Honeypot

Name
ABDULLAH SALEH AHMED QANAAN

Table of Contents

Table Of Figures

Abstract

Honeypots are intelligent safeguards meant to attract online criminals, gather information, and boost cybersecurity defenses. Honeypots assist organizations in identifying unauthorized access, analyzing the actions of attackers, and enhancing threat response strategies by simulating actual systems. This essay examines the various kinds of honeypots such as malware honeypots, honeynets, high-interaction, and low-interaction honeypots as well as their function in contemporary cybersecurity. Furthermore, it investigates possible weaknesses and assaults, including denial-of-service (DoS) attacks, honeypot profiling, and honeypot hijacking.

1.0 Introduction and Overview of Honeypot

1.1 Introduction

Honeypots are decoy servers or systems placed next to systems that your company actually uses for production in the field of cybersecurity. IT teams can monitor the system's security responses and divert the attacker from their intended target by installing honeypots, which are made to resemble appealing targets.

Honeypots come in a variety of configurations that can be designed for your organization's requirements. Honeypot's function performs as a trap, allowing you to detect attacks early and respond appropriately because they seem like real threats. They can be used to distract attackers from your most critical systems, as this honeypot definition illustrates. You can obtain critical data about the nature of the attack and the techniques the attacker is employing while the attacker is duped (*What Is a Honeypot? | Fortinet*, n.d.).

When a honeypot looks like a real system, it performs best. Stated differently, it needs to execute the same processes that your real production system would work. Decoy files that the attacker will view as suitable for the targeted processes should also be included. It is usually best to place the honeypot behind the firewall that guards the network of the company. By doing this, the company can stop attacks designed to be launched from inside a compromised honeypot and investigate threats that manage to bypass the firewall. Your firewall, placed between the honeypot and the internet, can intercept the attack as it progresses and remove the data.

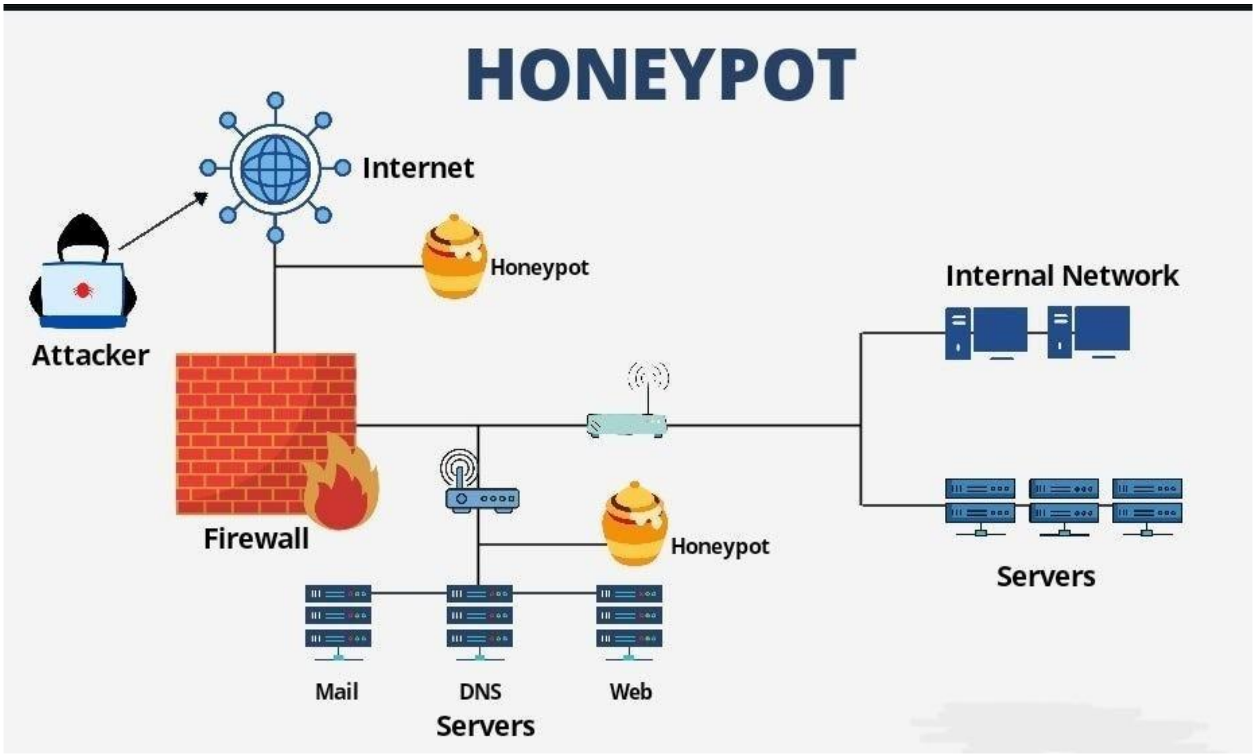


Figure 1

1.2 Types of Honeypots

1.2.1 Honeynet

A network of honeypots makes up a honeynet. A honeynet made up of various honeypot types allows for the study of various attack types, including ransomware, content delivery network (CDN), and distributed denial-of-service (DDoS) attacks. A honeynet contains all traffic, both inbound and outbound, to safeguard the rest of the organization's system, even though it is used to study various types of attacks (Vaideeswaran, 2025).

- Provides detailed attack analysis across multiple attack surfaces.
- a system of several honeypots intended to mimic the infrastructure of a whole company system.

1.2.2 High-Interaction Honeypot

An attacker may be given the opportunity to waste time on numerous services because highinteraction honeypots mimic the actions of production systems that house a range of services. It is possible to host several honeypots on a single physical machine by using virtual machines. This makes it possible to restore the honeypot faster, even if it is compromised. Although they are costly to maintain, high-interaction honeypots generally offer greater security because they are harder to find. In the absence of virtual machines, each honeypot requires a single physical computer, which can be extremely costly to maintain. Take Honeynet, for instance (Wikipedia contributors, 2024).

- Fully functional systems that allow attackers to engage deeply with the environment.
- Used for capturing advanced attack techniques but require strict monitoring to prevent real damage.

1.2.3 Low-interaction honeypot

Low-interaction honeypots only imitate the services that attackers commonly request. Several virtual machines can be easily hosted on a single physical system due to their low resource consumption, quick response times, and the need for less code, which lowers the security complexity of virtual systems (Vaideeswaran, 2025).

- Easy to deploy and maintain but provide limited insights into attacker behavior.
- Simulate only basic services and do not allow full system access.

1.2.4 Malware honeypot

A malware honeypot is a ruse created to draw in malicious software specifically. It accomplishes this by mimicking a network or system that is susceptible, like a web server. The honeypot is purposefully configured with security holes to try to attract these malware attacks. IT teams can examine the malware after it has been attacked to learn more about its background and behavior (*What Is a Honeypot? | Fortinet*, n.d.).

1.2.5 Email trap or spam trap

An automated address harvester or site crawler is the only way to identify a fake email address that has been implanted in a hidden field by an email or spam trap. The company can classify all emails sent to that inbox as spam because legitimate users cannot see the address. After that, the company has the ability to block the sender, its IP address, and any messages that contain the same content.

1.2.6 Decoy Database

A decoy database is a purposefully weak fake data set that helps organizations in keeping an eye on malicious internal actors, software flaws, and architectural flaws. The information gathered by the decoy database about an attacker's injection techniques, credential hijacking, or privilege abuse can then be incorporated into security policies and system defenses (Vaideeswaran, 2025).

1.3 How Does a Honeypot Work

The fundamental idea behind a honeypot is that it should be made to resemble the network target that a company wants to defend.

A honeypot trap can be made to resemble a payment gateway, which is a common target for hackers due to the fact that it contains a wealth of transaction details and personal data, including bank account information and encoded credit card numbers. In order to attract actors interested in obtaining trade secrets, intellectual property (IP), or other sensitive and valuable information, a honeypot or honeynet may also mimic a database. In order to trap adversaries who want to damage someone's reputation or use ransomware tactics, a honeypot may even seem to contain potentially compromising data or images.

