|  |  |
| --- | --- |
|  | **BỘ GIÁO DỤC VÀ ĐÀO TẠO**  **TRƯỜNG ĐẠI HỌC GIA ĐỊNH**  **KHOA CÔNG NGHỆ THÔNG TIN** |



**BÁO CÁO**

**THỰC TẬP TỐT NGHIỆP**

**TÊN ĐỀ TÀI**

**TRIỂN KHAI HỆ THỐNG CVAT, NESSUS VÀ QUẢN LÝ LOG BẰNG SIEM (SPLUNK)**

**Giảng viên hướng dẫn: Ths.Hồ Quý Thuận**

**Sinh viên thực hiện: Huỳnh Khôi Nguyên**

**MSSV: 22150411 Lớp: 221541 Khóa: 2022\_ĐHCQ\_K16**

*Thành phố Hồ Chí Minh, tháng 06 năm 2025*

**LỜI CẢM ƠN**

Em xin gửi lời cảm ơn chân thành đến quý thầy cô tại Trường Đại học Gia Định Thành phố Hồ Chí Minh đã tận tình giảng dạy, truyền đạt kiến thức và kinh nghiệm quý báu trong suốt thời gian học tập tại trường.

Đặc biệt, em xin gửi lời cảm ơn sâu sắc đến thầy Hồ Quý Thuận đã hướng dẫn, động viên và hỗ trợ em hoàn thành báo cáo tốt nghiệp này.

Em xin chân thành cảm ơn ban lãnh đạo và các anh chị tại công ty Công ty Cổ phần Hạ tầng Công nghệ Teknix Cloud đã tạo điều kiện cho em thực tập và học hỏi kinh nghiệm thực tế. Sự chỉ dẫn và hỗ trợ của các anh chị trong thời gian thực tập là nguồn động lực lớn giúp em hoàn thành dự án này.

Do kiến thức và kinh nghiệm còn nhiều hạn chế, nên bài báo cáo của em còn nhiều thiếu sót, kính mong nhận được sự đánh giá và góp ý của Thầy.

Xin chân thành cảm ơn!

|  |  |
| --- | --- |
| TRƯỜNG ĐẠI HỌC GIA ĐỊNH | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** |
| **KHOA CÔNG NGHỆ THÔNG TIN** | **Độc lập – Tự do – Hạnh phúc** |

**PHIẾU ĐÁNH GIÁ BÁO CÁO KẾT QUẢ**

**THỰC TẬP TỐT NGHIỆP**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tên học phần:** Thực tập tốt nghiệp | | **Lớp học phần:**………………... | | |
| **Họ và tên sinh viên:**…………….................................... | | **MSSV:**………………………… | | |
| **STT** | **Nội dung đánh giá** | | **Điểm** | **Ghi chú** | |
| **I. Hình thức trình bày** | | |  |  | |
| 1 | Cấu trúc báo cáo đầy đủ (bìa, mục lục, tài liệu tham khảo...) | |  |  | |
| 2 | Trình bày đúng quy định (font chữ, cỡ chữ, căn lề, khoảng cách dòng) | |  |  | |
| 3 | Bảng biểu, sơ đồ, hình ảnh minh họa rõ ràng, có chú thích | |  |  | |
| **II. Lịch làm việc** | | |  |  | |
| 1 | Tuân thủ thời gian thực tập | |  |  | |
| 2 | Thực hiện đầy đủ báo cáo tiến độ theo yêu cầu | |  |  | |
| **III. Nội dung thực tập** | | |  |  | |
| 1 | Có được sự hiểu biết tốt về đơn vị thực tập | |  |  | |
| 2 | Mô tả chi tiết công việc thực tập, nhiệm vụ được giao | |  |  | |
| 3 | Ứng dụng kiến thức lý thuyết vào thực tiễn | |  |  | |
| 4 | Kết quả rèn luyện kỹ năng thực hành | |  |  | |
| 5 | Kinh nghiệm thực tiễn thu thập được | |  |  | |
| 6 | Mức độ chủ động trong công việc hoặc khả năng thích nghi | |  |  | |
| 7 | Chất lượng nội dung, sự đầu tư và tính logic | |  |  | |
| **TỔNG ĐIỂM** | | |  |  | |

*Tp. Hồ Chí Minh, ngày tháng năm 2025*

**Giảng viên**

*(Ký và ghi rõ họ tên)*

**ĐÁNH GIÁ CỦA ĐƠN VỊ THỰC TẬP**

1. **Thái độ tác phong trong thời gian thực tập:**

1. **Kiến thức chuyên môn:**

1. **Nhận thức thực tế:**

1. **Đánh giá khác:**

**5. Đánh giá chung kết quả thực tập:**

*………………, ngày ……… tháng ……… năm …………*

**TM. Đơn vị thực tập**

(Ký tên, đóng dấu)

**ĐÁNH GIÁ CỦA GIẢNG VIÊN HƯỚNG DẪN**

1. **Thái độ tác phong trong thời gian thực tập:**

1. **Kiến thức chuyên môn:**

1. **Nhận thức thực tế:**

1. **Đánh giá khác:**

**5. Đánh giá chung kết quả thực tập:**

*………………, ngày ……… tháng ……… năm …………*

**Giảng viên hướng dẫn**

(Ký tên, ghi rõ họ tên)

|  |  |
| --- | --- |
| **TRƯỜNG ĐẠI HỌC GIA ĐỊNH**  **KHOA CÔNG NGHỆ THÔNG TIN** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập – Tự do – Hạnh phúc** |

**BÁO CÁO THỰC TẬP TỐT NGHIỆP HÀNG TUẦN**

Họ và tên SV: Huỳnh Khôi Nguyên MSSV: 22150411

Lớp: 221541

Giảng viên hướng dẫn: Ths.Hồ Quý Thuận

Tên doanh nghiệp (đơn vị) đến thực tập: Công ty Cổ phần Hạ tầng Công nghệ Teknix Cloud.

Địa chỉ: 6th Floor Golden House Tower – Sunwah Pearl Building, 90 Nguyen Huu Canh, Ward 22, Binh Thanh District, Ho Chi Minh City, Vietnam.

Điện thoại: 091 555 65 65

Tên cán bộ phụ trách thực tập tại doanh nghiệp:

Thời gian thực tập Từ: 28/04/2025 Đến: 20/06/2025

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Stt** | **Tuần thứ** | **Nội dung CV thực tập trong tuần** | **Nhận xét của CB hướng dẫn tại DN**  **(Ký tên và ghi rõ họ tên)** | **Nhận xét của giảng viên hướng dẫn**  **(Ký tên và ghi rõ họ tên)** |
| 1 | Tuần 1  (Từ ngày 28/04/2025 đến ngày04/05/2025) | - Tìm hiểu về lý thuyết và hệ thống:   * - Tìm hiểu về các hệ thống Spunk, Nessus, Cvat, Rclone. * Tìm hiểu mô hình triển khai trên hệ điều hành Ubuntu 24.04. |  |  |
| 2 | Tuần 2  (Từ ngày 05/05/2025 đến ngày 11/05/2025) | - Xây dựng mô hình hệ thống gồm:   * 1 máy chủ Ubuntu 24.04 để cài đặt Cvat, Nessus, Spunk * 1 máy phụ Windows Server để backup dữ liệu qua Rclone |  |  |
| 3 | Tuần 3  (Từ ngày 12/05/2025 đến ngày 18/05/2025) | - Cài đặt và cấi hình cho Cvat:   * Triển khai Docker và Docker Compose trên Ubuntu 24.04. * Tải mã nguồn CVAT từ GitHub và cấu hình môi trường. * Chạy CVAT thành công, tạo tài khoản admin và test chức năng gán nhãn dữ liệu. * Kiểm tra port mặc định (8080), và đảm bảo CVAT hoạt động ổn định. |  |  |
| 4 | Tuần 4  (Từ ngày 19/05/2025 đến ngày25/05/2025) | - Cài đặt và cấu hình cho Nessus:   * Cài đặt Nessus Essentials trên Ubuntu 24.04. * Kích hoạt bản miễn phí và cập nhật plugin quét lỗ hổng. * Quét thử lỗ hổng trong mạng nội bộ.   - Cài đặt và cấu hình cho Spunk:   * Cài đặt Splunk Enterprise trên Ubuntu 24.04. * Thiết lập chỉ mục (index), tạo dashboard đơn giản. * Kiểm tra hoạt động thu thập log hệ thống nội bộ. * Kết nối splunkForwarder từ máy khác gửi log về máy chủ. Splunk. |  |  |
| 5 | Tuần 5  (Từ ngày 26/05/2025 đến ngày 01/06/2025) | - Mở port Firewall và kiểm tra dịch vụ:   * Cấu hình tường lửa trên Ubuntu. * Kiểm tra kết nối từ xa đến các dịch vụ thông qua địa chỉ IP. * Đảm bảo an toàn và giới hạn truy cập cho các port quan trọng. |  |  |
| 6 | Tuần 6  (Từ ngày 02/06/2025 đến ngày 08/05/2025) | - Thiết lập hệ thống backup dữ liệu:   * Cài đặt Rclone trên máy chủ chính và máy backup. * Cấu hình đồng bộ thư mục chứa dữ liệu CVAT và Splunk về Google Drive. * Thiết lập cronjob tự động backup theo lịch mỗi ngày/lần. * Kiểm tra khả năng khôi phục dữ liệu từ bản sao lưu. |  |  |
| 7 | Tuần 7  (Từ ngày 09/06/2025 đến ngày 15/06/2025) | - Tối ưu và hoàn thiện hệ thống.   * Kiểm tra lại toàn bộ hệ thống: * Tính ổn định của CVAT khi có nhiều phiên chú thích dữ liệu. * Đảm bảo Nessus có thể cập nhật plugins mới. * Kiểm tra bảng điều khiển (dashboard) log trên Splunk. * Viết hướng dẫn vận hành hệ thống cho người dùng cuối. |  |  |
| 8 | Tuần 8  (Từ ngày 16/06/2025 đến ngày 20/06/2025) | **-** Viết báo cáo thực tập.  **-** Báo cáo sản phần cho doanh nghiệp, giảng viên hướng dẫn. |  |  |

