# Bài tập Final

## Nội dung

## Bài tập yêu cầu thực hiện cấu hình security cho toàn bộ ELK stack và thực hiện rule alert trên Kibana.

## Yêu cầu

1. Cấu hình security toàn bộ (Basic security +) cho cụm ELK stack đã có (3 node Elasticsearch, 1 Kibana):

* Kết nối mã hoá giữa các node Elasticsearch.
* Kết nối mã hoá từ Kibana đến Elasticsearch, có sử dụng Authentication.

1. Cài đặt và cấu hình Packetbeat trên server chạy Kibana, cấu hình kết nối mã hoá từ Packetbeat về cụm Elasticsearch và sử dụng API Key cho authentication.
2. Cấu hình alert rule: thực hiện cấu hình alert rule (với Connector là Index), thực hiện giám sát monitor việc thực hiện ping (type: icmp) đến IP 1.1.1.1

## Yêu cầu nộp bài

(các hình chụp phải rõ nét, các hình chụp không nhìn rõ text sẽ không được tính)

* 1 hình chụp curl GET cluster health với giao thức https và có authentication (bao gồm command curl và kết quả command).
* 1 hình chụp cấu hình alert trên giao diện Kibana (full màn hình Kibana).
* 1 hình chụp alert được ghi vào Index (giao diện Discover).