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. In this project we decide to 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[1] to alert us. To verify the solution and create pattern as exhaustive as possible, we decide to use Hynesim. It is a solution of network virtualization which permit a huge agility.

To begin, we will present Hynesim and the advantages of tis 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] Intrusion detection system

CHAPTER 1

Subject

1.1 Context

1.2 Aim

CHAPTER 2

Hynesim

CHAPTER 3

IDS

3.1 Presentation

Définition 3.1 : *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.

3.2 Detection methods

3.2.1 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

Protocol analysis

3.2.2 Anomaly detection

Conclusion

List of Figures

Bibliography

[1] Vangie BEAL. « intrusion detection system ». Webopedia.

[2] Jonathan KRIER. « Les systèmes de détection d'intrusions ». Technical Report, developpez.com, july 2006.