CT4001NI Communication Engineering

Report Title

Honeypots

Assessment Weightage & Type

10% Individual Coursework

2021 Spring

Student Name: Sujen Shrestha

London Met ID: 20049250

College ID: NP01NT4S210105

Assignment Due Date: May 30, 2021

Assignment Submission Date: May 31, 2021

Word Count: 3052

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a marks of zero will be awarded.

Table of Contents

List of Tables

List of Figures

Acknowledgements

I would like to thank all my lecturers of the module who have guided me to create this report. They have encouraged me a lot to boost my research, critical thinking and report writing skills. Without their support, I would not have been able to write an in-depth report about such a topic. Also, I am thankful to all the online websites, books and journals which have provided me with the necessary information to create this report. All of the sources which have helped me learn about this topic are mentioned in the reference section at the end of this document. I am truly grateful to above mentioned people and others who inspired me to develop my research and critical thinking skills. Lastly, I would like to thank Islington College and London Metropolitan University for giving me an opportunity to demonstrate my report writing skill.

Summary

A group of computers connected to a network is constantly at the risk of being attacked by various malicious users. These intruders have certain motives which is why they attack specific organizations. To penetrate the security of an organization and get access to their data, the intruder uses certain tools and methods which enable them to alter, misuse or destroy the data. In order to prevent this kind of malicious activity, there are various tools which help to act as a security barrier and restrict the intruder from causing severe damage to the data and reputation of the company. A honeypot is a tool which allows an organization to prevent such kind of illicit activity. The honeypots are set-up by mimicking all the files with fake information into a different server. The data is managed and configured in such a way that the intruder believes it to be highly confidential and sensitive information. Thus, the intruder tries to hack the fake system using various methods, tools and techniques. All the activity of the intruder is monitored and logged by the honeypot and an alert is sent to the organization as soon as it detects the unauthorized user accessing the system. Therefore, the honeypot prevents data in the actual system from being compromised and acts as a security barrier to protect the system against malicious intruders.

1 Introduction

A honeypot is a system created to lure malicious intruders to a duplicate system so that they can’t tamper the elements of the main system. It is generally used in the Intrusion Detection System (IDS). (Titarmare, et al., 2019) Honeypots respond to a range of requests and commands from a malicious user depending upon their type and are located on a network where the intruder is most likely to find it. Honeypots are extremely deceptive; they appear to be something they are not which entices the intruder to interact with it. This interaction is monitored and logged, and the system administrator is triggered with an alert of malicious activity as soon as it appears. (U.S Department of Health and Human Services, 2020)

Honeypots are versatile in nature; they are very flexible and can be used in various different situations. For example, honeypots can be used to prevent attacks similar to the function of firewalls. It can be used to detect attacks like an Intrusion Detection System (IDS. Likewise, it can be used to collect and examine automated attacks of worms, trojans or other malicious threats. Honeypots have the potential to investigate the activities of the hacker community by capturing the keystrokes or messages of attackers. So, the usage of honeypot is decided by the user according to their requirements and what they are trying to achieve. (Spitzner, 2002)

