HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

Báo cáo bài thực hành

Phát hiện và phản ứng sự cố ICMP Flood

Sinh viên thực hiện:

B20DCAT002 – Hoàng Thu Cúc

Giảng viên hướng dẫn: TS.Nguyễn Ngọc Điệp

HÀ NỘI 12-2025

MỤC LỤC

DANH MỤC CÁC HÌNH VẼ

NỘI DUNG THỰC HÀNH

1.1 Lab 2: Phát hiện và phản ứng sự cố ICMP flood

1.1.1 Giới thiệu chung

Bài thực hành "Phát hiện và phản ứng sự cố tấn công ICMP Flood" được xây dựng nhằm giúp sinh viên:

- Hiểu được quy trình giám sát lưu lượng mạng
- Phát hiện bất thường và phản ứng khi xảy ra tấn công từ chối dịch vụ dạng ICMP flood.

Bài thực hành hướng dẫn sinh viên:

- cấu hình Splunk để thu thập log mạng
- theo dõi spike ICMP bất thường
- sử dụng iptables để chặn nguồn tấn công
- triển khai các kỹ thuật hạn chế tốc độ (rate-limit) ICMP tại host.

1.1.2 Mục đích

Sinh viên sau khi làm bài thực hành sẽ hiểu:

- cách phát hiện và phân tích tấn công ICMP flood thông qua log thu thập từ tcpdump/syslog và Splunk.
- biết cách xác định IP tấn công
- áp dụng rule iptables để chặn lưu lượng gây hại
- thiết lập cơ chế rate-limit nhằm giảm thiểu rủi ro trong tương lai.

1.1.3 Yêu cầu đối với sinh viên

- Có kiến thức về các lệnh giám sát mạng như tcpdump, iptables.
- Hiểu khái niệm ICMP echo, ICMP flood.
- Nắm được nguyên lý thu thập log bằng Splunk.

1.1.4 Nội dung thực hành

Trước khi khởi động bài lab, cần đảm bảo labtainer được cấu hình như sau:

  - Memory (RAM): 10GB
  - Hard Disk: Tối thiểu 80GB (khuyến nghị 100GB)

- Tải bài lab:

  Vào /home/student/labtainer/labtainer-student và gõ lệnh sau trên terminal:

imodule
https://github.com/anhdnmit/do_an_tot_nghiep/raw/refs/heads/main/idr_splunk_icmpflood/imodule.tar

- Khởi động bài lab:

labtainer -r idr_splunk_icmpflood

- Sau khi khởi động xong, 3 terminal ảo : client, server, attacker
- Để kiểm tra địa chỉ IP của 3 máy, gõ lệnh sau trên từng máy:

ifconfig

1.1.4.1 Triển khai và cấu hình hệ thống

1.1.4.1.1 Ở server – Triển khai và khởi tạo Splunk Enterprise

Đã tải sẵn bộ cài đặt Splunk ở client và server nên sinh viên chỉ cần giải nén và thực hiện lệnh. Trên server, sinh viên thực hiện lệnh sau:

sudo tar -xzf splunk-8.2.6-a6fe1ee8894b-Linux-x86_64.tgz -C /opt

sudo chown -R ubuntu:ubuntu /opt/splunk

Tiếp đến, lệnh ghi cấu hình OPTIMISTIC_ABOUT_FILE_LOCKING = 1 được thêm vào file splunk-launch.conf.

echo "OPTIMISTIC_ABOUT_FILE_LOCKING = 1" | sudo tee -a /opt/splunk/etc/splunk-launch.conf

sudo /opt/splunk/bin/splunk start --accept-license

Cài đặt và đặt mật khẩu ngay trong quá trình khởi tạo xong thì thực hiện lệnh splunk status được dùng để bảo đảm dịch vụ splunkd đã hoạt động ổn định.

sudo /opt/splunk/bin/splunk status

Sinh viên sau đó mở trình duyệt (Firefox) tới địa chỉ http://127.0.0.1:8000, đăng nhập bằng tài khoản admin và mật khẩu đã đặt.

