# 

**BỘ THÔNG TIN VÀ TRUYỀN THÔNG**

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

------o0o------

**BÁO CÁO NHIỆM VỤ CẤP HỌC VIỆN**

**Mã số: 02-BTHS-ATTT-2024**

**Môn học:** An toàn mạng nâng cao

**Bài thực hành**: Giám sát và phân tích log bằng Splunk

**Hà Nội - 2025**

# 1. Nội dung và hướng dẫn bài thực hành

## 1.1. Mục đích

Giúp sinh viên hiểu biết về công cụ Splunk - là một phần mềm chủ yếu được sử dụng để tìm kiếm, giám sát và kiểm tra dữ liệu do máy tạo ra thông qua giao diện web từ đó phân tích để đưa ra báo cáo cũng như cảnh báo với thời gian thực.

Đồng thời giúp sinh viên biết cách cài đặt và cấu hình Splunk, sử dụng công cụ Splunk để thu thập log và phân tích, giám sát hệ thống của mình.

## 1.2. Yêu cầu đối với sinh viên

* Có kiến thức cơ bản về hệ điều hành Linux, mô hình mạng khách/chủ.
* Có kiến thức về các loại log trong hệ điều hành, web.

## 1.3. Nội dung bài thực hành

* **Khởi động bài lab:** 
  + Vào terminal, gõ:

*labtainer -r ptit-splunk-n13*

*(chú ý: sinh viên sử dụng email stu.ptit.edu.vn của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)*

Sau khi khởi độg xong 3 terminal ảo sẽ xuất hiện, một cái đại diện cho máy splunk, máy client và máy server. Biết rằng 3 máy nằm cùng mạng LAN.

* Trên terminal **client** sử dụng lệnh sau để truy cập vào web Splunk:

*firefox http://172.10.0.10:8000*

* Trên terminal **server** sẽ thực hiện các thao tác để Splunk thu thập log.
* **Kết thúc bài lab:**
  + Trên terminal đầu tiên sử dụng câu lệnh sau:

*stoplab ptit-splunk-n13*

* + Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo vào một vị trí được hiển thị bên dưới stoplab.
* **Khởi động lại bài lab:**
  + Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

*startlab -r ptit-splunk-n13*

# 2. Phân tích, thiết kế bài thực hành

## 2.1. Phân tích yêu cầu bài thực hành

Bài thực hành cần có 3 máy tính nằm trong mạng LAN. Trong đó một máy làm máy splunk, một máy làm máy chủ để tạo ra log và chuyển tới máy splunk, một máy làm máy khách để truy cập vào web splunk. Để hoàn thành bài thực hành, sinh viên cần sử dụng máy khách để truy cập vào web splunk sau đó tìm kiếm các log, tạo reports, dashboard, và xây dựng alert.

Để đáp ứng yêu cầu bài thực hành, cân cung cấp máy ảo chứa docker trong đó có 3 container, mỗi container là một máy tính ảo chạy hệ điều hành Linux. Để thực hiện được việc thu thập, lưu trữ hoặc phân tích log,...thì hệ thống cần cung cấp khả năng thiết lập mạng LAN giữa các máy, đồng thời cung cấp các thư viện cần có cho các máy container.

Hệ thống cần phải ghi lại được các thao tác sử dụng phần mềm splunk của sinh viên thông qua các câu lệnh để tạo ra được kết quả đánh giá. Hệ thống yêu cầu sinh viên nhập email gắn liền với danh tính của sinh viên, và ghi lại các thao tác …

Để bắt đầu bài thực hành, sinh viên cần phải sử dụng các câu lệnh khởi tạo (startlab <tên bài lab>) và câu lệnh kết thúc (stoplab <tên bài lab>) để hệ thống chạy bài lab cũng như lưu lại kết quả

## 2.2. Thiết kế bài thực hành

Trên môi trường máy ảo Ubuntu được cung cấp, sử dụng docker tạo ra 3 container: 1 container mang tên “splunk\_anm” chứa Splunk, tiếp theo là 1 container mang tên “logserver” đóng vai trò là tạo log và gửi chúng đến “splunk\_anm” qua giao thức như syslog, bash\_history, kernel,... Cuối cùng là 1 container mang tên “clientntk” đóng vai trò là máy khách – người truy cập vào giao diện web của Splunk để xem và truy vấn dữ liệu log đã được ghi vào “splunk\_anm” từ “logserver”.

**A diagram of a square with black text

Description automatically generated**

Hình 14. Sơ đồ thiết kế bài thực hành

* ***Cài đặt docker và môi trường máy ảo:***
  + Tạo mạng LAN có cấu hình: 172.10.0.0/24 và gateway: 172.10.0.1
* ***Cấu hình docker gồm có:***
  + Client: lưu cấu hình cho máy khách “clientntk”, trong đó gồm có:
    - Tên máy khách: clientntk
    - Địa chỉ trong mạng LAN: 172.10.0.30
    - Gateway: 172.10.0.1
  + Server: lưu cấu hình cho máy tạo log “logserver, trong đó gồm có:
    - Tên máy: logserver
    - Địa chỉ trong mạng LAN: 172.10.0.20
    - Gateway: 172.10.0.1
  + Splunk: lưu cấu hình cho máy “splunkanm”:
    - Tên máy: splunk
    - Địa chỉ trong mạng LAN: 172.10.0.10
    - Gateway: 172.10.0.1
* ***Config: lưu cấu hình hoạt động của hệ thống***
  + - Cài đặt và cấu hình Splunk trong container Splunk:
* Tải và cài đặt Splunk Index
* Cấu hình Splunk để lắng nghe trên cổng cụ thể (ví dụ: cổng 9997) để nhận log từ container "logserver".
* Đảm bảo rằng Splunk được cấu hình để lưu trữ dữ liệu log.
* Cấu hình máy tạo log (container "logserver"):
* Tải và cài đặt Splunk Forwarder để chuyển tiếp log đến splunk
* Cài đặt các thư viện và ứng dụng cần thiết để tạo và gửi log
* Cấu hình máy tạo log để gửi log đến Splunk container qua giao thức đã mô tả.
* Truy cập và xem dữ liệu log từ container "clientntk":
* Truy cập giao diện web của Splunk từ container "clientntk" thông qua trình duyệt web.
* Tìm kiếm, xem, và tạo các truy vấn trên dữ liệu log đã được ghi vào Splunk từ container "logserver".
  + - Các nhiệm vụ cần phải thực hiện để thực hành thành công:

***Nhiệm vụ 1: Cài đặt và cấu hình máy chủ log và máy chủ Splunk***

* Sinh viên cần cấu hình Splunk trên máy splunkanm và cấu hình Splunk Forwarder trên máy logserver để hai bên giao tiếp được log với nhau.

***Nhiệm vụ 2: Tìm được địa chỉ IP của các máy và cổng đang mở:***

* Sinh viên cần thực hiện nmap để tìm ra địa chỉ IP của máy Splunk và cổng web đang mở.
* Đồng thời sử dụng lệnh ping để kiểm tra kết nối tới máy chủ web Splunk
* Khi đầy đủ thông tin trên sinh viên có thể truy cập vào web Splunk và thu được log của máy logserver

***Nhiệm vụ 3: Tạo index và kiểm tra xem log của logserver đã được chuyển tới máy chủ web Splunk hay chưa:***

* Sinh viên cần thực hiện một truy vấn trong giao diện Splunk để kiểm tra xem có log của logserver chưa.
* Cụ thể: sinh viên sẽ thu thập toàn bộ log của máy logserver trong thời gian đã cho trước

*Câu truy vấn: index = “logserver”*

***Nhiệm vụ 4: Tạo truy vấn và bắt sự kiện log xảy ra trên máy logserver:***

* Sinh viên cần thực hiện một truy vấn trong giao diện Splunk để tìm kiếm log của logserver.

***Nhiệm vụ 5: Tạo report từ dữ liệu log thu được:***

* Sinh viên cần tạo một báo cáo hoặc biểu đồ từ dữ liệu log bằng các tính năng của Splunk.
* Xác định xem báo cáo hoặc biểu đồ có được tạo ra một cách chính xác và thể hiện thông tin log một cách hợp lý hay không.

***Nhiệm vụ 6: Tạo dashboard từ dữ liệu log để trực quan hoá dữ liệu:***

* Sinh viên cần tạo một báo cáo hoặc biểu đồ từ dữ liệu log bằng các tính năng của Splunk.
* Xác định xem báo cáo hoặc biểu đồ có được tạo ra một cách chính xác và thể hiện thông tin log một cách hợp lý hay không.

***Nhiệm vụ 7: Tạo alert cảnh báo về sự kiện đăng nhập quá số lần cho phép:***

* Sinh viên cần tạo thành công một cảnh báo về sự kiện sử user trên logserver đăng nhập tài khoản quá số lần cho phép
* Sau đó alert này sẽ được gửi cảnh báo qua thông báo hoặc qua log event
* Thiết lập hệ thống mạng sao cho 3 máy cùng một mạng LAN.
* Các thư viện cần cho 3 máy để sử dụng các dịch vụ cần thiết.
* Để đánh giá được sinh viên đã hoàn thành bài thực hành hay chưa, cần chia bài thực hành thành các nhiệm vụ nhỏ, mỗi nhiệm vụ cần phải chỉ rõ kết quả để có thể dựa vào đó đánh giá và chấm điểm. Do vậy trong bài thực hành này hệ thống cần ghi nhận các thao tác, sự kiện được mô tả và cấu hình như bảng sau:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Result Tag** | **Container** | **File** | **Field Type** | **Field ID** | **Timestam p Type** |
| \_splunk | splunkanm | splunk.stdout | CONTAINS | http://splunkanm:8000 | File |
| \_splunkforwader | logserver | splunk.stdout | CONTAINS | 172.10.0.10:9997 | File |
| \_nmapip | clientntk | nmap.stdout | CONTAINS | 172.10.0.10 | File |
| \_ping | clientntk | ping.stdout | CONTAINS | 172.10.0.10:icmp\_seq=1 | File |
| \_nmapport | clientntk | nmap.stdout | CONTAINS | 8000 | File |
| logall | clientntk | head.stdout | CONTAINS | 172.10.0.20 | File |
| useradd | clientntk | head.stdout | CONTAINS | new user | File |
| report | clientntk | head.stdout | CONTAINS | failure | File |
| dashboard | clientntk | head.stdout | CONTAINS | date\_hour, count | File |
| logalert | clientntk | head.stdout | CONTAINS | Login attempts exceeds | File |

Bảng 1.1. Cấu hình cho kiểm tra kết quả

* Sau khi nhận được file đóng gói từ sinh viên, giảng viên sử dụng chức năng chấm điểm để xem kết quả được thiết kế dạng bảng trong đó ghi rõ email của sinh viên thực hiện, từng tiêu chí chấm điểm được ghi nhận ( nếu có chữ “Y” là đã hoàn thành, nếu không có là chưa hoàn thành) và kết luận là sinh viên đã hoàn thành bài thực hành đó hay chưa. Kiểm tra bài thực hành đúng do sinh viên làm bằng cách kiểm tra email (xem bảng 1.2).

