ENSTA Bretagne
2, rue François Verny
29806 BREST cedex
FRANCE
Tel +33 (0)2 98 34 88 00
www.ensta-bretagne.fr

Status Report

promo 2017

February 28, 2017

Sniff Hynesim

RIGAUD MICHAËL

Contents

Introduction

The cyber security is one of the major thread of the 21th century, and attackers use techniques more and more sophisticated. So one of the most important aim for cyber security engineer is to find a way to detect and stop attacks. To do that effectively cyber engineer need to analyze cyber attack to find a way to detect them. A solution is use simulators of network and information system to reproduce as much as they want, without injury, and huge agility scenario of cyber attack. To do that, the ENSTA Bretagne has decided as many company like Thales or the DGA to use Hynesim[1].

The aim of this project is elaborate a solution to alert when a strategy of attack is spotted out. To do that, we have to create pattern of attack and use an IDS[2] to alert us. To verify the solution and create pattern as exhaustive as possible, we will use Hynesim.

To begin, we will present Hynesim and the advantages of this software. Then, we are going to present the aim of an IDS and the most popular IDS. And to finish we will present the aim of this project and the organization of the project.

[1]This software is presented in the chapter 1

[2]Intrusion detection system

Part I

Status report

CHAPTER 1

Hynesim

Firstly, we will present Hynesim. In fact, we will use this tool to create all our network and test our solution so it is important to introduce it.

1.1 Presentation

Figure 1.1: Hynesim logo

Définition 1.1 : *Hynesim*
Means HYbrid NEtwork SIMulation, is a distribute platform of simulation of information system developed by Diateam. [3]

The platform was initially developed by Diateam for DGA MI (Maitrise de l'information) to create virtual network. But now is a major project to develop information system and automatize cyber security attacks. This project has two version, an open source version and an professional version. The open source version as less option, but we will use this version for this project.

1.2 Architecture

To work, Hynesim need a server with on it the main software. This software is the virtualization part. It manage virtual machine and network.

Moreover, to see virtual machine and interact with them, users need to have the client interface. This interface can be install on a simple computer.

To add virtual machine on Hynesim, we need to create them on Virtual Box[1] or VMWare[2] and then import them on Hynesim.

[1]More information here: `https://www.virtualbox.org/`
[2]More information here: `https://www.vmware.com/`