**MỤC LỤC**

[**MỞ ĐẦU** 1](#_Toc200828059)

[**GIỚI THIỆU VỀ DOANH NGHIỆP** 3](#_Toc200828060)

[**CHƯƠNG 1: TỔNG QUAN ĐỀ TÀI** 4](#_Toc200828061)

[**1.1. Đặt vấn để.** 4](#_Toc200828062)

[**1.2. Nhiệm vụ của đề tài.** 5](#_Toc200828063)

[**1.3. Cấu trúc của đề tài.** 6](#_Toc200828064)

[**CHƯƠNG 2: CƠ SỞ LÝ THUYẾT** 7](#_Toc200828065)

[**2.1. Giới thiệu về các công cụ được dùng trong đề tài.** 7](#_Toc200828066)

[**2.1.1. Giới thiệu về công cụ Spunk.** 7](#_Toc200828067)

[**2.1.2. Giới thiệu về công cụ Cvat.** 7](#_Toc200828068)

[**2.1.3. Giới thiệu về công cụ Nessus.** 7](#_Toc200828069)

[**2.1.4. Giới thiệu về công cụ Rclone.** 8](#_Toc200828070)

[**2.1.5. Giới thiệu về công cụ Cronjob.** 8](#_Toc200828071)

[**2.2. Giới thiệu về Ubuntu.** 8](#_Toc200828072)

[**2.3. Tổng quan về giám sát và ghi log hệ thống.** 9](#_Toc200828073)

[**2.3.1. Các loại log thường gặp.** 9](#_Toc200828074)

[**2.3.2. Mục đích của việc ghi log.** 10](#_Toc200828075)

[**2.4. Khái niệm kiểm thử và đánh giá lỗ hổng bảo mật.** 10](#_Toc200828076)

[**2.4.1. Kiểm thử lỗ hổng là gì.** 10](#_Toc200828077)

[**2.4.2. Các khái niệm liên quan.** 10](#_Toc200828078)

[**2.5. Giới thiệu Rclone và Cronjob – Cơ chế sao lưu và đồng bộ log tự động.** 11](#_Toc200828079)

[**2.5.1. Giới thiệu Rclone.** 11](#_Toc200828080)

[**2.5.2. Giới thiệu Cronjob.** 12](#_Toc200828081)

[**CHƯƠNG 3: MÔ HÌNH THỰC NGHIỆM** 14](#_Toc200828082)

[**3.1. Giới thiệu dự án.** 14](#_Toc200828083)

[**3.2. Mô hình tổng quan hệ thống.** 15](#_Toc200828084)

[**3.3. Các bước cài dặt và cấu hình hệ thống.** 16](#_Toc200828085)

[**3.3.1. Cài đặt và cấu hình Splunk.** 16](#_Toc200828086)

[**3.3.2. Cài Đặt và cấu hình Cvat.** 17](#_Toc200828087)

[**3.3.3. Cài đặt và cấu hình Nessus.** 18](#_Toc200828088)

[**3.3.4. Cài đặt Rclone và cấu hình đồng bộ log.** 19](#_Toc200828089)

[**3.4. Các bước triển khai backup.** 20](#_Toc200828090)

[**3.4.1. Backup log Cvat lên Google Drive.** 20](#_Toc200828091)

[**3.4.2. Backup log Splunk lên Google Drive.** 21](#_Toc200828092)

[**3.4.3. Backup log Nessus lên Google Drive.** 22](#_Toc200828093)

[**3.4.4. Backup log lên Window Server 2019.** 22](#_Toc200828094)

[**3.5. Tự động hóa backup log bằng cronjob.** 23](#_Toc200828095)

[**3.6. Kết quả đạt được.** 24](#_Toc200828096)

[**CHƯƠNG 4: KẾT LUẬN** 27](#_Toc200828097)

[**4.1. Đánh giá kết quả đạt được và những khó khăn gặp phải.** 27](#_Toc200828098)

[**4.2. Đề xuất các cải tiến và hướng phát triển tiếp theo.** 27](#_Toc200828099)

[**4.3. Kết luận và những bài học kinh nghiệm rút ra từ dự án.** 28](#_Toc200828100)

[**DANH MỤC HÌNH ẢNH** 29](#_Toc200828101)

[**TÀI LIỆU THAM KHẢO** 30](#_Toc200828102)

# **MỞ ĐẦU**

Trong thời kỳ chuyển đổi số mạnh mẽ hiện nay, việc ứng dụng các công nghệ hiện đại vào công tác quản lý dữ liệu, giám sát bảo mật và xử lý thông tin đóng vai trò vô cùng quan trọng, đặc biệt trong lĩnh vực Công nghệ Thông tin. Những công cụ hỗ trợ như hệ thống gán nhãn dữ liệu, giải pháp quét lỗ hổng và nền tảng quản lý log theo mô hình SIEM (Spunk) ngày càng được quan tâm và ứng dụng rộng rãi trong cả doanh nghiệp và tổ chức nghiên cứu.

Đề tài “Triển khai hệ thống CVAT, Nessus và quản lý log bằng SIEM (Splunk) trên Ubuntu 24.04” được thực hiện trong khuôn khổ chương trình thực tập của trường Đại Học Gia Định Thành phố Hồ Chí Minh tại Công ty Cổ phần Hạ tầng Công nghệ Teknix Cloud – một đơn vị hoạt động trong lĩnh vực hạ tầng công nghệ, dịch vụ đám mây và bảo mật hệ thống. Đây là cơ hội để tiếp cận môi trường làm việc thực tế và áp dụng kiến thức đã học vào triển khai những công cụ chuyên sâu:

* CVAT (Computer Vision Annotation Tool): nền tảng mã nguồn mở hỗ trợ gán nhãn dữ liệu ảnh, phục vụ cho các bài toán học máy trong thị giác máy tính.
* Nessus: công cụ quét lỗ hổng bảo mật được sử dụng phổ biến nhằm đánh giá mức độ an toàn và tuân thủ của hệ thống mạng.
* Splunk: nền tảng SIEM mạnh mẽ hỗ trợ thu thập, phân tích và giám sát log trong thời gian thực, giúp phát hiện sớm các hành vi bất thường trong hệ thống.

Việc triển khai các hệ thống trên nền tảng Ubuntu 24.04 không chỉ đảm bảo tính ổn định, bảo mật và linh hoạt, mà còn giúp học viên rèn luyện kỹ năng cấu hình, tích hợp, xử lý dữ liệu và vận hành các công cụ trong môi trường thực tiễn. Thông qua quá trình thực hiện, người viết có cơ hội nâng cao kiến thức chuyên ngành An toàn Thông tin, đồng thời học hỏi kinh nghiệm thực tế từ đội ngũ kỹ sư tại Teknix Cloud – một môi trường làm việc chuyên nghiệp và năng động.

Báo cáo này được viết nhằm trình bày kết quả của quá trình thực tập của tôi và đồng thời chia sẽ kinh nghiệm, kiến thức mà tôi đã học được. Báo cáo này bao gồm các phần chính sau:

**Chương 1:** Tổng quan về đề tài.

**Chương 2:** Cơ sở lý thuyết.

**Chương 3:** Mô hình thực nghiệm.

**Chương 4:** Kết luận.

# **GIỚI THIỆU VỀ DOANH NGHIỆP**

Công ty Cổ phần hạ tầng Công nghệ TekNix Cloud tọa lạc tại 6th Floor Golden House Tower – Sunwah Pearl Building, 90 Nguyen Huu Canh, Ward 22, Binh Thanh District, Ho Chi Minh City, Vietnam., Hồ Chí Minh. Công ty Cổ phần Hạ tầng Công nghệ Teknix Cloud (TekNix Cloud) là một doanh nghiệp công nghệ thông tin tại Việt Nam, chuyên cung cấp các giải pháp hạ tầng công nghệ và dịch vụ đám mây toàn diện cho doanh nghiệp.

TekNix Cloud cung cấp đa dạng dịch vụ công nghệ, tập trung vào việc triển khai hạ tầng mạng và dịch vụ đám mây như máy chủ, hệ thống mạng và lưu trữ dữ liệu. Ngoài ra, công ty còn phát triển các giải pháp số hóa trong các lĩnh vực như thương mại điện tử, FinTech, Blockchain, DApps, Affiliate Marketing và Wifi Marketing. Trong mảng phát triển phần mềm, TekNix Cloud cung cấp dịch vụ thiết kế website và ứng dụng theo yêu cầu. Bên cạnh đó, công ty cũng cung cấp thiết bị công nghệ phần cứng và dịch vụ tư vấn, vận hành hệ thống, cũng như cung ứng nhân sự công nghệ. TekNix Cloud hiện sở hữu mạng lưới trung tâm dữ liệu tại 25 địa điểm trên toàn cầu, cho phép triển khai linh hoạt các dịch vụ VPS, máy chủ vật lý và lưu trữ dữ liệu một cách hiệu quả. Với khẩu hiệu “Innovate the Future”, công ty cam kết đổi mới liên tục và ứng dụng công nghệ tiên tiến nhằm mang lại giá trị tối ưu cho khách hàng và đối tác.

