International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 04 Issue 12 December 2021
DOI: 10.47191/ijcsrr/V4-i12-10, Impact Factor: 5.825
IJCSRR @ 2021
www.ijcsrr.org

A Review on the Different Types of Honeypots in Information Security

I Putu Elba Duta Nugraha
Department of Electrical Engineering, Udayana University, Jimbaran, Badung Regency 80361, Indonesia

ABSTRACT: Honeypotting has evolved into a crucial tool in information security analysis, despite the fact that the concept of enticing enemies in order to watch their activities is not new. Honeynets, honeytokens, and adaptive honeypots are examples of recent advancements in network intrusion detection. This article will look at modern applications, as well as the technical issues that go into developing honeypot solutions for dynamically blocking emerging attack vectors and exploitation of sophisticated persistent threats.

KEYWORDS: Honeypots, Information Security

1. INTRODUCTION

The metaphorical honeypot is a trap that targets potentially malevolent actors. Prior to the late twentieth century, common examples included police departments using bait cars to attract potential car thieves or undercover operatives trapping criminals. Since the dawn of the Information Age, the notion has resurfaced as a useful investigative tool in computer security. Honeypots are weak computer systems or networks that are meant to be attractive to hackers as a target for entry. [6]

2. HONEYPOTS IN INFORMATION SECURITY

2.1. Honeypot

Honeypots are defined by the SANS Institute as "*an information system resource whose value lies in unauthorized or illicit use of that resource*" [1]. That concept, according to many in the IT security world, falls short of capturing much of what distinguishes honeypots from other security solutions. In the following part, several subcategories of classifications, designs, and foci will be examined in depth. When considering honeypots, it's vital to remember that an information system resource doesn't have to be limited to computing.

2.2. Honeynet

As the number of computers connected in a network grows, the chances of a single honeypot detecting up intrusion activities decrease. As a result, larger and more diversified networks sometimes necessitate the deployment of many honeypot instances. When set to function together, the result is a network of high-interaction honeypots that mimic a production network and are programmed to monitor, record, and govern all activities in a discrete manner.

Honeypots in several iterations have the extra benefit of being strategically placed in crucial subsystems or zones across the network. The correlation of logs from several honeypots can be used to create a history of an intruder's activity, as well as providing more information for forensic investigation and clean up. The analysis can be sped up even further by centralizing the collected activity logs and analytical tools in an administrative management client. Honeyfarms are the name given to these management clients.

2.3. Honeytoken

One of the most common misconceptions regarding honeypots is that they have to be a computer or interactive resource. It's vital to note that an information system resource doesn't have to be confined to physical assets or computers but can also comprise data. Whether it's a forged database entry or a forged email, the value is in the unauthorized use of the information.

Uniqueness and an uncommon likelihood of appearing in legitimate traffic are two crucial criteria of an effective honeytoken. These capabilities will go beyond simply assuring the integrity of the system resource by allowing the adoption of reactive security measures like discarding honeytoken-containing packets at the border router to prevent a data spill. Simple alert rules triggered by the detection of unique honeytokens could potentially give system administrators advance notification of an incident. If the honeytoken emerges in legitimate traffic and produces false positives, the value swiftly depreciates.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 04 Issue 12 December 2021
DOI: 10.47191/ijcsrr/V4-i12-10, Impact Factor: 5.825
IJCSRR @ 2021
www.ijcsrr.org

2.3.1. HoneyCreds

Honey credentials (also known as HoneyCreds, Honey Hashes, and/or Canary Credentials) are a newer implementation of the Honeytoken concept that has found traction in web-facing login security. As the number and sophistication of brute-force attacks has grown, network administrators have begun to include faked logins and passwords in lists of valid credentials. They're mixed in with valid credentials, salted and hashed, and only root can view them. The decoy credentials can thus give early warning of unauthorized access even if the hash file is stolen and cracked [10].

2.4. Honeytrap

While many in the IT security field use the term interchangeably with honeypots, a honeytrap is a more practical term for a premeditated cyber warfare operation aimed at extorting important information from a specific target.

3. DESIGN CRITERIA

3.1. Classification

3.1.1. Production

Production honeypots are commonly used as a litmus test to detect unauthorized access to a company's or corporation's production systems. They're usually installed alongside critical servers and just simulate the services that a hacker would use. They're easy to maintain and restore, and they only use a small amount of network resources.

3.1.2. Research

Research honeypots are fully interactive devices that are meant to be hacked. Rather than just indicating that an intrusion has happened, these honeypots provide information on hacker communities' motives and strategies. Researchers can then look at specific exploits and learn how to better secure systems from them. Research honeypots are exceedingly expensive to deploy, maintain, and examine due to their complexity. They are generally employed by major companies with considerable security research and development interests, such as the government, IT security leaders, the military, and academic institutions.

3.2. Design

3.2.1. Full

These are full-fledged production systems, often known as pure honeypots. Taps on the honeypots' network connections is used to record attacker interactions. Except for the fact that they are not in operation, these systems are identical to other production systems. Any action on the honeypot indicates that it is being used without permission.