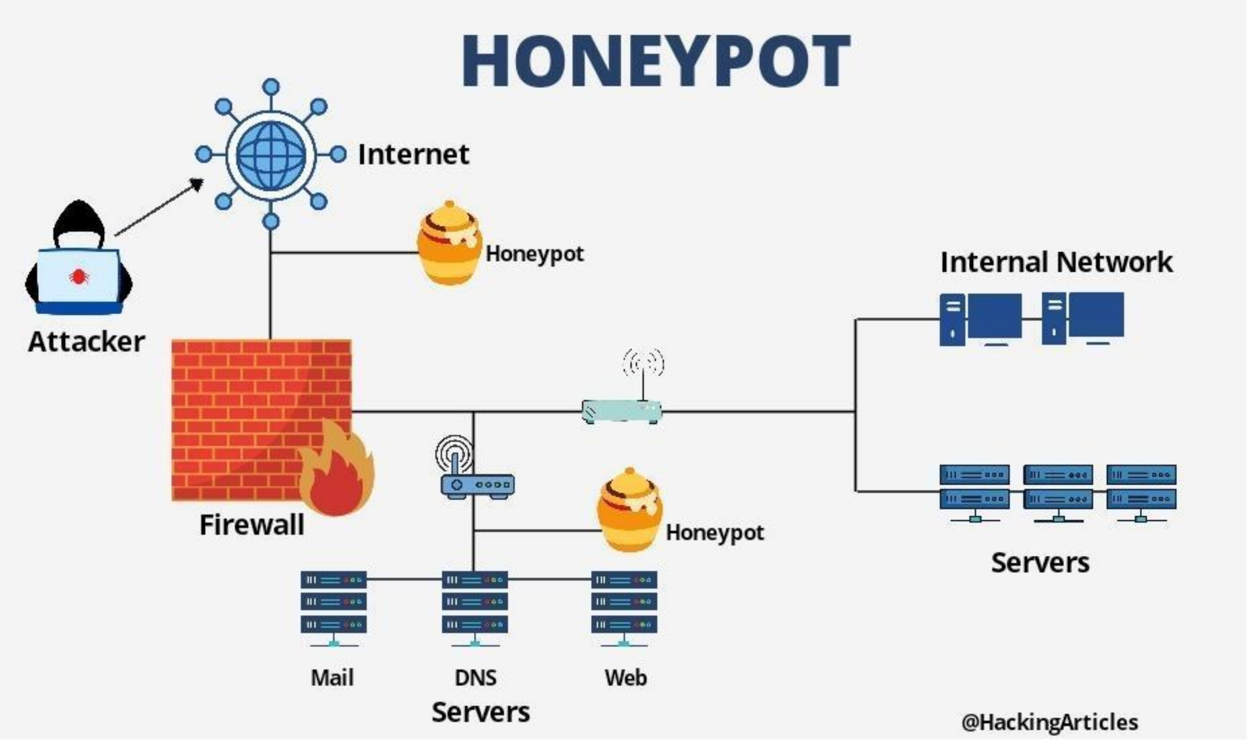

Figure 1: Honeypot system

(Chandel, 2020)

1.1 A brief history of Honeypots

Honeytokens have been used in the computing system even before the terminology originated. A honeytoken is a fake record deliberately placed in a legitimate database which can be accessed only by malicious queries or intruders. In the late 1980s, Clifford Stoll brought up an idea of planting interesting data in suitable places to grab the attention of blackhat hackers. He found a hacked computer and wanted to learn how the intruder had gained access to it. So, he developed a lookalike environment to keep the attacker engaged so that he could track the connection and find out the intruders' origin and how they got in. (Barfar & Mohammadi, 2007) Likewise, some key events in the history of honeypots are summarized below:

- 1990/1991 - First public works documenting honeypot concepts—Clifford Stoll's The Cuckoo's Egg and Bill Cheswick's "An Evening With Berferd."

- 1997 - Version 0.1 of Fred Cohen's Deception Toolkit was released, one of the first honeypot solutions available to the security community.
- 1998 - Development began on CyberCop Sting, one of the first commercial honeypots sold to the public. CyberCop Sting introduces the concept of multiple, virtual systems bound to a single honeypot.
- 1998 - Marty Roesch and GTE Internetworking begin development on a honeypot solution that eventually becomes NetFacade. This work also begins the concept of Snort.
- 1998 - BackOfficer Friendly was released—a free, simple-to-use Windows-based honeypot that introduced many people, including me, to honeypot concepts.
- 1999 - Formation of the Honeynet Project and publication of the "Know Your Enemy" series of papers. This work helped increase awareness and validate the value of honeypots and honeypot technologies.
- 2000/2001 - Use of honeypots to capture and study worm activity. More organizations adopting honeypots for both detecting attacks and for researching new threats.
- 2002 - A honeypot is used to detect and capture in the wild a new and unknown attack, specifically the Solaris dtspcd exploit.
  (Spitzner, 2002)

2 Features, Design and Specifications

2.1 Features

The features of honeypots which make them useful to an organization are:

- It prevents attacks and malicious activity on the network.
- It enhances the attack detection and response time.
- It collects the intrusion behaviour profiles, system behaviour and attack methods.
- It records the activity patterns of the intruder.
- It almost never generates false alarms.
- It can be set-up physically or by using various virtual machine softwares. (Titarmare, et al., 2019)