Once inside the network, one can follow the movements of cybercriminals to gain a better understanding of their tactics and intentions. This will assist the company in modifying current security processes to prevent such attacks on valid targets in the future.

Honeypots frequently have intentional but not always obvious weaknesses in security to increase their appeal. Because many digital adversaries are highly skilled, it is critical for organizations to strategically consider how easy it is to access a honeypot. A highly skilled adversary is unlikely to be fooled by a poorly secured network, and the bad actor may even spread false information or alter the environment in other ways to lessen the tool's effectiveness.

1.4 Current Challenges in Honeypot Implementation

Despite honeypots being advantageous for cybersecurity, implementing them comes with various challenges. To begin with, attackers can detect honeypots, and sophisticated hackers tend to recognize fake environments and avoid them, which lessens their effectiveness. Furthermore, if honeypot is not properly contained, it can be taken over and exploited to launch attacks on genuine systems which often go undetected. Cost and resource allocation also become major problems, as honeypots necessitate frequent modifications, surveillance, and skilled personnel to evaluate the information gathered. All these factors would bring about not only economic but also legal and ethical dilemmas regarding breaching privacy issues tailored towards attackers. Thus, organizations must comply with cybersecurity regulations. In addition, honeypots do not cater to advanced persistent threats (APTs), social engineering attacks and zero-day exploits, which need more complex security methods. The last problem to consider would be sorting through the enormous amounts of log data generated by honeypots. Identifying actual threats from benign network scans becomes a daunting task with overwhelming volumes of information. Nonetheless, when combined with intrusion detection systems, automated threat analysis, firewalls and other tools designed to bolster network security, honeypots strike as the most critical cybersecurity strategies.

2.0 Vulnerabilities and Potential Attacks in Honeypot

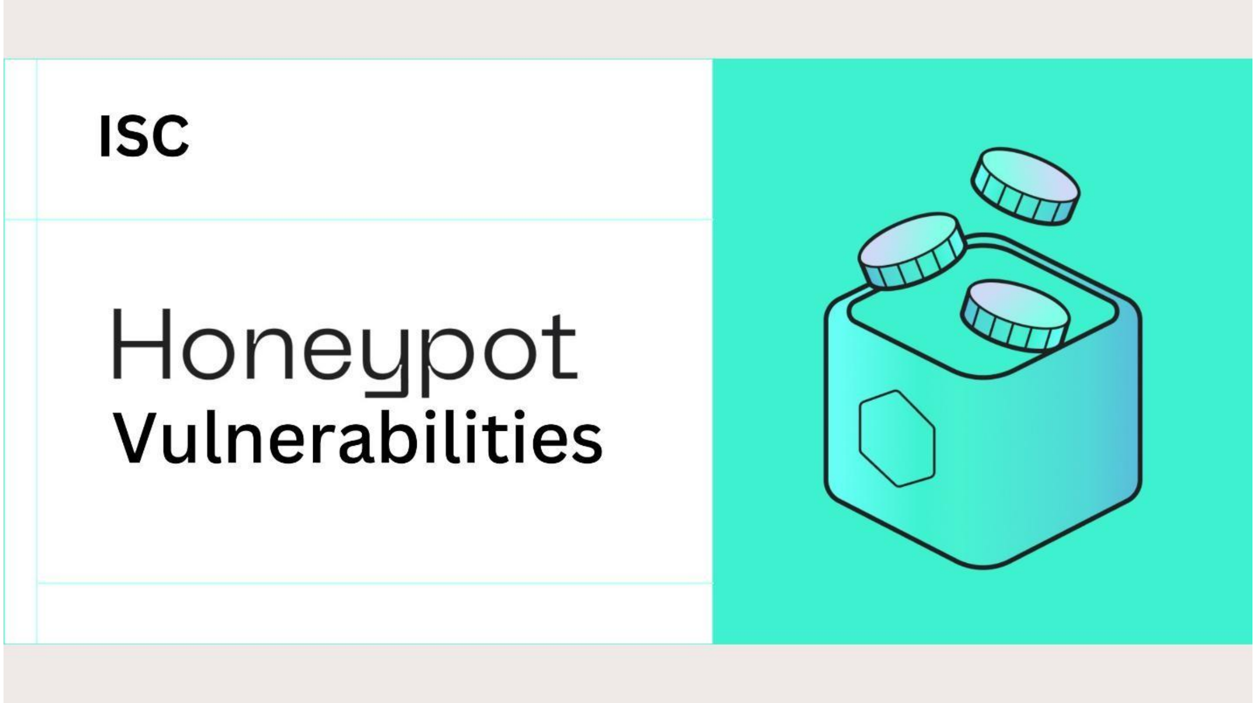


Figure 2

2.1 Vulnerabilities of Honeypot

You would think honeypots would be the best security solution with all these wonderful advantages. Sadly, that isn't true. They have several drawbacks. Because of these drawbacks, honeypots only complement and improve your overall security architecture—they don't replace any security measures.

2.1.1 Narrow Field of View/

The biggest drawback of honeypots is their Narrow Field of View; they can only see activity that is aimed at them. Your honeypot won't be aware of any activity if an attacker breaches your network and targets multiple systems unless it is attacked directly. The attacker can now circumvent that system and enter your company without the honeypot noticing if she has recognized your honeypot for what it is. As previously mentioned, honeypots allow you to concentrate on data that is known to be valuable by creating a microscope effect on the value of the data you gather. The honeypot's extremely small field of view, however, can block out events occurring all around it, much like a microscope (*Disadvantages of Honeypots | InformIT*, n.d.).

2.1.2 Fingerprinting and Detection

To find fake environments, experienced hackers frequently employ honeypot detection techniques. Hackers can identify whether they are dealing with a honeypot or an actual system by examining response times, service banners, and network activity. After being discovered, attackers might choose to avoid interacting with the honeypot or purposefully provide it with erroneous information in order to deceive security analysts. Fingerprinting is more likely to occur in honeypots with recognizable configurations or antiquated signatures. The risk of detection can be decreased by using dynamic configurations and randomized responses.

2.1.3 Denial-of-Service (DoS) Attacks

A honeypot may be overloaded with traffic by hackers, making it useless and using up system resources. Due to their limited computational capacity, low-interaction honeypots are especially affected by Denial-of-Service (DoS) Attacks. This prevents security teams from analyzing legitimate threats and clogs network monitoring tools.

2.1.4 Misconfiguration Risks

A poorly set-up honeypot may cause more problems than it solves. It might unintentionally help attackers in comprehending an organization's security posture if it makes too much information to the public. Attackers may use unpatched vulnerabilities in the honeypot system, exposed ports, or weak authentication to get around security measures. Furthermore, security teams risk missing important threat intelligence if logging and monitoring are not set up correctly. Strict access controls, controlled exposure, and frequent security audits are required to stop misconfigurations.

2.2 Potential Attacks in Honeypot

A honeypot is an intentional decoy designed to attract the hacker's attention so they can be studied and monitored. While designed to appear like a real system, honeypots do not have any data or bases for legitimate business functions. Even though honeypots can be a useful tool in understanding an attacker’s behavior and projecting new methods of security, they are still immensely vulnerable and can be hacked or misused by advanced highly sophisticated opponents.

2.2.1 Reverse Honeypot Attacks

As a part of some advanced schemes, attackers customize their honeypots for the purpose of gathering valuable information related to the defenders or researchers. As an example, an attacker sets up a malicious server that poses as some legitimate service with the aim of enticing both automated security tools and security researchers to interact with it.

Mitigation: When using such systems, if they look like they are vulnerable, one should be careful not to engage normally. Work with isolated sandboxes that ensure no leakage of sensitive information.

2.2.2 Data Poisoning

Attackers could try to alter the data collected by the honeypot and get defenders to focus on the wrong things or at the very least waste their valuable time. In doing so, malicious logs can be injected, fake malware samples dropped, or misleading network traffic generated by the attackers to achieve the aim of deceiving the analyzing defenders and reducing the effectiveness of the honeypot. For example: An attacker could upload benign files or generate fake network traffic to make it appear as though an attack is in progress when it is not.

