Cybersecurity in TIC-Scientist Network Infrastructures by Honeypots: Catching Cyber Threat Passively

Juan Luis Martin Acal[1], Pedro A. Castillo Valdivieso[1], and Gustavo Romero Lpez

Springer-Verlag, Computer Science Editorial III, Postfach 10 52 80,
69042 Heidelberg, Germany
jlmacal@correo.ugr.es
{pcv, gustavo}@ugr.es
http://www.springer.de/comp/lncs/index.html

Abstract. There is a balance between security concerns and the right to privacy. Universities have a high risk of attack as a source of valuable information. Private and scientific information have a enormous value for an attacker but the end user is worried about his privacy too. For this reason passive detection methods in cybersecurity like honeypots are the cornerstone in the defence plan. We expose the practical case of the University of Granada in the application of honeypots for the detection and study of intrusions. . . .

1 Introduction

From the earliest days, the networks have been experiencing an increasing number of attacks. Nowadays, the number of attacks increases continuously and scientist networks are a special and interesting case. There is a strong demand of security in the network and the services which are listening. On the other hand, the end users demand privacy in his network traffic. In this scene the honeypots have an important role in the detection and protection against cyber attacks.

1.1 Cyber-Space and Cyber-Threats

The cyberspace is a virtual space that wraps all types of digital communication infrastructures and the entities that use them. The hostile actions from these entities against the security and safety of the information and others entities are ciberthreats. Internet is the most popular inhabitant of this space and for years we have seen how the number and complexity of attacks against information and resources has increased. This increase is sometimes for economic, politic or military interests other by the same entities interested in exercise a bigger control over communication freedom in the cyberspace.

1.2 Scientist Networks

In contrast to the corporate networks which usually have grown from the inside to outside and which have most hosts behind the DMZ[1] , the scientist networks were born

[1] Demilitarized Zone.

with a open to outside conception but security and technical requirements due to the limited number of public IPs, were expanding private services to the intranet.

The information related to research, patents, computer and human resources is a juicy target for hostile agents. Also, the big size of the DMZ makes it prone to be attacked massively and increases the possibility of finding a security breach or hidden advance vectors of attack.

1.3 Privacy and Passive Sensors

A honeypot is a trap that exposes itself, while is scanned, probed or compromised by a hostile entity, the trap collect information about de malicious activity.
We differentiate between hierarchy and interaction in our taxonomy. The hierarchy is the complexity goes from a simple service like ssh, through a network, to a cloud. The interaction is the degree of fidelity in the response of the trap and goes from low to high. TABLE HERE.

There isn't a ideal configuration of features because is the nature of the threats and the infrastructure which we want protect, the key for a correct selection of them. In a develop software environment, high interactions is used for test a new product with ''fuzzers'' or another type of pentesting[2] tool in order to discover potential vulnerabilities. On other hand, low interaction are used like intrusion detection system, warning about activity of scans or jumping attempts from compromised internal hosts. But both have a common point, they are not intrusive with the network traffic.

2 Deployment of a Security System Based in Honeypots

The architecture of the system is divided in two front lines, one centred in the detection and collection of all attacks and another in the management of all the incident in security detected. It is in the first front line where sensors based in software honeypot works detecting non-intrusively attacks vectors.

2.1 Sensors and Collector

Sensors were deployed in different production subnets and each content honeypot software. Specifically Dionaea and Kippo which are low and medium interaction honeypot respectively. Each sensor has local data bases for save the information attacks efficiently in space while is waiting for its saved in the collector in order to keep the information by duplicate and not to increase the network traffic in case of massive scans/attacks. Obviously, in the time space between informations dumps each sensor send by telegram incidents defined by the security operator like critical.

The collector is a corporate database that feeds the incidents management system and is the core of all information analysis.

[2] Penetration Testing.

2.2 Attacks Profiles

For three years each sensor collects information of more of half million of connections. The information analysis shows that prevail external attacks for all types of the vulnerabilities emulates by the honeypots.

3 Weaknesses and Strengths of Honeypots

4 Honeypots, Elements in Hybrid Machine Learning S.I.E.M

5 Conclusions and Future Works