

# Honeypots as a Security Mechanism

Émerson Salvadori Virti, Liane Tarouco, Lisandro Z.  
Granville

Computer Science Institute, Universidade Federal do Rio  
Grande do Sul - UFRGS  
Porto Alegre, Brazil  
{emerson,liane,lisandro}@penta.ufrgs.br

Leandro Márcio Bertholdo, João Marcelo Ceron  
Point of Presence of the National Network of Research  
(POP-RS)  
Porto Alegre, Brazil  
{berthold,ceron}@pop-rs.rnp.br

**Abstract**—This article proves the necessary dissemination of the use of honeypots as an important security mechanism for corporative networks. This fact resulted from an experiment executed in the Point of Presence of the National Research Network (Rio Grande do Sul - Brazil), where a vast network of honeypots was implemented, totalizing more than 65000 emulated operational systems. This article analyzes the existing relationship between the source and destination addresses of the attacks directed to these honeypots. As result of this work, we have the evidence that the majority of malwares try to propagate themselves to the nearest addresses to its IP addresses.

*Keywords-component; security; honeypot; malware;*

## I. INTRODUCTION

At the beginning of the age of computers all networks had been projected with research purpose, where the main objective was to allow various kinds of connectivity between the networks that were interacting. Because of this, it was giving emphasis to the interoperability and not to the security [3].

With the development of the Internet, millions of people and institutions were now connected into a world-wide network of computers. The security come out to be important and started being the core of all the discussions at the networking community [3].

In this context, systems administrators had looked for ways to improve their network security. Diverse security mechanisms and solutions had been used more and more. Among these, the most spread out are firewalls and the Intrusion Detection Systems (IDS). However, instead of a mere passive position, researchers started trying to attract the aggressors for systems especially constructed in order to propitiate the inspection and the study of the techniques and strategies of digital attack. Thus adopting a more active position in the combat against incidents on the Internet. Such systems had been called honeypots and appeared to look after the necessity of understanding the profile of the attacks as well as detecting the last tendencies about the most explored vulnerabilities [4].

This work describes some results found in an experiment carried through using honeypots in the Point of Presence of the National Research Network in Rio Grande do Sul - Brazil

(POP-RS). In the experiment, with the objective of evaluating and measuring a type of unusual traffic also known as Background Noise of the Internet [5], it had been created honeypots to answer a great space of routed IP addressing, totalizing more than 65000 hosts being emulated.

Intrusion Detection System (IDS) is a security mechanism whose main function is to detect incorrect, malicious or anomalous activities inside a network. This tool runs constantly in the background and does not cause great interferences in the normal functioning of the network. When this mechanism detects some action that is suspicious or illegal it is capable of generating a notification to the network administrator. Also, it can try to interact with hosts, firewalls and routers to prevent or to brighten up the actual damages of the incident.

More recently, a new alternative began to be used involving the use of honeypots and honeynets [2]. In 1999, Lance Spitzner connected to the Internet a computer executing applications with vulnerabilities obviously known. The idea would be that this system would function as a honey pot (from there the name) attracting the aggressors. Spitzner was surprised, because in less than 15 minutes its host had been already compromised [2]. Then appeared the honeypot concept: a network resource whose function is to be attacked and compromised (invaded). It means to say that a honeypot could be tested, be attacked and invaded. In allowing such attacks, it is capable to register what it is happening in fact and then supply valuable information on the strategies used by the aggressors [2]. In the episode planned by Spitzner, the invader perceived that he was being monitored and erased the logs of the system. Thus, it became clear the need of an environment that could better manage and monitor the activities of the invaders and register the actions inside the honeypot in a safe way. The Honeynets had appeared then: networks that have in its architecture, sub-nets of honeypots. In these networks, the administrators could create safer environments, having the possibility to keep in different hosts all logs generated [4].

With the increasing number of networks that used honeypots in its architectures it was necessary to exchange information about the attacks and the discoveries of new resources employed in the monitoring of the invader actions. With this purpose some institutions in the world became part of the so called Honeynet Research Alliance.

The use of honeypots and honeynets improves network

security and its systems. Bruce Schneier [3], professional cryptograph researcher, founder and manager of the Counterpane Internet Security, decomposes the security in three distinct areas: prevention, detention and reaction. A honeypot will be useful in these three areas.

A honeypot will not stop an aggressor from enter into a network. But, on the other hand, all traffic originated by the intruder is registered and can be analyzed, therefore it is possible to get information that will allow, in another occasion, the prevention of the same attack. That is, honeypot does not stop attacks against the network or against one determined ports (firewall) of a system. That's why it is not like an Intrusion Detection System (IDS). However, as it is simpler to invade, it can make the aggressors invest its efforts in attacking it, instead of trying to penetrate inside strategical servers.