Mitigation: Strong validation and verification mechanisms need to be formulated and implemented to facilitate data collected by the honeypot. Whenever necessary, cross-source the logs with other intelligence sources to identify them.

2.2.3 Honeypot Hijacking

Attackers may occasionally try to take control of the honeypot itself in order to utilize it as a base from which to launch additional attacks. The honeypot may turn into a vector for attacks on other network systems if it is not adequately isolated. For instance, if the honeypot is compromised, the attacker may use it as a relay to launch attacks on other targets or as a command-and-control (C2) server for a botnet.

Mitigation: Make certain that the honeypot is entirely segmented from the network. Utilize virtual machines, containers, or air-gapping to mitigate lateral movement.

2.3 Real-World Examples of Honeypot-Related Breaches

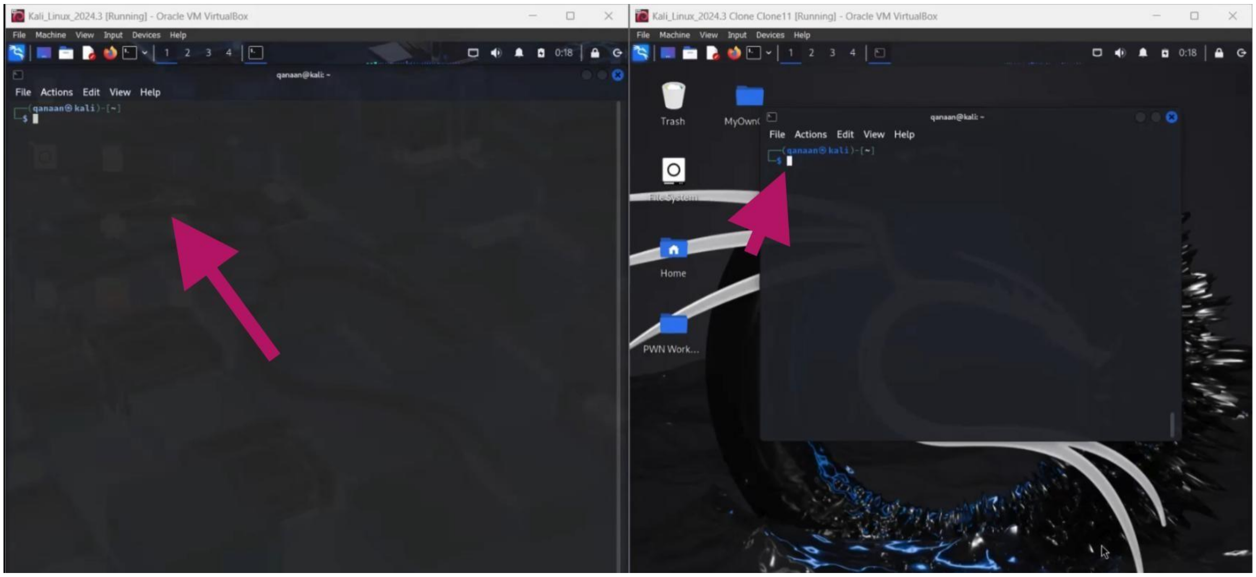
Microsoft implemented IoT honeypots in 2019 to analyze cyber assaults inflicted on devices such as routers, cameras, and industrial systems. In less than 30 minutes, the honeypots had recorded countless automated log-in attempts, most of which employed unused basic passwords. The attacks were associated with Mirai-like botnets whose purpose was to compromise IoT devices to execute DDoS attacks, credential stuffing, and crypto-jacking.

3.0 Best practices / techniques for Honeypot

Figure 3

Honeypots remain an important element in network communication security in that they allow for the detection, analysis, and mitigation of attacks from malicious users through deception and baiting.

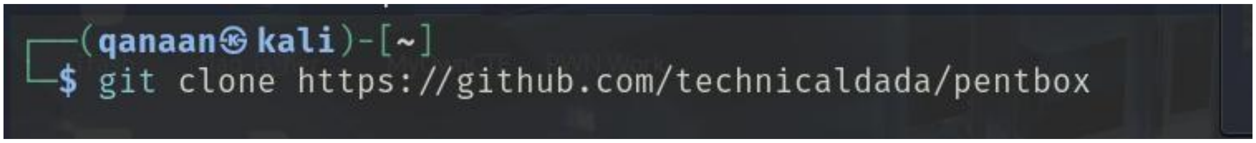
3.1 Installation of Honeypot


Kali_Linux_2024.3 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
qanaan@kali: ~
File Actions Edit View Help
Kali_Linux_2024.3 Clone Clone11 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
MyOwn
File System
Home
PWN Work...
qanaan@kali: ~
File Actions Edit View Help

```
┌──(qanaan㉿kali)-[~]
└─$
```

Figure 4

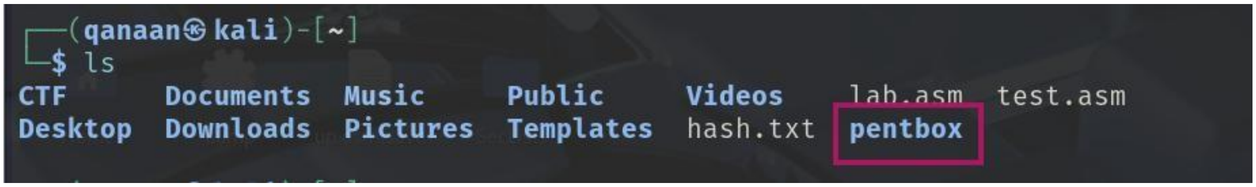
First, we have 2 two Kali Linux Virtual machines, the one on the left where we will implement Honeypot, and the one on the right side is the attacker machine.



```
┌──(qanaan㉿kali)-[~]
└─$ git clone https://github.com/technicaldada/pentbox
```

Figure 5

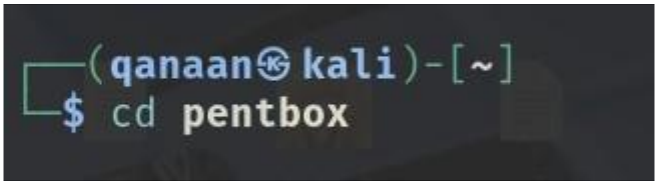
You ran the following command to download **PentBox** from GitHub. This command fetches the **PentBox** repository, which contains security and network tools, including a honeypot module.



```
┌──(qanaan㉿kali)-[~]
└─$ ls
CTF      Documents  Music     Public     Videos    lab.asm  test.asm
Desktop  Downloads  Pictures  Templates  hash.txt  pentbox
```

Figure 6

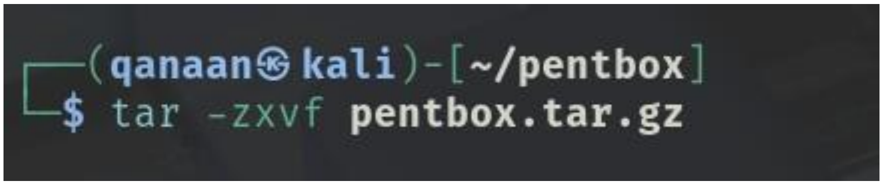
Next, we will see a directory with the name Pentbox in Kali Linux.



```
┌──(qanaan㉿kali)-[~]
└─$ cd pentbox
```

Figure 7

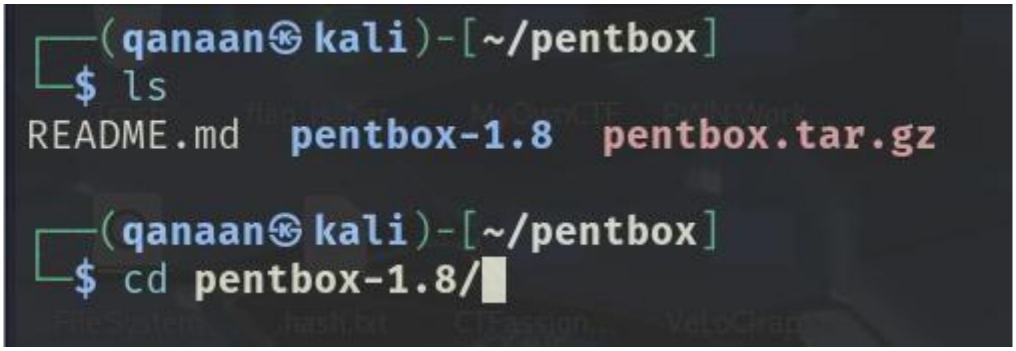
After that we go inside the **PentBox** directory, using the “cd” command where the scripts are stored.



```
┌──(qanaan㉿kali)-[~/pentbox]
└─$ tar -zxvf pentbox.tar.gz
```