|  |  |
| --- | --- |
| **Student** | **tcpdump\_ping** |
| Email của sinh viên | Y (Y là đã hoàn thành) |

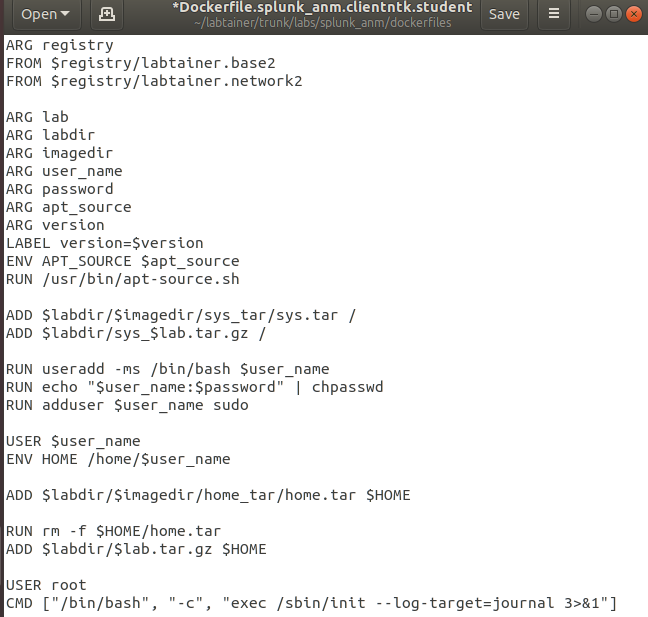
Bảng 1.2. Kết quả chấm điểm

|  |  |  |  |
| --- | --- | --- | --- |
| ***Goal ID*** | ***Goal Type*** | ***Goal 1*** | ***Goal 2*** |
| \_testone | time\_not\_during | \_nmapip | \_ping |
| \_testtwo | time\_not\_during | \_ping.stdout | \_nmapport |
| \_testthree | time\_not\_during | \_nmapip | \_nmapport |
| \_splunkweb | time\_not\_during | \_splunk | \_splunkforwader |
| \_splunkforwaders | time\_not\_during | \_splunkforwader | \_splunk |
| testconnect | boolean | (\_testone and \_testtwo and \_testthree) | |
| splunk | boolean | (\_splunkweb and \_splunkforwaders) | |

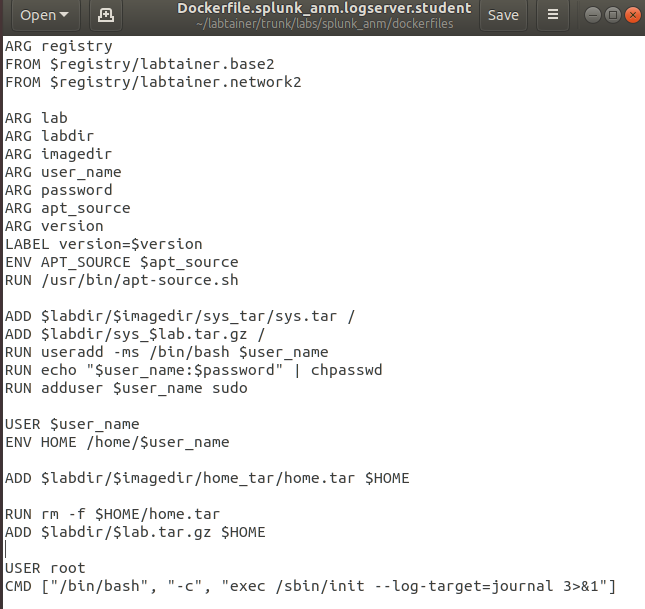
Bảng 1.3. Cấu hình Goals

# 3. Cài đặt và cấu hình máy ảo

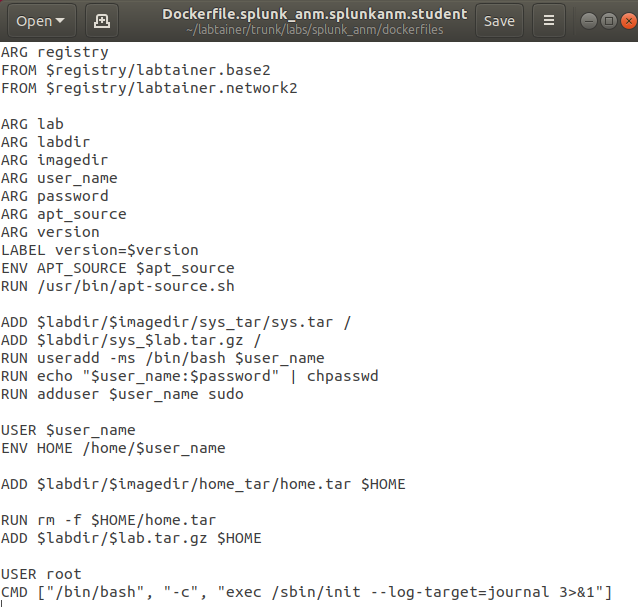
Cấu hình file máy ảo:



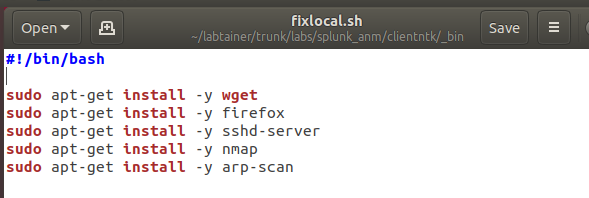
Hình 15. Cấu hình máy ảo clientntk

**

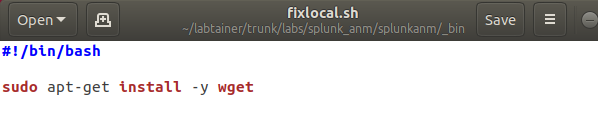
Hình 16. Cấu hình máy ảo logserver



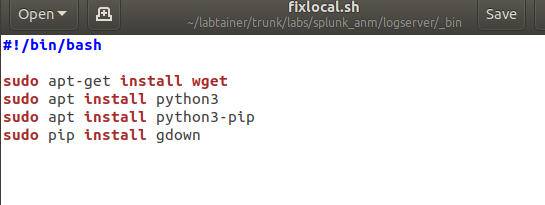
Hình 17. Cấu hình máy ảo splunkanm



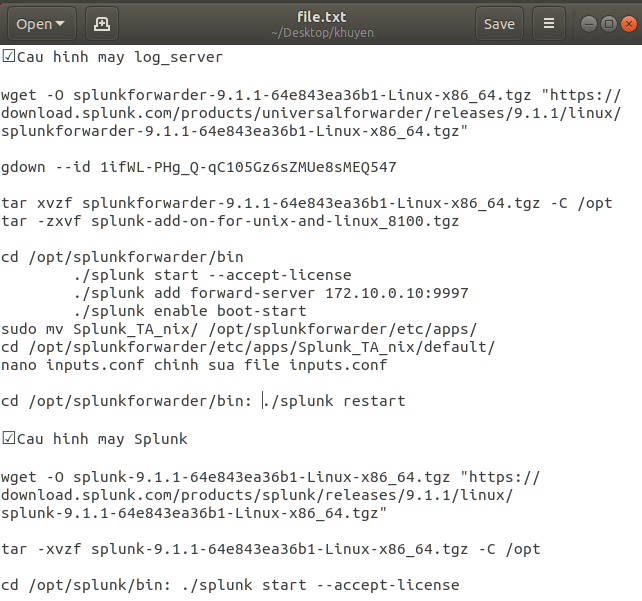
Hình 18. Cấu hình file fixlocal.sh máy ảo clientntk



Hình 19. Cấu hình file fixlocal.sh máy ảo splunkanm



Hình 20. Cấu hình fixlocal.sh máy ảo logserver

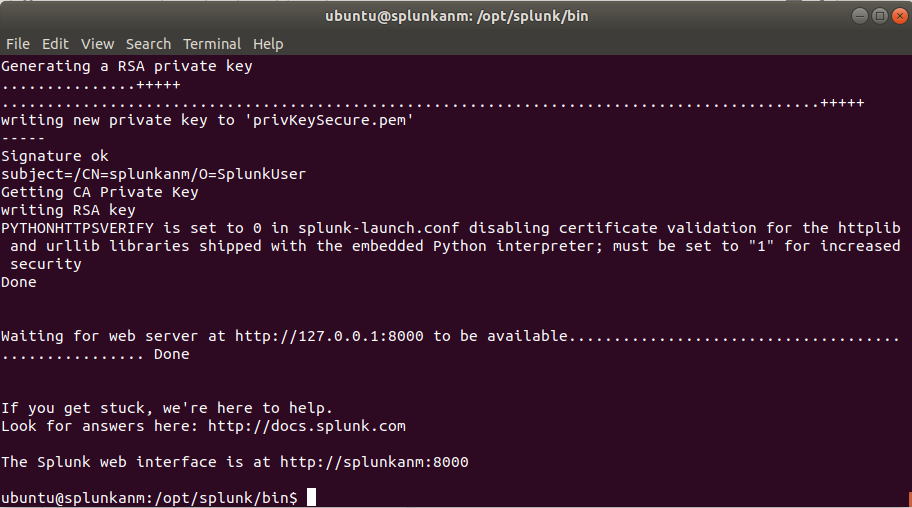


Hình 21. Hướng dẫn cụ thể cài và cấu hình web Splunk và logserver

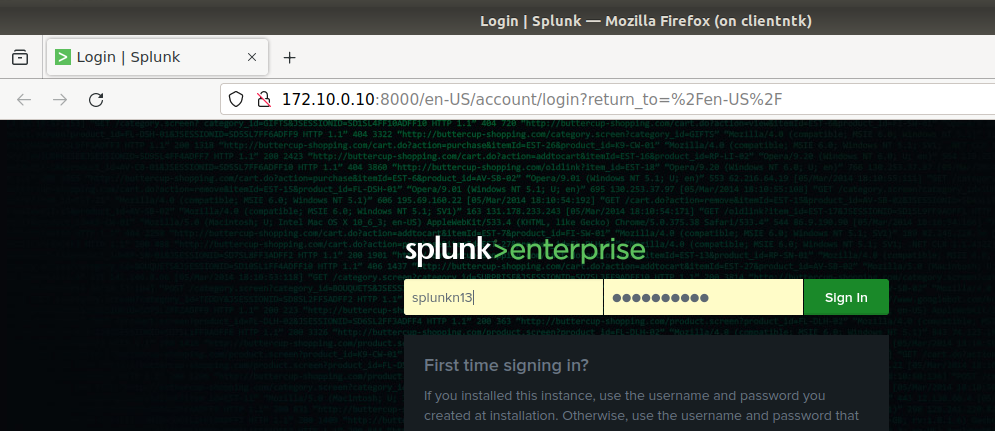
# 4. Thử nghiệm và đánh giá

Chúng tôi đã xây dựng thành công bài thực hành, dưới đây là các hình ảnh minh họa về bài thực hành:

