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 20, 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 the 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.

[1] This software is presented in the chapter 1

[2] Intrusion detection system

Chapter 1

Hynesim

1.1 Presentation

Définition 1.1 : *Hynesim*
Means HYbrid NEtwork SIMulation, is a distribute platform of simulation of information system developed by Diateam. [2]

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.

CHAPTER 2

IDS

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

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. [1]

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.

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 we this technique is not always very effective.

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

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.

[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.

CHAPTER 3

Position of the Project

3.1 Resume

3.2 Technical choice

3.3 Forecasting organization

3.3.1 Kanban

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

Définition 3.1 : *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 [4]

Kanban is an inventory-control system to control the supply chain. It use a board with columns. Each column 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.

Conclusion

List of Figures

Bibliography

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

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

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

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