Figure 8

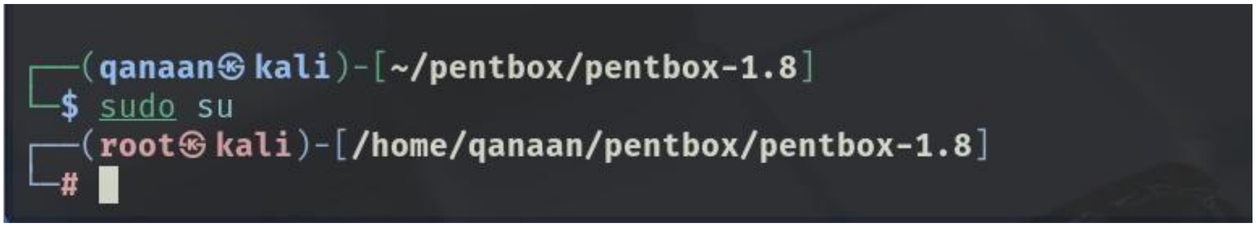
This command extracts the pentbox.tar.gz archive, unpacks the **PentBox** tool into the current directory, and displays the extracted files on the terminal.



```
┌──(qanaan㉿kali)-[~/pentbox]
└─$ ls
README.md  pentbox-1.8  pentbox.tar.gz

┌──(qanaan㉿kali)-[~/pentbox]
└─$ cd pentbox-1.8/
```

Figure 9

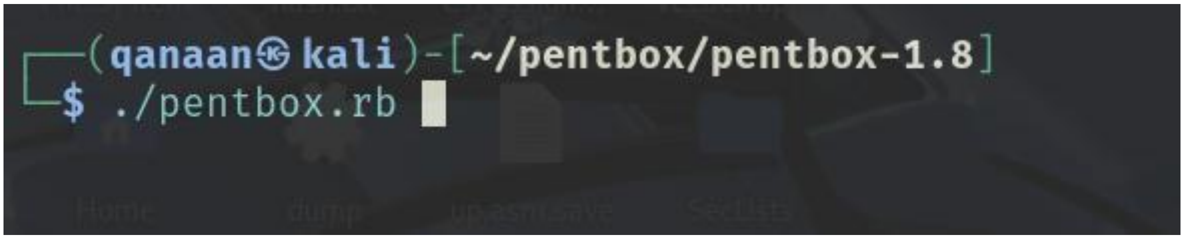
This command navigates into the **pentbox-1.8** directory, where the extracted PentBox tool is stored.



```
┌──(qanaan㉿kali)-[~/pentbox/pentbox-1.8]
└─$ sudo su
┌──(root㉿kali)-[/home/qanaan/pentbox/pentbox-1.8]
└─# 
```

Figure 10

But first we need to be change to the root user to run Pentbox and use Honeypot.



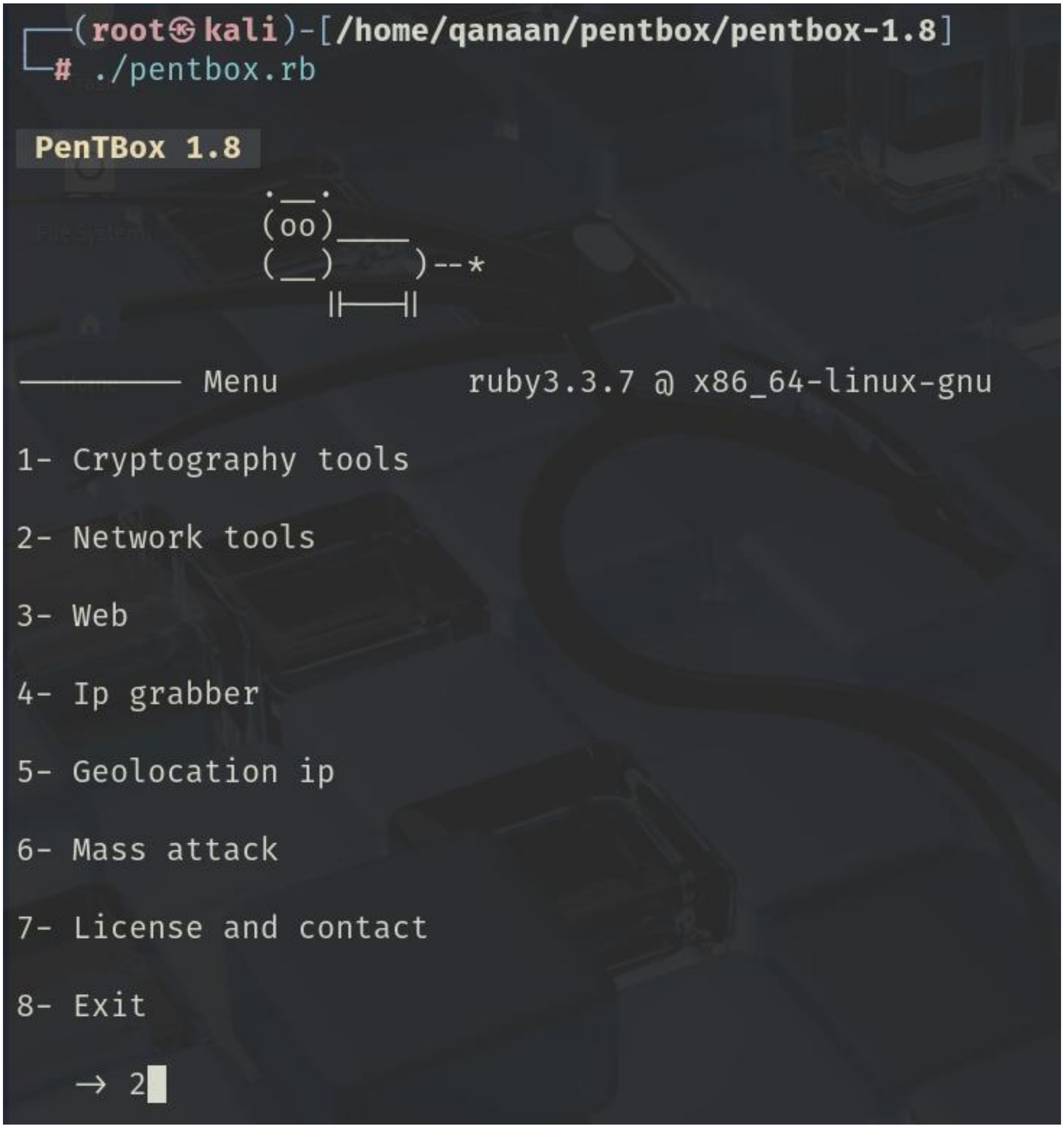
```
┌──(qanaan㉿kali)-[~/pentbox/pentbox-1.8]
└─$ ./pentbox.rb 
```

Figure 11

Run the following command to start Pentbox in Kali Linux:

3.2 Testing Honeypot

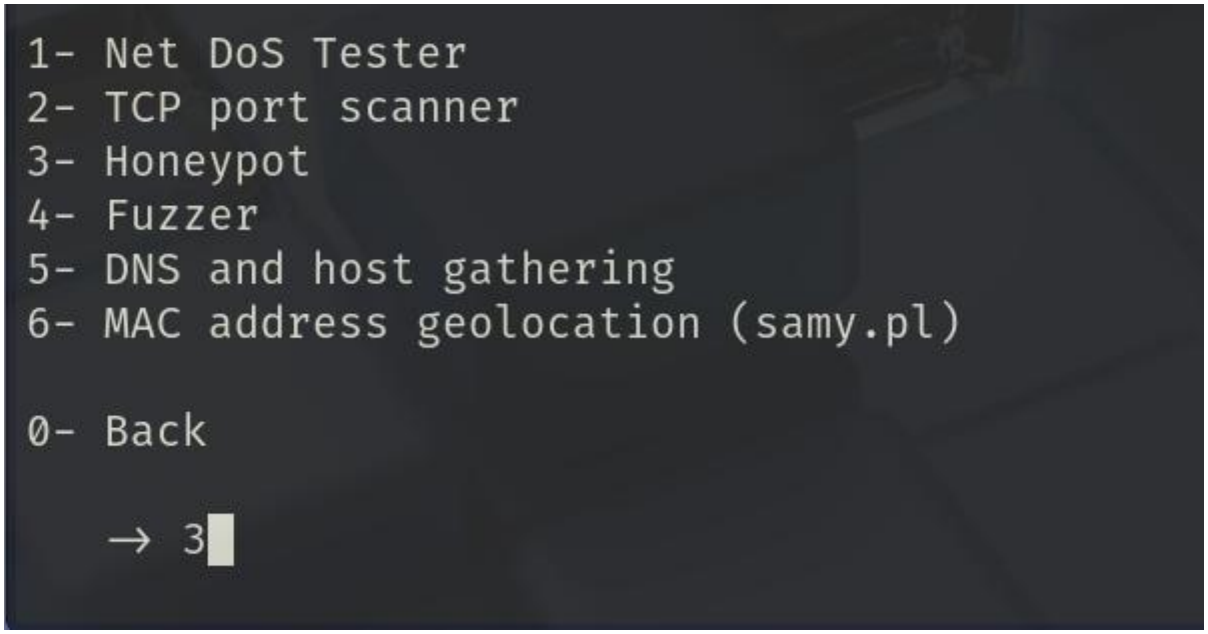
3.2.1 Fast Auto Configuration Option for Honeypot



```
┌──(root㉿kali)-[/home/qanaan/pentbox/pentbox-1.8]
└─# ./pentbox.rb

 PenTBox 1.8
               .__.
               (oo)____
               (__)    )--*
                  ||--||

 ───────── Menu         ruby3.3.7 @ x86_64-linux-gnu

 1- Cryptography tools

 2- Network tools

 3- Web

 4- Ip grabber

 5- Geolocation ip

 6- Mass attack

 7- License and contact

 8- Exit

    → 2
```

Figure 12

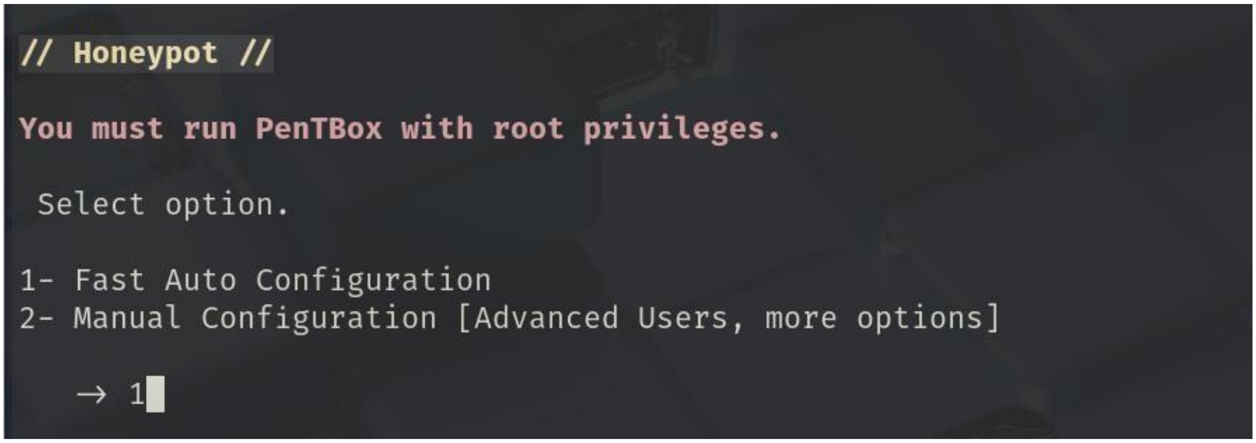
From the Pentbox menu, choose the Network tools section by typing number 2.



```
1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)

0- Back

   → 3
```

Figure 13

On this menu screen, type number 3 to select HONEYPOT.



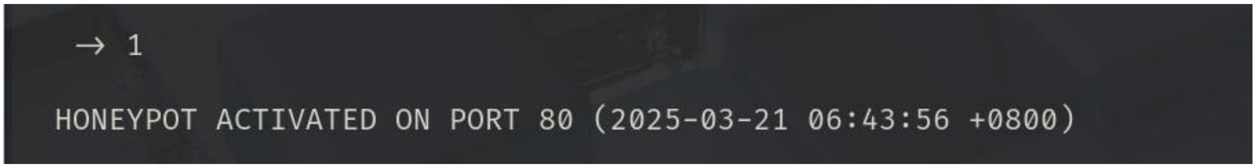
```
// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   → 1
```

Figure 14 Here,

there are 2options:

1. Fast Auto Configuration option,
2. Manual Configuration Functionality

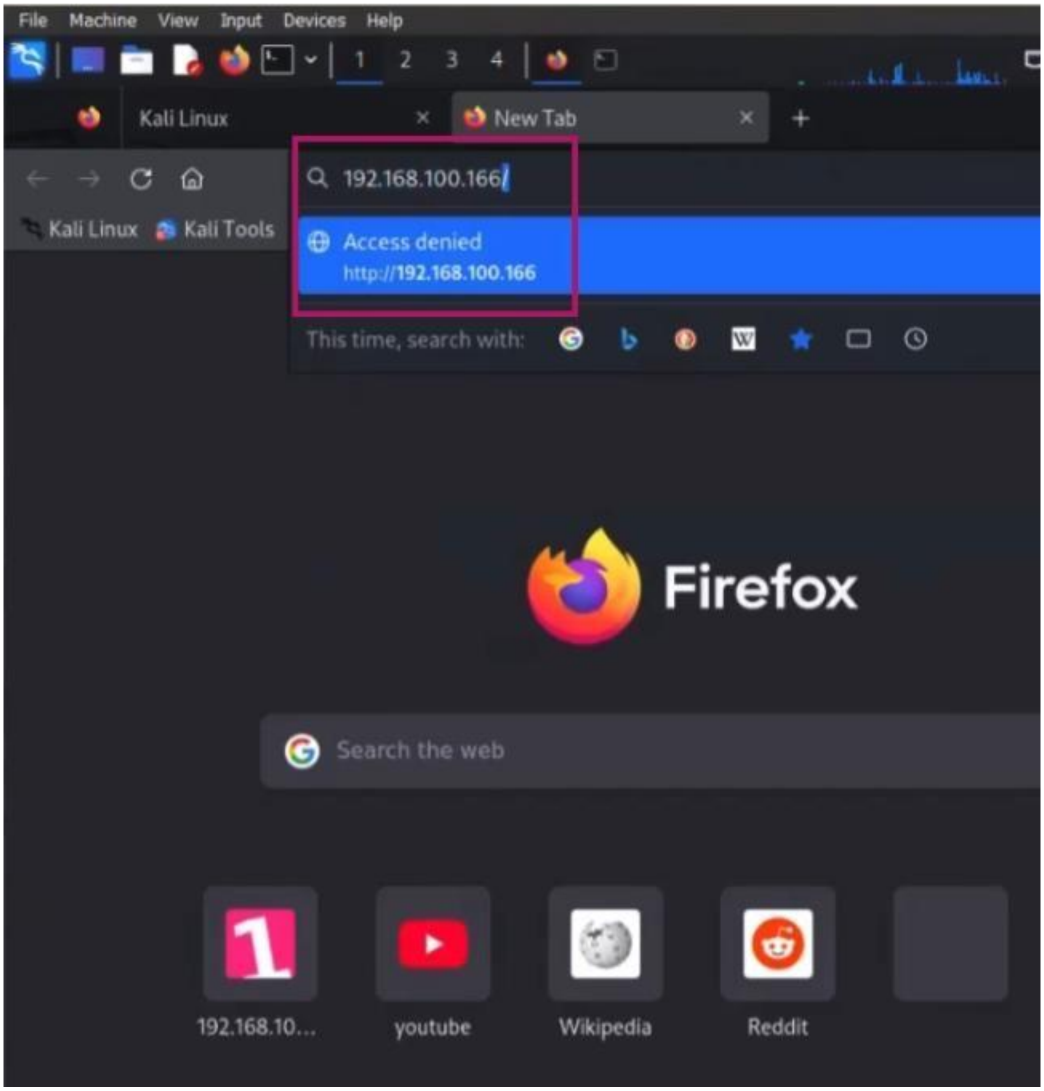
On the run Pentbox screen, type 2 to choose the Fast Auto Configuration option.



```
  → 1

HONEYPOT ACTIVATED ON PORT 80 (2025-03-21 06:43:56 +0800)
```