2.2 Design

The honeypots are designed to entice the intruders and keep them occupied for as long as possible to understand the kinds of methods they use to hack the system. Based on the nature of the organization and its needs, there are four types of honeypots on the basis of their level of interaction. Each has their specific purpose and are used in specific types of organizations. They can be described as:

Interaction level	Installation and configuration	Deployment and Maintenance	Information Gathering	Level of risk
Low	Easy	Easy	Limited	Low
Medium	Involved	Involved	Variable	Medium
High	Difficult	Difficult	Substantial	High
Pure	Difficult	Difficult	Extensive	Very High

Table 1: Honeypot interaction trade offs

i. Low Interaction Honeypots:

The low interaction honeypots are the most basic form of honeypots. It runs on an emulated environment and is mainly used for detecting unauthorized scans or connection attempts. The type of information that low interaction honeypots provide are mainly the time and date of the attack, the source and destination IP address and the source and destination port of the attack. (Spitzner, 2002) It is very easy to install and maintain as no complex or valuable information needs to be managed and possesses the least risk compared to the other type of honeypots. Honeyd is an example of low interaction honeypots. (Titarmare, et al., 2019)

ii. Medium Interaction Honeypots:

The medium interaction honeypots provide greater functionality when compared with the low interaction honeypots and lesser features when compared with high interaction honeypots. It also runs on an emulated environment and is mainly used to capture the payloads from worms for future analysis. Since the attackers have greater interaction with this type of system, various structures must be developed to make sure that the attackers cannot harm other systems. Also, various precautions must be taken so that its increased functionality is not exploited by the intruder which may grant them access to the real operating system. (Spitzner, 2002) Mwcollect, honeytrap and Nepenthes are some of the examples of medium interaction honeypots. (Titarmare, et al., 2019)

iii. High Interaction Honeypots:

The high interaction honeypots provide greater functionality compared to low and medium interaction honeypots but less compared to pure honeypots. It runs on an operating system where the functionality is not restricted or emulated. The information that high interaction honeypots provide is of immense value. It helps us to learn about new tools, find out new vulnerabilities in operating systems or applications and know how the black hats communicate among one another. This type of honeypots poses a very high risk for the organization as the attackers have a fully operational system to interact with, which they can use to capture production activity, attack other systems or perform various other malicious activities. The high interaction honeypots are generally kept inside a regulated environment, like beneath of a firewall. Such an architecture is very complex to maintain and deploy whilst making sure the attacker does not notice they are being monitored. (Spitzner, 2002)

iv. Pure Honeypots:

The pure honeypots provide higher functionality than the other honeypots. It is a full-scale system running on various servers. The data stored in it is also fake but it is created in such a way that it looks very confidential and sensitive. It completely imitates the production system which deceives the intruders in thinking that it is a real system. It has a lot of trackers and sensors attached to it which enables the organization to monitor the activities of the intruder continuously and learn their hacking methods. It is also very difficult to maintain and configure but it provides extensive data.

2.3 Specification

There are many types of honeypots. Some of them don’t require much resource or manpower to maintain and configure. While others may require a substantial amount of time and resources to operate without risking the organization. So, honeypots can be used by organizations based on the size of the organization and what type of data they store. The various types of honeypot software and their requirements are given below:

1. Low-interaction honeypot software:

BackOfficer Friendly (BOF) is a low interaction honeypot which is developed to function on Unix or almost any Windows system like Windows 95, Windows 98 and so on. Similarly, Specter is another low interaction honeypot like BackOfficer Friendly, however it provides additional features like the ability to emulate OS. This service can run on

Windows NT SP6A, 2000 SP1 and Windows XP. It requires at least a Pentium II 450 MHz processor and 128 MB of RAM. Likewise, Honeyd is another low-interaction honeypot; however, unlike the previous ones, it can monitor a network of millions of systems. It can emulate hundreds of OS at the application and IP stack levels. It is an open-source honeypot which uses a command-line interface to give instructions. It can also run on a single computer and is designed for the Unix platform. (Spitzner, 2002)