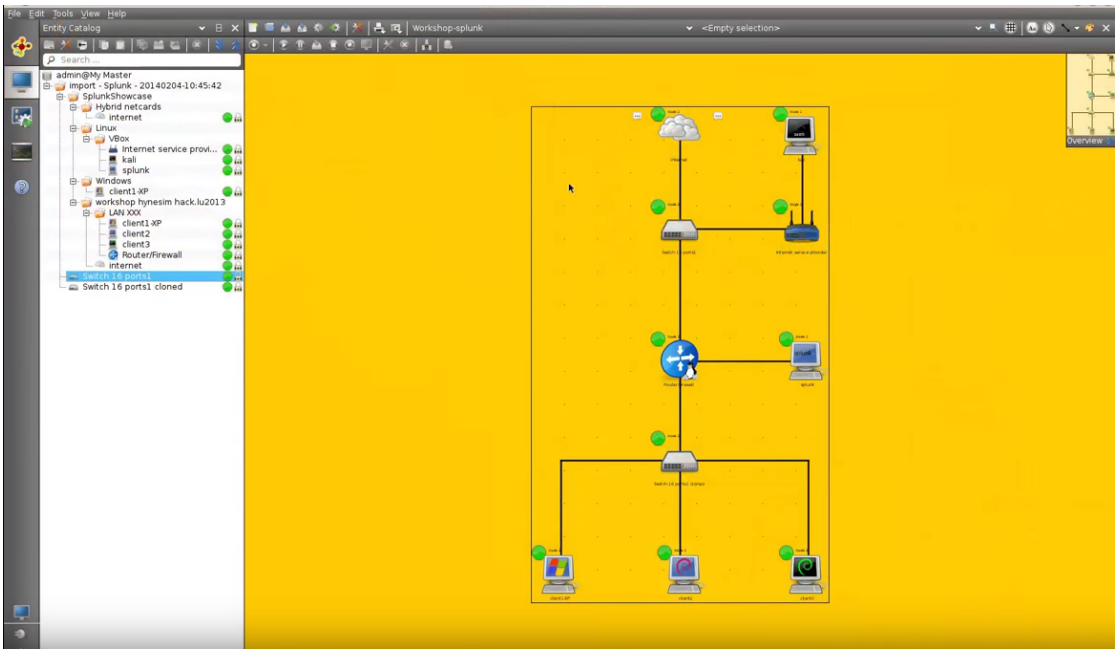

Figure 1.2: An example of an client Hynesim interface

CHAPTER 2

IDS

In this subject, we will have to create probe to detect attack. It is the aim of IDS that we are going to introduce.

2.1 Presentation

Définition 2.1 : *IDS*
An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. [2]

There is many type of IDS:

- NIDS, network IDS. They listen and analyze the network and detect attack from network packet. They are the most interesting for our subject, so this document will focus primarily on this type of IDS.
- HIDS, host IDS. These IDS are on a system and they detect intrusion inside it.
- Hybrid IDS. They are composed with NIDS and HIDS.
- IPS. They are NIDS with active functions which permit to stop attackers.
- KIDS/KIPS, kernel IDS. They are type of HIDS. They are on the system kernel. They are more effective and slower than HIDS.

In the following of this document we will talk about NIDS. But to detect attack there is also many methods.

To be efficient and IDS should have a good balance between some features.

- **Speed:** In fact an IDS should analyze packet as fast as possible, otherwise, it will behind the network traffic.
- **False alarm:** An IDS raise an alert when it detect attack. But it could raise alarm during a normal utilization. It is name false alarm. It is one of the most important feature, because at every alarm a system administrator need to analyze the alert. So in company, every alarm cost time and money.
- **Probability of detection:** It is for an IDS the capacity of detecting attack. More this probability is high more the IDS will raise false alarm. In some sensitive system, we prefer detect every attack and raise many false alarm. That depends on the system.

2.2 Detection methods

2.2.1 Misuse detection

This technique is the simplest. It use attack signature to raise alert. In fact, all attacks have a particularity, if we detect this particularity we can detect the attackers. There is three sub methods.

Pattern matching

In this technique we have a based of signature and the IDS is looking for the pattern. If the pattern match perfectly, this IDS raise an alert.

The problem is, only attacks which are in our based can be detected. So if there is a new attack (zero day), or if the attack is not perfectly the same, we can't detect it.

However, this method is much used because it is high-performance, and with this method the IDS don't raise a lot of false alerts

Dynamic pattern matching

In this techniques the IDS is also based on signature but this data base is dynamic. In other words, the IDS has the faculty of adaptation and learning. The IDS improve his data base of signature automatically.

Protocol analysis

The last sub method we will present is the protocol analysis. This technique is based on the verification of protocol. The IDS will check if flows are compliant with RFC[1] standards. It will verify parameters of packets and fields of them. An IDS can check many protocol as FTP, HTTP, ICMP, ...

The advantages of this methods is that we can detect unknown attacks in contrary of pattern matching. However, software publishers don't often respect RFC so this technique is not always very efficient.

2.2.2 Anomaly detection

This technique consists in detecting an intrusion with the analysis of the user's past behavior. So the IDS should create a profile of users from his use and raise alert when there is an event outside this profile. To create profile the IDS could use machine learning.

Advantages	Drawbacks
The IDS should be able to detect every type of attack even unknown (zero days) attacks.	This method is not reliable. Every alteration of the use create an alert
The IDS is autonomous	This method need a learning period. In fact, this method need to learn the habit of users, so we need a period without attacks
	An hackers can need only time. In fact, if the attacker arrive to create a new profile after month with his attacks, he could attack silently

[1]Requests for Comments, is a type of publication from the Internet Engineering Task Force (IETF) and the Internet Society (ISOC), the principal technical development and standards-setting bodies for the Internet.