Figure 15

Now Honeypot is running, and will display a message says “HONEYPOT ACTIVATED ON PORT 80”

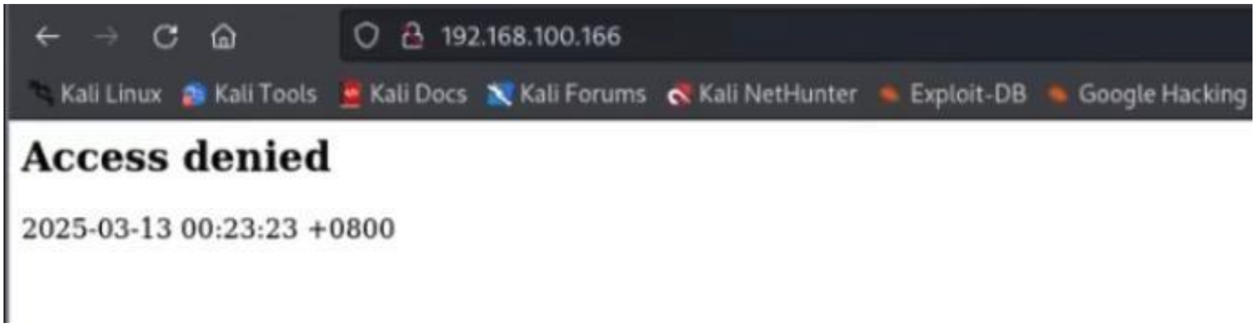


192.168.100.166/

Access denied
http://192.168.100.166

Figure 16

Open Firefox on the Kali machine, click on the address bar, and type the IP address of the Honeypot machine, which is: 192.168.100.166

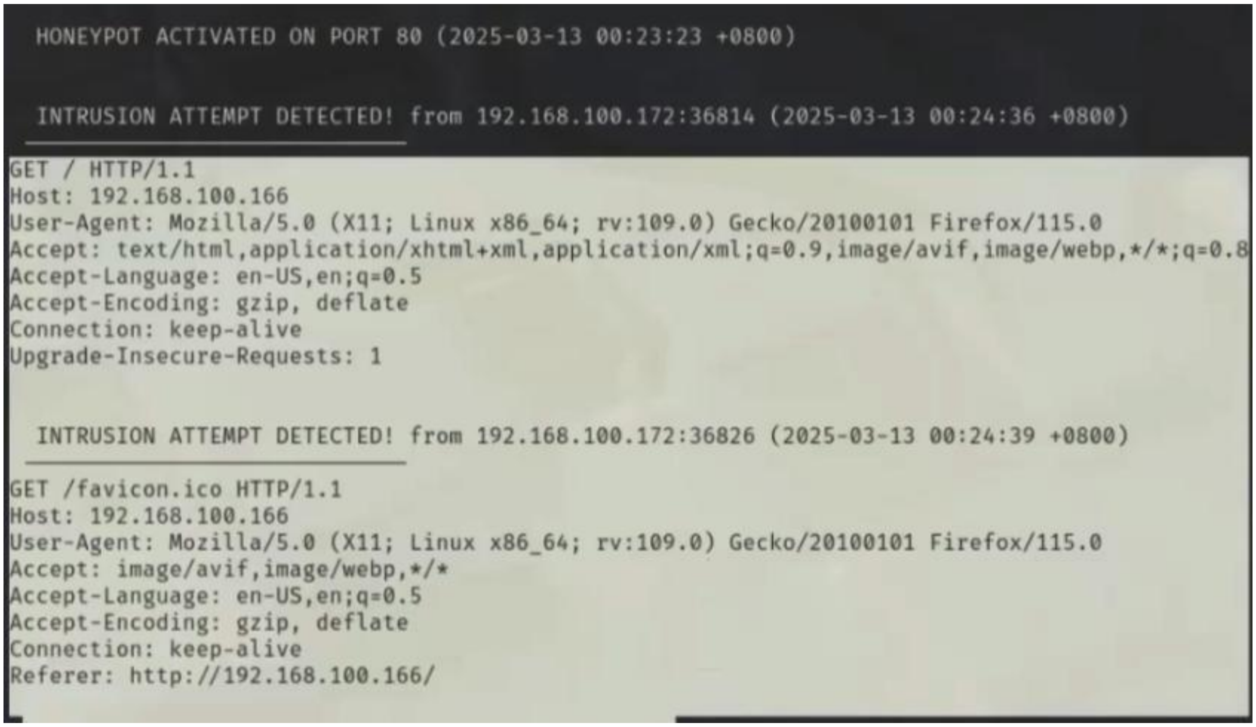


Access denied

2025-03-13 00:23:23 +0800

Figure 17

The webpage displays an "Access denied" message.

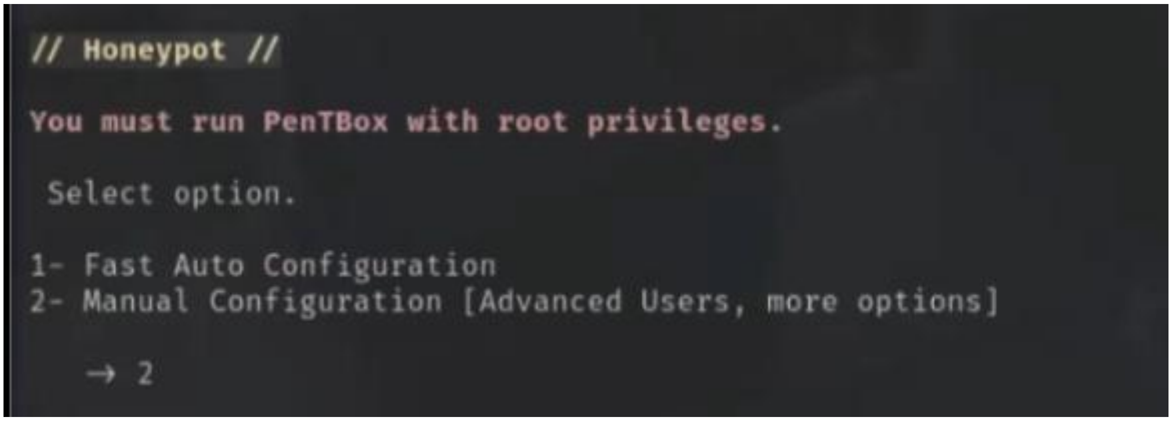


```
  HONEYPOT ACTIVATED ON PORT 80 (2025-03-13 00:23:23 +0800)

  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:36814 (2025-03-13 00:24:36 +0800)

GET / HTTP/1.1
Host: 192.168.100.166
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1


  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:36826 (2025-03-13 00:24:39 +0800)

GET /favicon.ico HTTP/1.1
Host: 192.168.100.166
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.100.166/
```

Figure 18

The message INTRUSION ATTEMPT DETECTED from the IP address 192.168.100.172 appears in the Kali terminal window.

