

Honeypot - a weapon for cyber combat

Paulo V. Monteiro

Assistant Professor at ISTECS Porto – paulo.monteiro@my.istec.pt

João Emílio Almeida

Assistant Professor at ISTECS Porto – joaoalmeida@my.istec.pt

Diogo Cunha

diogo.cunha.20349@my.istec.pt

Student at ISTECS-Porto

Diana Rodrigues

diana.rodrigues.743@my.istec.pt

Student at ISTECS-Porto

Abstract: *In this article the honeypot concept is presented, starting with its features, advantages, and disadvantages. High and low interactivity honeypot types are detailed and compared. An open implementation is provided by means of an example, showing how honeypots can be used as an asset defending against cyberattacks.*

Keywords: *Honeypot; Hacker; Computer Security; Cybersecurity; Countermeasures; Open code; T-Pot.*

1. Introduction

Computer security has been a key priority for IT technicians and managers, at least, since 1967, when Willis Ware addresses this issue, including cultural, political, and social concerns [1]. Since those early computation days, the evolution of information and communication systems technology led them as being the target of numerous attacks. The widespread of the Internet has made this challenge even more worrisome. The year 2022 will be remembered in the Portuguese cybersecurity history as one of the most affected by cyber-attacks, with impacts both on private and public organizations, never seen before. Health institutions, such as hospitals and clinical analysis centers, were the target of cyber-attacks, which left them unable to assist populations [2]. One major private mobile company was put off grid, for hours. The disruption made took several weeks to normalize

its service [3]. And one of the main press and TV network of Portugal had a major attack in the first days of the year, causing huge damage to its reputation [4]. As the year progresses, and it's not even halfway through yet, a large business group, linked to retail, has seen most of its servers go out of order [5].

With so many and important cyber-attacks, it is natural that the topic of cybersecurity is on the agenda.

This article presents one counter-weapon to try to traceback, seek and identify the individuals or groups responsible for these attacks.

2. Honeypot

One of the first documented cases of the use of a honeypot in computer security began on January 7, 1991. Cheswick, while working at AT&T Bell Laboratories, observed a criminal hacker infiltrating the password files to obtain a copy. Cheswick and his co-workers came out with a trap designed to allow the hacker to enter the system, but into a safe zone, like a “prison” in so that they could observe the intruder for a period of several months. In this way, the honeypot was created, which revolutionized computer defense to this day [7].

The honeypot is like a mirror of a real computer system, with applications and data, having a single purpose, to divert the attention of hackers long enough for them to be observed and eventually caught.

It accepts any required communication request, pays attention to the most common service ports

and simulates the communication with the attacker through different protocols, such as TCP, UDP, FTP and VoIP, among others.

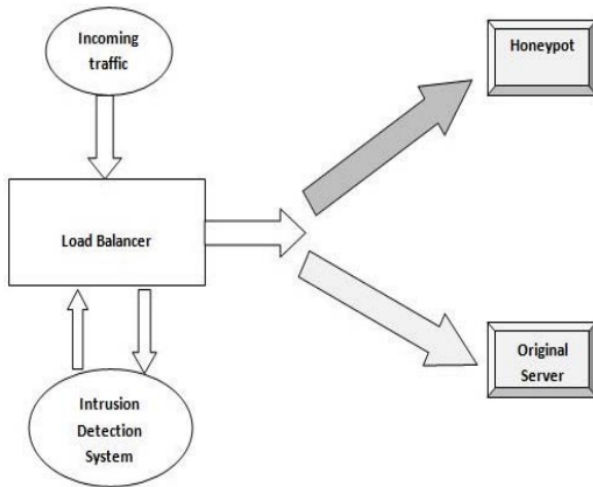


Figure 1 – Flow of packets through IDS in Honeypot[8]

The honeypot becomes attractive to criminals when security vulnerabilities are deliberately built in. A honeypot may, for example, have unprotected files or weak passwords. The honeypot method is not exactly an offensive method, but an information collection method. In a honeypot, in addition to being able to obtain information about the attacker, it also makes it possible to improve computer security and understand existing threats consistently.

3. Honeypot Types

3.1. High interactivity

These are servers that offer real services installed like any other server in the organization. These can be mail servers, file transfer servers or access to a command shell. Care must be taken to ensure that this server is perfectly isolated from the rest of the network, so that it can prevent an attack from succeeding and gain access to the network. The great advantage of highly interactive honeypots is the fact that it will be more difficult for the attacker to perceive that he is falling into a trap, as the information generated is extremely detailed.

In this type of honeypot, it is possible to implement its own tools, such as an http service

that obtains the fingerprint of the attacker and consequently, uniquely identifies the computer of origin of the attack.

3.2. Low interactivity

Unlike high-interactivity honeypots, low-interactivity honeypots simulate all their services, that is, the attacker will never have access to the real system.

As the intruder does not interact with the real system, this type of honeypot is very advantageous when it comes to security, because as it is a simulator, the intruder does not have his computer compromised or the network he is on. However, if there is a hacker with more skills and experience, it is possible that he will realize the trap and, with that, retreat from the attack, losing the possibility of obtaining information about it, but the attack is registered [9].