2. Medium-interaction honeypot software:

ManTrap can be considered as a medium or high interaction honeypot. It does not emulate services, instead it uses an OS to create up to four virtual OS. It provides the functionality to run production applications such as DNS, Web Servers and even a database. It is mostly used as a production honeypot although it has the capability to be used as a research honeypot. ManTrap can collect information regarding unknown attacks, discussion of black hats or new security flaws. One of its weak points is that it can only run-on Solaris OS. (Spitzner, 2002)

3. High-interaction honeypot software:

Honeynets are high-interaction honeypots. This type of honeypot requires building a standard network of systems like the ones built for real organizations. It gives the attackers a full operating system and applications to interact within the honeynet. The honeynet software can operate an Oracle database running on a Solaris server, an IIS Web server running on a Windows server, a router like Cisco, and many more. It is complex to manage as it requires establishing a managed network which gathers and administers all the data coming in and out of the honeypots. There are various types of honeynets. Each of them has different specifications and requirements.

For instance, Virtual honeynets can run on a single computer but are restricted by hardware and virtualization software. It can be divided into two types: self-contained and hybrid virtual honeynets. Virtual software like VMware workstation can support various OS within the virtual environment including Windows, Linux, Solaris and FreeBSD honeypots but it limits the number of virtual OS. VMware Ground Storm X (GSX) Server:

It supports all versions of OS like Windows, Linux, BSD and Solaris. VMware GSX recommends memory of 256 MB or higher for CUI-based OS and another 256 MB for GUI-based OS for each virtual OS. (Mohammed & Rehman, 2015) It supports up to 64GB for Windows hosts and Linux hosts that support large memory or are PAE-enabled, 4GB for non-PAE-enabled Windows hosts or 2GB for Linux hosts with kernels in the 2.2.x series. (VMware, 2004).

These are some of the honeypot softwares each with their specifications. There are various other honeypot softwares which can be used to improve the security of an organization. Most of the low and medium interaction honeypots are able to run on a single computer with certain system requirements. While some medium and high interaction honeypot software like honeynets requires either a very powerful computer or multiple computers in order to function properly.

3 Applications

3.1 Based on type of activity

There are mainly two types of honeypots that are used by various organizations for various purposes. Each of them is described below:

i. Production Honeypots:

The production honeypots are primarily used by private companies or corporations. This type of honeypot is used by the organizations to improve their overall security. They are generally placed within the production network amongst other production servers. The production honeypots help to minimize the risks of a company by keeping their servers safe and mimicking the information in a duplicate server to keep the intruders away from the main system. Generally, the production honeypots provide less information compared to the research honeypots. The production honeypots are easier to build and deploy and maintain compared to the research honeypots. It generally provides little information about the attack or the attacker. It can provide information about the systems from which the attacks originated and what exploits they launched. But it does not provide information on how they interact and discuss among themselves or how they create the applications to penetrate the security. The benefit of such a system is that it is less risky and does not require a great deal of time and effort to manage. (Mohammed & Rehman, 2015)

ii. Research Honeypots:

The research honeypots are mainly used by military or government organizations. However, it may also be used by researchers from private organizations. Research honeypots are usually very complex to deploy. The primary objective of this type of honeypot is to collect a massive amount of information to find the motive and strategies of the blackhat community who target various organizations. This type of honeypot is used mainly to find out the vulnerabilities which organizations encounter and learn how to create measures to prevent such types of attacks in the future. It can provide information about the hackers' identity, how they communicate with each other and how they create and use tools to penetrate the security. However, the downside of such a system is that it brings a great risk and requires more time and effort to manage. Such type of honeypots could result in loss for organizations as it requires a lot of resources and manpower to maintain. (Mohammed & Rehman, 2015)

3.2 Goals and Objective

There are many things which we can accomplish with honeypots. But we can narrow it down to a few main aspects. The three main goals of honeypots are:

- To learn about the attacker's strategy, process and techniques.
- To keep the attacker occupied and engaged for as long as possible.
- To alert the presence of an attacker on the network to the organization.