Probabilistic method

Bayésien network is a learning machine based on probability. The IDS will create a probabilistic model and if the user and will raise an alert if the user don't respect this model.

For example, we know that in 90% of cases in an HTTP request the first parameter is GET after a connection to the port 80.

2.3 Main IDS

There is many IDS on the market. The most popular open source solution are Snort, Suricata, Bro, Fail2Ban, ACARM ... There is also some tools «all in one». It is usually OS[2] with an IDS, a tool to analyze alert, a tool to create rules,... The most popular are SELKS and ELKS. A description of SELKS is available page 15.

[2]Operating system

CHAPTER 3

SIEM

After some new discussion with my tutor, we decide to had a new component in our architecture. So we will add a SIEM to analyze all alert and take care of server's log. So we will add in this status report a part about SIEM which was not initially.

3.1 Description

Définition 3.1 : *SIEM*

In the field of computer security, security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by network hardware and applications.

CHAPTER 4

Position of the Project

4.1 Resume

This project is to automate a sniffer to detect attack. The most important fact is that our sensors need to detect a strategy of attack and not only patterns of attack. After our bibliographic studies, it is simple to understand that we will use an IDS with an anomaly detection method. We will use SELKS[1] because it is the main free open source IDS available on the market. A description of our technical choice is explain on the next section.

As it is suggest in the description of the project deliver by our professor, we also use Hynesim to automate test and simulate our solution. In this way, we will have the ability to justify the effectiveness of our solution. To do that we will run many possible attack scenarios.

4.2 Technical choice

We will firstly realize a network infrastructure on Hynesim. We will do a basic infrastructure with only one server. Then, we will put on our network a SLEKS server as a simple IDS and we will configure. We choose, to implement firstly a pattern matching method. We will also put an attacker on the network and we will realize simple attack to test our infrastructure. It is possible to see the infrastructure on the figure 4.1.

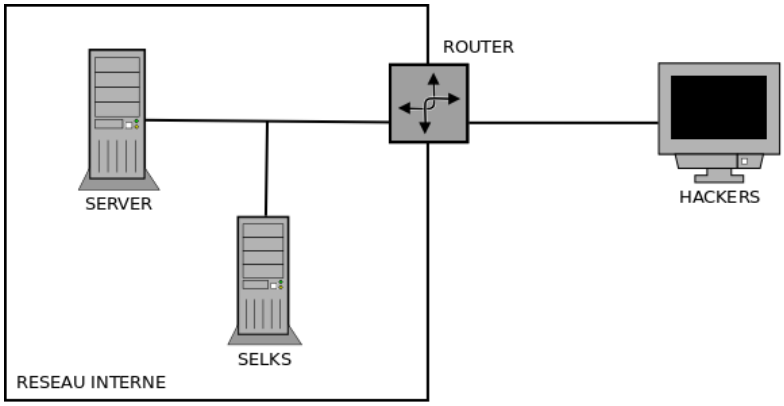

Figure 4.1: Hynesim network architecture

After this installation, we will try to improve the system. we will implement an anomaly detection method. In this way, the IDS will have the ability to detect a will

[1] A description of SELKS is available page 15

to attack. One of the most important difficulty will be to not raise alert for a normal utilization.

4.3 Forecasting organization

4.3.1 Kanban

To realize this project, we decided to use some tools to arrange our work. First of all, we decided to use a agile technique of management which name Kanban.

Définition 4.1 : *Kanban*
Kanban is a new technique for managing a software development process in a highly efficient way. Kanban underpins Toyota's "just-in-time" (JIT) production system. kanban system consists of a big board on the wall with cards or sticky notes placed in columns with numbers at the top [9]

Kanban is an inventory-control system to control the supply chain. It use a board with columns. Each columns represent a status, for example: to do, doing, done. In each column we put «notes» which represent a task. Moreover, each column have a maximum number of notes authorized.