# **CHƯƠNG 1: TỔNG QUAN ĐỀ TÀI**

**1.1. Đặt vấn đề.**

Trong thời đại công nghệ phát triển nhanh chóng, các hệ thống thông tin ngày càng trở nên phức tạp và yêu cầu cao về hiệu năng, tính sẵn sàng cũng như độ an toàn bảo mật. Song song đó, sự gia tăng về quy mô dữ liệu và mức độ tinh vi của các mối đe dọa mạng khiến cho việc quản lý, giám sát và bảo vệ hệ thống CNTT trở nên cấp thiết hơn bao giờ hết.

Ba vấn đề nổi bật hiện nay đặt ra cho các kỹ sư hệ thống và chuyên viên an ninh thông tin bao gồm:

* **Tự động hóa trong xử lý dữ liệu:** đặc biệt là dữ liệu phục vụ cho trí tuệ nhân tạo (AI), đòi hỏi công cụ gán nhãn trực quan, chính xác và có khả năng tùy biến cao.
* **Kiểm thử bảo mật hệ thống định kỳ:** nhằm phát hiện sớm các điểm yếu có thể bị khai thác, từ đó giảm thiểu nguy cơ mất an toàn thông tin.
* **Giám sát log hệ thống tập trung và hiệu quả:** phục vụ cho việc phát hiện hành vi bất thường, truy vết sự cố và đảm bảo tuân thủ.

Để giải quyết các vấn đề trên, việc triển khai tích hợp ba công cụ mã nguồn mở hoặc thương mại phổ biến hiện nay là một hướng đi thiết thực:

* **CVAT (Computer Vision Annotation Tool)**: công cụ hỗ trợ gán nhãn dữ liệu hình ảnh, phục vụ cho các ứng dụng học máy và thị giác máy tính.
* **Nessus:** phần mềm quét lỗ hổng bảo mật có khả năng phát hiện hàng ngàn điểm yếu tiềm ẩn trong hệ thống.
* **Splunk:** nền tảng SIEM mạnh mẽ, cho phép thu thập, phân tích và trực quan hóa log hệ thống một cách hiệu quả.

Việc triển khai ba hệ thống trên nền tảng Ubuntu 24.04 – một hệ điều hành mã nguồn mở phổ biến, ổn định và thân thiện với người dùng – không chỉ giúp làm chủ công nghệ mà còn tăng tính linh hoạt, giảm chi phí triển khai, phù hợp với các mô hình thử nghiệm, học tập và nghiên cứu trong lĩnh vực An toàn Thông tin.

Thông qua đề tài này, người thực hiện có điều kiện tiếp cận các công cụ chuyên sâu, rèn luyện kỹ năng triển khai thực tế và hiểu rõ hơn vai trò quan trọng của mỗi thành phần trong tổng thể một hệ thống CNTT an toàn, hiện đại.

**1.2. Nhiệm vụ của đề tài.**

* Triển khai hệ thống CVAT (Computer Vision Annotation Tool).
* Cài đặt CVAT trên Ubuntu để thực hiện tác vụ gán nhãn dữ liệu hình ảnh.
* Thực hiện một project gán nhãn thực tế và xuất kết quả dưới định dạng COCO.
* Tự động backup dữ liệu gán nhãn định kỳ sang Google Drive và Windows Server thông qua Rclone.
* Triển khai hệ thống quét lỗ hổng với Nessus.
* Cài đặt và cấu hình Nessus trên Ubuntu để kiểm thử an toàn hệ thống.
* Thực hiện quét thử nghiệm, trích xuất báo cáo và lưu log kết quả.
* Thiết lập cơ chế đồng bộ file log của Nessus lên Google Drive và Windows Server định kỳ bằng Rclone.
* Triển khai hệ thống quản lý log tập trung với Splunk.
* Cài đặt Splunk trên Ubuntu để thu thập và phân tích log.
* Kết nối và thu log từ các dịch vụ khác trong hệ thống (ví dụ: CVAT, Nessus).
* Xuất log và thực hiện backup định kỳ lên Google Drive và Windows Server thông qua Rclone.
* Thiết lập hệ thống backup tự động với Rclone.
* Cài đặt và cấu hình Rclone để đồng bộ dữ liệu log và annotation từ Ubuntu lên Google Drive và một máy chủ Windows thông qua mount CIFS.
* Tạo các cronjob tự động hóa quy trình backup theo chu kỳ 10 phút/lần.
* Đảm bảo hệ thống vận hành ổn định và bảo mật.
* Kiểm tra các dịch vụ sau khi triển khai, đảm bảo tính sẵn sàng và bảo mật dữ liệu log.
* Xây dựng mô hình tổng thể có khả năng áp dụng cho các hệ thống giám sát an toàn thông tin thực tế.

**1.3. Cấu trúc của đề tài.**

Đề tài gồm 4 chương chính được trình bày như sau:

* **Chương 1: Tổng quan về đề tài.**

Trình bày lý do chọn đề tài, mục tiêu, nhiệm vụ thực hiện và cấu trúc nội dung báo cáo.

* **Chương 2: Cơ sở lý thuyết.**

Giới thiệu các công cụ, phần mềm và nền tảng được sử dụng, bao gồm CVAT, Nessus, Splunk, Rclone, Cronjob và hệ điều hành Ubuntu. Đồng thời trình bày khái niệm về giám sát hệ thống và kiểm thử bảo mật.

* **Chương 3: Mô hình thực nghiệm.**

Mô tả quá trình triển khai mô hình thực tế trên hệ điều hành Ubuntu 24.04, các bước cài đặt, cấu hình hệ thống và minh chứng hoạt động của các công cụ đã tích hợp.

* **Chương 4: Kết luận.**

Đánh giá kết quả đạt được, những khó khăn trong quá trình thực hiện, đề xuất cải tiến và những bài học kinh nghiệm rút ra.

# **CHƯƠNG 2: CƠ SỞ LÝ THUYẾT**

## **2.1. Giới thiệu về các công cụ được dùng trong đề tài.**

### **2.1.1. Giới thiệu về công cụ Spunk.**

Splunk là một nền tảng phần mềm mạnh mẽ dùng để tìm kiếm, giám sát và phân tích dữ liệu máy (machine data) thông qua giao diện dạng web. Nó có khả năng thu thập, lập chỉ mục và trực quan hóa log từ nhiều nguồn khác nhau như hệ điều hành, phần mềm, thiết bị mạng hoặc hệ thống bảo mật. Splunk được ứng dụng rộng rãi trong giám sát hệ thống, điều tra sự cố, phân tích bảo mật và phát hiện các hành vi bất thường. Giao diện Splunk cho phép tạo các dashboard trực quan, các cảnh báo (alerts) theo thời gian thực và dễ dàng mở rộng theo nhu cầu của doanh nghiệp.

### **2.1.2. Giới thiệu về công cụ Cvat.**

CVAT (Computer Vision Annotation Tool) là một công cụ mã nguồn mở do Intel phát triển nhằm phục vụ các tác vụ ghi nhãn dữ liệu hình ảnh và video trong lĩnh vực thị giác máy tính. CVAT hỗ trợ nhiều định dạng annotation như COCO, Pascal VOC và YOLO, phù hợp với nhiều bài toán khác nhau như nhận diện đối tượng, phát hiện vật thể hay phân đoạn ảnh. Giao diện người dùng của CVAT rất trực quan, hỗ trợ nhiều công cụ vẽ như hình chữ nhật, đa giác, đường thẳng, và có thể phân quyền cho nhiều người làm việc đồng thời. CVAT cũng có thể chạy trên nền tảng Docker, dễ triển khai và tùy biến.

### **2.1.3. Giới thiệu về công cụ Nessus.**

Nessus là một trong những công cụ quét lỗ hổng bảo mật phổ biến và mạnh mẽ nhất hiện nay. Nó cho phép phát hiện các điểm yếu trong hệ thống như lỗi cấu hình, lỗ hổng phần mềm, dịch vụ mở không cần thiết, và các vấn đề liên quan đến bảo mật mạng. Nessus hỗ trợ cập nhật cơ sở dữ liệu liên tục nhằm phát hiện các lỗ hổng mới nhất. Giao diện đồ họa của Nessus giúp người dùng dễ dàng khởi tạo các phiên quét, quản lý báo cáo và đề xuất giải pháp khắc phục chi tiết cho từng lỗ hổng.

### **2.1.4. Giới thiệu về công cụ Rclone.**

Rclone là một công cụ dòng lệnh dùng để đồng bộ và truyền tải dữ liệu giữa các dịch vụ lưu trữ đám mây và máy chủ nội bộ. Nó hỗ trợ nhiều nhà cung cấp dịch vụ như Google Drive, OneDrive, Dropbox, Amazon S3, v.v. Với khả năng tạo lịch trình sao lưu, mã hóa dữ liệu, kiểm tra checksum và hỗ trợ mount ổ đĩa ảo, Rclone trở thành công cụ rất hữu ích trong việc tự động hóa sao lưu dữ liệu. Ngoài ra, Rclone còn được dùng để đồng bộ dữ liệu giữa các hệ thống máy chủ khác nhau một cách bảo mật và hiệu quả.