3.2.2. High Interactive

Honeypots with a high level of interaction are designed to imitate the services provided by production systems. They give superior security in obscurity by doing so, and they trick malevolent actors into wasting their time and resources in the process. These honeypots should be put up as virtual machines so that they may be readily recovered if they are hacked.

3.2.3. Low Interactive

Low-interaction honeypots just replicate the services that attackers commonly request. They're ideal for virtualization because they require fewer resources. The virtual systems also have a quick response time and require less code, decreasing the virtual system's security complexity.

3.3. Focus

3.3.1. Malware

These are malware detection honeypots that use well-known replication and attack vectors, such as removable media. Manual scans or the usage of special-purpose honeypots that simulate disks in a proxy environment are used to check for signs of alterations on these vectors. Any odd action will raise an alert, and the media may be placed under investigation.

3.3.2. Email/Spam

The first email honeypots, often known as spamtraps, were just unused email accounts. Any unsolicited electronic messages sent to these email addresses have a high likelihood of being spam. While most spam is easy to spot, an email honeypot can better tell the difference between complex phishing attempts and real emails.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 04 Issue 12 December 2021
DOI: 10.47191/ijcsrr/V4-i12-10, Impact Factor: 5.825
IJCSRR @ 2021
www.ijcsrr.org

3.3.3. Database

Databases are a great place to use honeytokens to their maximum extent. When a few erroneous entries in an authentic table are linked to intrusion detection system (IDS) warnings, firewall rules might be triggered to drop egress packets and dynamically block unknown IPs used by attackers.

4. HONEYPOT TOOLS

4.1. VMWare

VMware is becoming more and more popular as a honeypot tool. Virtual machines (VMs) that replicate hardware drivers are created and hosted by the desktop virtualization solution. For semi-autonomous network connections, a VMware virtual machine is given a distinct IP address from the host. A VM seems to be an independent system from the outside, making it ideal for low-interaction honeypot operations.

However, a VMWare honeypot's major flaw is that it may be easily discovered by inspecting the MAC address. Remember that MAC addresses are fixed to the network interface card and cannot be modified, and that the first three octets reflect the vendor ID number. The virtual MAC address will fall into one of three subsets in the case of VMWare [4]:

1. 00-05-69-xx-xx-xx
2. 00-0C-29-xx-xx-xx
3. 00-50-56-xx-xx-xx

The attacker has several means to check the MAC address [4]:

1. In a UNIX environment, run ‘ifconfig –a’.
2. In a Windows environment, run ‘ipconfig/all’.
3. ‘arp –a’ is also an option from the router.

4.2. Chroot

Another frequent approach for building a honeypot is to utilize the change root command (chroot) in a Unix system. An attacker's access to the system is limited by a chroot jail, which separates processes from outside the directory tree. The jail, unlike a virtual machine, runs on the same kernel as the primary operating system. This creates the impression that the attacker is at the root of the file system.

Regardless of these characteristics, there are several unmistakable signals that an attacker is in a chroot jail. The first and most straightforward method is to run 'ls–lia' on the root directory and look at the inodes of the '.' and '..' directories. A normal system, for example, will display the two directories as [4]:

1. 2 drwxrxrx 21 root root 2096 Feb 16 08:37 .
2. 2 drwxrxrx 21 root root 2096 Feb 16 08:37 ..

When the same command is executed in a chroot jail, the inodes of the chroot directory are displayed at a considerably higher value [4]:

1. 1553552 drwxrxrx 6 1000 100 4096 Mar 11 17:22 .
2. 1553552 drwxrxrx 6 1000 100 4096 Mar 11 17:22 ..

4.3. Honeyd

Honeyd is an open source daemon that uses packet manipulation to imitate a variety of hosts. It operates by listening for packets destined for specified IP addresses and ports and crafting answers based on a configuration file. Honeyd can simulate 65536 IP addresses on a single host. It can run on both Unix and Windows hosts and can be configured using Perl scripts to mimic common services for improved usability. By constructing a needle-in-a-haystack strategy to finding the genuine host, Honeyd becomes a relatively inexpensive and effective honeypot against potential hackers.

When compared to real systems, emulation has various drawbacks. Honeyd's answers are exclusively based on IP and port addresses, and it may react to invalid packets. For example, a response to a packet constructed with an erroneous checksum may alert an attacker that something is wrong. Script simulated services, such as troute telnet, which comes with the Honeyd installation, have also been known to fail on occasion.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 04 Issue 12 December 2021
DOI: 10.47191/ijcsrr/V4-i12-10, Impact Factor: 5.825
IJCSRR @ 2021
www.ijcsrr.org

5. HONEYPOT VULNERABILITIES

Some commercial software developers have been known to leave I/O backdoors available for product configuration during runtime, particularly in solutions that aren't explicitly designed for security. VMWare is a good example of a program that can be hacked or 'broken' with a few assembly lines [4]:

```
mov eax, VMWARE_MAGIC ; 0x564D5868
mov ebx, b; <parameter of command>
mov ecx, c ; <number of command>
mov edx, VMWARE_PORT ; 0x5658
in eax, dx
```

The following are some examples of commands that can be used with this [4]:

1. 04h - Get current mouse cursor position
2. 05h - Set current mouse cursor position
3. 06h - Get data length in host's clipboard
4. 07h - Read data from host's clipboard
5. 08h - Set data length to send to host's clipboard
6. 09h - Send data to host's clipboard
7. 0Ah - Get VMware version
8. 0Bh - Get device information

A hacker could determine that they are inside a VMWare virtual computer by running the code above. The backdoor might also be used to cause disruptions, such as altering mouse movement across the screen or even causing a buffer overflow to cause the virtual machine to crash. Despite the fact that patches to change the value of VMWARE MAGIC to hide the backdoor are available, there is no documentation on how effective this strategy is.

