**Project #1:** Implement centralized logging solutions using ELK Stack (Elasticsearch, Logstash, & Kibana)

**Mentor:** Dang Ngoc Cuong - IT Faculty

**Description:**

The ELK Stack is a collection of three open-source products — Elasticsearch, Logstash, and Kibana — from Elastic. Elasticsearch is a NoSQL database that is based on the Lucene search engine. Logstash is a log pipeline tool that accepts inputs from various sources, executes different transformations, and exports the data to various targets. Kibana is a visualization layer that works on top of Elasticsearch.

Together, these three different open source products are most commonly used in log analysis in IT environments (though there are many more use cases for the ELK Stack starting including business intelligence, security and compliance, and web analytics). Logstash collects and parses logs, and then Elasticsearch indexes and stores the information. Kibana then presents the data in visualizations that provide actionable insights into one’s environment.

**Time:** 14 weeks

**Required:**

* Group of 3 or 4 students
* Vmware Workstation 12 or Virtual Box
* GNS3
* Cisco IOU
* CentOS or Ubuntu

**References:**

[1] <https://logz.io/learn/complete-guide-elk-stack/>

**Project #2:** Implement the Next-Generation Firewall for DTU Network System using OPNsense

**Mentor:** Dang Ngoc Cuong - IT Faculty

**Description:**

A Next-Generation Firewall (NGFW) is an integrated network platform that is a part of the third generation of firewall technology, combining a traditional firewall with other network device filtering functionalities, such as an application firewall using in-line deep packet inspection (DPI), an intrusion prevention system (IPS). Other techniques might also be employed, such as TLS/SSL encrypted traffic inspection, website filtering, QoS/bandwidth management, antivirus inspection and third-party identity management integration (i.e. LDAP, RADIUS, Active Directory).

Next Generation Firewalls (NGFWs) provide the blended features of a standard firewall along with advanced security features. They apply deep packet inspection (DPI) technology with integrated intrusion prevention systems (IPS), along with application intelligence and control to visualize the content of the data being accessed and processed.

Apart from these security capabilities, NGFW’s offer additional features such as SSL/ SSH inspection, reputation-based malware filtering and Active Directory integration support too. These granular security policies and controls help NGFW’s to detect application-specific attacks, making them capable to capture more malicious activity than traditional firewalls.

Organizational network communications are no longer restricted to simple emails; but have expanded to include real-time collaboration tools like Web 2.0 applications, instant messenger (IM), peer-to-peer applications, VoIP, streaming media and teleconferencing. These tools automatically open new avenues for potential attacks. Enterprises need tools to guarantee bandwidth for critical business relevant applications while ensuring speed and security for a productive work environment.

**Time:** 14 weeks

**Required:**

* Group of 3 or 4 students
* Vmware Workstation 12 or Virtual Box
* GNS3
* Cisco IOU
* CentOS or Ubuntu

**References:**

[1]<http://www.esecurityplanet.com/security-buying-guides/intro-to-next-generation-firewalls.html>

[2]<https://www.cyberoam.com/ngfw.html/>

[3]<http://www.niiconsulting.com/solutions/next-generation-firewalls.html>

**Project #3- Nghiên cứu triển khai giải pháp nâng cao độ an toàn bảo mật mạng sử dụng mạng 3 lớp CISCO.**

**Ths. Nguyễn Quốc Long**

**Mô tả yêu cầu:**

**Project #4- Nghiên cứu triển khai giải pháp phát hiện và ngăn chặn mã độc sử dụng mã nguồn mở.**

**Ths. Nguyễn Quốc Long**

**Mô tả yêu cầu:**