Ngay sau khi đăng nhập, một bước quan trọng khác là cấu hình Splunk lắng nghe dữ liệu gửi đến từ Universal Forwarder trên client.

sudo /opt/splunk/bin/splunk enable listen 9997 -auth <tài khoản>:<mật khẩu>

sudo netstat -tulpn | grep 9997

1.1.4.1.2 Ở client – Cài đặt Splunk Universal Forwarder (UF)

Phía client đóng vai trò nguồn gửi log về server nên cần triển khai Splunk Universal Forwarder.

sudo tar -xzf splunkforwarder-8.2.6-a6fe1ee8894b-Linux-x86_64.tgz -C /opt

sudo chown -R ubuntu:ubuntu /opt/splunkforwarder

Rồi đặt mật khẩu quản trị riêng :

sudo /opt/splunkforwarder/bin/splunk start --accept-license

Lệnh splunk status sau đó được dùng để kiểm tra xem UF đã khởi động đầy đủ hay chưa:

sudo /opt/splunkforwarder/bin/splunk status

Từ đó, ta thiết lập kết nối giữa UF và Splunk Enterprise:

sudo /opt/splunkforwarder/bin/splunk add forward-server 176.28.0.5:9997 -auth <tài khoản>:<mật khẩu>

1.1.4.1.3 Thiết lập log trên client – Tạo index trên server

Để mô phỏng sự cố, sinh viên tạo một script nhỏ (tcpdump_icmp.sh) để chạy tcpdump rồi ghi log vào trong /var/log/tcpdump_icmp.log :

sudo nano /usr/local/bin/tcpdump_icmp.sh

Nội dung file:

```
#!/bin/bash
LOG_FILE="/var/log/tcpdump_icmp.log"
: > "$LOG_FILE"
tcpdump -ni any icmp -tttt >> "$LOG_FILE"
```

Khi script được cấp quyền thực thi và chạy nền bằng ./tcpdump_icmp.sh &, tcpdump bắt đầu theo dõi toàn bộ ICMP trong hệ thống.

Sau khi log ICMP đã sẵn sàng, bước tiếp theo là hướng Splunk UF theo dõi file đó. Điều này được thực hiện thông qua file cấu hình inputs.conf. Trong file này, một khối monitor được thêm vào:

```
[monitor:///var/log/tcpdump_icmp.log]
sourcetype = tcpdump_icmp
index = icmp_lab
```

Sau khi chỉnh cấu hình, UF phải được khởi động lại để nhận thay đổi. Vì client gửi log vào index icmp_lab, Splunk Enterprise phải tạo index này trước

sudo /opt/splunk/bin/splunk add index icmp_lab -auth <tài khoản>:<mật khẩu>

1.1.4.2 Phát hiện và phản ứng sự cố ICMP flood

1.1.4.2.1 Ở server : Phát hiện sự cố ICMP flood

Sau khi attacker tạo icmp flood bằng :

sudo hping3 --icmp -i u1000 -d 120 176.28.0.7

sudo hping3 --icmp --flood -d 120 176.28.0.7

sinh viên sẽ truy cập giao diện Splunk thông qua trình duyệt tại địa chỉ http://127.0.0.1:8000 rồi đăng nhập bằng tài khoản quản trị.

Trong Splunk, chỉ cần một truy vấn đơn giản như:

index=icmp_lab "ICMP"

là đã có thể thấy ngay các bản ghi mô tả gói tin ICMP echo request hoặc echo reply. Tuy nhiên, để quan sát có hệ thống hơn, Splunk cho phép tách riêng trường địa chỉ IP nguồn và đích bằng cách sử dụng biểu thức rex.

```
index=icmp_lab "ICMP"
| rex "IP (?<src_ip>\d+\.\d+\.\d+\.\d+) > (?<dst_ip>\d+\.\d+\.\d+\.\d+)"
| table _time src_ip dst_ip
```

Bên cạnh giao diện web, Splunk cũng cho phép truy vấn trực tiếp từ terminal bằng :

sudo /opt/splunk/bin/splunk search 'index=icmp_lab "ICMP"' -auth <tài khoản>:<mật khẩu> -maxout 20 | tee -a evidence.txt

1.1.4.2.2 Ở client : Kiểm soát và chặn sự cố (Containment)

Khi đã xác định được IP tấn công từ Splunk, sinh viên cần kiểm soát sự cố tại client.

Ta cài đặt công cụ iptables để chặn nhanh lưu lượng từ attacker :

iptables -A INPUT -s 176.28.0.3 -p icmp -j DROP

1.1.4.2.3 Ở client : Diệt bỏ nguyên nhân (Eradication)

Client cho phép ICMP nhưng giới hạn tần suất tối đa:

iptables -A INPUT -p icmp -m limit --limit 10/s --limit-burst 20 -j ACCEPT

Rule này cho phép tối đa 10 gói ICMP mỗi giây, với khả năng “burst” tạm thời 20 gói. Người dùng bình thường (ping vài lần) vẫn hoạt động bình thường, nhưng attacker gửi hàng trăm hoặc hàng nghìn gói mỗi giây sẽ nhanh chóng vượt ngưỡng.