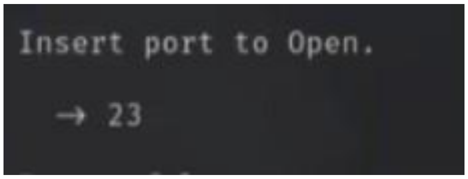
3.2.2 Manual Configuration for Honeypot



```
// Honeypot //

You must run PenTBox with root privileges.

 Select option.

1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]

   → 2
```

Figure 19

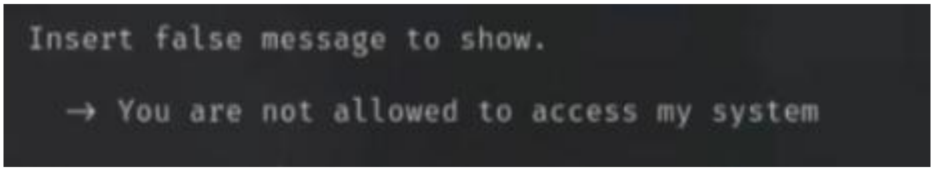
Now let’s test Honeypot with the manual configuration option by typing number 2.



```
Insert port to Open.

  → 23
```

Figure 20

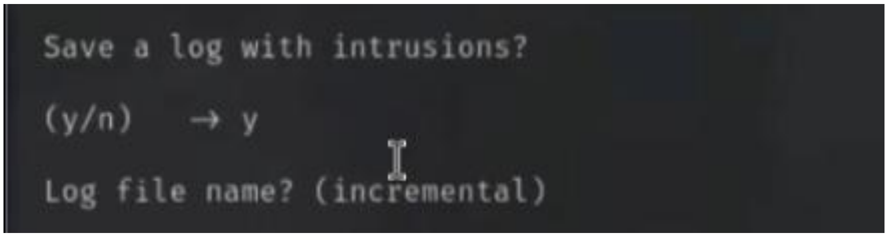
Set a port number, in this case is 23.



```
Insert false message to show.

  → You are not allowed to access my system
```

Figure 21 Insert

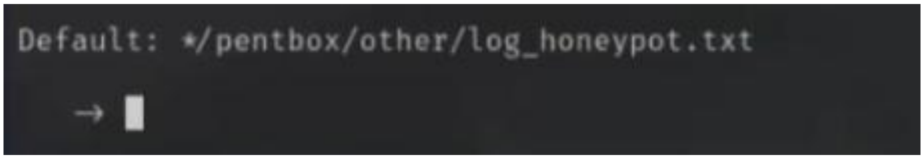
a false message to show the attacker.



```
Save a log with intrusions?

(y/n)   → y

Log file name? (incremental)
```

Figure 22 Here

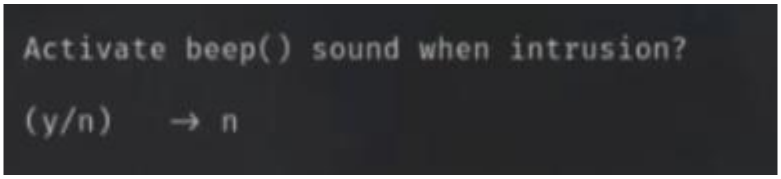
we need to press ‘y’ to save the logs.



```
Default: */pentbox/other/log_honeypot.txt

   → 
```

Figure 23

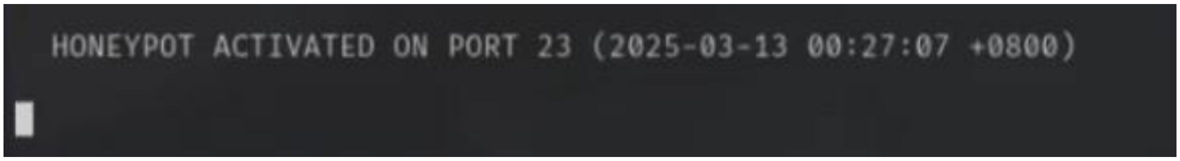
Press **Enter** for Default: */pentbox/other/log_honeypot.txt.



```
Activate beep() sound when intrusion?

(y/n)   → n
```

Figure 24 To

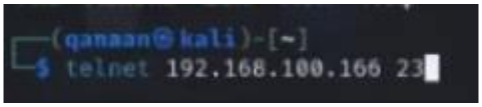
not activate the beep sound, we press ‘n’.



```
  HONEYPOT ACTIVATED ON PORT 23 (2025-03-13 00:27:07 +0800)
```

Figure 25

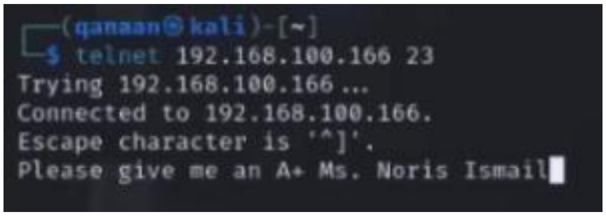
Now Honeypot is running, and will display a message says “HONEYPOT ACTIVATED ON PORT 23”



```
┌──(qanaan㉿kali)-[~]
└─$ telnet 192.168.100.166 23
```

Figure 26

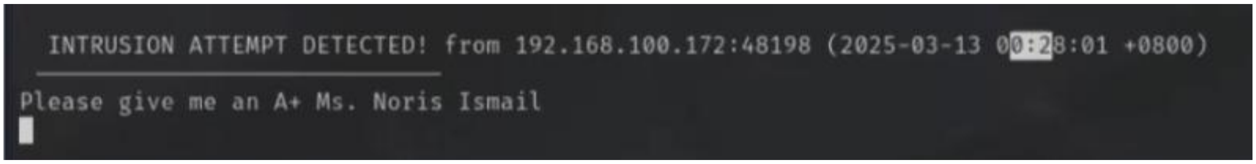
In the attacker kali machine, launch a new terminal and enter the telnet command, then the port number and the IP address of the Honeypot host 192.168.100.166 port number 23.



```
┌──(qanaan㉿kali)-[~]
└─$ telnet 192.168.100.166 23
Trying 192.168.100.166 ...
Connected to 192.168.100.166.
Escape character is '^]'.
Please give me an A+ Ms. Noris Ismail
```

Figure 27

Now the attacker machine is connected to the Honeypot machine successfully. The attacker will try to send a message to the Honeypot machine.

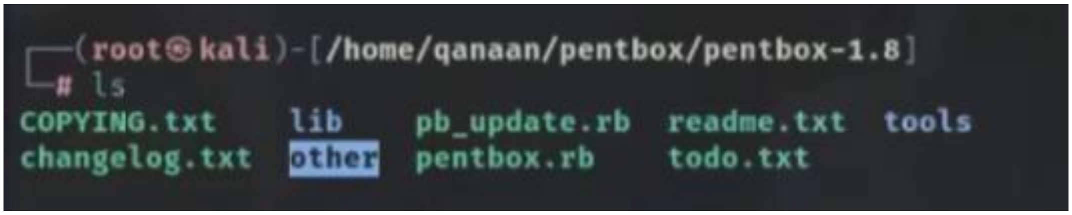


```
  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:48198 (2025-03-13 00:28:01 +0800)
 ─────────────────────────────────────
Please give me an A+ Ms. Noris Ismail
```

Figure 28

The message intrusion attempt detected from the ip address 192.168.100.172 appears in the Kali terminal window with the attacker message “Please give me an A+ Ms. Noris Ismail”.