As for the detection, the profits are more considerable. The reason of this is simple: if the complementary tools, such as networks IDS, were flooded with great flows of traffic, they will have difficulties in processing them. Separating the useful traffic out from the malicious traffic is some times very complicate. One of the strategies of crackers consists of occupying a IDS, in order to generate a great number of alarms. These false positives (false alarms) and the filtering of the useful data continue to be issues where the IDS need to be improved. A honeypot does not have this problem, because all traffic originated or destined to the emulated hosts by default suspected /hostile. There should not be traffic for such systems because they are not announced or registered in DNS. Although this does not mean that the false positives are impossible, the possibility to happen is far less of that using a network IDS.

Finally, the reply (or reaction) is a question that needs to be verified with care. The detection does not have any value when there isn't an adequate reply. Through the analysis of logs generated by honeypots the security team can determine technical ways for the protection against the explored vulnerability and even looking for the identification and the legal punishment of the aggressors.

To study the behavior and the amount of hostile traffic in the network, one honeypot was installed at POP-RS, having used the honeyd software [8]. This honeypot is said to be like "low interactivity", therefore it only emulates the behavior of several operational systems without giving access to the real operational system of the computer where the software is installed.

## II. HONEYD CHARACTERISTIC

Honeyd, used by the honeynet project, makes it possible to create virtual hosts inside a network, simulating different operating systems and services. Aiming at the increased security and its allegiance, the virtual simulated operational systems is made at the network level considering the TCP / IP stack. Another resource of honeyd is the possibility of a station to answer for multiple IP addresses. That is made through the use of some specific functionalities: arpd tool [10], and the packages manipulation libraries (Libnet and Libcap) [9].

Also it is possible to simulate the existence of a complex computer network, through the virtual interconnection of these emulated systems, producing a structure with routers and stations on different subdomains, as for example the structure represented in fig. 1.

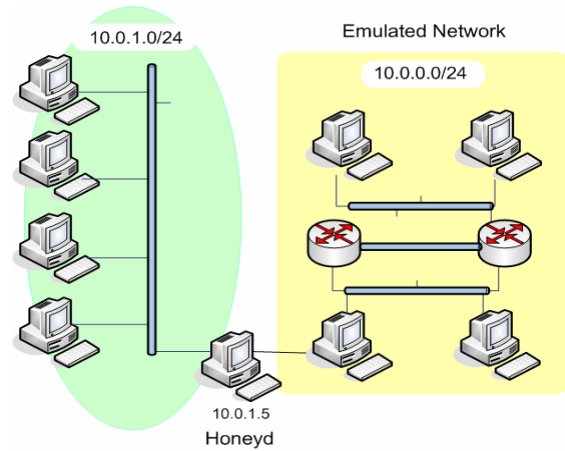


Figure 1. Honeyd Capabilities

The main functionalities of the Honeyd, the figure above shows a honeynet structure using this software. For this example, invalid IP addresses had been used (block 10.0.0.0 /8). However, in the actual system tested, valid IP addresses had been used. In the presented case, only 5 actually exist: 4 desktops and a computer operating with Honeyd. Although this machine to possess the 10.0.1.5 address, it is capable of answering to all connections directed to any existing IP in the block 10.0.0.0 /24. In the described configuration shown in the picture, from 255 available addresses in the block, only 6 had been used: 4 to simulate hosts and two to simulate routers. In this configuration it was still opted to emulate a network with 10% of package lost between the router R1 and the router R2 aiming at giving the simulation a bigger realism.

For the objectives of this project, the main desired characteristic was the possibility of the system to register any attempt to access the IPs addresses simulated by honeypot. Doing this, putting the honeypot facing the Internet, it could be verified the access number to determined ports and therefore evaluate the most explored vulnerabilities.

## III. IMPLANTATION AND ANALYSIS OF THE HONEYPOTS RESULTS

The use of honeypots of low interactivity initially was created with the objective of verifying the unusual behavior from machines that are part of the costumer's networks from this Point of Presence (POP-RS). Doing this, it was desired to detect attempts of connections from these computers to the honeypots, trying to detect infections as soon as possible, preventing big damages caused by the contaminations in the computers mentioned.

Being based on the "principle of the proximity", displayed for Thorsten Holz in its thesis "New Fields of Application will be Honeynets" [1], the majority of malwares (Virus, Worms and Trojan Horses), tries to attack targets next to its

addressing space (same subnet or class B). This indicates that the closer to a contaminated machine the bigger the possibility of suffering an attack from the beginning of the contamination (reference proximity). Considering this, a structure of supernets was proposed using great IP blocks allocated for many institutions but without real use. With the authorization of the owners of all the IP addresses, all these networks had been announced using BGP4 and directed to one honeynet. This honeynet was able to answer an addressing space equivalent to a class B (65536 addresses IP) This experiment was run during one whole week (December 2005).

