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 worries and 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 end user is worry 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 honeypot for the detection and study of intrusions. ...

1 Introduction

From earliest days, the networks have been experiencing an increasing number of attacks. Nowadays, the number of attacks increases continuously and scientist networks are a stage very interesting. There is a strong demand of security in the network and the services which are listening. In 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

1.2 Scientist Networks

In contrast to the corporate networks that usually have grown from the inside to outside and the most of host are behind the DMZ[1], the scientist networks were born with a open to outside conception but security and technical requirements due to the limited number of public ip, they were expanding private services to the intranet.

The big size of the DMZ make it prone to be attacked massively. Also,

[1] Demilitarized Zone.

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 Deploy of a S.I.E.M Based in Honeypots

3 Weaknesses and Strengths of Honeypots

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

5 Conclusions and Future Works

[2] Penetration Testing.