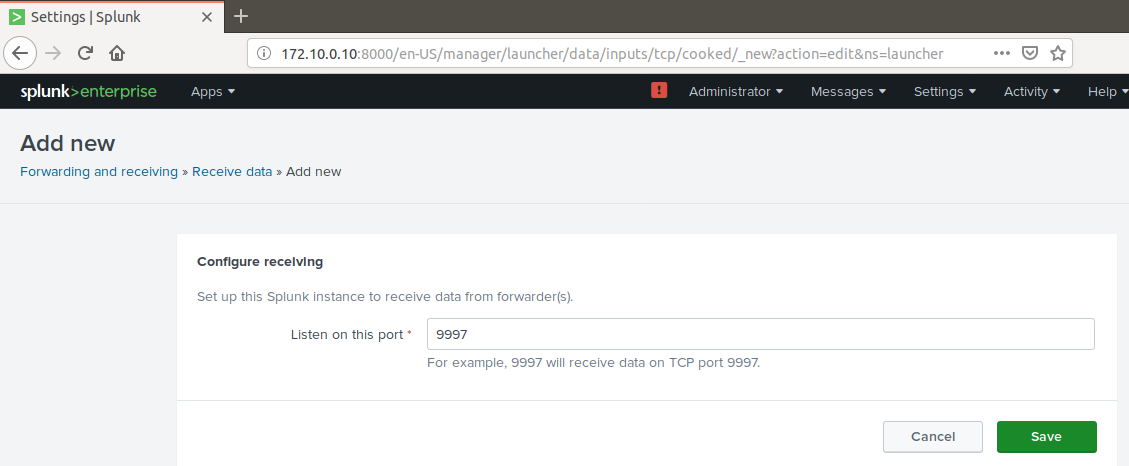
**Task 1: Cài đặt và cấu hình máy chủ log và máy chủ Splunk**



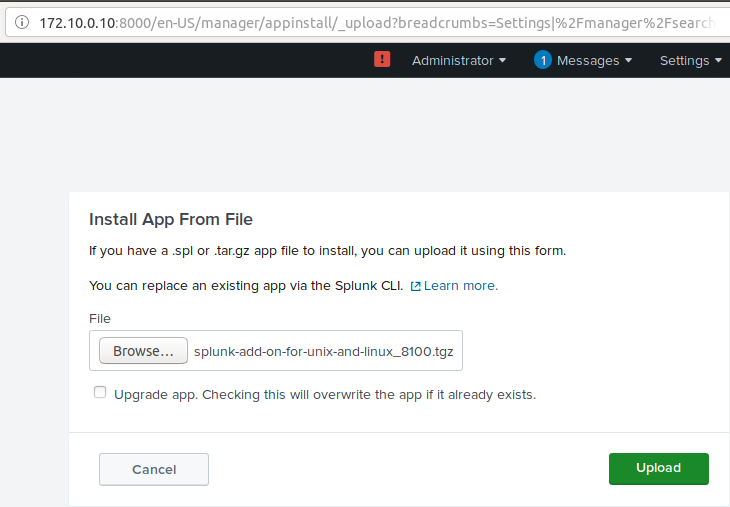
Hình 22. Cài đặt thành công máy chủ web Splunk trên máy splunk\_anm



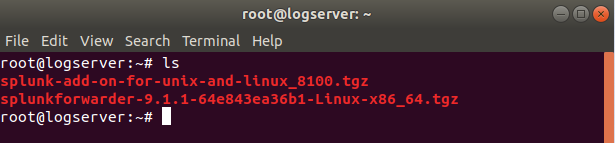
Hình 23. Truy cập vào web Splunk



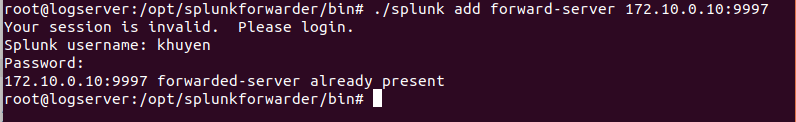
Hình 24. Cấu hình cổng lắng nghe để thu thập log của máy logserver



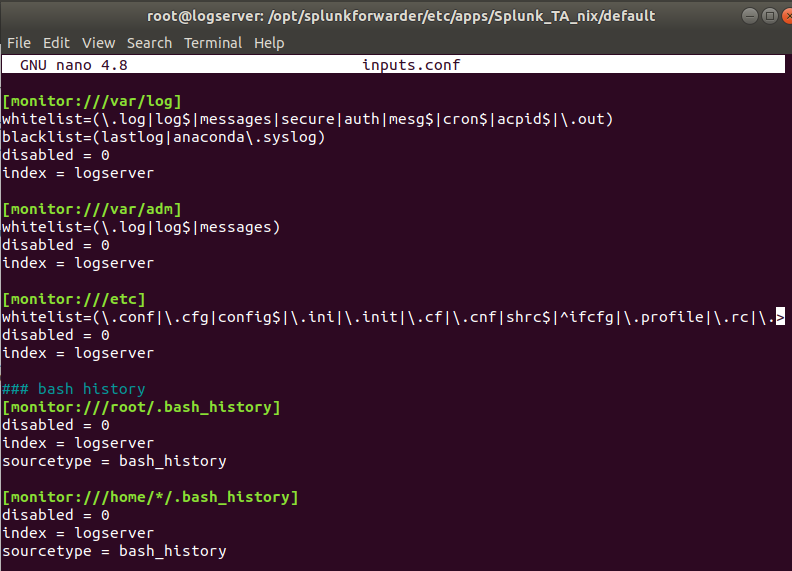
Hình 25. Install tiện ích Splunk Forwarder trên web Splunk



Hình 26. Trên máy logserver cài tiện ích Splunk Forwarder và Add\_on\_for\_unix

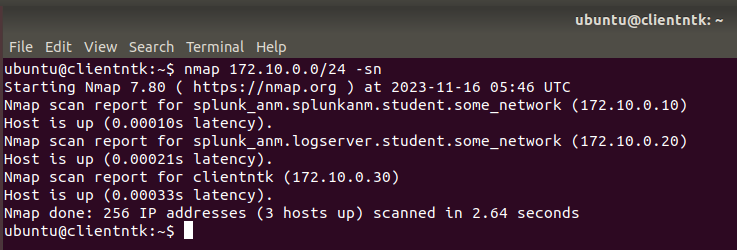


Hình 27. Cấu hình Splunk forwarder để gửi log về máy chủ splunk qua port 9997

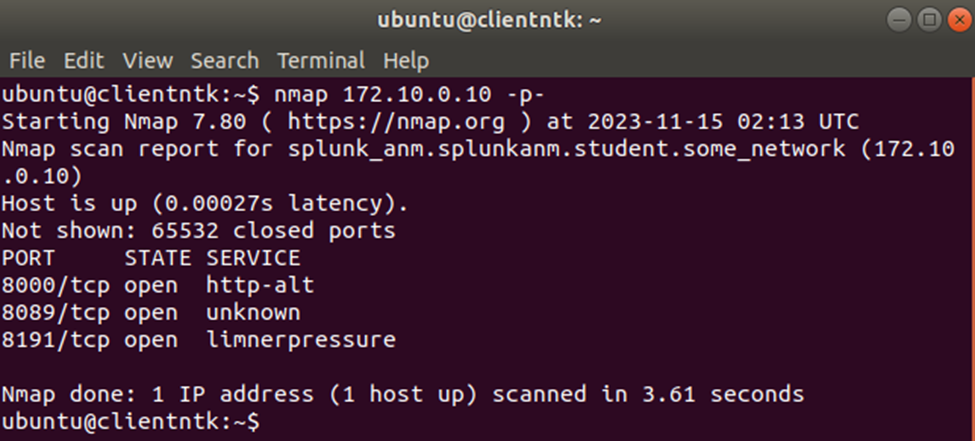


Hình 28. Thiết lập các path log cho máy logserver

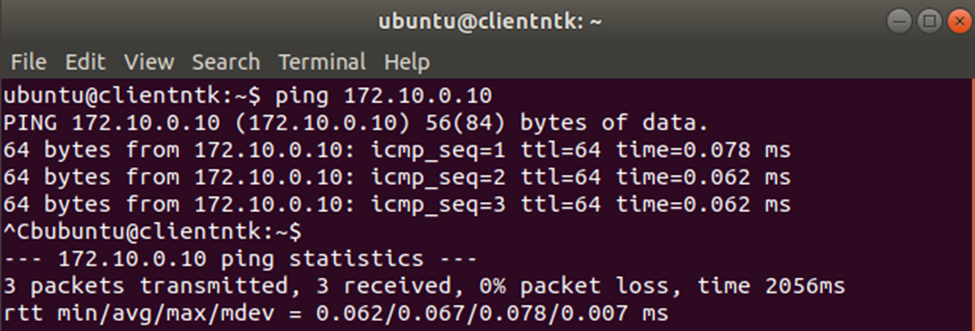
**Task 2: Tìm được địa chỉ IP của các máy và cổng đang mở**



