

# HONEYPOT SYSTEMS AND CHALLENGES

CENG 3544, COMPUTER AND NETWORK SECURITY

Uzay Işın Alici  
uzayisinalici@mu.edu.tr

Monday 6<sup>th</sup> June, 2022

## Abstract

Information security has become one of the most important problems with the gradual development of the digital age. Honeypot is an effective system to keep up with this development and learn new strategies and also a trap; as it attracts its prey, it also reveals the ways and methods of its prey. Besides that, there are some challenges that will be covered in this page.

**Keywords :** Honeypots , Challenges, Security , Network , Privacy

## 1 Introduction

In the advancing computer age, passive protection methods have been insufficient due to the use of undiscovered methods by attackers. Honeypot systems are the best solution, especially against zero-day attacks. Zero-day attacks are unidentified attacks using unknown vulnerabilities. Honeypot system's already aim is to discover these new methods and detect attackers activity. Because of this, they are open targets with vulnerabilities. Honeypot systems should look like any other machine on the network, but with no traffic on them. If it does, this interaction is a sign that an attacker has entered the system.

## 2 Types Of Honeypots

### 2.1 Based On Level Of Interactions

#### 2.1.1 High Interaction Honeypots

They can collect comprehensive information due to the fact that the operating systems and applications are imitations of real systems. Because of that, their installation and maintenance are more difficult than low-interaction honeypots. This type of traps are more convincing for the attacker to not understand, but they are costly.

#### 2.1.2 Low Interaction Honeypots

Although they are easy to use, easy to configure and cost less, they are mostly good for the same types of attacks that occur constantly. Services or commands that this trap type

does not support may attempt to be used by an attacker. As a result, it is more likely to be compromised.

## 2.2 Based On The Purpose

### 2.2.1 Research Honeypot

They are especially used by military institutions, research institutions, and government institutions to collect more comprehensive information and to create a more secure network. Their configuration and maintenance are complex.

### 2.2.2 Production Honeypot

They are honeypots in the production network that are easy to configure and maintain but provide limited information.

## 3 CHALLENGES

1. **Limited Vision** : The attacker is tracked and logged only if the system is directly threatened. This shows that if the honeypot system does not detect a threat, it does not see it as an attacker and does not follow it.
2. **Compromised** : It is the moment when it is revealed that it is a honeypot. Small details or errors can reveal that the system is not real. The attacker or software can penetrate the real system.
3. **Capturing** : Honeypot systems can be hijacked by attacker or malware .
4. **For Evil Purpose** : Nowadays, new risks have emerged with the development of new technologies. With the spread of crypto money technology, the use of honeypot systems for fraud has been made possible. All it takes is a smart contract and bait. The movements in the transaction history of the contract can be followed. There is no sales history when there are too many purchases in the trap coin. [3]

## 4 RELATED WORKS

There are a few honeypot systems and challenges proposals in the literature regarding new technologies [1]. These are mostly for showing the types of honeypots or focusing the advantages [2].