Ngay sau rule ACCEPT theo limit là rule DROP:

iptables -A INPUT -p icmp -j DROP

Bất kỳ ICMP nào vượt ngưỡng sẽ bị loại bỏ hoàn toàn.

➔ Từ đó, sinh viên sẽ thấy hai rule được tạo, với số lượng packet tăng dần khi attacker flood, chứng minh rằng rule hạn chế hoạt động hiệu quả.

Kết quả kỳ vọng: log ICMP sẽ không còn ngập tràn như ban đầu; các gói vượt ngưỡng bị DROP thay vì tràn vào hệ thống.

1.1.4.2.4 Trên client và server– Thu thập chứng cứ

Trước hết, sinh viên tạo thư mục lưu trữ bằng chứng:

mkdir -p ~/ir-backup

Sau đó, file log ICMP được nén lại bằng:

tar czf ~/ir-backup/icmp_lab_logs.tar.gz /var/log/tcpdump_icmp.log

Tiếp theo, sinh viên sinh mã băm SHA-256 cho file nén:

sha256sum ~/ir-backup/icmp_lab_logs.tar.gz

Giá trị mã băm này được lưu trong file .sha256 nhằm bảo đảm tính toàn vẹn chứng cứ – nếu file bị sửa đổi, hash sẽ thay đổi.

Tương tự ở bên server với file evidence.txt

1.1.4.3 Theo dõi hậu sự cố

Việc theo dõi được thực hiện trực tiếp trong Splunk Web thông qua truy vấn thống kê ICMP theo thời gian, sau đó lưu truy vấn này thành một cảnh báo tự động (Alert) để Splunk tự giám sát mỗi phút.

Truy cập vào ứng dụng Search & Reporting. Tại đây, Splunk cung cấp toàn bộ dữ liệu mà Universal Forwarder đã gửi từ client.

Trong ô Search, Splunk được sử dụng để phân tích log theo hướng thống kê thay vì chỉ xem từng dòng thô. Câu truy vấn sau được dùng:

```
index=icmp_lab "ICMP"
| rex "IP (?<src_ip>\d+\.\d+\.\d+\.\d+) > (?<dst_ip>\d+\.\d+\.\d+\.\d+)"
| bin _time span=10s
| stats count AS icmp_count BY _time src_ip dst_ip
| where icmp_count > 200
```

Chọn “Save As → Alert”, Splunk mở giao diện cấu hình Alert.

- Phần thông tin Alert
    - Title: ICMP Flood from Attacker.

- Description: mô tả mục tiêu <tùy chọn>
- Quyền truy cập có thể để mặc định (Private).
- Alert Type chọn Scheduled
- Lịch chạy: Run on Cron Schedule, điền ô nhập : * * * * *

- Phần Trigger (điều kiện bắn cảnh báo)
  - Trigger alert when: Number of Results → is greater than: 0
  - Chế độ Trigger: Once – mỗi lần Splunk chạy truy vấn mà thấy kết quả, sẽ bắn một alert.
- Phần Actions (thao tác khi alert kích hoạt)
  - Event: ICMP flood detected:

    src_ip=$result.src_ip$,dst_ip=$result.dst_ip$,icmp_count=$result.icmp_count$
  - Sourcetype: icmp_flood_alert
  - Index: icmp_lab

Để kiểm tra alert vận hành đúng, attacker tạo lại tấn công bằng lệnh flood.

Sau đó, sinh viên có thể kiểm tra lại theo 2 cách.

Vào Search & Reporting, đặt câu truy vấn:

index=icmp_lab sourcetype=icmp_flood_alert

Splunk sẽ hiển thị các event cảnh báo mới sinh ra.