Hình 29. Sử dụng nmap tìm địa chỉ IP các máy liên quan

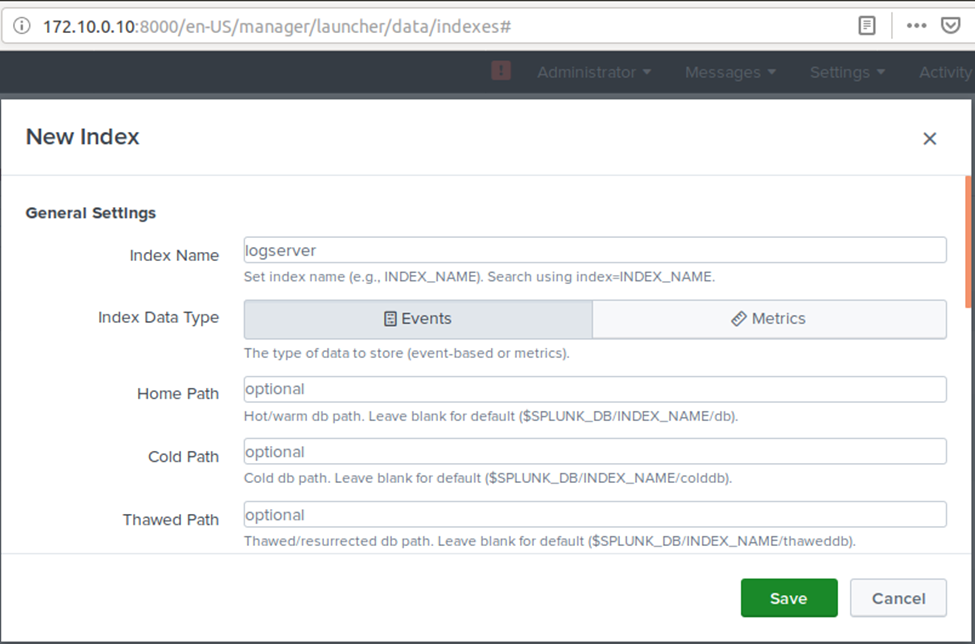


Hình 30. Sử dụng nmap để tìm ra cổng đang mở của máy chủ web Splunk

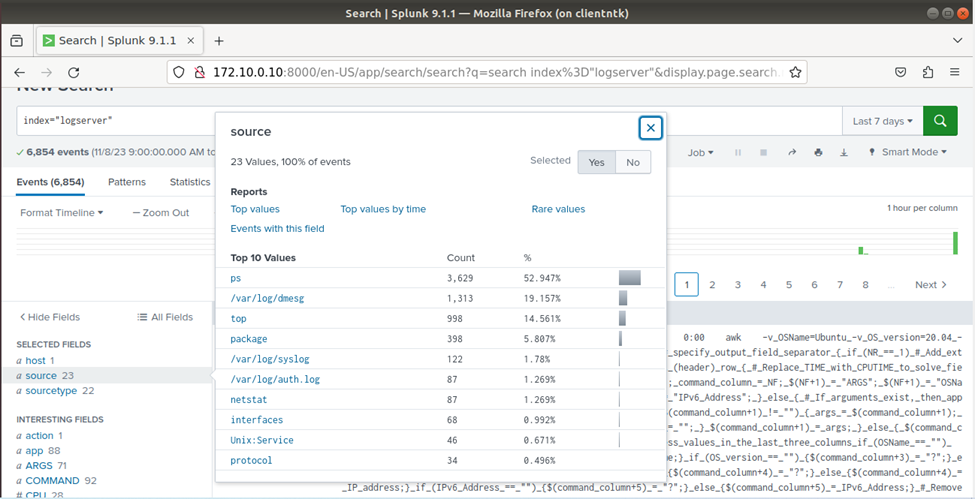


Hình 31. Sử dụng ping để kiểm tra kết nối từ clientntk tới splunk\_anm

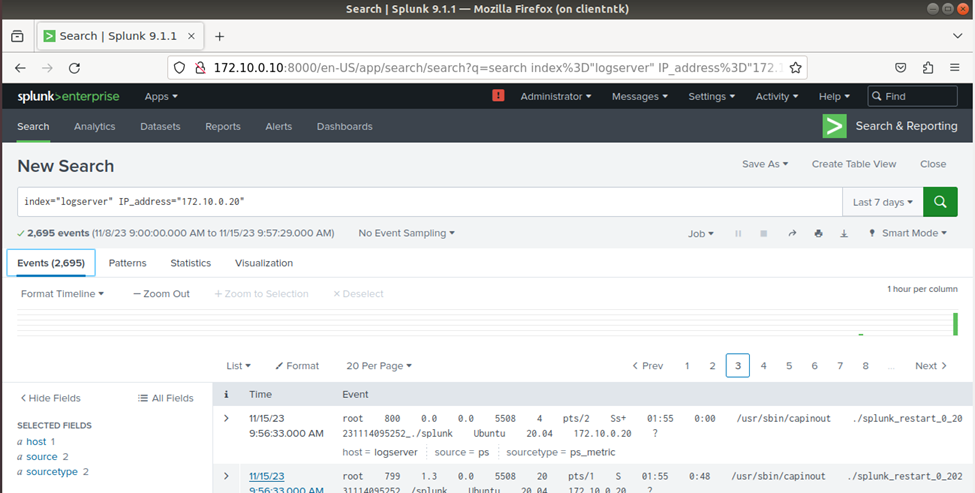
**Task 3: Tạo index và kiểm tra xem log của logserver đã được chuyển tới máy chủ web Splunk hay chưa:**



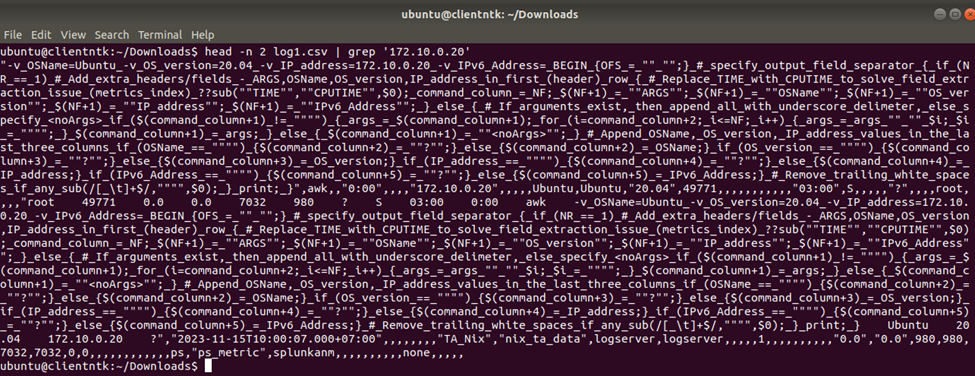
Hình 32. Tạo index để logserver sẽ đổ log về index này



Hình 33. Truy cập vào web Splunk để kiểm tra xem đã thu được log của logserver

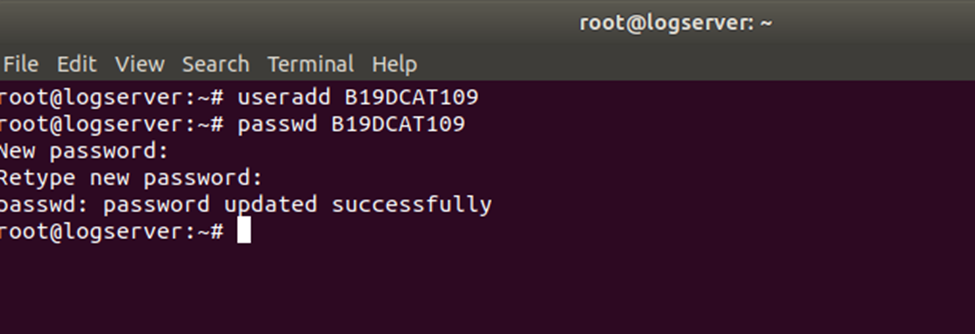


Hình 34. Sinh viên xuất file kết quả thu được dưới dạng csv

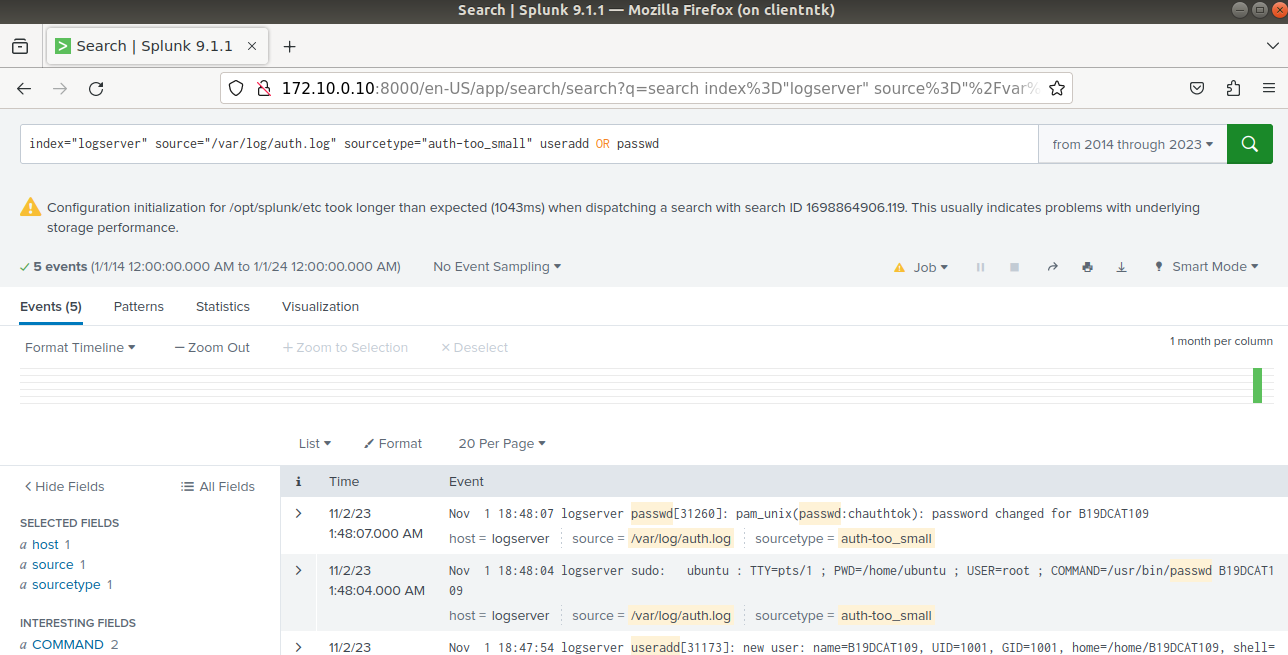


Hình 35. Sử dụng lệnh head để đọc log1.csv

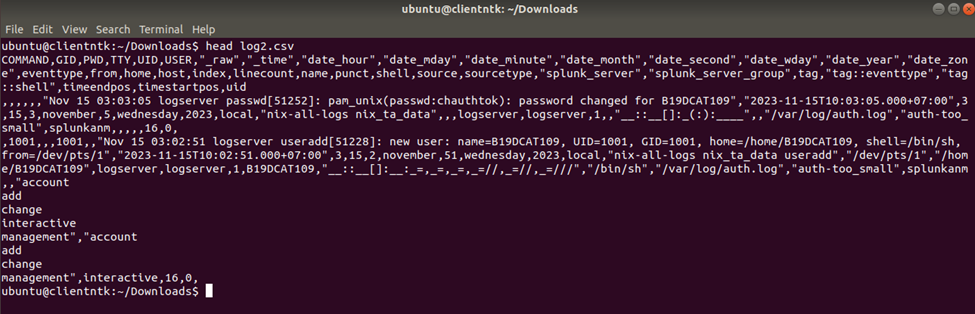
**Task 4: Truy vấn tìm kiếm dữ liệu log**



