Lesson 9.

IDS/IPS, SIEM

Outline

1. IDS/IPS
2. SIEM
3. Labs

IDS – Intrusion Detection System

- The main function of an IDS is to warn about suspicious activity taking place, but not to prevent them

- An IDS specifically looks for suspicious activity and events that might be the result of a virus, worm or hacker

IDS – Intrusion Detection System

All IDS have three things in commons:

- **Sensors**: collect traffic and user activity data and sends to analyzer
- **Analyzer**: looks for suspicious activity
- **Administrator interface**: If analyzer detects suspicious activity, sends an alert to the Admin interface.

IDS – Intrusion Detection System

Types of IDS

- NIDS
  - Use sensors to monitor all network traffic
  - Cannot see the activities within the computer itself
- HIDS
  - Install on workstations/Servers
  - Watches for abnormal activity

IDS – Intrusion Detection System

- Signature based
  - Pattern matching
  - Stateful matching
- Anomaly based
  - Statistical anomaly based
  - Protocol anomaly based
  - Traffic anomaly based
- Rule based

IPS – Intrusion Prevention System

- IPS is any device (hardware or software) that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful

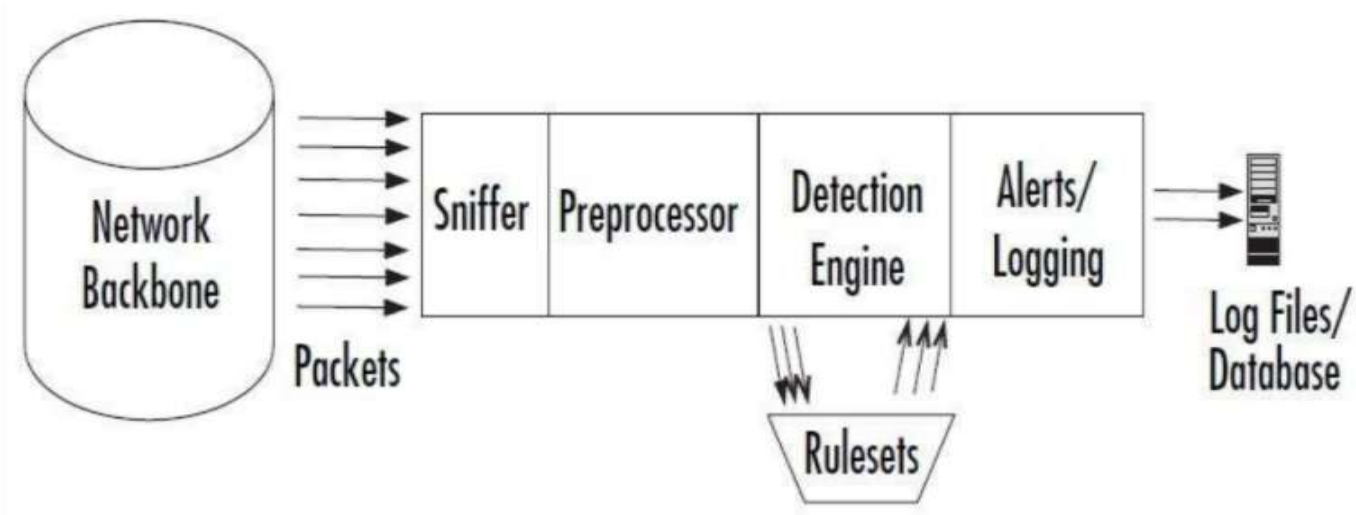
- Classification of IPS

  - **HIPS**

  - **NIPS**

Lab : Snort IDS

- There are four basic components of Snort's architecture:
  - The Sniffer
  - The Preprocessor
  - The Detection Engine
  - The Output




snort.org
Search...
Rule Doc Search
Documents
Downloads
Products
Community
Talos
Resources
Contact
Sign In
Protect your network with the world's most powerful Open Source detection software.
Get Started
Download Rules
Documents
SNORT®
Snort 3.0 is here!
Upgrade to experience a slew of new features and improvements.
Upgrade Now
Snort 3 is available!

SIEM

Security Information and Event Management

Giới thiệu

● SIEM được thiết kế thu thập thông tin nhật ký các sự kiện an ninh từ các thiết bị đầu cuối và lưu trữ dữ liệu một cách tập trung

● Cho phép phân tích tập trung và báo cáo các sự kiện an toàn mạng của tổ chức

● Phát hiện các cuộc tấn công mà không thể phát hiện được theo phương pháp thông thường

●Có thể ngăn chặn các cuộc tấn công mà chúng phát hiện ra

Kiến trúc SIEM

- Phần mềm SIEM cài đặt trên máy chủ cục bộ
- Phần cứng hoặc máy ảo dành riêng cho SIEM
- Dịch vụ đám mây SIEM

Lợi ích của SIEM

- Quản lý tập trung
- Giám sát an toàn mạng
- Cải thiện hiệu quả trong hoạt động xử lý sự cố

Quản lý tập trung

- Tập hợp dữ liệu thông qua giải pháp nhật ký tập trung
- Mỗi thiết bị đầu cuối cần có hệ thống ghi lại sự kiện an ninh và thường xuyên truyền log về máy chủ SIEM
- Máy chủ SIEM nhận dữ liệu nhật ký từ rất nhiều thiết bị khác nhau và sau đó thực hiện thống kê, phân tích, báo cáo
- Tạo ra báo cáo duy nhất cho thấy sự tương quan giữa các sự kiện an ninh của các thiết bị

Giám sát an toàn mạng

● Nhiều thiết bị có khả năng ghi log sự kiện an ninh nhưng thiếu khả năng phân tích để xác định các hành vi độc hại

● SIEM có khả năng cho thấy sự tương quan sự kiện giữa các thiết bị

● SIEM thấy được nhiều phần khác nhau của các cuộc tấn công thông quan nhiều thiết bị và sau đó tái cấu trúc lại chuỗi sự kiện và xác định cuộc tấn công ban đầu là gì và nó đã thành công hay chưa.

Ví dụ:

●IPS có thể thấy được một phần của cuộc tấn công và HĐH của máy chủ mục tiêu cũng cho thấy một phần khác của cuộc tấn công đó

●SIEM có thể kiểm tra dữ liệu nhật ký của tất cả các sự kiện này và xác định máy chủ mục tiêu đó đã bị nhiễm mã độc hay tấn công thành công hay chưa

●Từ đó có thể thực hiện cách ly chúng ra một mạng riêng và xử lý cuộc tấn công.

●SIEM không thay thế các sản phẩm kiểm soát an ninh phát hiện tấn công như IPS, firewall, phần mềm diệt virus

●SIEM được thiết kế để sử dụng các dữ liệu nhật ký được ghi lại bởi các phần mềm khác nhau từ đó phân tích tương quan và đưa ra các cảnh báo.

●Nhiều sản phẩm SIEM có khả năng ngăn chặn các cuộc tấn công mà chúng phát hiện. SIEM không trực tiếp ngăn chặn mà kết nối vào hệ thống an ninh khác như firewall để ngăn chặn

Cải thiện hoạt động xử lý sự cố hiệu quả

●Cung cấp giao diện đơn giản để xem xét tất cả dữ liệu nhật ký an ninh từ nhiều thiết bị.

●Xác định nhanh chóng tất cả các thiết bị đầu cuối bị ảnh hưởng bởi cuộc tấn công

●Cung cấp cơ chế tự động nhằm ngăn chặn các cuộc tấn công và cách ly các thiết bị đầu cuối đã bị tấn công.