BÁO CÁO TIẾN ĐỘ GIỮA KỲ

**Môn học: Pháp chứng kỹ thuật số**

**Lab 1: Memory Forensic**

*GVHD: Lê Đức Thịnh*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT334.O21.ATTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Lê Hà Quang Thịnh | 19522277 | 19522277@gm.uit.edu.vn |
| 2 | Mai Văn Hùng | 20521367 | 20521367@gm.uit.edu.vn |
| 3 | Huỳnh Dương Đức Toàn | 19521028 | 19521028 @gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Thành viên thực hiện** |
| 1 | Mô phỏng về cuộc tấn công | Mai Văn Hùng |
| 2 | Tìm hiểu và soạn lý thuyết | Huỳnh Dương Đức Toàn |
| 3 | Dựng mô hình demo | Lê Hà Quang Thịnh |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

**Nghiên cứu các loại Logs trong Network Forensics.**

-Logging trong lĩnh vực network forensics đóng vai trò quan trọng để ghi lại và phân tích các hoạt động trên mạng để điều tra các sự cố bảo mật hoặc vi phạm chính sách. Có các loại logging thông dụng như sau:

+Packet Capture (PCAP): bao gồm việc ghi lại và lưu trữ dữ liệu giao tiếp mạng khi nó di chuyển qua mạng; công cụ: Wireshark, tcpdump, hoặc Bro (hiện đã được đổi tên thành Zeek) thường được sử dụng để bắt và ghi lại các gói tin mạng; các tệp PCAP chứa thông tin chi tiết về mỗi gói tin, bao gồm địa chỉ IP nguồn và đích, cổng, giao thức và dữ liệu gói tin; những tệp này rất quan trọng để xây dựng lại các phiên mạng và phân tích hành vi mạng trong quá trình xảy ra sự cố.

+NetFlow/SFlow: là các định dạng giao thức mạng được sử dụng để thu thập và tổng hợp dữ liệu lưu lượng IP; thay vì bắt mỗi gói tin, NetFlow và sFlow thu thập dữ liệu metadata về các luồng lưu lượng mạng, chẳng hạn như địa chỉ IP nguồn và đích, cổng, giao thức và số byte; Metadata này cung cấp một cái nhìn tổng quan về mô hình lưu lượng mạng và có thể giúp xác định hành vi bất thường hoặc phát hiện các loại tấn công cụ thể.

+Syslog: là một giao thức tiêu chuẩn được sử dụng để ghi lại các thông báo và sự kiện hệ thống; thiết bị mạng như router, switch, firewall và hệ thống phát hiện/phòng ngừa xâm nhập có thể tạo ra các thông báo syslog về các sự kiện mạng, lỗi hoặc cảnh báo bảo mật; các thông báo syslog thường được gửi đến một máy chủ ghi nhật ký tập trung để lưu trữ và phân tích;

+DNS Logging: bao gồm việc ghi lại dữ liệu truy vấn và phản hồi DNS; nhật ký DNS có thể tiết lộ tên miền được yêu cầu bởi người dùng, địa chỉ IP liên kết với các tên miền đó, và bất kỳ hành vi DNS bất thường nào, chẳng hạn như túi thông tin DNS hoặc các thuật toán tạo ra tên miền (DGA) được sử dụng bởi phần mềm độc hại.

+Endpoint Logs: log endpoint, được tạo ra bởi các thiết bị cá nhân như máy tính, máy chủ hoặc thiết bị di động, cung cấp thông tin quý báu về các hoạt động mạng cục bộ và sự kiện hệ thống; bao gồm Windows Event Logs (ví dụ: Security, Application, System logs), macOS Unified Logs và các nhật ký hệ thống Linux (ví dụ: syslog, auth logs).

Cấu trúc của các loại logs

-Packet Capture (PCAP): Timestamp, Source IP, Destination IP, Source Port, Destination Port, Protocol, Packet Payload.

- NetFlow/SFlow: Timestamp, Source IP, Destination IP, Source Port, Destination Port, Protocol, Bytes Transferred.

-Syslog: Timestamp, Device IP/Hostname, Severity/Priority, Facility, Message.

- DNS Logging:

- Endpoint Logs:

Tools cho logs forensics: Wireshark, tcpdump, Bro/Zeek, Elastic Stack/ELK Stack, Snort, Suricata.

Demo các nội dung ở trên, tổ chức theo 1 kịch bản cụ thể: thu thập, phân tích, kết quả

Các kịch bản:

-PCAP: sử dụng wireshark bắt gói tin từ client ra ngoài internet

-Syslog: sử dụng, thiết lập router/switch/firewall vật lí hoặc ảo để theo dõi và logging hoạt động của máy client.

-PCAP: thiết lập wireshark như một ids theo dõi các client.

**Mô Hình Hoá**

Trong mô hình hệ thống về Network Logs Forensics nhóm em sẽ thiết lập một quy trình bằng Wireshark và Opensearch Stack có thể trông như thế này:

A diagram of a computer server

Description automatically generated

Mô hình tổng quan của một hệ thống Network Logs gồm 3 thành phần:

1. **Packet capture** - Ghi lại lưu lượng gói trên mạng.
2. **Protocol parsing**- Phân tích các giao thức và trường mạng khác nhau.
3. **Search and Visualize** - Khám phá dữ liệu một cách chi tiết hoặc tổng hợp.