### **2.1.5. Giới thiệu về công cụ Cronjob.**

Cronjob là một tiện ích lập lịch công việc được sử dụng phổ biến trong các hệ điều hành Unix/Linux. Nó cho phép người dùng thiết lập các tác vụ tự động chạy theo lịch định kỳ, ví dụ như sao lưu dữ liệu, cập nhật hệ thống, gửi email báo cáo hoặc đồng bộ dữ liệu. Cấu hình của cronjob được lưu trong các file crontab, nơi người dùng có thể chỉ định thời gian chạy và lệnh cần thực thi. Cronjob đơn giản nhưng rất mạnh mẽ, đặc biệt phù hợp với các công việc cần lặp đi lặp lại trong quản trị hệ thống.

## **2.2. Giới thiệu về Ubuntu.**

Ubuntu là một hệ điều hành mã nguồn mở dựa trên nhân Linux, được phát triển và bảo trì bởi công ty Canonical. Đây là một trong những bản phân phối Linux phổ biến nhất trên thế giới nhờ tính thân thiện, ổn định và có cộng đồng hỗ trợ rộng lớn. Ubuntu được sử dụng rộng rãi trong môi trường máy chủ, máy trạm, cũng như trong các hệ thống xử lý dữ liệu, nghiên cứu khoa học, và cả trong các dự án phát triển phần mềm.

Một số đặc điểm nổi bật của Ubuntu 24.04:

* **Cập nhật kernel mới:** Hỗ trợ tốt hơn cho phần cứng mới, cải thiện hiệu năng và bảo mật.
* **Tối ưu hóa hệ thống:** Hiệu năng khởi động nhanh, giảm mức tiêu thụ tài nguyên hệ thống.
* **Hỗ trợ Snap và APT:** Cho phép cài đặt phần mềm linh hoạt qua nhiều nguồn khác nhau.

Trong bối cảnh đề tài thực tập triển khai nhiều công cụ bảo mật và giám sát, Ubuntu 24.04 được lựa chọn vì khả năng tương thích cao với các phần mềm như Splunk, Nessus, Rclone và CVAT.

## **2.3. Tổng quan về giám sát và ghi log hệ thống.**

Giám sát và ghi log là hoạt động cơ bản nhưng quan trọng trong quản trị hệ thống và an ninh mạng. Log là dữ liệu ghi lại các hành động, sự kiện xảy ra trên hệ thống hoặc ứng dụng. Việc theo dõi log giúp quản trị viên nắm được tình trạng hoạt động của hệ thống, phát hiện bất thường và xử lý sự cố hiệu quả.

### **2.3.1. Các loại log thường gặp.**

* **System log:** Bao gồm thông tin về kernel, các dịch vụ nền (daemon), quá trình khởi động, tắt máy,...
* **Authentication log:** Ghi lại các hoạt động liên quan đến đăng nhập, xác thực, sai mật khẩu...
* **Application log:** Do các ứng dụng tự tạo ra, ví dụ: log của Splunk, Nessus, CVAT...
* **Security log:** Phản ánh các sự kiện quan trọng liên quan đến bảo mật như lỗi truy cập, tấn công mạng.

### **2.3.2. Mục đích của việc ghi log.**

* Phát hiện và xử lý sự cố kịp thời.
* Theo dõi và đánh giá hiệu suất hệ thống.
* Phục vụ điều tra trong trường hợp có sự cố an ninh.
* Tuân thủ các tiêu chuẩn an toàn thông tin (như ISO 27001).

## **2.4. Khái niệm kiểm thử và đánh giá lỗ hổng bảo mật.**

Trong lĩnh vực an toàn thông tin, việc kiểm thử và đánh giá lỗ hổng là một bước quan trọng giúp phát hiện các điểm yếu có thể bị tin tặc khai thác. Đây là bước đầu tiên trong quy trình phòng thủ chủ động, góp phần đảm bảo hệ thống được vận hành một cách an toàn.

### **2.4.1. Khái niệm kiểm thử lỗ hổng.**

Kiểm thử lỗ hổng (Vulnerability Assessment) là quá trình đánh giá các hệ thống mạng, phần mềm, ứng dụng nhằm xác định những điểm yếu về mặt bảo mật. Quá trình này có thể thực hiện thủ công hoặc sử dụng công cụ tự động.

Các công cụ kiểm thử thường so sánh hệ thống đang hoạt động với cơ sở dữ liệu các lỗ hổng đã biết (CVE) để xác định mức độ rủi ro, từ đó đưa ra khuyến nghị xử lý.

### **2.4.2. Các khái niệm liên quan.**

* **CVE (Common Vulnerabilities and Exposures):** Hệ thống đặt mã số cho các lỗ hổng bảo mật đã được công bố.
* **CVSS (Common Vulnerability Scoring System):** Thang điểm đánh giá mức độ nghiêm trọng của một lỗ hổng.
* **Quét Internal vs. External:** Quét từ bên trong mạng nội bộ (Internal Scan) hay từ bên ngoài (External Scan).

## **2.5. Giới thiệu Rclone và Cronjob – Cơ chế sao lưu và đồng bộ log tự động.**

Trong quản trị hệ thống hiện đại, việc sao lưu log định kỳ và đồng bộ lên các máy chủ lưu trữ hoặc nền tảng đám mây là một yếu tố quan trọng nhằm đảm bảo tính toàn vẹn và sẵn sàng của dữ liệu. Đặc biệt trong lĩnh vực an toàn thông tin, việc lưu trữ log ở nơi an toàn còn giúp hỗ trợ truy vết, kiểm tra và điều tra sự cố hiệu quả. Hai công cụ phổ biến và dễ triển khai cho mục tiêu này là Rclone và Cronjob.

### **2.5.1. Giới thiệu Rclone.**

Rclone là một công cụ dòng lệnh mã nguồn mở mạnh mẽ dùng để quản lý và đồng bộ dữ liệu với hơn 40 dịch vụ lưu trữ đám mây khác nhau như Google Drive, OneDrive, Dropbox, Amazon S3, v.v.

**Các tính năng nổi bật của Rclone:**

* **Hỗ trợ đồng bộ hai chiều hoặc một chiều:** Giúp đồng bộ dữ liệu từ máy chủ lên cloud hoặc ngược lại.
* **Tương thích tốt với Google Drive:** Dễ cấu hình thông qua trình duyệt, không cần viết API thủ công.
* **Tốc độ cao, kiểm tra hash:** Đảm bảo tính toàn vẹn của tệp khi sao chép.
* **Hỗ trợ mount thư mục cloud như ổ đĩa ảo:** Có thể truy cập cloud như ổ đĩa hệ thống thông thường.
* **Tự động hóa bằng script:** Phối hợp dễ dàng với cronjob hoặc systemd timer để sao lưu định kỳ.

**Ứng dụng thực tế:**

Trong đề tài, Rclone được cấu hình để:

* **Đồng bộ log của Splunk, Nessus, và CVAT lên Google Drive.**
* **Tự động sao lưu log sang một thư mục chia sẻ từ Windows Server thông qua giao thức CIFS/SMB.**

### **2.5.2. Giới thiệu Cronjob.**

Cron là một trình lập lịch trên hệ điều hành Linux/Unix dùng để thực hiện các lệnh hoặc script vào thời điểm được xác định sẵn. Các tác vụ định kỳ này được gọi là cronjob.

**Cấu trúc Cronjob tiêu chuẩn:**

|  |
| --- |
| \*/10 \* \* \* \* /path/to/script.sh |

**Trong đó:**

* \*/10 là lặp lại mỗi 10 phút.
* /path/to/script.sh là đường dẫn đến script thực hiện sao lưu hoặc đồng bộ log.

**Ứng dụng trong đề tài:**

* Thiết lập cronjob chạy mỗi 10 phút để đồng bộ log từ Ubuntu sang:
  + **Google Drive** (qua Rclone).
  + **Windows Server** (qua mount thư mục chia sẻ).
* Cronjob cũng có thể ghi lại log quá trình backup để kiểm tra sau này nếu có lỗi xảy ra.

**2.5.3. Lợi ích của việc sao lưu log tự động.**

* **Bảo vệ dữ liệu:** Tránh mất log khi hệ thống gặp sự cố hoặc bị tấn công.
* **Tăng cường truy vết:** Dữ liệu log luôn sẵn có cho việc phân tích hoặc điều tra.
* **Giảm tải công việc thủ công:** Tự động hóa giúp tiết kiệm thời gian và công sức.

# **CHƯƠNG 3: MÔ HÌNH THỰC NGHIỆM**

## **3.1. Giới thiệu dự án.**

Trong thời đại công nghệ số, việc giám sát, kiểm thử và bảo vệ hệ thống thông tin đóng vai trò quan trọng đối với mọi tổ chức. Đặc biệt trong môi trường học thuật và thực hành an toàn thông tin, việc triển khai một mô hình thực nghiệm tích hợp nhiều công cụ là cần thiết để hiểu rõ cách thức vận hành, thu thập log và phát hiện lỗ hổng bảo mật trong hệ thống.

