XÂM NHẬP**

**1.1.Tổng quan về xâm nhập**

**1.2. Hệ thống phát hiện xâm nhập**

*1.2.1.Hệ thống phát hiện xâm nhập cho mạng*

*1.2.2.Hệ thống phát hiện xâm nhập cho host*

**1.3. Kỹ thuật phát hiện xâm nhập**

*1.3.1. Phát hiện xâm nhập dựa trên chữ ký*

*1.3.2. Phát hiện xâm nhập dựa trên bất thường (Anomaly Intrusion Detection)*

*1.3.3. Phát hiện xâm nhập dựa trên phân tích giao thức trạng thái (Stateful Protocol Analysis)*

**CHƯƠNG 2. GIỚI THIỆU SECURITY ONION**

**2.1. Giới thiệu tổng quát**

**2.2. Các chức năng của Security Onion**

*2.2.1. Bắt tất cả gói tin (Full Packet Capture)*

*2.2.2. Phát hiện mạng và các điểm cuối*

*2.2.3. Các công cụ phân tích*

*2.2.4. Các công cụ NIDS*

*2.2.5. Các công cụ hỗ trợ phân tích điểm cuối (Host Visibility)*

**CHƯƠNG 3. CÁCH THỨC HOẠT ĐỘNG CỦA SECURITY ONION**

**3.1. Kiến trúc của Security Onion**

*3.1.1. Import*

*3.1.2. Evaluation*

*3.1.3. Standalone*

*3.1.4. Distributed*

*3.1.5. Các loại nodes*

**3.2. Cách thức hoạt động của Security Onion**

*3.2.1. IDS*

*3.2.2. IPS*

**3.3. Cài đặt Security Onion**

*3.3.1. Yêu cầu phần cứng*

*3.3.2. Môi trường cài đặt*

*3.3.3. Các tác vụ cần thực hiện sau khi cài đặt*

**KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN**

**TÀI LIỆU THAM KHẢO**

**PHỤ LỤC** (nếu có)

|  |  |
| --- | --- |
|  | Hà nội, ngày 22 tháng 9 năm 2023 |
|  | **XÁC NHẬN CỦA GIẢNG VIÊN HƯỚNG DẪN** |
|  | **TS. NGUYỄN ĐÀO TRƯỜNG** |