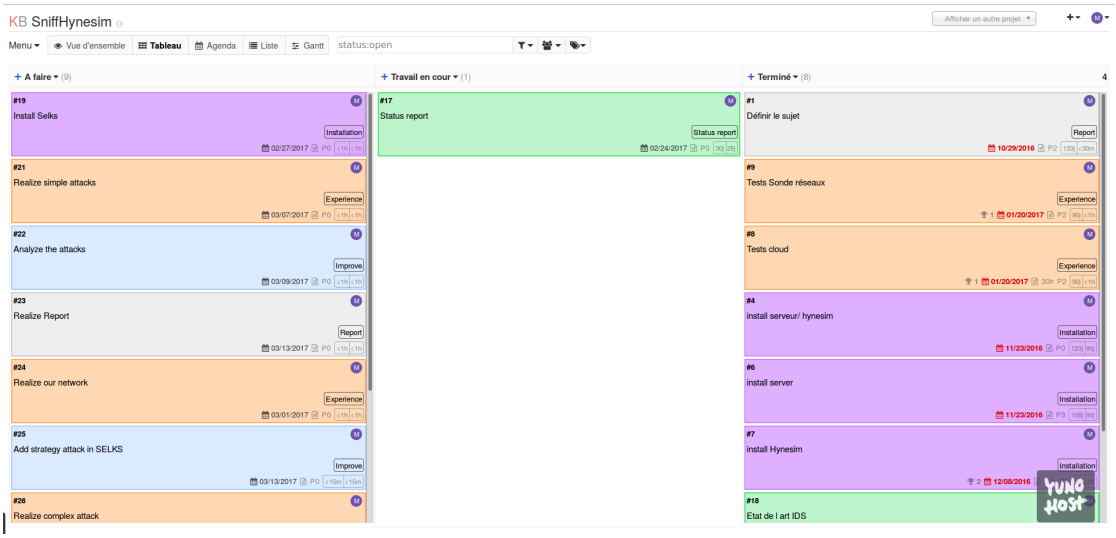

Figure 4.2: Kanboard of this project

Limiting the amount of task, at each step in the process, prevents overproduction and revels bottlenecks dynamically. In fact, with this technique it is possible to have a better overview of the project and control it dynamically.

For this project, we use Kanboard[5] self-hosted on our own Yunohost server.[2]. You can see at the figure 4.2 the kanboard of this project. Each color represent a category of tasks: blue: improvement , purple: installation, red : experience, green: status report, and grey: report.

With this tool, it is also possible to see tasks as a Grantt diagram. The figure 4.3 present our Grantt diagram.

[2] It is possible to see our kanboard at this link: `https://mic-rigaud.fr/kanboard/?controller=BoardViewController&action=readonly&token=10ea65eca908023dbcd8bc8dce75791c7a14d67912627dafaa5b71033222`