Tương tự bằng lệnh:

*sudo /opt/splunk/bin/splunk search *

*'index=icmp_lab sourcetype=icmp_flood_alert "ICMP flood detected"' *

-auth <tài khoản>:<mật khẩu>-maxout 50 | tee -a evidence.txt

1.1.4.4 Kết thúc bài lab:

Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab

Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

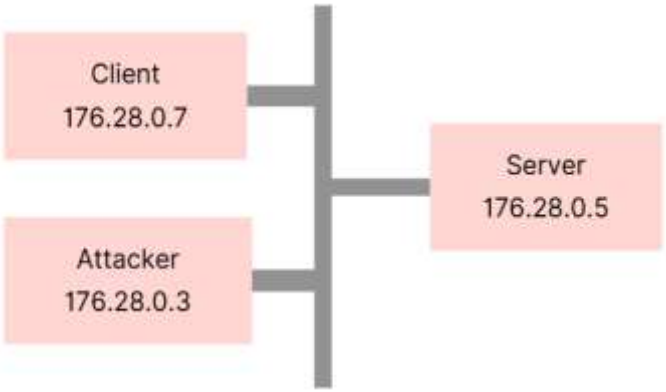
Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

labtainer -r idr_splunk_icmpflood

1.1.5 Thiết kế bài thực hành

1.1.5.1 Cấu hình docker

- Trong môi trường máy ảo Ubuntu, sử dụng docker tạo ra 3 container: : 1 container "client", 1 container "server, 1 container "attacker".
- Tạo mạng có cấu hình:
  - Subnet: 176.28.0.0/24
  - External Gateway: 176.28.0.1
- Cấu hình docker gồm có:
  - Server: Cấu hình cho máy server
    - Tên máy: server
    - Địa chỉ trong mạng LAN: 176.28.0.5
    - Gateway: 176.28.0.1
  - Client: Cấu hình cho máy client
    - Tên máy: client
    - Địa chỉ trong mạng LAN: 176.28.0.7
    - Gateway: 176.28.0.1
  - Attacker: Cấu hình cho máy tấn công 2 sự cố
    - Tên máy: attacker
    - Địa chỉ trong mạng LAN: 176.28.0.3
    - Gateway: 176.28.0.1



Hình 1 Topo mạng bài idr_splunk_icmpflood

- config: lưu cấu hình hoạt động của hệ thống

- dockerfiles: mô tả cấu hình của các container, gồm:
    - server: sử dụng các thư viện mặc định hệ thống, cập nhật hệ thống và cài sẵn Splunk Enterprise 8.2.6.
    - client: sử dụng các thư viện mặc định hệ thống, cập nhật hệ thống và cài sẵn Splunk Universal Forwarder
    - attacker: sử dụng các thư viện mặc định hệ thống và cập nhật hệ thống, cài đặt thêm công cụ hping3.

1.1.5.2 Các nhiệm vụ cần thực hiện

- Đảm bảo hệ thống Splunk server đang hoạt động để thu thập và phân tích log.
- Đảm bảo Splunk Forwarder trên client đang hoạt động để gửi log về server.
- Ghi nhận lưu lượng tấn công giữa máy tấn công và máy nạn nhân làm bằng chứng trong báo cáo.
- Áp dụng luật tường lửa nhắm đúng địa chỉ IP của máy attacker.
- Áp dụng cơ chế giới hạn lưu lượng nhằm giảm thiểu ảnh hưởng của tấn công flood.
- Tạo bản sao lưu log và kiểm tra tính toàn vẹn bằng mã băm để phục vụ điều tra, lưu trữ.
- Ghi nhận IP nguồn và đích của lưu lượng tấn công trong bằng chứng

1.1.5.3 Các kết quả cần đạt được

Mỗi nhiệm vụ nhỏ sẽ được chia ra thành các mục chấm điểm để xác nhận sinh viên đã làm đúng các bước và hoàn thành bài thực hành hay chưa. Vì vậy, hệ thống sẽ ghi nhận các thao tác, sự kiện được mô tả theo bảng dưới đây để chấm điểm cho sinh viên:

Bảng 1. Bảng result của bài idr_splunk_icmpflood

Result Tag	**Container 1**	**File1**	**File Type**	**Field ID**	**Timestamp Type**
server1	server	/opt/splunk/bin/splunk	CONTAINS	splunkd is running	File
client1	client	/opt/splunkforwarder/bin/splunk	CONTAINS	splunkd is running	File
server2	server	evidence.txt	CONTAINS	176.28.0.3 > 176.28.0.7	File
client2	client	iptables.stdin	CONTAINS	176.28.0.3	File

client3	client	iptables.stdin	CONTAINS	limit	File
client4	client	sha256sum.stdin	CONTAINS	backup	File
server3	server	evidence.txt	CONTAINS	src_ip=176.28.0.3, dst_ip=176.28.0.7	File