## 5 IMPLEMENTATION

HoneyDrive, the Linux distribution that includes many honeypot software and tools, is used to demonstrate how traps work. The ifconfig command is used to find out the IP address. Kippo is used as a Honeypot. Among the many software on HoneyDrive, the reason for using Kippo is that the attacker reports every SSH attempt in the logs. After running Kippo, a network scan was conducted with the IP address using the Nmap tool. The first scan is done after installing the Nmap tool on another machine.

```
Terminal - honeydrive@hon... Mon, 06 Jun 04:45 honeydrive
Terminal - honeydrive@honeydrive:/honeydrive/kippo
File Edit View Terminal Go Help
honeydrive@honeydrive:~$ cd ..
honeydrive@honeydrive:/home$ cd ..
honeydrive@honeydrive:/$ ls
bin      etc          initrd.img.old  mnt      run        sys        vmlinuz
boot     home         lib             opt      sbin       tmp         vmlinuz.old
cdrom    honeydrive  lost+found      proc     selinux    usr
dev      initrd.img  media          root     srv        var
honeydrive@honeydrive:/$ cd honeydrive/
honeydrive@honeydrive:/honeydrive$ ls
amun      dionaea-scripts  honeyd2mysql    kippo2mysql  thug
amun-scripts  dionaea-vagrant  honeyd-scripts  kippo-malware  wordpot
conpot      glastopf         kippo           kippo-scripts
DionaeaFR   glastopf-honeypot kippo2elasticsearch  phoneyc
honeydrive@honeydrive:/honeydrive$ cd kippo
honeydrive@honeydrive:/honeydrive/kippo$ ls
data  fs.pickle  kippo      kippo.pid  private.key  start.sh  utils
dl    .gitignore kippo.cfg  kippo.tac  public.key   stop.sh
doc   honeyfs    kippo.cfg.dist  log        README.md    txtcmds
honeydrive@honeydrive:/honeydrive/kippo$ ./start.sh
Starting kippo in the background...

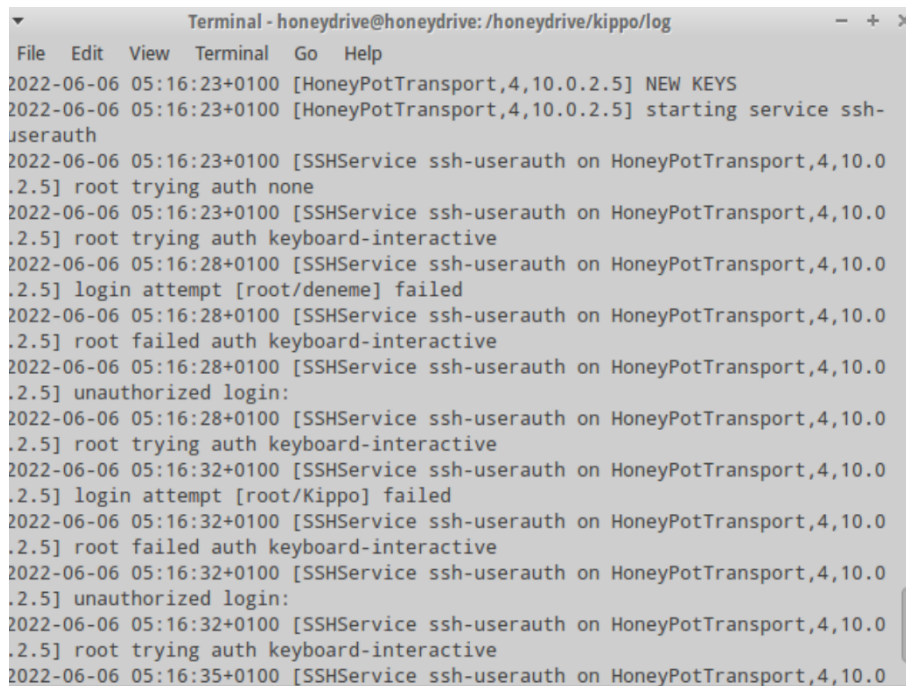
Removing stale pidfile /honeydrive/kippo/kippo.pid
Loading dblog engine: mysql
honeydrive@honeydrive:/honeydrive/kippo$
```

Figure 1: Running Kippo

```
lilith-root@lilithroot-VirtualBox:~$ nmap -sV 10.0.2.5
Starting Nmap 7.01 ( https://nmap.org ) at 2022-06-06 06:58 +03
Nmap scan report for 10.0.2.5
Host is up (0.00031s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.1p1 Debian 5 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.2.22
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.31 seconds
lilith-root@lilithroot-VirtualBox:~$
```

Figure 2: First Scan with Nmap



```
Terminal - honeydrive@honeydrive: /honeydrive/kippo/log
File Edit View Terminal Go Help
2022-06-06 05:16:23+0100 [HoneyPotTransport,4,10.0.2.5] NEW KEYS
2022-06-06 05:16:23+0100 [HoneyPotTransport,4,10.0.2.5] starting service ssh-
userauth
2022-06-06 05:16:23+0100 [SSHSservice ssh-userauth on HoneyPotTransport,4,10.0
.2.5] root trying auth none
2022-06-06 05:16:23+0100 [SSHSservice ssh-userauth on HoneyPotTransport,4,10.0
.2.5] root trying auth keyboard-interactive
2022-06-06 05:16:28+0100 [SSHSservice ssh-userauth on HoneyPotTransport,4,10.0
.2.5] login attempt [root/deneme] failed
2022-06-06 05:16:28+0100 [SSHSservice ssh-userauth on HoneyPotTransport,4,10.0
.2.5] root failed auth keyboard-interactive
2022-06-06 05:16:28+0100 [SSHSservice ssh-userauth on HoneyPotTransport,4,10.0
.2.5] unauthorized login:
2022-06-06 05:16:28+0100 [SSHSservice ssh-userauth on HoneyPotTransport,4,10.0
.2.5] root trying auth keyboard-interactive
2022-06-06 05:16:32+0100 [SSHSservice ssh-userauth on HoneyPotTransport,4,10.0
.2.5] login attempt [root/Kippo] failed
2022-06-06 05:16:32+0100 [SSHSservice ssh-userauth on HoneyPotTransport,4,10.0
.2.5] root failed auth keyboard-interactive
2022-06-06 05:16:32+0100 [SSHSservice ssh-userauth on HoneyPotTransport,4,10.0
.2.5] unauthorized login:
2022-06-06 05:16:32+0100 [SSHSservice ssh-userauth on HoneyPotTransport,4,10.0
.2.5] root trying auth keyboard-interactive
2022-06-06 05:16:35+0100 [SSHSservice ssh-userauth on HoneyPotTransport,4,10.0
```