Dự án thực tập này được xây dựng với mục tiêu:

* Triển khai và cấu hình các công cụ giám sát, kiểm thử và phân tích log trên hệ điều hành Ubuntu 24.04.
* Tự động hóa quá trình sao lưu log định kỳ, đảm bảo an toàn dữ liệu log trong quá trình hoạt động.
* Kết nối và đồng bộ dữ liệu giữa máy chủ Ubuntu và hệ thống lưu trữ như Google Drive và Windows Server.

**Các hệ thống và công cụ chính được triển khai bao gồm:**

* **Splunk**: Công cụ thu thập và phân tích log chuyên sâu.
* **Nessus**: Công cụ quét lỗ hổng bảo mật mạnh mẽ.
* **CVAT**: Công cụ hỗ trợ gán nhãn dữ liệu hình ảnh (Annotation tool).
* **Rclone**: Dùng để đồng bộ và sao lưu log lên Google Drive và Windows Server.
* **Cronjob**: Tự động hóa quá trình backup log theo lịch trình định kỳ.

Toàn bộ hệ thống được triển khai tập trung trên một môi trường Ubuntu 24.04, sử dụng CIFS để kết nối đến thư mục chia sẻ trên Windows Server, và cấu hình Rclone để liên kết với Google Drive, từ đó tạo thành một mô hình quản lý log hoàn chỉnh, ổn định và có tính sẵn sàng cao.

## **3.2. Mô hình tổng quan hệ thống.**

Hệ thống thực nghiệm được triển khai trên nền tảng Ubuntu 24.04, đóng vai trò như một máy chủ trung tâm, nơi cài đặt và vận hành toàn bộ các công cụ gồm: Splunk, Nessus, CVAT, Rclone và Cronjob. Bên cạnh đó, hệ thống còn tích hợp với Windows Server (qua giao thức chia sẻ tệp CIFS) và Google Drive để phục vụ cho mục đích sao lưu log từ các dịch vụ theo lịch trình định kỳ.

Mô hình hệ thống bao gồm các thành phần chính như sau:

**1. Ubuntu 24.04 Server**

* Đóng vai trò trung tâm của hệ thống.
* Cài đặt các công cụ chính:
  + **Splunk** để thu thập và phân tích log hệ thống.
  + **Nessus** để quét và đánh giá lỗ hổng bảo mật.
  + **CVAT** để thực hiện gán nhãn dữ liệu hình ảnh phục vụ các bài toán học máy.
  + **Rclone** để đồng bộ log lên Google Drive và chia sẻ sang Windows Server.
  + **Cronjob** để tự động hóa quá trình backup log theo chu kỳ 10 phút một lần.

**2. Google Drive**

* Nơi lưu trữ log online, được kết nối với Ubuntu thông qua Rclone.
* Dữ liệu log được phân chia thành từng thư mục: splunk, nessus, cvat\_logs.

**3. Windows Server 2019**

* Máy chủ nội bộ chia sẻ thư mục qua giao thức CIFS.
* Được mount vào Ubuntu để sao lưu song song log hệ thống vào ổ đĩa dùng chung.

**4. Kết nối mạng**

* Các thành phần đều nằm trong cùng một mạng nội bộ (LAN) hoặc kết nối mạng ảo (nếu dùng môi trường mô phỏng).
* Dữ liệu log được đẩy định kỳ từ Ubuntu đến Google Drive và Windows Server thông qua các tác vụ tự động được lập lịch.

|  |
| --- |
|  |

**Hình 3.1**: Mô hình hệ thống

## **3.3. Các bước cài dặt và cấu hình hệ thống.**

Hệ thống được triển khai tuần tự theo từng công cụ trên môi trường Ubuntu 24.04. Dưới đây là các bước chính:

### **3.3.1. Cài đặt và cấu hình Splunk.**

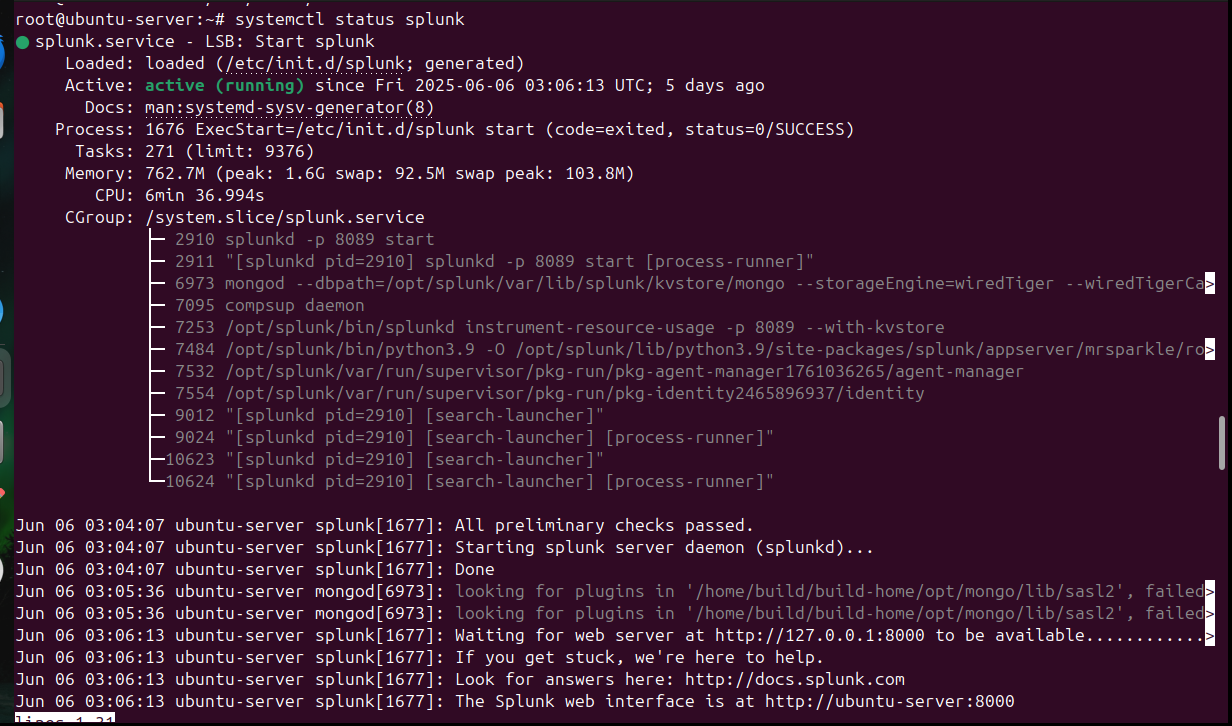
* Tải và cài đặt Splunk phiên bản dành cho Linux.

Khởi động Splunk bằng lệnh sau:

|  |
| --- |
| systemctl start splunk |

Tiếp đó dùng lệnh sau kiểm tra xem trạng thái của Splunk đã khởi động chưa:

|  |
| --- |
| Systemctl status splunk |



**Hình 3.2**: Kiểm tra trạng thái của spunk.

* Tạo tài khoản đăng nhập và truy cập giao diện Splunk qua [**http://127.0.0.1:8000**](http://127.0.0.1:8000)**.**

### **3.3.2. Cài Đặt và cấu hình Cvat.**

* Cập nhật hệ thống và cài Docker, Docker Compose.
* Clone mã nguồn CVAT từ GitHub chính thức.
* Sau đó khởi động CVAT bằng lệnh dưới, lệnh này sẽ chạy các container của CVAT ở chế độ nền:

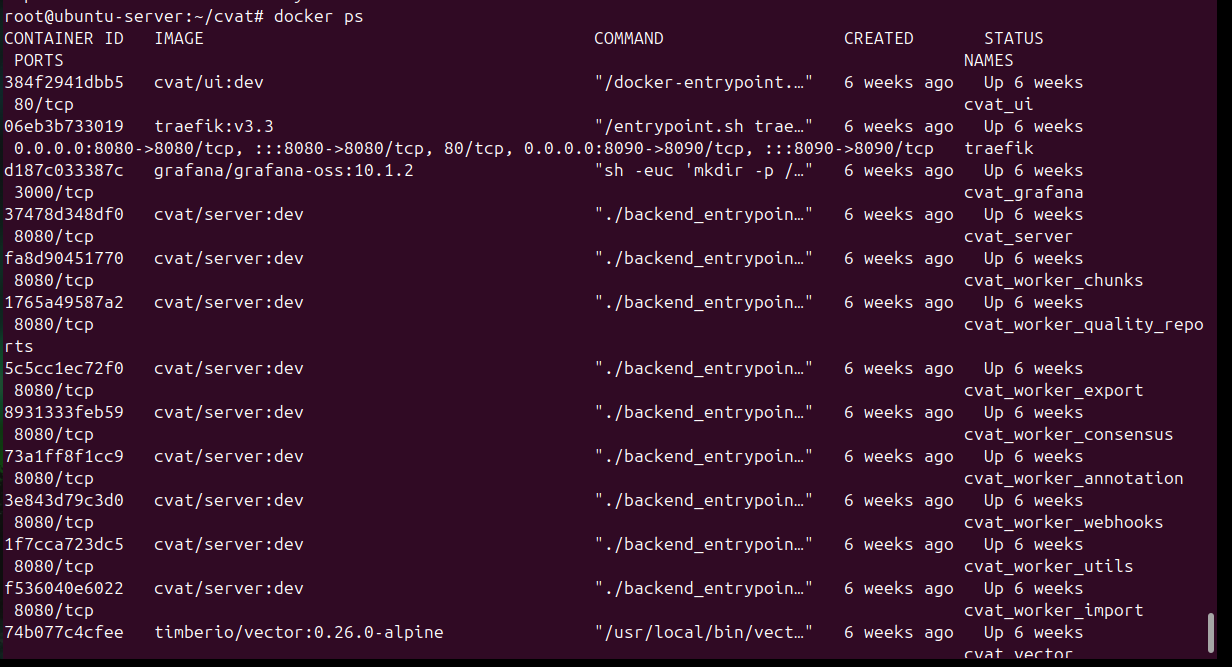
|  |
| --- |
| docker compose up -d |



**Hình 3.3**: Khởi động các container dịch vụ của CVAT bằng Docker.

Tiếp theo dùng lệnh sau để kiểm tra container:

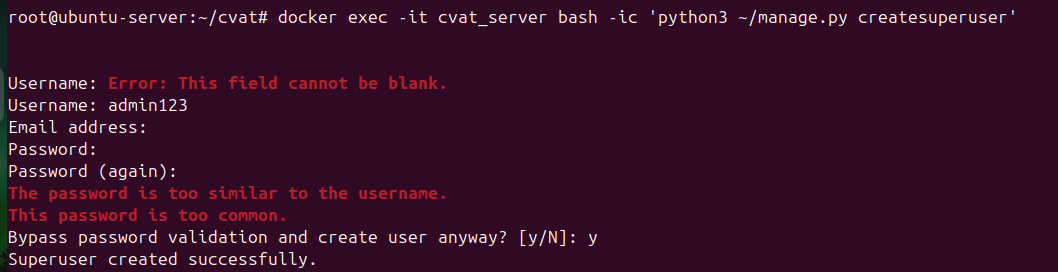
|  |
| --- |
| docker ps |



**Hình 3.4**: kiểm tra container của docker.

* Truy cập giao diện web CVAT qua địa chỉ [**http://192.168.177.189:8080**](http://192.168.177.189:8080)**.**
* Tạo tài khoản người dùng bằng lệnh sau:

|  |
| --- |
| docker execit cvat\_server bash ic ‘python3 ~/manage.py createsuperuser ‘ |

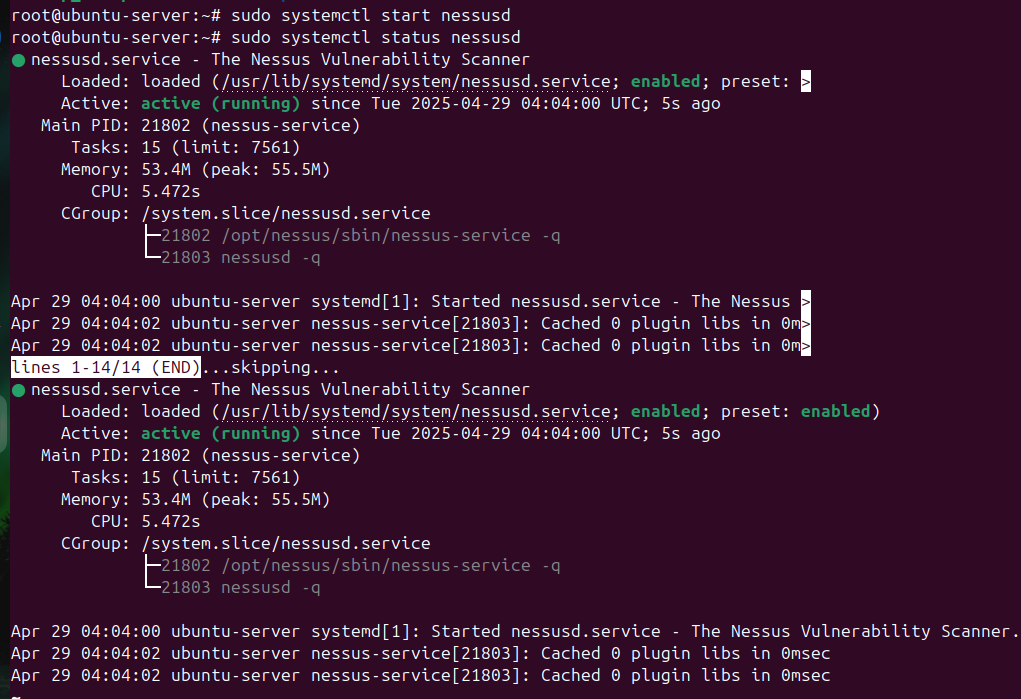


**Hình 3.5**: Tạo tài khoản đăng nhập vào Cvat.

### **3.3.3. Cài đặt và cấu hình Nessus.**

* Tải về gói cài đặt .deb từ trang chính thức Tenable Nessus.
* Cài đặt bằng lệnh:

|  |
| --- |
| sudo dpkg -i Nessus-10.8.4-ubuntu1604\_amd64.deb  sudo systemctl start nessusd  sudo systemctl status nessud |



**Hình 3.6**: Khởi động và kiểm tra trạng thái của Nessus.

* Truy cập trình duyệt tại https://localhost:8834, tạo tài khoản và kích hoạt.

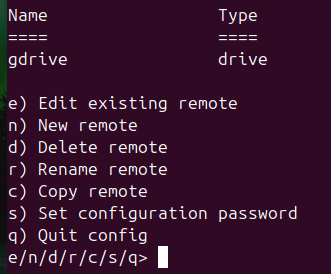
### **3.3.4. Cài đặt Rclone và cấu hình đồng bộ log.**

Cài dặt Rclone bằng lệnh sau:

|  |
| --- |
| Sudo apt install rclone |

Chạy cấu hình bằng lệnh:

|  |
| --- |
| Rclone config |



**Hình 3.7**: Tạo remote kết nối tới google Drive.

## **3.4. Các bước triển khai backup.**

Trong quá trình triển khai mô hình, các log từ các hệ thống như CVAT, Splunk và Nessus được backup định kỳ lên hai điểm lưu trữ khác nhau: Windows Server 2019 (thông qua mount ổ đĩa CIFS) và Google Drive (sử dụng Rclone). Việc này giúp đảm bảo khả năng phục hồi và giám sát log tập trung. Dưới đây là mô tả chi tiết các bước thực hiện.

### **3.4.1. Backup log Cvat lên Google Drive.**

Tạo thư mục backup tạm thời đặt tên là upload\_log.sh.

* File log /var/log/cvat.log được sao chép và đổi tên theo định dạng thời gian để lưu tạm vào /tmp.
* Sau đó Rclone sẽ thực hiện upload log đã được đặt tên sang Google Drive, thư mục cvat\_logs.

|  |
| --- |
| #!/bin/bash  # thoi gian hien tai  now=$(date +"%Y-%m-%d\_%H-%M-%S")  # doi ten file log de tranh ghi de  cp /var/log/cvat.log "/tmp/cvat\_${now}.log"  #upload len ggdrive  rclone copy "/tmp/cvat\_${now}.log" gdrive:cvat\_logs/  #xoa file tam sau khi upload  rm"/tmp/cvat\_${now}.log" |

### **3.4.2. Backup log Splunk lên Google Drive.**

Tạo thư mục backup tạm thời đặt tên là backup\_script.sh.

|  |
| --- |
| #!/bin/bash  #Ngày giờ để đặt tên thư mục  NOW=$(date +"%Y-%m-%d\_%H-%M")  # Tạo thư mục backup tạm  mkdir -p/home/nguyen/backup/splunk\_$NOW  # Dùng rsync đề sao lưu dữ liệu Splunk  Rsync -avz/opt/splunk/var/lib/splunk/ /home/nguyen/backup/splunk\_$NOW/  #Dùng rclone để đẩy thư mục lên Google Drive  rclone copy /home/nguyen/backup/splunk\_$NOW gdrive: splunk  # (Tùy chọn) Xoá thư mục Local sau khi đẩy  rm -rf /home/nguyen/backup/splunk\_$NOW |

* Sử dụng rsync để sao lưu thư mục /opt/splunk/var/lib/splunk vào thư mục tạm này.
* Sau đó Rclone được sử dụng để upload toàn bộ thư mục backup lên Google Drive.
* Tùy chọn có thể xóa thư mục local sau khi hoàn tất upload để tiết kiệm dung lượng máy chủ.

### **3.4.3. Backup log Nessus lên Google Drive.**

Sử dụng Rclone để sao chép tất cả log từ thư mục :

|  |
| --- |
| #!/bin/bash  /usr/bin/rclone copy /opt/nessus/var/nessus/logs/ gdrive cvat\_logs/nessus/ --include "\*.log" --log-file /var/log/rclone\_upload\_nessus.log |

* Sử dụng Rclone để sao chép tất cả log .log từ thư mục /opt/nessus/var/nessus/logs/ lên thư mục cvat\_logs/nessus trên Google Drive.
* Thêm tùy chọn --log-file để ghi log quá trình upload, giúp giám sát và debug nếu cần.