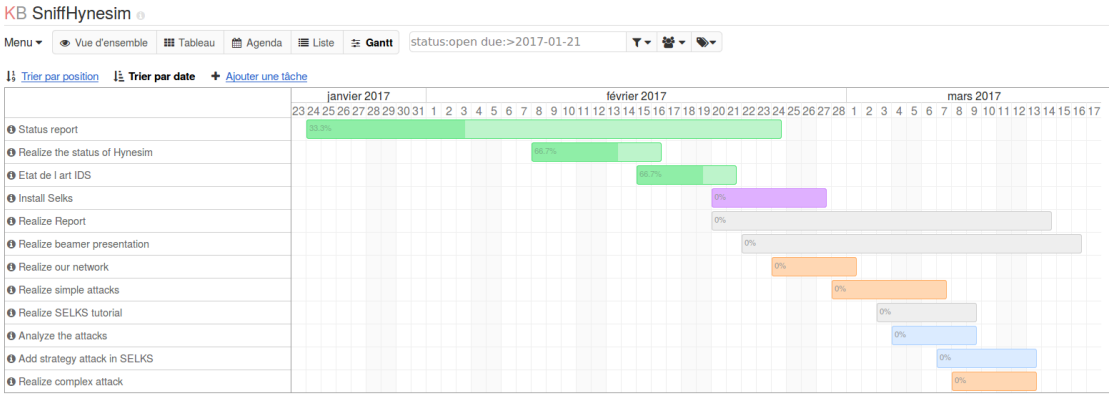

Figure 4.3: Grantt diagram of the project

4.3.2 Github

To realize this project, we also decided to use Git and Github as Git server.

Définition 4.2 : *Git*
Git is a version control system for tracking changes in computer files and coordinating work on those files among multiple people.

Git permit to control version of our work and have a real showcase of it for our tutor. The figure 4.4 is a screenshot of our Github server.

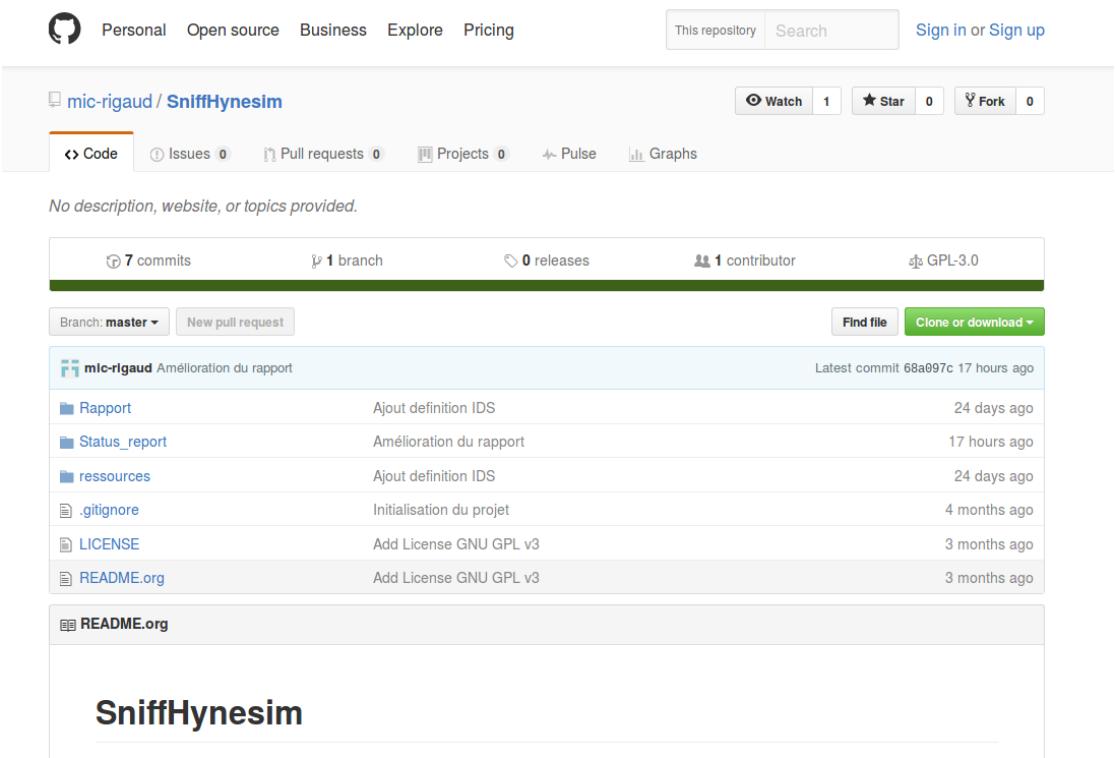

Figure 4.4: Github server

Part II

Technical study

CHAPTER 5

Hynesim installation

CHAPTER 6

SELKS

Définition 6.1 : *SELKS*

SELKS is a free and open source Debian (with LXDE X-window manager) based IDS/IPS platform released under GPLv3 from Stamus Networks (https://www.stamus-networks.com/).[10]

The SELKS ISO is both Live and Installable ISO in one. Once installed it is ready to use out of the box solution.