Figure 3: Report of Honeypot

The report of the nmap scan is kept as a report in the Kippo logs on the HoneyDrive machine. If an attempt is made to connect via ssh on Honeypot, password records are also kept in the logs. The /etc/passwd file is very important for penetration testing.

## 5.1 Evaluation

Honeypot reports can be examined by different attacker scenarios. It is a scenario to make an SSH connection in the honeypot. Another scenario is to scan from another machine using tools like Nmap to the honeypot.

## 6 RESULTS and DISCUSSION

Kippo graphs are available at the localhost/kippo-graph url. The effectiveness of the attackers can be determined from the graphical distribution of the most used passwords and methods in the honeypot system. Real systems become safer and more effective when precautions are taken by considering these graphics. Since honeypot systems are systems that adapt easily, they occupy an important place in the developing information world and their challenges are eliminated over time.

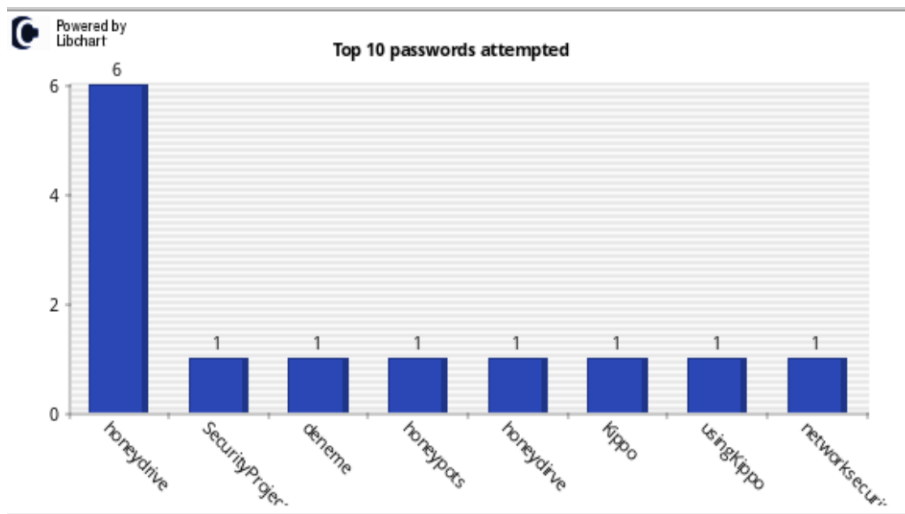


Figure 4: Top 10 Passwords Attempted

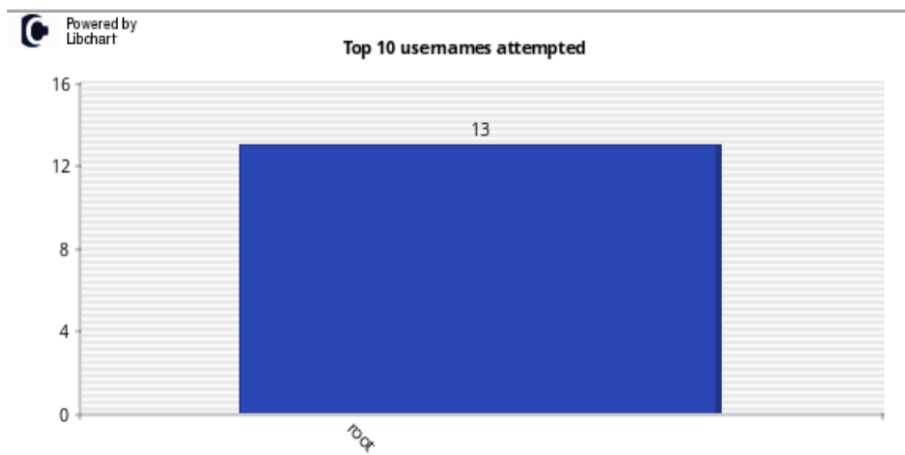


Figure 5: Top 10 Usernames Attempted

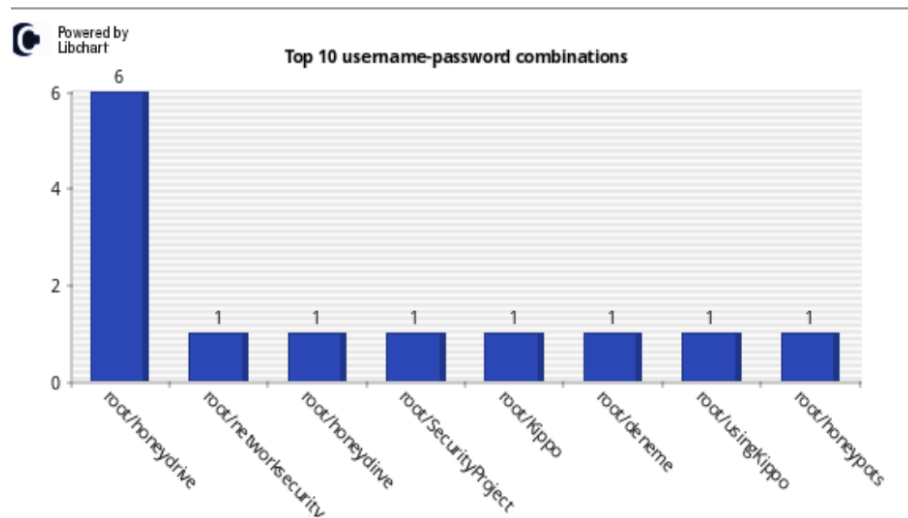


Figure 6: Top 10 Username-Password Combinations

## 7 CONCLUSION

Honeypot systems, which actually have the working logic of IDS (Intrusion Detection Systems) systems, detect attacks and report log records. It is indeed a pot of honey for attackers as it has security holes. This is what lures the attacker into the trap. As a result, new methods and strategies can be learned as long as the attacker does not understand that the system is not genuine. As cyberbullying increases in the developing digital world, it will continue to be one of the most effective methods as long as measures can be taken