### **3.4.4. Backup log lên Window Server 2019.**

Viết Script để backup qua Window Server 2019:

|  |
| --- |
| #!/bin/bash  # ngay và gio hien tai  Now=$ (date +"%Y-%m-%d\_%H-%M-%S")  # duong den Log nguon  cvat\_log="/tmp/"  splunk\_log="/opt/splunk/var/log"  nessus\_log="/opt/nessus/var/nessus/logs"  # dich den tren o windows mount tai /mnt/winserver  target\_base="/mnt/winserver"  # backup CVAT  if [ -d "$cvat\_log ]; then  tar -czf "$target\_base/cvat\_logs\_$now.tar.gz" -C "$cvat\_log".  fi  #backup Splunk  if [ -d “$splunk\_log ]; then  tar -czf “$target\_base/splunk\_logs\_$now.tar.gz” -C “$splunk\_log”.  fi  #backup Nessus  if [ -d “$nessus\_log ]; then  tar -czf “$target\_base/nessus\_logs\_$now.tar.gz” -C “$nessus\_log”.  fi |

* Script này nhằm backup lấy log của Cvat, Splunk, Nessus.
* Các thư mục log này được nén bằng tar.gz và lưu trữ vào đường dẫn đã mount từ Windows Server: /mnt/winserver/.
* File được đặt tên theo thời gian thực thi để tránh trùng lặp.

## **3.5. Tự động hóa backup log bằng cronjob.**

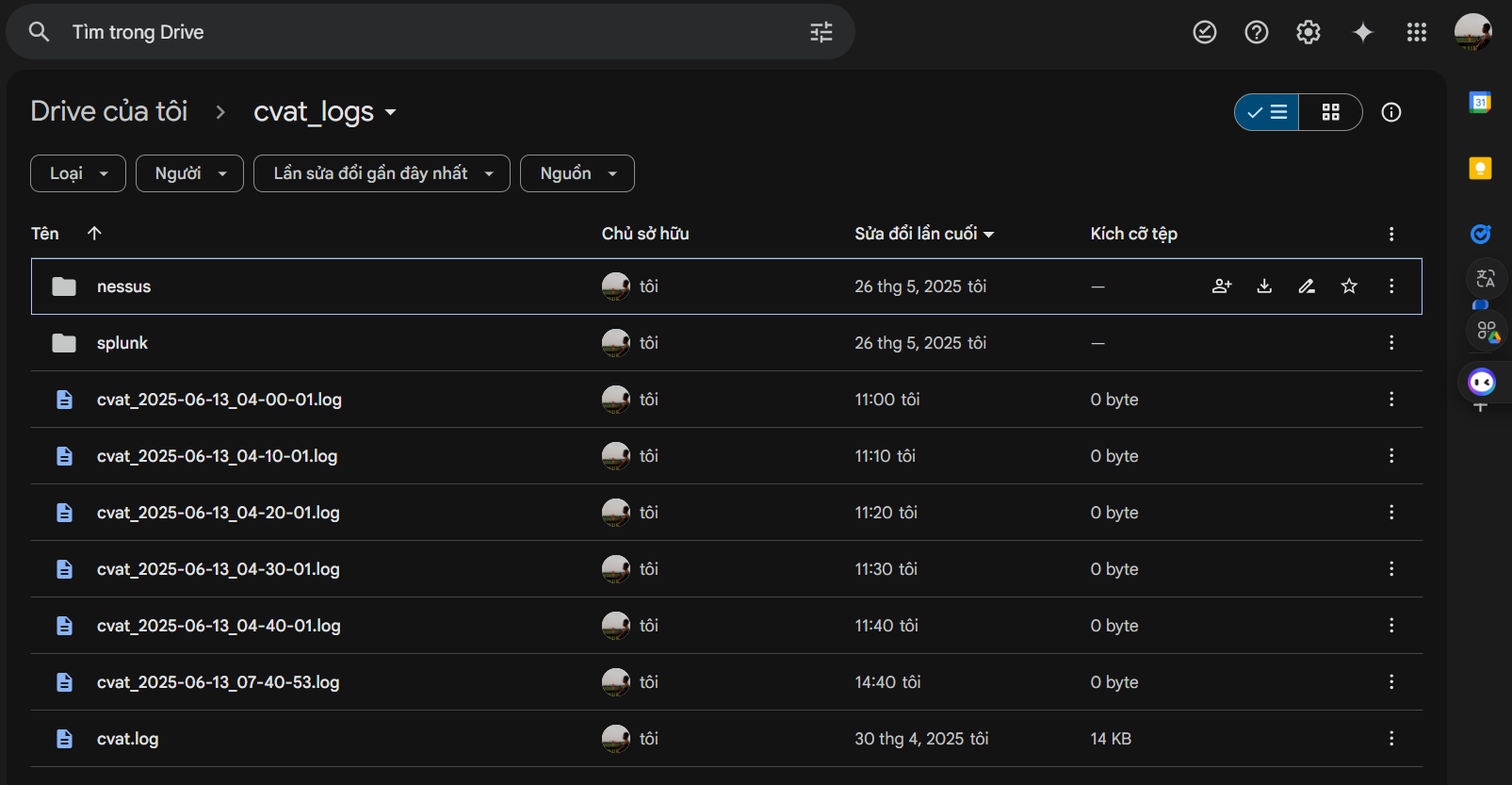
Sau khi viết đầy đủ các Script và cấp quyền cho các Script thì ta sẽ dùng Cronjob để thiết lập tự động hóa backup log.

Thiết lập tự động:

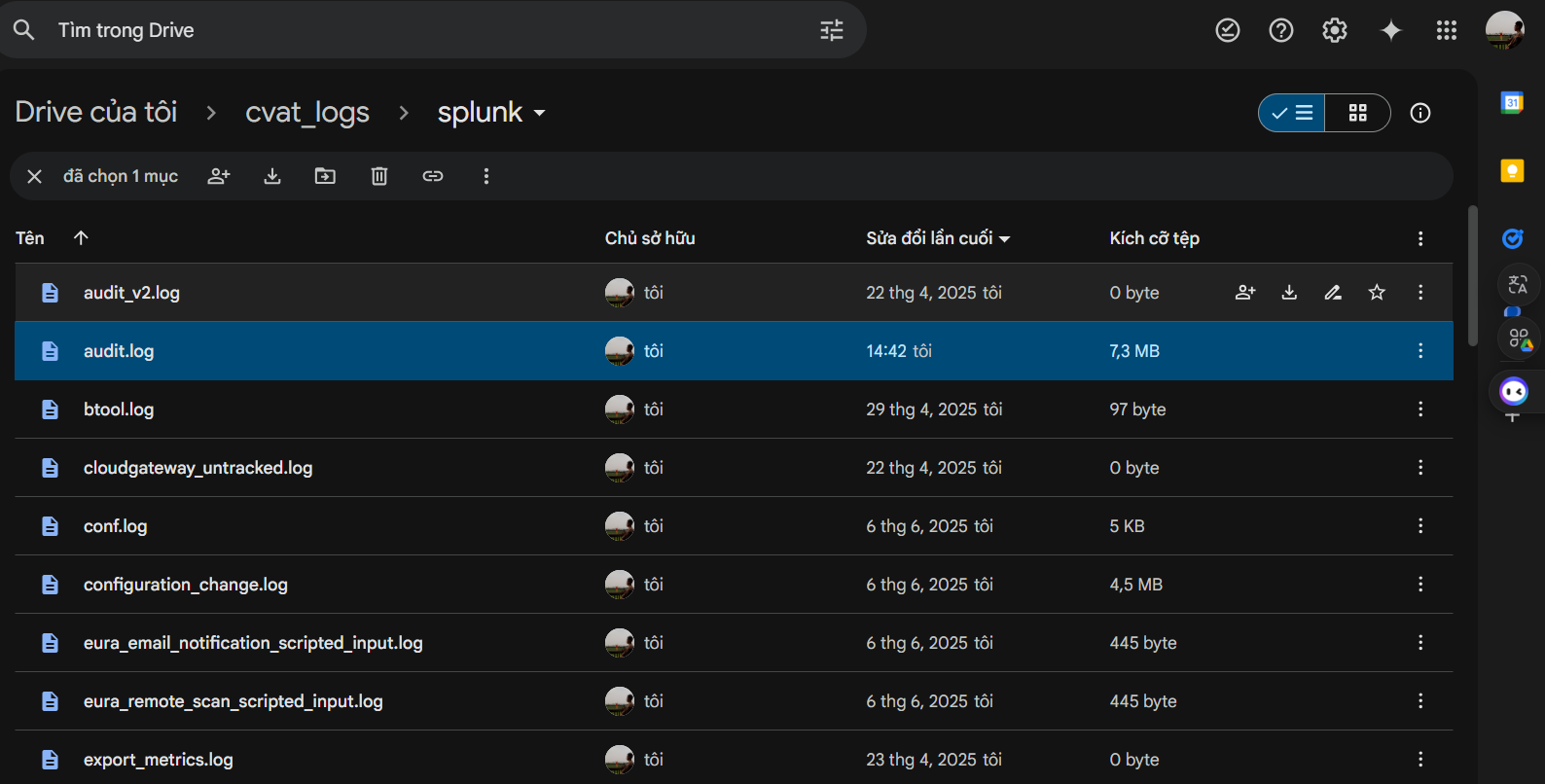
|  |
| --- |
| # log tu dong cvat  \*/10 \* \* \* \* /usr/local/bin/upload\_log.sh  # log tu dong splunk  \*/10 \* \* \* \* /usr/local/bin/backup\_script.sh  # splunk  \*/10 \* \* \* \* /usr/bin/rclone copy /opt/splunk/var/log/splunk/ gdrive:cvat\_logs/splunk/ --include "\*. log" --log-file /var/log/rclone\_upload\_splunk.log  \*/10 \* \* \* \* /usr/bin/rsync -av --include="\*.log" --exclude="\*" /opt/splunk/var/log/splunk//mnt/winserver/cvat\_logs/splunk/>> /var/log/rsync\_to\_winserver\_splunk.log 2>&1  # log tu dong nessus  \*/10 \* \* \* \* /usr/local/bin/backup\_nessus\_logs.sh  # log tu dong window2019  \*/10 \* \* \* \* /usr/local/bin/backup\_logs\_to\_winserver.sh >> /var/log/backup\_winserver.log 2>&1 |