(U.S Department of Health and Human Services, 2020)

3.3 Uses

There are many reasons as to why the honeypots are used by various organizations. Some of which are elaborated below:

i. Data Value:

An organization collects a huge volume of data regularly from the logs of their firewall, intrusion prevention system and intrusion detection system. Due to this enormous size of information, determining valuable data is extremely difficult. However, this is not the case with honeypots. Honeypots collect very little data, generally few KB or MB of data but the data collected is of high value. This is because any data recorded by honeypot is usually a malicious activity. So, analysing the data is much easier and the malicious activity can be responded to quickly. (Spitzner, 2002)

ii. Resources:

Many security structures face limitations of resources and get exhausted. Resource exhaustion is the condition where a security resource is unable to keep their activities running because the activity input is greater than the resource is capable of handling. The honeypots only collect information directed towards it. Therefore, it does not get congested with other traffic. Since, honeypots do not have to deal with large amounts of data, it does not require a high-end computer. It can be set up easily on an old computer or laptop from the organization which is no longer used by the company. So, it is very cheap to install a honeypot as it does not require powerful hardware for its functions. (Spitzner, 2002)

iii. Simplicity:

Simplicity is one of the biggest features of honeypots. It does not require complex algorithms to create, signature databases to maintain or rule base to configure. The honeypot can be placed anywhere in an organization and it will notify the administrator upon encountering any malicious activity. Few of the honeypots, particularly research honeypots, could be a little complicated however, every honeypot works the principle that when an unauthorized user gets connected, monitor the activity. Due to its simple nature, it is less likely to have breakdowns and failures. So, it is a very reliable security measure. (Spitzner, 2002)

iv. Return on Investment:

Unlike other security resources such as firewalls, Intrusion Detection Systems (IDS), Intrusion Protection System (IPS), etc. Honeypots are extremely cheap. The malicious attacks, scans or probe detected on a honeypot system shows the unauthorized activity from the intruder and the type of activity threat they pose.to the organization. In this way, the honeypots continuously demonstrate their value and they also help to identify whether the current security measures in the organization need to be upgraded or downgraded based upon the type of threats observed from the honeypots. For this reason, it is important to invest in honeypots for the security of an organization. (Spitzner, 2002)

4 Conclusion

Honeypots are very powerful tools in the world of cyber security. It is very useful because of its ability to monitor the activities of the intruder in a network. This technology helps us to learn about various new attack methods used by intruders, blackhats or any malicious user. Because of this feature, it helps us learn about the loopholes in the security and create a security patch to prevent any major loss for organizations in the future.

The honeypots provide value to an organization by securing their data from intruders, understanding the flaws in their network. An organization should use the honeypot technology based on the type of data they store. The big companies who have a lot of sensitive data should definitely use medium or high interaction honeypots for preventing data loss or misuse. Also, the small organizations should also consider using a suitable honeypot system in order to maintain their data security and integrity.

If an organization which does not have a honeypot setup gets attacked, then it is most likely to lose data irreversibly and suffer a huge loss. Such is not the case with an organization where honeypot is set up and configured. If an intruder tries to attack this system, an alert message will be sent to the administrator of the organization who can then take the necessary actions to prevent the intruder from getting control of the system. Therefore, a honeypot is very useful for organizations to secure themselves from various kinds of threats which may harm the organization's data and reputation.

References

Barfar, A. & Mohammadi, S., 2007. Honeypots: Intrusion deception. *The Information Systems Security Association (ISSA Journal),* pp. 28-31.

Chandel, R., 2020. *Comprehensive Guide on Honeypots.* [Online]
Available at: https://www.hackingarticles.in/comprehensive-guide-on-honeypots/
[Accessed 5 May 2021].

Mohammed, M. & Rehman, H.-u., 2015. *Honeypots and Routers : Collecting Internet Attacks.* Boca Raton: CRC Press.

Spitzner, L., 2002. *Honeypots: Tracking Hackers.* 2nd ed. s.l.:Addison Wesley.

Titarmare, N., Hargule, N. & Gupta, A., 2019. An Overview of Honeypot Systems. *International Journal of Computer Science and Engineering,* 2, 7(2), pp. 349-397.

U.S Department of Health and Human Services, 2020. *Using Honeypots for Network Intrusion Detection.* [Online]
Available at: https://www.hhs.gov/sites/default/files/using-honeypots-network-intrusion-detection.pdf
[Accessed 30 April 2021].

VMware, 2004. *GSX Server 3.* [Online]
Available at: https://www.vmware.com/pdf/gsx31admin_manual.pdf
[Accessed 05 May 2021].