SELKS is comprised of the following major components:

S Suricata IDPS - http://suricata-ids.org/

E Elasticsearch - http://www.elasticsearch.org/overview/

L Logstash - http://www.elasticsearch.org/overview/

K Kibana - http://www.elasticsearch.org/overview/

S Scirius - https://github.com/StamusNetworks/scirius

So SELKS is an OS which contains many softwares. Firstly there is Suricata which is the network analyzer which raise alerts. Alerts produce by Suricata are written in a EVE file. Then Logstash traduce this file into a JSON file readable by Elasticsearch. Elasticsearch is a data base. It keep all event and permit a navigation into many millions of events almost instantaneous. And to finish Kibana propose a User interface for this data base. The figure 6.2 represents this architecture.[1]

You can see on figure 6.3, an example of the interface of kibana which give an overview of alerts. This image was extract from the Twitter of Stamus Networks.

Figure 6.1: screenshot of SELKS desktop

[1]SIEM (security information and event management) which are not developed here, are software to analyze and display event of every security tools.

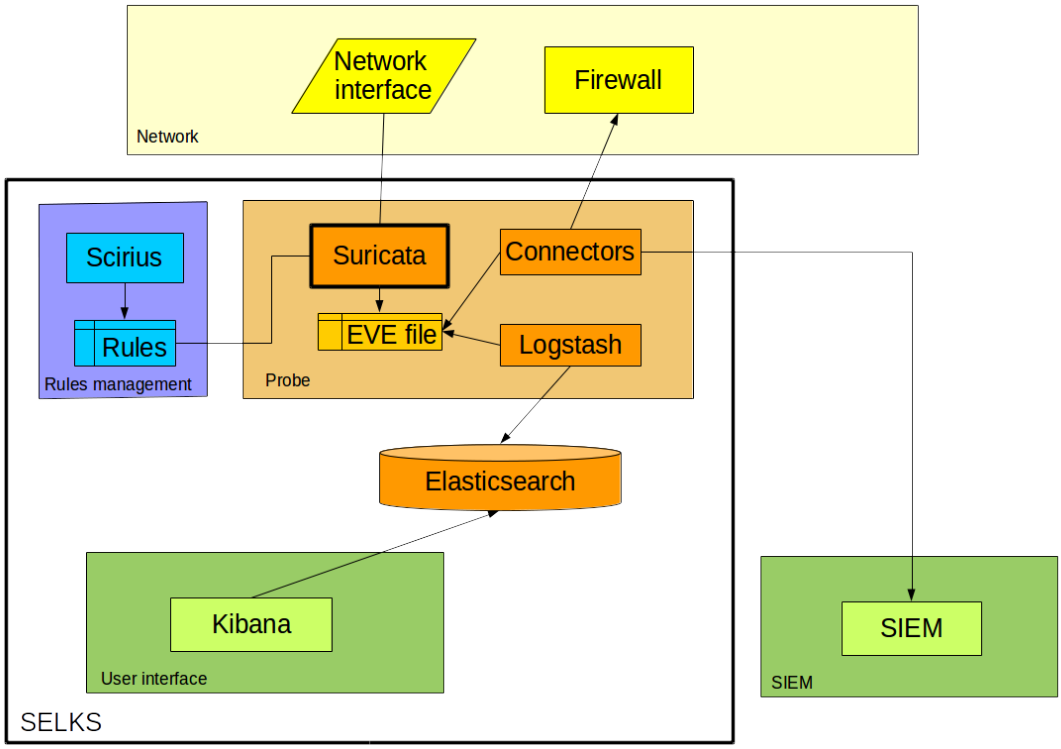

Figure 6.2: Selks architecture

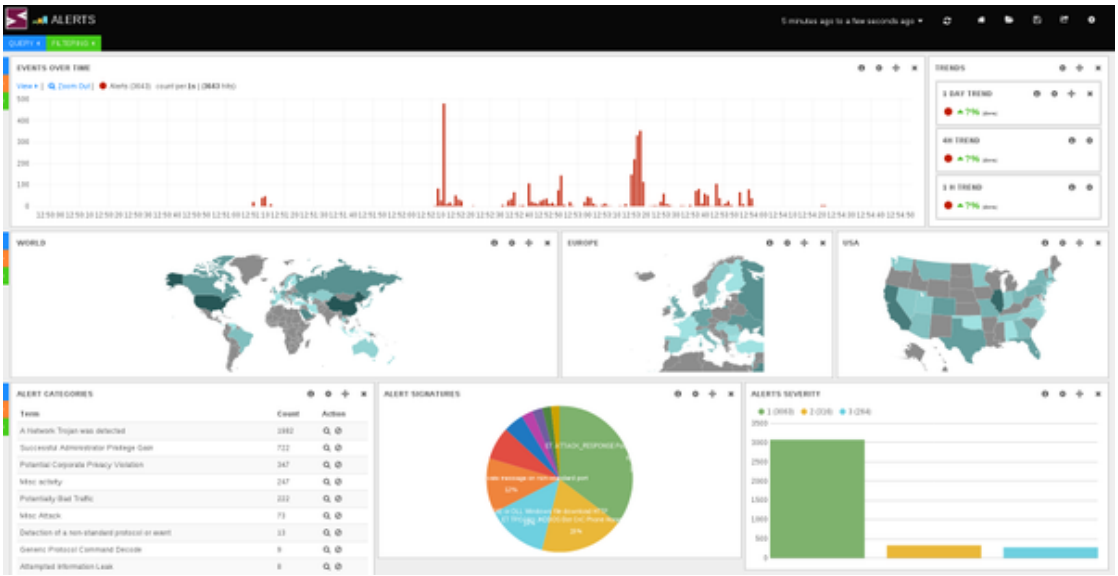

Figure 6.3: Kibana interface

CHAPTER 7

Prelude

Part III

Improvement

CHAPTER 8

Attacks

Conclusion