Hình 36. Trên máy logserver thực hiện hành động tạo user, passwd cho tài khoản

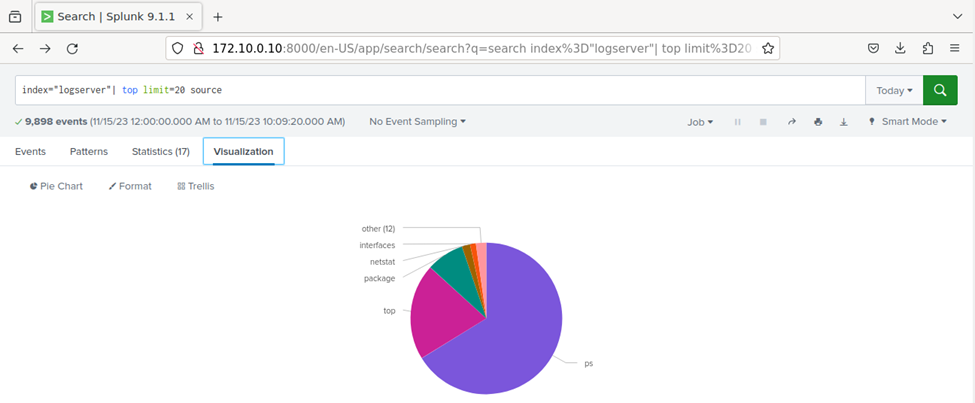


Hình 37. Trên web Splunk thực hiện câu truy vấn tìm kiếm sự kiện trên logserver

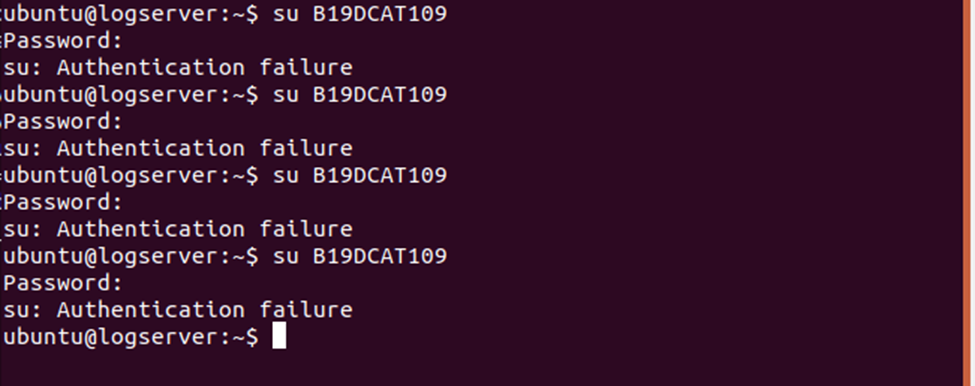


Hình 38. Sử dụng lệnh head để đọc log2.csv

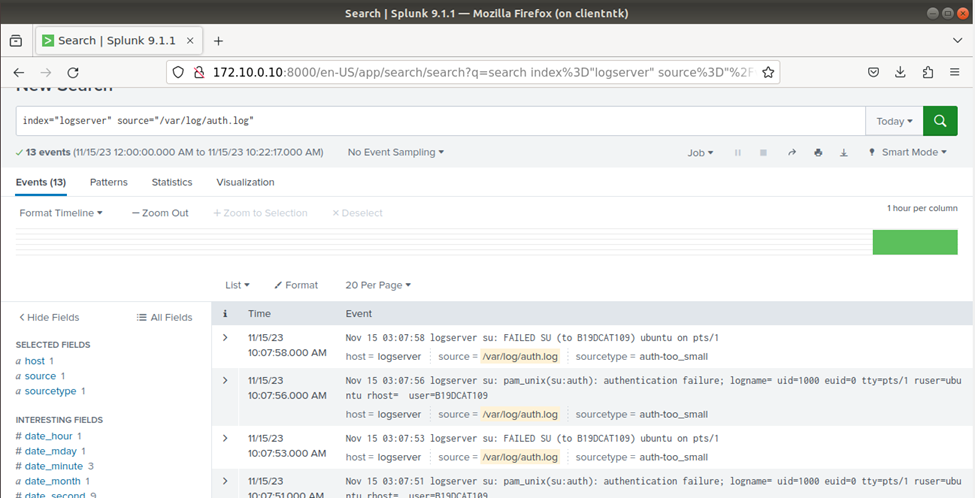
**Task 5: Tạo báo cáo( Reports) cho tìm kiếm định kỳ:**

****

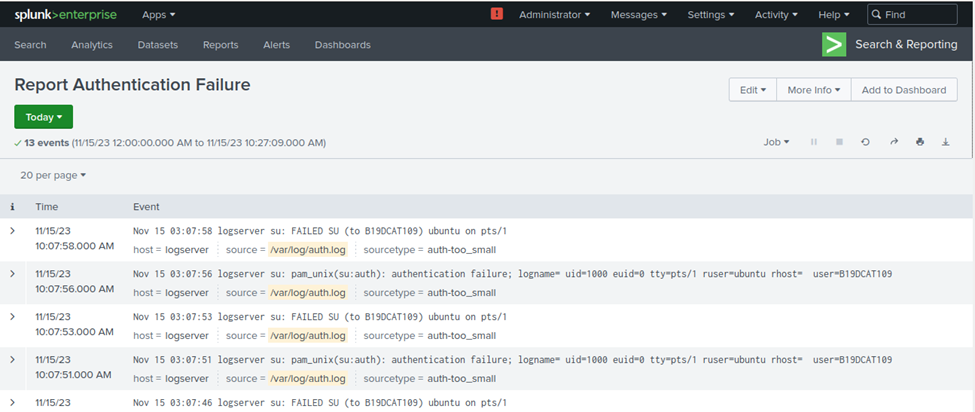
Hình 39. Tạo report cho source top 20



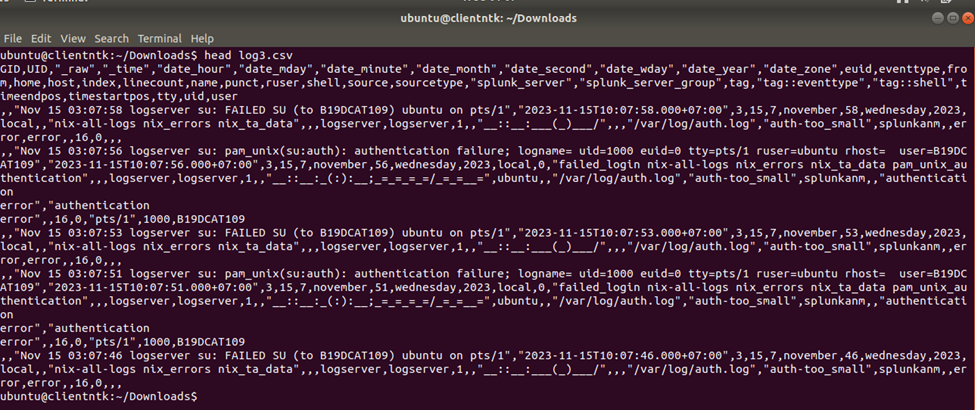
Hình 40. Ví dụ cụ thể với câu lệnh chuyển đổi user



Hình 41. Log sự kiện vừa xảy ra

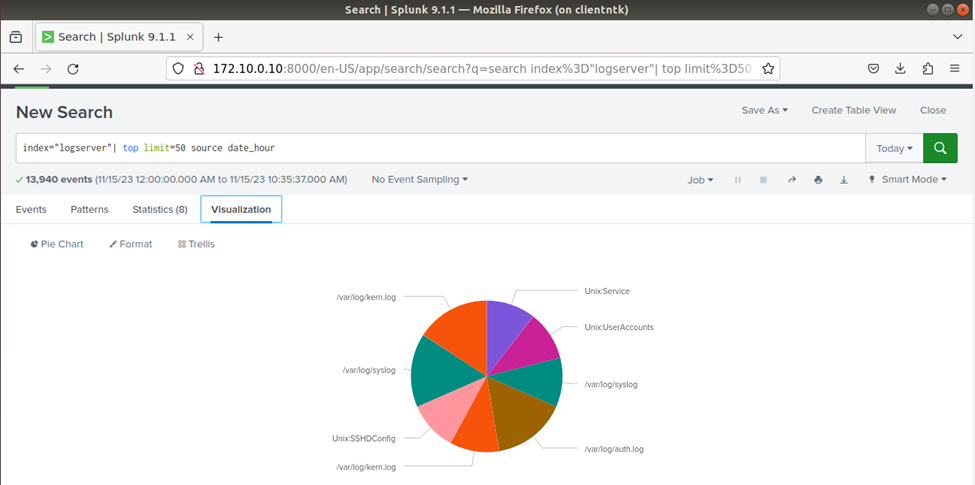


Hình 42. Lưu lại báo cáo cho sự kiện đó

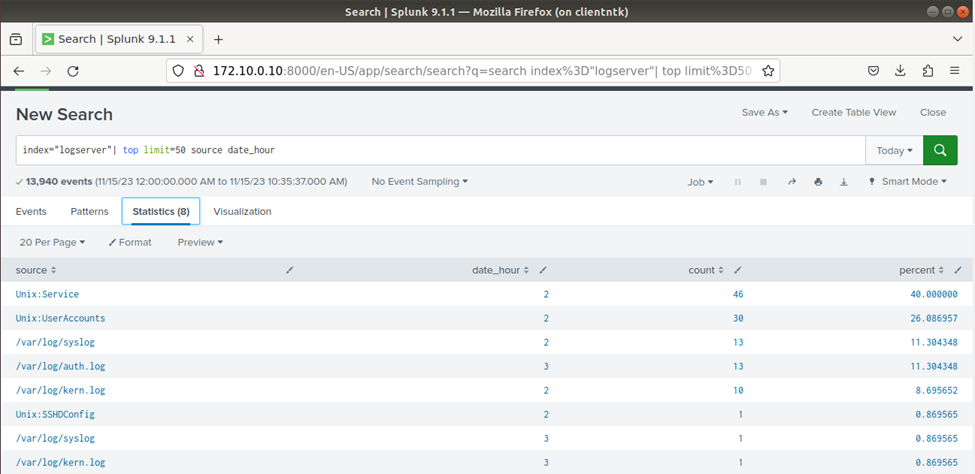


Hình 43. Đọc log3.csv

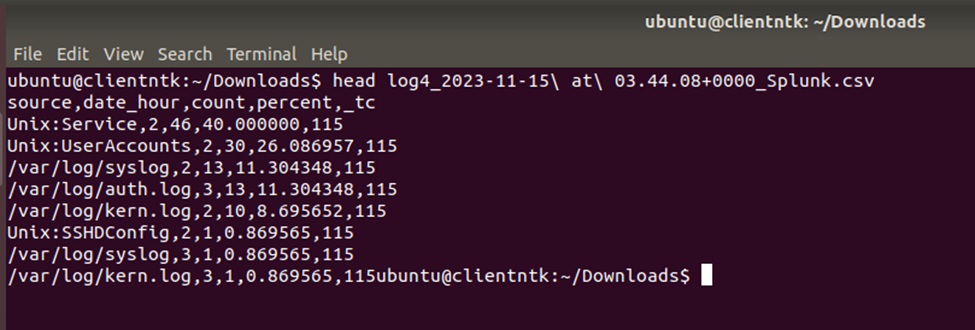
**Task 6: Tạo bảng điều khiển (DashBoards) để trực quan hoá dữ liệu.**