1.1.6 Cài đặt và cấu hình các máy ảo

Hình 2 Giao diện bài lab idr_splunk_icmpflood

Hình 3 Result

Open ▾ Dockerfile.idr_splunk_icmpflood.attacker.student Save

```
ARG registry
FROM $registry/labtainer.base2
#FROM $registry/labtainer.network
#FROM $registry/labtainer.centos
#FROM $registry/labtainer.lamp
ARG lab
ARG labdir
ARG imagedir
ARG user_name
ARG password
ARG apt_source
ARG version
LABEL version=$version
ENV APT_SOURCE $apt_source
RUN /usr/bin/apt-source.sh
ADD $labdir/$imagedir/sys_tar/sys.tar /
ADD $labdir/sys_$lab.tar.gz /
RUN useradd -ms /bin/bash $user_name
RUN echo "$user_name:$password" | chpasswd
RUN adduser $user_name sudo
# replace above with below for centos/fedora
#RUN usermod $user_name -a -G wheel
######################################
RUN apt-get update && \
    DEBIAN_FRONTEND=noninteractive apt-get install -y --no-install-
recommends \
        hping3 \
        iputils-ping \
    && apt-get clean && rm -rf /var/lib/apt/lists/*
######################################

USER $user_name
ENV HOME /home/$user_name
ADD $labdir/$imagedir/home_tar/home.tar $HOME
```

Hình 4 Dockerfiles của máy attacker

Open ▾ Dockerfile.idr_splunk_icmpflood.client.student Save

```
LABEL version=$version
ENV APT_SOURCE $apt_source
RUN /usr/bin/apt-source.sh
ADD $labdir/$imagedir/sys_tar/sys.tar /
ADD $labdir/sys_$lab.tar.gz /
RUN useradd -ms /bin/bash $user_name
RUN echo "$user_name:$password" | chpasswd
RUN adduser $user_name sudo
# replace above with below for centos/fedora
#RUN usermod $user_name -a -G wheel

############################ CLIENT ###################################

# Đặt file UF 8.2.6 vào home ubuntu
COPY _bin/splunkforwarder-8.2.6-a6fe1ee8894b-Linux-x86_64.tgz \
     /home/ubuntu/splunkforwarder-8.2.6-a6fe1ee8894b-Linux-x86_64.tg

RUN chown ubuntu:ubuntu /home/ubuntu/splunkforwarder-8.2.6-a6fe1ee88
Linux-x86_64.tgz \
 && chmod 0640 /home/ubuntu/splunkforwarder-8.2.6-a6fe1ee8894b-Linux-
x86_64.tgz

RUN apt-get update && \
    apt-get install -y tcpdump && \
    rm -rf /var/lib/apt/lists/*


#################################################################
USER $user_name
ENV HOME /home/$user_name
ADD $labdir/$imagedir/home_tar/home.tar $HOME
# remove after docker fixes problem with empty tars
RUN rm -f $HOME/home.tar
```

Hình 5 Dockerfiles của máy client

Hình 6 Dockerfiles của máy server

1.1.7 Tích hợp và triển khai

1.1.7.1 Docker Hub

Hình 7 Bài thực hành được lưu trữ trên docker hub

1.1.7.2 Github

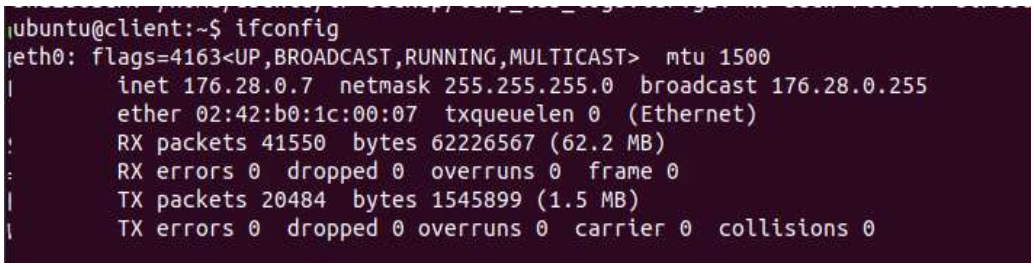
Link github:
https://github.com/anhdnmit/do_an_tot_nghiep/blob/main/idr_splunk_icmpflood/imodule.tar