After this bibliographic study, to implement our network sniffer which detect strategy of attack we have to improve an IDS. In fact, IDS have the ability to detect attack with many methods. Here, we have to use an anomaly detection method to find attackers. However, as we see, this method has many disadvantages so we have to improve it.

Moreover, as it was advise by the subject we will use Hynesim. In fact, Hynesim is a very interesting tool to virtualize and simulate network. By this way, we could test under many attacks our solution to secure network.

After this study, we have only a partial view of how implement this detection method. So one of the most important work for the next two weeks will be find the way to detect strategy of attacks. It is a difficult objective but also one of the most interesting for the security of our networks.

Annexe

List of Figures

Bibliography

[1] 3ilson.org. Selks + esxi installation guide. Youtube, October 2016.

[2] Vangie Beal. intrusion detection system. Webopedia.

[3] Diateam. Hynesim. https://www.hynesim.org/.

[4] Solange Ghernaouti. *Sécurité informatique et réseaux*, volume 4, chapter 8.4. Dunod, 2013. At Ensta Bretagne code: I11 GHE.

[5] Frédéric Guillot. Kanboard. https://kanboard.net/.

[6] Jonathan Krier. Les systèmes de détection d'intrusions. Technical report, developpez.com, july 2006.

[7] Eric Leblond. Let's talk about selks. In *SSTIC conference*, June 2014.

[8] Eric Leblond. Suricata, dévoilez la face sécurité de votre réseau. *Gnu Linux Magazine France Hors-série*, 76:9, 2015.

[9] David Peterson. What is kanban. Technical report, KanbanBlog, 2009.

[10] StamusNetworks. Selks. `https://github.com/StamusNetworks/SELKS`, 2014.