Hình 44. Tạo dashboard chuẩn hoá dữ liệu

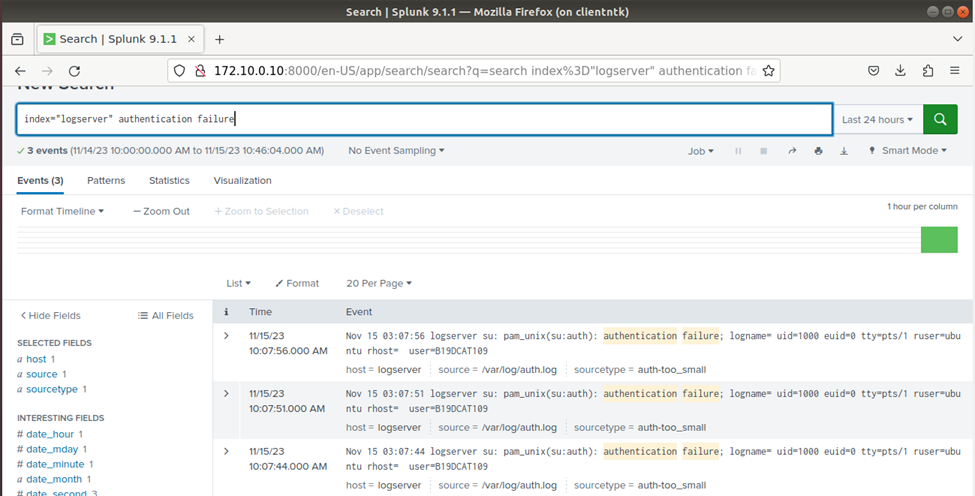


Hình 45. Kết quả dưới dạng Statistics

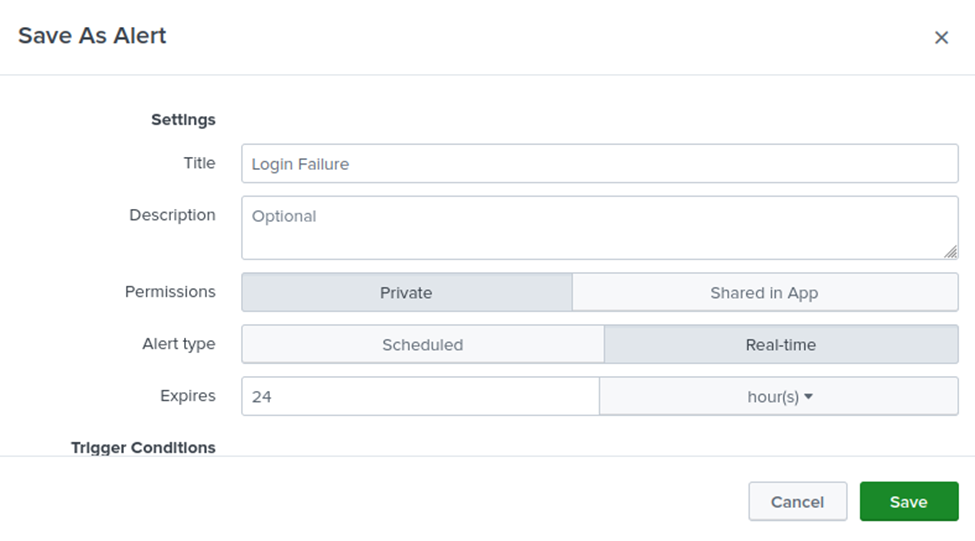


Hình 46. Đọc log4.csv

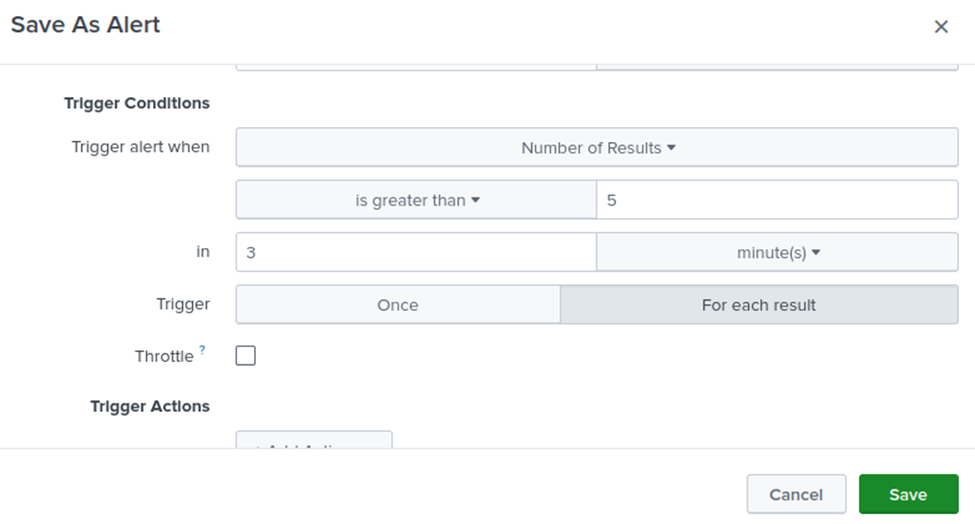
**Task 7: Tạo cảnh báo khi số lần đăng nhập của người dùng quá số lần cho phép**



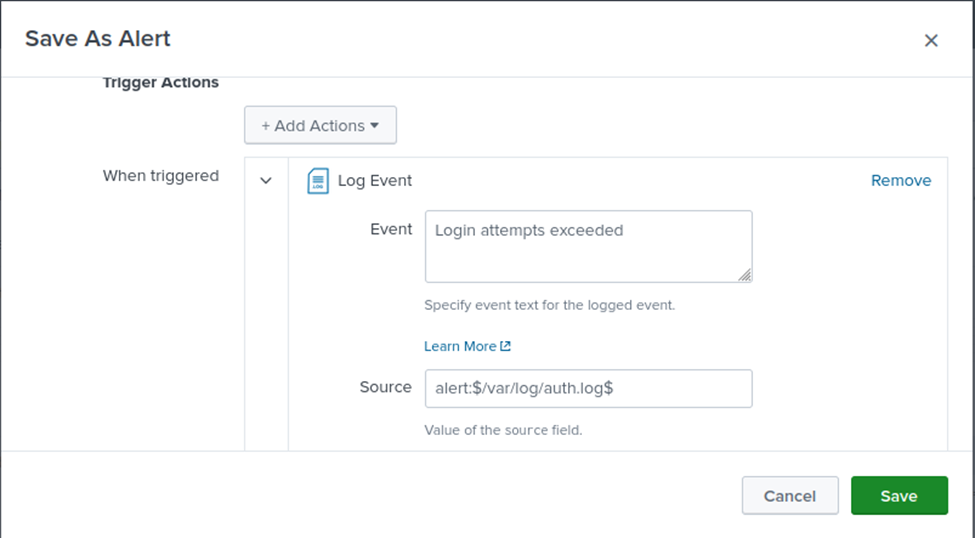
Hình 47. Truy vấn sự kiện authentication failure để tạo alert



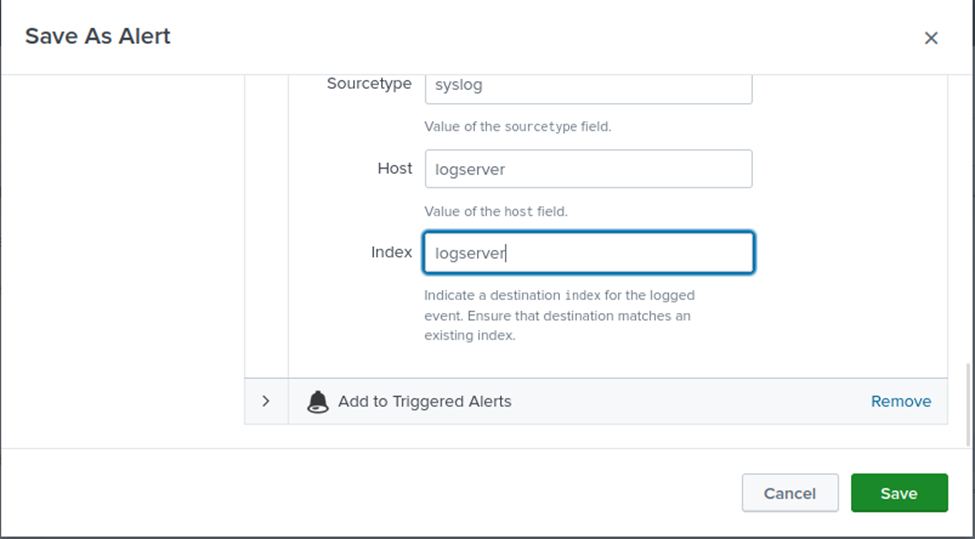
Hình 48. Cấu hình alert(1)



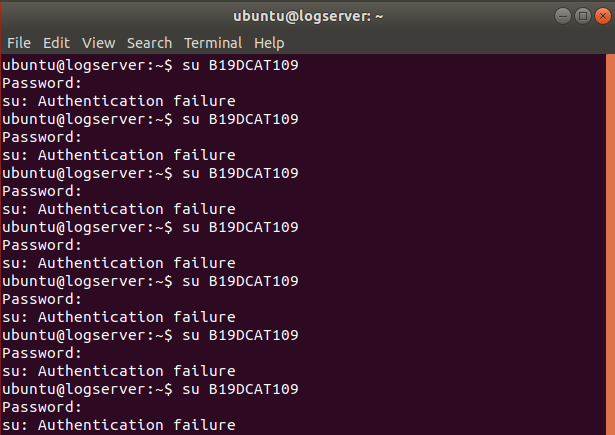
Hình 49. Cấu hình alert(2)



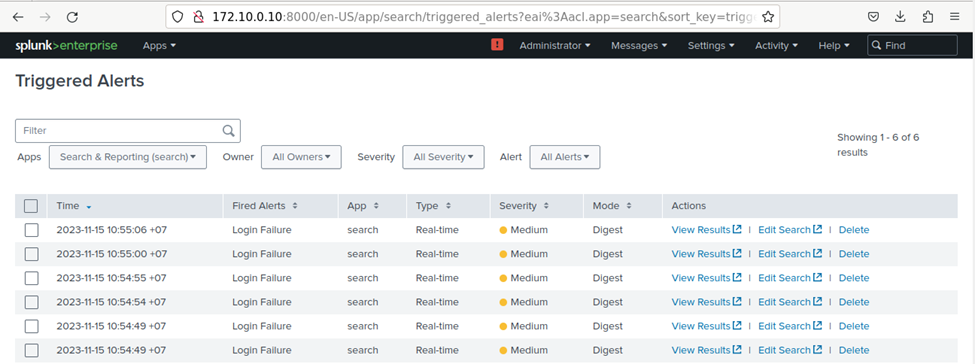
Hình 50. Cấu hình alert(3)