The purpose of low-interactivity honeypots is to detect the attack so that it is possible to take the necessary measures to prevent any damage from being caused to the system. As the level of interaction is low, the information captured is limited and, due to this, it is mostly used by organizations to reduce security risks.

3.3. Other types of Honeypot

Besides the classification of honeypots based on the activity of the attacker, there are other types, such as: production honeypots, research, pure and sugarcane. Their main differences reside on the design criteria used and the approaches to their implementation [10].

3.4. Comparison between low and high interactivity Honeypot types

Each type of honeypot has its function. Low interactivity ones are more focused on security protection and reconfiguration, and high interactivity ones are used to obtain information.

Table 1 - comparison between the characteristics of the two types of honeypots.

Characteristic	Low Interactivity	High Interactivity
----------------	-------------------	--------------------

Installation	Simple	Complex
Manutenção	Simple	Complex
Risk of compromise	Low	High
Information	Essential	Detailed
Attacker has access to the real operating system	No	Yes
Applications and services offered	Emulated	Real

Table 1 summarizes a comparison of the characteristics of the two types of honeypots.

4. Pros and cons of Honeypots

4.1. Advantages

As all traffic directed to a honeypot is from malicious actions and knowing that it does not spontaneously interact with the outside, the reduction in the occurrence of false positives is very large. This facilitates the identification of patterns, such as similar IPs, making it possible to clean up the network.

Network utilization is low and because few resources are used, minimal hardware is required. They can also be used as a basis for personal training in computer security, allowing to identify and act in the best way against attacks.

4.2. Disadvantages

A honeypot can only identify threats that are directed at it, which means that if the attack is not carried out, it does not mean that it does not exist, so every precaution is necessary.

There is, in the worst-case scenario, a possibility that the honeypot could be used as an attack on its own, which is why honeypots cannot replace other security systems such as firewalls and must be kept isolated from the real system.

5. Open-source example

T-Pot is an open-source development that combines low and high interactivity honeypots in a single system. Its implementation is very simple and allows us to simulate network services such as Android ADB, SSH, FTP, MSSQL, HTTPs, among others.

Ideally, you should create a custom honeypot with the same services that the company has, however if there are no resources to develop your own system (ideal for freelancers), T-Pot is the fastest and easiest way to implement a honeypot.

One of the advantages of T-Pot is that it provides a graphical interface so that it is possible to visualize the information generated more easily.

In Figure 1 it is possible to see an example of a hon "An Evening with BerferdIn Which a Cracker is Lured, Endured, and Studied" (PDF). cheswick.com. Retrieved 3 Feb 2021.eyopot graphical interface.



Figure 2 – Graphical interface of a honeypot

6. Conclusion

Honeypots are a good way to get information about hackers and other cyber criminals, conducting cyber-attacks, how they behave, and which strategies they use. They are also great for identifying possible flaws in the system and establish mitigation procedures or counter-measure improvements, to be implemented in computer systems.

Albeit this safety and security approach to build defense systems is considered a good technique to improve the safety level and help detect possible security flaws, it must be considered as part of a larger strategic plan. As such, honeypots are just another weapon to be used for the safety and security of information systems to fight against cyber criminals .

7. References

- [1] Misa, Thomas J. (2016). "Computer Security Discourse at RAND, SDC, and NSA (1958-1970)". *IEEE Annals of the History of Computing*, 38 (4): 12–25. doi:10.1109/MAHC.2016.48. S2CID 17609542.
- [2] The Portuguese News (2022). "Hospital target of cyberattack". <https://www.theportuguese.com/news/2022-04-26/hospital-target-of-cyberattack/66614> consulted on May 7, 2022.
- [3] Silicon Republic (2022). "Targeted cyberattack takes out Vodafone Portugal". <https://www.siliconrepublic.com/enterprise/vodafone-portugal-cyberattack>, consulted on May 7, 2022.
- [4] Cybernews (2022). "Major Portuguese media conglomerate hit by ransomware". <https://cybernews.com/news/major-portuguese-media-conglomerate-hit-by-ransomware/>, consulted on January 15, 2022.
- [5] Reuters (2022). "Portugal's largest retailer's websites, some services hit by hackers". <https://www.reuters.com/technology/portugals-largest-retailers-websites-some-services-hit-by-hackers-2022-03-30/>, consulted on May 7, 2022.
- [6] Szor, Peter. *The Art Of Computer Virus Research*. Addison Wesley Professional, 2005.
- [7] Cheswick, Bill (1992). "An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied" (PDF). <http://cheswick.com/ches/papers/berferd.pdf> Retrieved 3 Feb 2022.
- [8] Singh, R. K., & Ramajujam, P. (2009). *Intrusion Detection System Using Advanced Honeypots*. arXiv preprint arXiv:0906.5031.
- [9] Nicomette, V., Kaâniche, M., Alata, E., & Herrb, M. (2011). Set-up and deployment of a high-interaction honeypot: experiment and lessons learned. *Journal in computer virology*, 7(2), 143-157.
- [10] Mokube, I., & Adams, M. (2007, March). Honeypots: concepts, approaches, and challenges. In *Proceedings of the 45th annual southeast regional conference* (pp. 321-326).