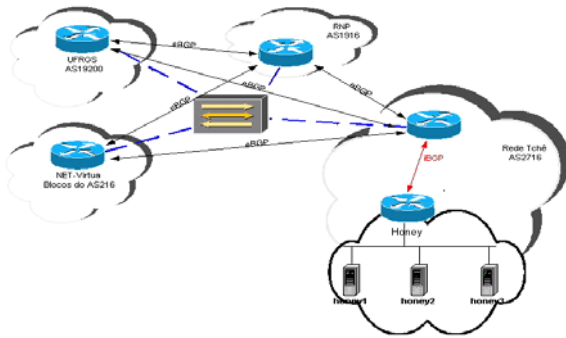


Figura 2. Structure of the Network

#### IV. REACHED RESULTS

Verifying of the obtained data, an important and unusual activity was detected. This generated countless difficulties against the implantation of the initially considered project. Hard situations as the lack of processing in the responsible router for the BGP announcement due to the high volume of packages per second (fig 3) with the RAM memory lack (due to the ARP table of the networking devices), had created the necessity of configuring small adjustments in the solution initially implemented.

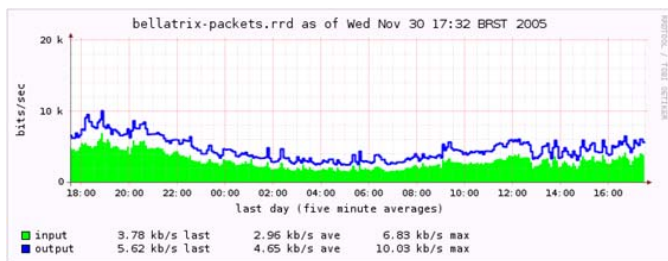


Figure 3. Number of packages per second for honeypots IP addresses

Amongst the obtained data, the noise verified in these unused addresses surprised in all senses, such as its volume of bits per second transferred, that reached the cipher of Megabits per second (fig 4). It is stand out that this traffic is considered noise because it simply shouldn't have to ever exist.

Inside of super nets announced by BGP, they were blocks of academic institutions before-CIDR (addresses IPV4 that did

not have 200 or 201 as initial octet) and after-CIDR. Also it had been used addresses from "domestic" blocks (Cablemodem), attributed to the companies and academic blocks. Each one of these blocks is represented according to Table 1.

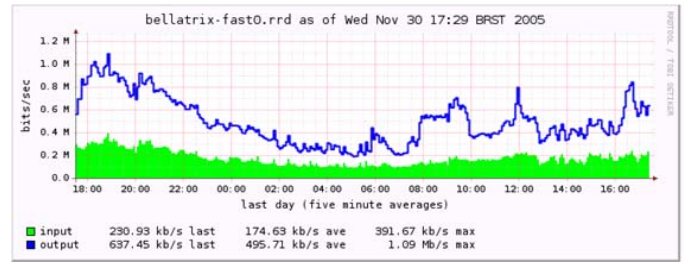


Figure 4. Traffic Volume about not used Ip addresses

The data contained in Table 1 demonstrate the discrepancy among the number of access attempts to honeypots in the different networks. This can be explained by the description of the security incidents of each networks, by the number of hosts attached to these class B networks and the number of machines with malicious behavior that could be connected to these networks.

Another excellent point that proves the hypothesis of the proximity for reference is proven in Figure 6, where it can be verified that the addresses sources of the attempts of accesses to honeypots tend to be inside of the same country. That is, they tend to belong to a block of addressing next to the IP destination of these attacks.

TABLE 1. AVERAGE OF THE DAILY ACCESS ATTEMPTS SEGMENTED BY ADDRESS CLASS

Address Space	Total per day	Total scans per IP address	Scans mean per IP per hour
Academic /18	32.145.835	1977,48	82,39 1,4 access/min
Comercial /18	32.145.835	236,16	9,84 0,16 access/min
Academic /17	3.838.989	121,23	5,05 0,08 access/min
Cable modem /20	3.941.556	1272,85	53,4 0,89 access/min

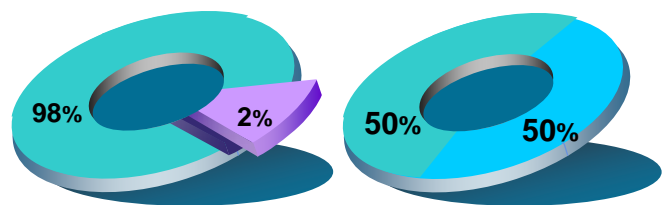


Figure 5. Address Source Origin

Figure 5 still demonstrates the results of the source addresses of the accesses to honeypots of a comparative institution that uses a block pre-CIDR to the other institution that has its IPV4 addresses of the block 200.0.0.0 /8 inside (attributed to Brazil). As it can be perceived, for the academic institution, it has a bigger trend of suffering illegal attempts of access coming from the exterior and not coming from Brazilian addresses.