to counter the disadvantages of honeypot systems. In fact, the advantages of honeypot systems are greater than their disadvantages. One of its important and distinctive advantages is that its false positive rate is very low compared to other detection and prevention tools. Therefore, exact evidence can be reached through these systems. Because while passive protection methods are mostly successful, there is no active learning process and it is insufficient to discover new methods. A honeypot is a nice defense mechanism at this point. If desired, more than two honeypot systems (Honeynets) can be installed to ensure the security of large networks. In this age, where we face new problems every day, honeypot systems will shed light on our way with their new solutions and will continue to trap attackers.

## References

- [1] Naeem Ansab. "Honeypots: Concepts, Approaches and Challenges" (2021).
- [2] Arıkan S. , Benzer , R. , "Bir Güvenlik Trendi: Bal Küpü". (2018)
- [3] Camino Ramiro , Torres Christof State, Radu. (2019). "A Data Science Approach for Honeypot Detection in Ethereum"
- [4] Shukla Maitri Verma Pranav , "Honeypot: Concepts, Types and Working" (2015)

- [5] Yun Yang, Jia Mi, "Design and Implementation of Distributed Intrusion Detection System based on Honeypot" (2010).
- [6] KARAARSLAN Enis , AKIN Gökhan , Hüsnü DEMİR , "Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Yöntemleri" (2008).
- [7] Iyatiti Mokube , Michele Adams "Honeypots: Concepts, Approaches, and Challenges" (2007).
- [8] <http://www.honeynet.org/papers/kye.html>.
- [9] P. Diebold , A. Hess , G. Schaer. "A Honeypot Architecture for Detecting and Analyzing Unknown Network Attacks" (2005).
- [10] Aleksey A. Egupov, Sergey V. Zareshin, Igor M. Yadikin, Dmitry S. Silnov. "Development and Implementation of a HoneypotTrap" (2017).