Mô hình demo hệ thống em dựng gồm 3 máy chủ Ubuntu 22.04 với các IP: 172.16.100.225, 172.16.100.226, 172.16.100.227. Với các vai trò như sau:

* 172.16.100.227 sẽ là server agent đóng vai trò là nạn nhân trong các cuộc tấn công, có thể đại diện cho một cụm mạng hoặc một subnet. Được cài Tshark và Filebeat để capture các gói tin và lưu trữ Network Logs.
* 172.16.100.226 sẽ là server Logging được cài Logstash nhận nhiệm vụ lấy logs bắn từ Filebeat sau đó xữ lý log filter logs,…
* 172.16.100.225 sẽ là server được cài đặt Opensearch với mục tiêu nhận logs, metric,… Để phân tích và đánh giá.

Trong một hệ thống phân tích network logs phục phụ cho forensics, Tshark phục vụ cho việc capture các gói tin mạng trong một host sau đó chuyển đổi sang định dạng Json để Filebeat đọc được. Filebeat được sử dụng để thu thập các log file json của Tshark từ các thiết bị mạng, Logstash được sử dụng để xử lý và chuyển đổi các log này thành định dạng phù hợp, và OpenSearch có thể được sử dụng để lưu trữ, tìm kiếm và phân tích dữ liệu log này để hỗ trợ các hoạt động forensics.

**Server 172.16.100.227 sẽ được cài Filebeat và Tshark:**

**Filebeat:** Là một công cụ thu thập log từ các nguồn khác nhau như các file log, logs hệ thống, hoặc các nguồn log khác. Filebeat có khả năng theo dõi các thay đổi trong các file log và gửi dữ liệu từ những thay đổi này đến các hệ thống khác như Elasticsearch hoặc Logstash để lưu trữ và phân tích.

Vì mục dích học tập và điều kiện tài nguyên còn hạn chế nên em ưu tiên chạy container để dễ dàng quản lí up/down cho việc demo học thuật.

File docker-compose.yml của filebeat.

A screenshot of a computer program

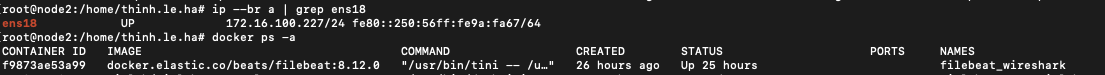
Description automatically generated

Filebeat.yml dùng để chứa các config của filebeat container được mount ra ngoài.

A screen shot of a computer program

Description automatically generated

Dưới đây là Ip và tình trạng container filebeat



**Server 172.16.100.226 sẽ được cài Logstash:**

**Logstash**: Là một công cụ xử lý và chuyển đổi dữ liệu log từ nhiều nguồn khác nhau vào định dạng chuẩn và phù hợp để lưu trữ hoặc phân tích. Logstash có thể được sử dụng để lọc, chuyển đổi, và tiêu hao dữ liệu log từ Filebeat hoặc các nguồn khác, trước khi chuyển tiếp chúng đến một hệ thống lưu trữ hoặc phân tích dữ liệu khác như Elasticsearch hoặc OpenSearch.

File docker-compose.yml của logstash.

A screenshot of a computer program

Description automatically generated

File pipelines của logstash container config, với mỗi pipeline ta có thể nhận logs từ một agent hoặc một tags log khác nhau, điều này thuận tiện cho việc lấy logs số lượng lớn và đa dạng từ nhiều agent.

A black and white screen with white text

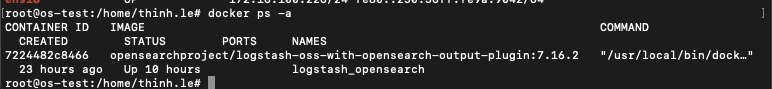
Description automatically generated

File wireshark.yml chứa các thông tin config gồm thông tin cổng lấy dữ liệu filebeat, các plugins filter dịnh dạng thời gian. Và out đẩy logs lên Opensearch cluster.

A screenshot of a computer

Description automatically generated

Dưới đây là Ip và tình trạng container Logstash



**Server 172.16.100.225 sẽ được cài Opensearch cluster:**

Opensearch: OpenSearch là một hệ thống tìm kiếm và phân tích dữ liệu mạnh mẽ, được phát triển từ dự án mã nguồn mở Elasticsearch. OpenSearch cung cấp khả năng lưu trữ, tìm kiếm và phân tích dữ liệu log từ nhiều nguồn khác nhau, cho phép các nhà phân tích forensics thực hiện các tìm kiếm, truy vấn và phân tích dữ liệu log một cách hiệu quả.

Riêng code của để dựng Opensearch Cluster gồm 3 node runner và một Dashboard để hiển thị thông tin.

Mô hình opensearch này nhóm dựng theo chuẩn failover 2k+1 gồm 3 node: 1 master và 2 slave với cơ chế đồng thuận raft để bầu node master khi bị chết.

A black screen with white text

Description automatically generated

Dưới đây là file Docker compose của Openseach

A screenshot of a computer

Description automatically generatedA screenshot of a computer program

Description automatically generated

Dưới đây là dashboard của openseach

A screenshot of a computer

Description automatically generated

BÁO CÁO CHI TIẾT

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-ExeX\_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

*Ví dụ: [*NT101.K11.ANTT*]-Exe01\_Group03.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**:

* Hoàn thành tốt yêu cầu được giao.
* Có nội dung mở rộng, ứng dụng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)