## **3.6. Kết quả đạt được.**

Sau khi dùng Cronjob thiết lập tự động upload qua Google Drive và Window Server 2019 thì ta có kết quả sau :



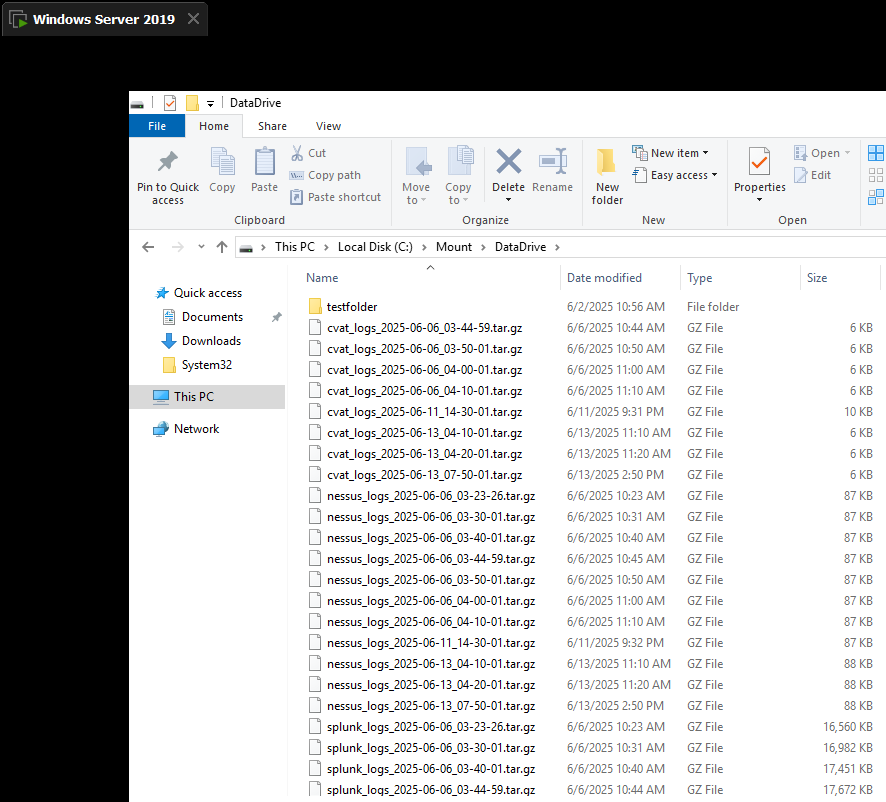
**Hình 3.8**: Log upload thành công Cvat lên Google Drive.



**Hình 3.9**: Log upload thành công Splunk lên Google Drive.



**Hình 3.10**: Log upload thành công Nessus lên Google Drive.



**Hình 3.11**: Log upload thành công các dịch vụ lên Window Server 2019.

# **CHƯƠNG 4: KẾT LUẬN**

## **4.1. Đánh giá kết quả đạt được và những khó khăn gặp phải.**

Sau quá trình thực hiện đề tài “Triển khai hệ thống CVAT, Nessus và quản lý log bằng SIEM (Splunk) trên Ubuntu 24.04”, các mục tiêu chính đã được hoàn thành đầy đủ. Cụ thể:

* Đã triển khai thành công các công cụ CVAT (gán nhãn dữ liệu), Nessus (kiểm thử lỗ hổng), Splunk (SIEM – giám sát log) và Rclone (đồng bộ dữ liệu) trên hệ điều hành Ubuntu 24.04.
* Cấu hình cronjob giúp tự động backup log từ các công cụ nói trên về Windows Server 2019 và đồng bộ lên Google Drive, đảm bảo an toàn và tiện lợi trong lưu trữ.
* Hiểu và thực hành được các quy trình giám sát hệ thống, tổ chức log và đánh giá an ninh mạng cơ bản.
* Xử lý thành công nhiều lỗi phát sinh trong quá trình cài đặt, đặc biệt với Docker, mount CIFS, và tương thích hệ thống.

**Khó khăn gặp phải:**

* Việc cài đặt và cấu hình một số công cụ như Splunk và Nessus đòi hỏi nhiều bước và kiến thức hệ thống, gây khó khăn lúc ban đầu.
* Giao diện quản trị của Splunk và Nessus khá phức tạp, mất thời gian để làm quen.
* Phải thực hiện kiểm tra và sửa lỗi thủ công nhiều lần khi backup qua máy phụ hoặc đồng bộ rclone không thành công do quyền truy cập và sai đường dẫn.

## **4.2. Đề xuất các cải tiến và hướng phát triển tiếp theo.**

* Tự động hóa nâng cao: Có thể phát triển thêm các kịch bản tự động gửi cảnh báo từ Splunk khi phát hiện hành vi bất thường.
* Mở rộng tích hợp: Kết hợp thêm công cụ như Wazuh, ELK Stack hoặc Grafana Loki để mở rộng khả năng phân tích và trực quan hóa dữ liệu log.
* Tăng cường bảo mật: Áp dụng các kỹ thuật mã hóa log, giới hạn quyền truy cập để tăng độ an toàn của hệ thống log.
* Triển khai thực tế: Đưa hệ thống vào môi trường có nhiều máy chủ và nhiều người dùng để đánh giá hiệu suất và khả năng đáp ứng.

## **4.3. Kết luận và những bài học kinh nghiệm rút ra từ dự án.**

Đề tài đã giúp sinh viên tiếp cận thực tế với nhiều công cụ mã nguồn mở và thương mại được sử dụng phổ biến trong quản trị hệ thống và an toàn thông tin. Ngoài kiến thức lý thuyết, sinh viên còn rèn luyện được khả năng:

* Tự học, tra cứu tài liệu tiếng Anh và tài liệu kỹ thuật chính thức.
* Phân tích và xử lý lỗi hệ thống, nâng cao kỹ năng quản trị trên Linux.
* Làm việc có hệ thống và ghi chép quy trình rõ ràng để tái sử dụng hoặc bảo trì sau này.

Thông qua đề tài này, tôi đã rút ra được bài học quý giá về tính kiên trì, cẩn thận, và tầm quan trọng của việc kiểm thử và giám sát liên tục trong hệ thống CNTT.

# **DANH MỤC HÌNH ẢNH**

[**Hình 3.1**: Mô hình hệ thống 15](#_Toc200912368)

[**Hình 3.2**: Kiểm tra trạng thái của spunk. 16](#_Toc200912369)

[**Hình 3.3**: Khởi động các container dịch vụ của CVAT bằng Docker. 17](#_Toc200912370)

[**Hình 3.4**: kiểm tra container của docker. 17](#_Toc200912371)

[**Hình 3.5**: Tạo tài khoản đăng nhập vào Cvat. 18](#_Toc200912372)

[**Hình 3.6**: Khởi động và kiểm tra trạng thái của Nessus. 19](#_Toc200912373)

[**Hình 3.7**: Tạo remote kết nối tới google Drive. 20](#_Toc200912374)

[**Hình 3.8**: Log upload thành công Cvat lên Google Drive. 25](#_Toc200912375)

[**Hình 3.9**: Log upload thành công Splunk lên Google Drive. 25](#_Toc200912376)

[**Hình 3.10**: Log upload thành công Nessus lên Google Drive. 26](#_Toc200912377)

[**Hình 3.11**: Log upload thành công các dịch vụ lên Window Server 2019. 26](#_Toc200912378)

# **TÀI LIỆU THAM KHẢO**

[1] Splunk Inc. (nd). *Dowload Splunk*. Retrieved from Splunk: https://www.splunk.com/en\_us/download.html

[2] Canonical Ltd. (nd). *Ubuntu Desktop*. Retrieved from Ubuntu: https://ubuntu.com/download/desktop

[3] OpenCV. (nd). *Computer Vision Annotation Tool*. Retrieved from Cvat: https://opencv.github.io/cvat/

[4] CVAT.ai. . (nd). *Dowload Cvat*. Retrieved from Cvat: https://docs.cvat.ai/docs/administration/basics/installation/

[6] Splunk Inc. (nd). *Search Tutorial*. Retrieved from Welcome to the Search Tutorial: https://docs.splunk.com/Documentation/Splunk/latest/SearchTutorial/WelcometotheSearchTutorial

[7] Rclone.org. (nd). *Rclone Documentation*. Retrieved from Rclone: https://rclone.org/docs/

[8] S., K. (2022, April 5). *20 Useful Crontab Examples in Linux*. Retrieved from Tecmint: https://www.tecmint.com/crontab-in-linux-with-20-examples-of-cron-schedule/

[9] GeeksforGeeks. (nd). *How to Use Cron in Linux?* Retrieved from Crontab: https://www.geeksforgeeks.org/how-to-use-cron-in-linux/