Hình 8 Đẩy file imodule.tar lên github

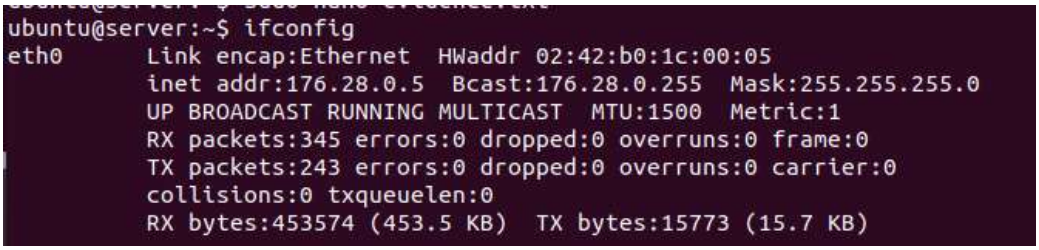
1.1.8 Thử nghiệm và đánh giá

Bài thực hành đã được xây dựng thành công. Bây giờ ta sẽ đánh giá về 1 trong các nhiệm vụ bài lab yêu cầu.

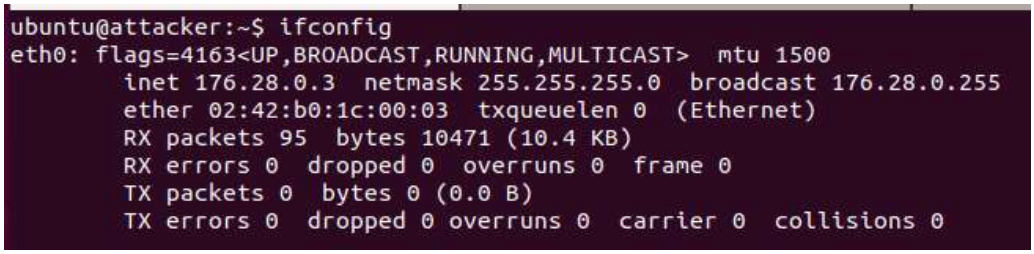
Trước hết, ta kiểm tra ip trên 3 máy.



Hình 9 IP client



Hình 10 IP server



Hình 11 IP attacker

Ở phần đánh giá này, ta tập trung làm nhiệm vụ 1 là "Đảm bảo hệ thống Splunk server đang hoạt động để thu thập và phân tích log". Khi Splunk server đã cài đúng, chạy ổn định và kiểm tra được trạng thái, các nhiệm vụ sau chỉ cần gửi log đúng về Splunk và bám theo hướng dẫn chung là sẽ ra kết quả checkwork.

Người thiết kế đã để sẵn file cài đặt splunk-8.2.6.tgz nên giờ nó cần được giải nén vào thư mục /opt. Lưu ý là cần thêm một cấu hình nhỏ để Splunk ít bị lỗi khóa file trong môi trường container:

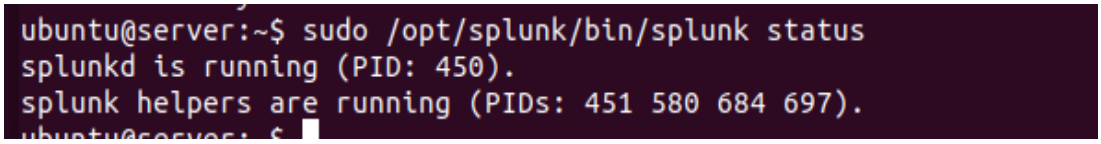
Hình 12 Phần cài đặt Splunk Enterprise cơ bản

Ta khởi động Splunk lần đầu tiên và chấp nhận điều khoản sử dụng. Toàn bộ thao tác này gói trong 1 lệnh ở ảnh

Hình 13 Nhập tài khoản và mật khẩu ở Splunk

Địa chỉ web để truy cập Splunk sẽ được cung cấp khi khởi động : http://<ĐỊA_CHỈ_IP>:8000

Cuối cùng, ta kiểm tra lại trạng thái dịch vụ Splunk trên server bằng lệnh:



Hình 14 Kiểm tra trạng thái dịch vụ Splunk

Nếu lệnh trả về trạng thái splunkd is running → ta có thể khẳng định Splunk server đã hoạt động ổn định, sẵn sàng thu thập và phân tích log cho các nhiệm vụ tiếp theo trong bài lab.

Hình 15 Checkwork bài idr_splunk_icmpflood