Figure 6 evaluates the proximity among the source IP addresses of the accesses and the IP addresses emulated by honeypots. A comparison was made among the address involved in the communication with the intention to verify the proximity between this IPs.

As it can be noticed, there is a tendency that the illegal access attempts origin is next to the aimed destinations. For the "academic/18" block we had almost 5.000.000 accesses coming from same class B subnet throughout the monitoring week. These accesses numbers to the honeypots are also influenced by the degree of security of the neighboring networks.

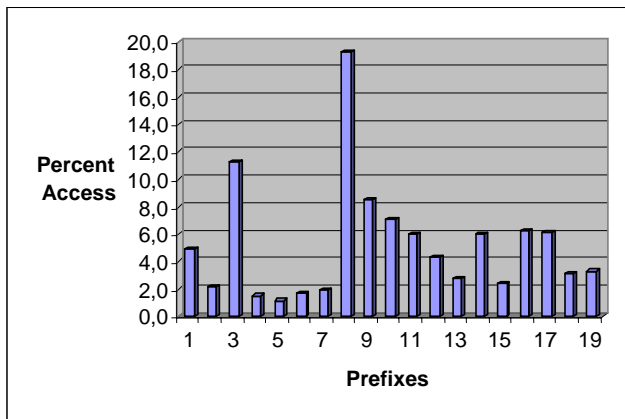


Figure 6. Address IPs proximity

### V. FUTURE WORKS

As a future work we will contact some of the POP-RS customers in order to be able to install honeypots inside their address blocks. We believe that having honeypots answering smaller IP blocks or answering unique IP address inside the institution, there will be a greater probability for an illegal access attempt coming from the IP blocks of the same institution.

### VI. CONCLUSION

This work has its importance proven in the analysis of the results of the implantation of a great architecture of honeypots in the dependences of the POP-RS. To all, they had been emulated the equivalent to a classroom B of IPv4 addressing, that is, approximately 65536 virtual computers. Each one of these computers had its IP address (valid) belonging to the addressing space of some institutions hardwired to the Point of Presence of the National Research Network of the Rio Grande Do Sul - Brazil.

The answers obtained on this work had been surprising. Since they had demonstrated that each computer hardwired to the Internet is displayed to a great volume of malicious attempts of access. For the verification of IP source addresses of the packages, the hypothesis of the proximity for reference could still be proven, where, the majority of malwares looks for for vulnerabilities in IPs addresses next to the addressing space which they belong. Hence this paper shows that the use of honeypots in a local network is a valuable resource due to the many possibilities of being accessed by a computer controlled by a malware or a cracker.

### REFERENCES

- [1] T. Holz, "New Fields of Application for Honeynets" Diploma Thesis, Department for Computer Science of Aachen University, Germany, 2005
- [2] L. Spitzner, Honeypots: Tracking Hackers. Addison-Wesley, 2003. [Online]. Available: <http://www.tracking-hackers.com/book/>
- [3] B. Schneier. "Secrets and lies: digital security in a networked world", Willey & Sons , 2000.
- [4] Dornseif, M.; May, S.: Modelling the costs and benefits of Honey-nets. In: The Third Annual Workshop on Economics and Information Security (WEIS '04). 2004. Minneapolis.
- [5] E. Linehan, "Internet Worm Detection as part of a Distributed Network Inspection System". MSc thesis Univerity of Dublin, 2004.
- [6] Honeynet Research Alliance, <http://www.honeynet.org/>, 2006
- [7] Brazilian Honeypots Alliance - Distributed Honeypots Project, <http://www.honeynet.org.br/>, 2006
- [8] N. Provos, "Honeyd - A Virtual Honeypot Daemon," in 10th DFN-CERT Workshop, Hamburg, Germany, February 2003.
- [9] S. McCanne, C. Leres, and V. Jacobson, "tcpdump/libpcap," <http://www.tcpdump.org/>, 1994.
- [10] N. Provos, Arp Deamon, Arpd Source, <http://www.citi.umich.edu/u/provos/honeyd>, 2004