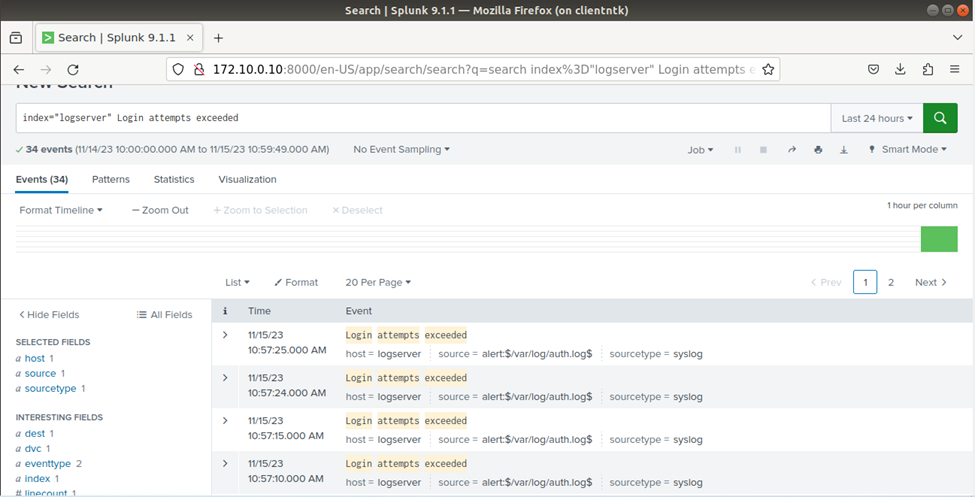
Hình 51. Cấu hình alert(4)



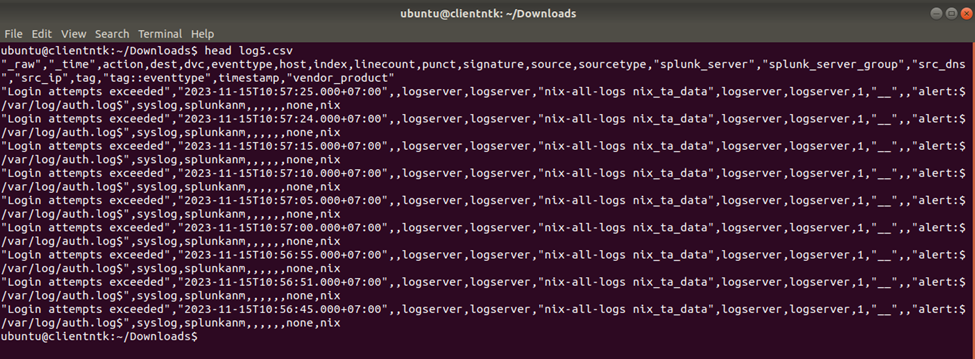
Hình 52. Thực hiện hành động để sinh log



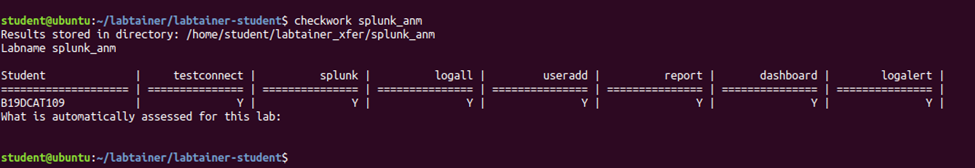
Hình 53.Alert đã đổ về thông báo



Hình 54. Aler đã đổ về log



Hình 55. Đọc log5.csv



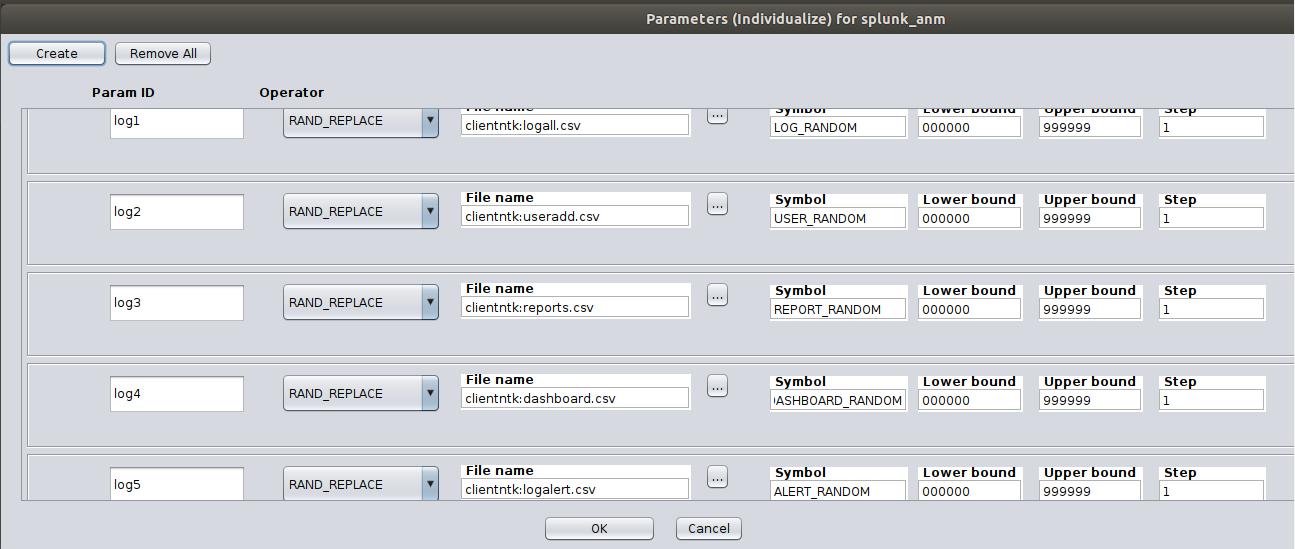
Hình 56. Checkwork tổng bài lab

**Bổ sung phần cá nhân hoá:**

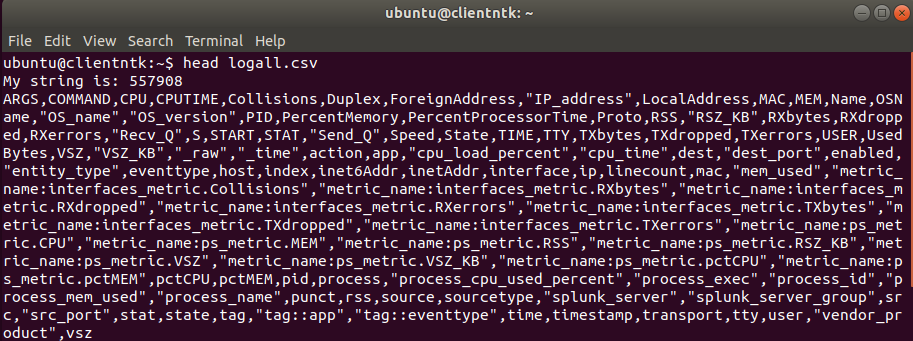
* *Cách triển khai:* 
  + Nhóm em sẽ cá nhân hoá theo chuỗi số random.
  + Khi sinh viên export file log từ web Splunk về máy client, thì sinh viên sẽ cần thực hiện câu lệnh mà giáo viên yêu cầu:

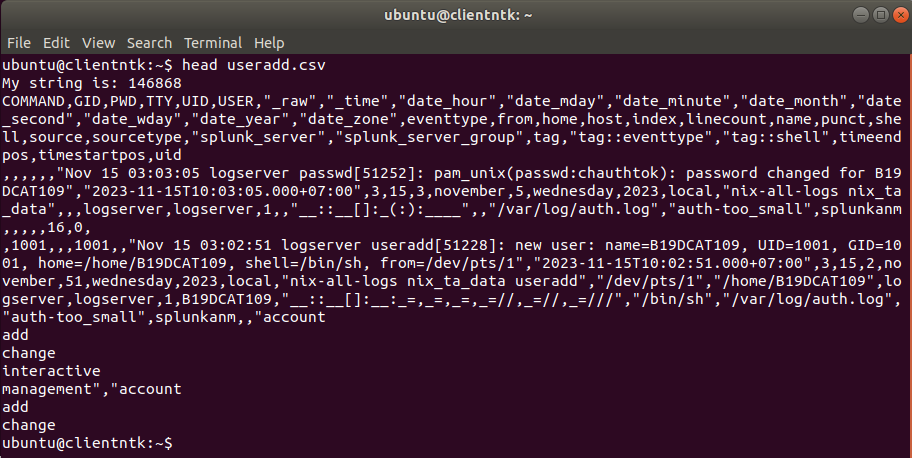
*Ví dụ minh hoạ: cat log1.csv >> logall.csv*

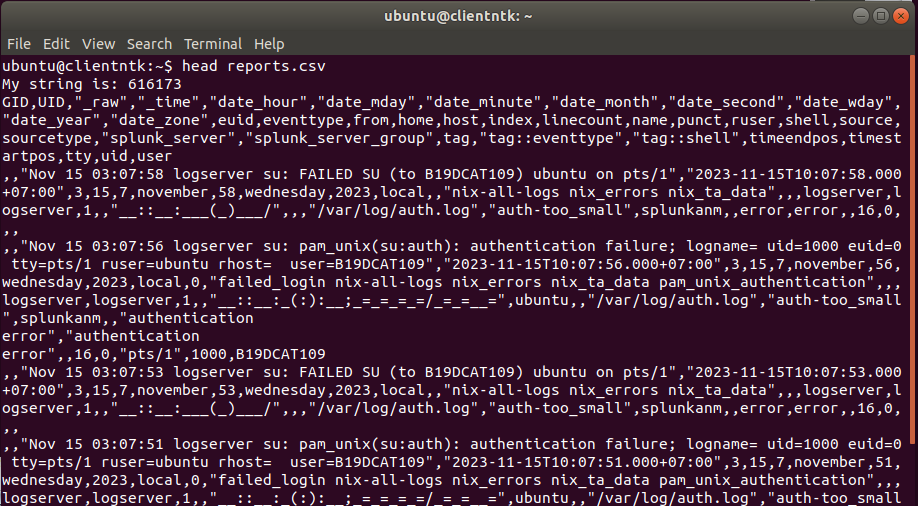
* + Ở đây file logall.csv sẽ được ẩn đi và trong file sẽ chứa chuỗi random
  + Sinh viên sau khi thực hiện nối nội dung file log1.csv vào file logall.csv sẽ thực hiện đọc file logall.csv để hoàn thành task
  + Nội dung tham số hoá như minh hoạ:

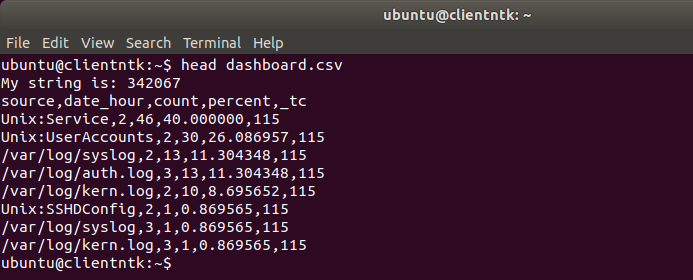
****

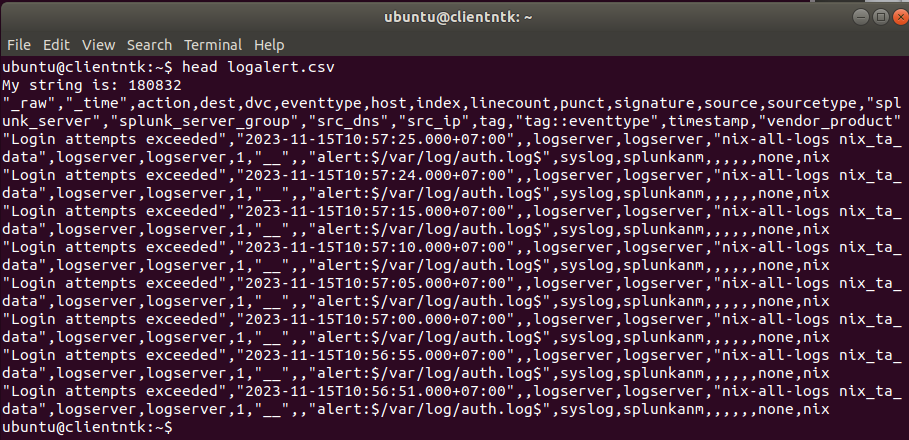
* **Kết quả: Nhóm em sẽ cá nhân hoá 5 task thu log từ web Splunk về, lần lượt theo từng ảnh.**

****

****

****

****

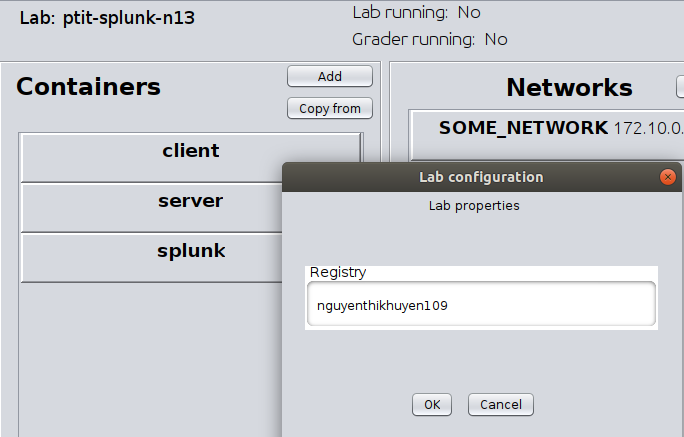
****

# 5. Triển khai bài lab

**Link tải imodule:**

[**https://github.com/khuyennguyen128/AnNinhMang/releases/download/new/imodule.tar**](https://github.com/khuyennguyen128/AnNinhMang/releases/download/new/imodule.tar)

* Xác định Registry (tên DockerHub để thiết lập push và tự động pull image khi tải về và sử dụng lab ) bằng cách chọn Edit / Config (registry).



* Thêm bài thực hành vào git

A screen shot of a computer code

Description automatically generated

* Vào thư mục trunk/distrib/ và sử dụng lệnh ./publish.py -d -l ptit-splunk-n13

để đẩy image lên DockerHub

* Lưu ý cần tạo 1 tài khoản dockerhub( Mình sử dụng đăng nhập bằng tài khoản github)
* Sử dụng lệnh docker login
* Đăng nhập Docker sau đấy sử dụng lệnh ./publish.py -d -l ptit-splunk-n13

A computer screen shot of a computer code

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

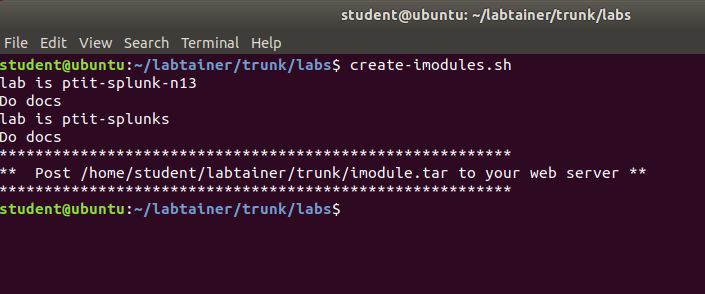
* Sau khi hoàn tất, image của các vùng chứa (container) bao gồm attacker và server sẽ được đẩy lên

<https://hub.docker.com/repositories/khuyennguyen128>

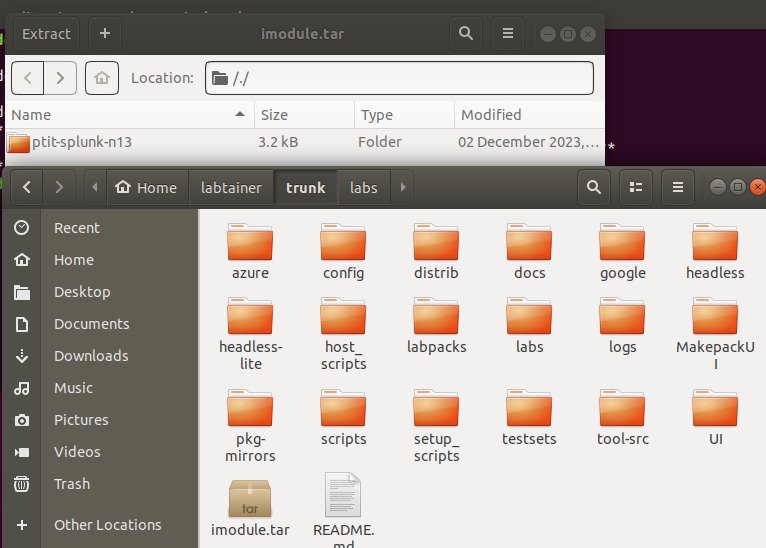
A screenshot of a computer

Description automatically generated

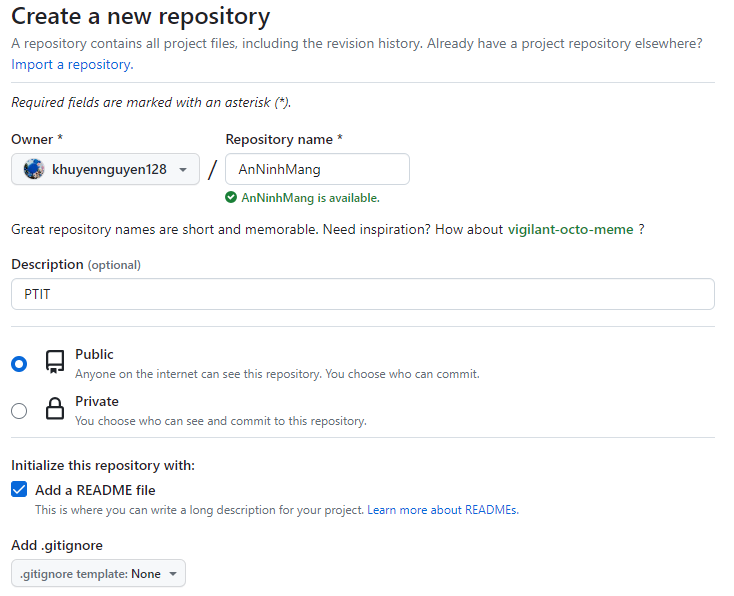
* Tạo file IModule tar chứa bài thực hành

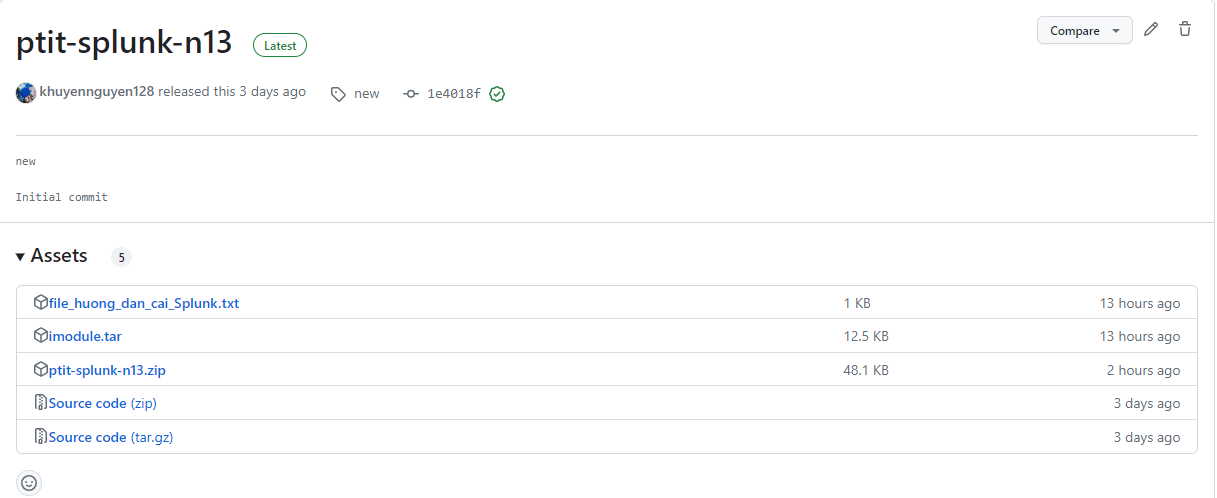


* File này nằm ở Labtainer/trunk/Imodule



* Kéo file này ra Imodule.tar hoặc copy ra máy thật .
* Trên git hub tạo một kho lữu trữ mới và Tạo Phát hành và đẩy file tar này lên phần phát hành.
* Thực hiện đẩy lên github lưu trữ bài lab để sinh viên có thể tải về thực hiện.





Sinh viên sẽ sử dụng lệnh:

* Thực hiện tải và giải nén bài lab. Di chuyển bài lab sang thư mục /labtainer/trunk/labs
* Sử dụng lệnh khởi động bài lab để thực hiện pull image của bài lab được lưu trữ lên docker