6. TRAPPING TECHNIQUES

In 1999, Lance Spitzner published one of the first studies on honeypots as a supplement to regular intrusion detection systems (IDS) [7]. In three easy steps, he summarizes his strategy:

1. Build the box. Recreate the system for which you want to learn about vulnerabilities.
2. Connect it to the internet. Wait for an attacker to get root access and then keep an eye on them.
3. Eject the attacker. The operator must kick the attacker out of the system before they understand it is a honeypot, which is an essential but often missed step. As previously stated, the actions could shift from covert information probing to full-fledged attacks, resulting in the destruction of key information and resources [2].

7. EMERGING HONEYPOT TECHNICS

7.1. Cloud-based Honeypots

Cloud computing is a commercial and technology distribution strategy that allows users to connect to a pool of shared and adjustable computer resources through the internet on demand. The key service types that may be swiftly supplied with minimal monitoring and service provider involvement are software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) [5]. Cloud computing has become an appealing solution for online applications and services start-up enterprises because to its scalability and transference of technical overhead expenses and risk.

Unused cloud resources should be assigned as possible honeypots, according to a unique solution suggested by Alert Logic. A cloud provider could divert attacker attention away from clients by creating evident weaknesses in IP space assigned to honeypots. Furthermore, because any connection with the honeypots from the public domain indicates illegal activity, those IP addresses can be placed to a blacklist for edge firewalls to block incoming traffic [9].

7.2. Adaptive Honeypots

Honeypots that adapt or self-configure are a solution under development for generating a reactive environment employing game theory features [8]. Dr. Gérard Wagener discovered a link between a honeypot's permissiveness and the speed with which a hacker completes their aim, comparing it to the time it takes the same hacker to abandon an extremely restrictive honeypot. The scholarly

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 04 Issue 12 December 2021
DOI: 10.47191/ijcsrr/V4-i12-10, Impact Factor: 5.825
IJCSRR @ 2021
www.ijcsrr.org

goal is to keep hackers engaged with incremental obstacles for as long as possible in order to divulge as much information about themselves as feasible, such as reasons, techniques, and tactics.
Through successive interactions with hackers, the honeypot 'learns,' or statistically decides the most accurate and effective strategy, including blocking commands, returning erroneous signals, and even insulting the invader in a quasi-reverse Turing test [3]. Adaptive versions of honeypots may be seen in the near future of internet security, albeit they have yet to be implemented to commercially available honeypots.

8. CONCLUSION

Honeypots are undeniably a versatile instrument that is gaining in popularity in the field of information security. They can be configured in a variety of ways to detect, deceive, or neutralize attackers' actions. Despite their versatility, honeypots should be used in conjunction with traditional security appliances and should not be used in place of firewalls, IDS/IPS, or defense-in-depth tactics. It's critical to realize that installing a honeypot will always pose some risk to the network as a whole. To ensure that production honeypots do not provide an attacker an advantage, interfere with existing IDS/IPS activities, or attract undue malevolent attention from the Blackhat community, careful design, testing, and development are required [2]. As with any defense in depth strategies, organizations must carefully define the goals they want to achieve as well as the risks they are prepared to accept, as honeypots may not always be the most successful or cost-efficient way to improve overall network security posture [1].

REFERENCES

1. Cole, E., & Northcutt, S. (2008). Honeypots: a security manager's guide to honeypots. SANS Institute.
2. Chismon, D. (2016). Hunting with honeypots. MWR Infosecurity.
3. Even, L. R. (2000). Intrusion detection FAQ: what is a honeypot? SANS Institute.
4. Innes, S. & Valli, C. (2006). Honeypots: how do you know you're in one? Edith Cowan University.
5. Nithin Chandra, S., & Madhuri, T. (2012). Cloud security using honeypot systems. International Journal of Scientific & Engineering Research [Vol 3, No 3].
6. Spitzner, L (2003). Honeytokens: the other honeypot. Symantic.
7. Spitzner, L (1999). To build a honeypot. SCN Research.
8. Wagener, G. & Dulaunoy, A. (2011). Adaptive and self-configuring honeypots. IEEE.
9. Winder, D. (2014). How to use the cloud as a honeypot. CloudPro.
10. (2015). Detecting mimikatz use on your network. SANS ISC InfoSec Forums.

Cite this Article: *I Putu Elba Duta Nugraha (2021). A Review on the Different Types of Honeypots in Information Security. International Journal of Current Science Research and Review, 4(12), 1679-1683*