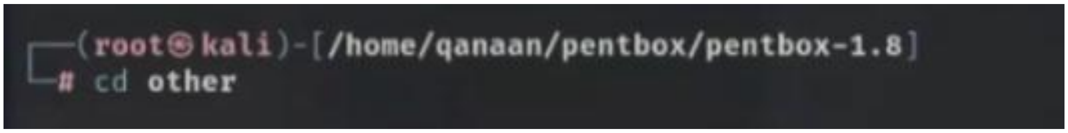
3.2.3 Viewing the Honeypot Logs



```
┌──(root㉿kali)-[/home/qanaan/pentbox/pentbox-1.8]
└─# ls
COPYING.txt    lib    pb_update.rb  readme.txt  tools
changelog.txt  other  pentbox.rb    todo.txt
```

Figure 29

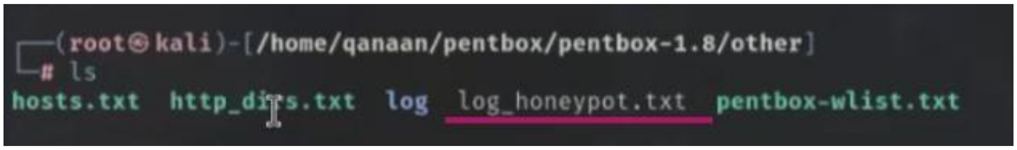
Listening the contents of the pentbox directory, the **"other"** directory is significant as it contains of honeypot including logs.



```
┌──(root㉿kali)-[/home/qanaan/pentbox/pentbox-1.8]
└─# cd other
```

Figure 30 Use

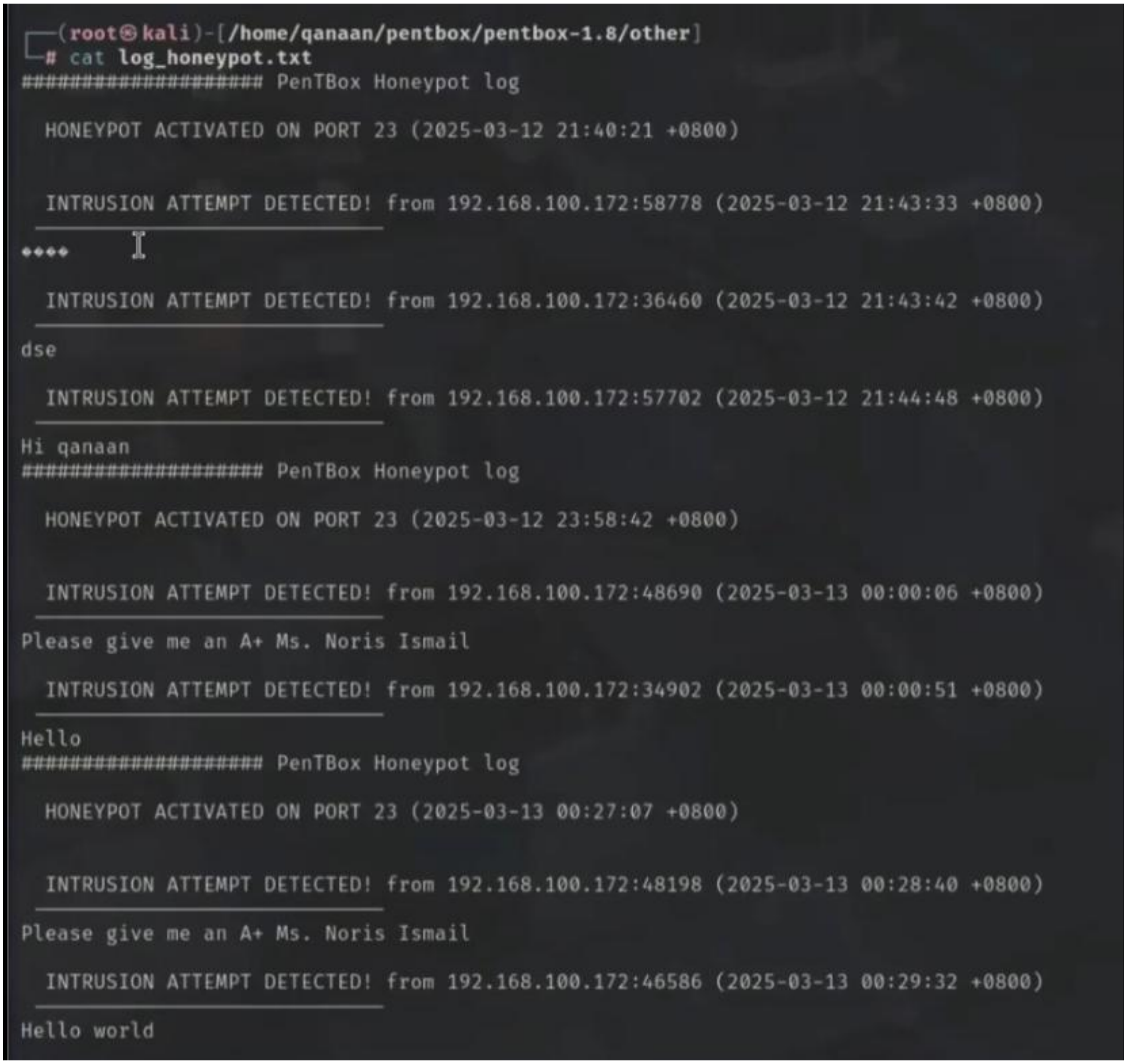
the “cd other” command to enter the directory.



```
┌──(root㉿kali)-[/home/qanaan/pentbox/pentbox-1.8/other]
└─# ls
hosts.txt  http_dirs.txt  log  log_honeypot.txt  pentbox-wlist.txt
```

Figure 31 Listing

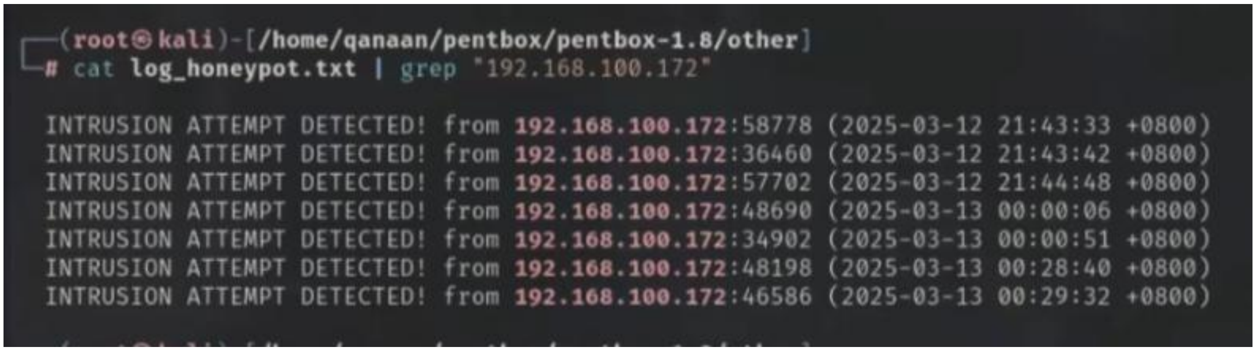
the files in the "other" directory.



```
┌──(root㉿kali)-[/home/qanaan/pentbox/pentbox-1.8/other]
└─# cat log_honeypot.txt
#################### PenTBox Honeypot log

  HONEYPOT ACTIVATED ON PORT 23 (2025-03-12 21:40:21 +0800)


  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:58778 (2025-03-12 21:43:33 +0800)
 -----------------------------
****

  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:36460 (2025-03-12 21:43:42 +0800)
 -----------------------------
dse

  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:57702 (2025-03-12 21:44:48 +0800)
 -----------------------------
Hi qanaan
#################### PenTBox Honeypot log

  HONEYPOT ACTIVATED ON PORT 23 (2025-03-12 23:58:42 +0800)


  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:48690 (2025-03-13 00:00:06 +0800)
 -----------------------------
Please give me an A+ Ms. Noris Ismail

  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:34902 (2025-03-13 00:00:51 +0800)
 -----------------------------
Hello
#################### PenTBox Honeypot log

  HONEYPOT ACTIVATED ON PORT 23 (2025-03-13 00:27:07 +0800)


  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:48198 (2025-03-13 00:28:40 +0800)
 -----------------------------
Please give me an A+ Ms. Noris Ismail

  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:46586 (2025-03-13 00:29:32 +0800)
 -----------------------------
Hello world
```

Figure 32

To View the Honeypot Logs, we use “cat log_honeypot.txt” command to reveal the output of multiple intrusion attempts.



```
┌──(root㉿kali)-[/home/qanaan/pentbox/pentbox-1.8/other]
└─# cat log_honeypot.txt | grep "192.168.100.172"

  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:58778 (2025-03-12 21:43:33 +0800)
  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:36460 (2025-03-12 21:43:42 +0800)
  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:57702 (2025-03-12 21:44:48 +0800)
  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:48690 (2025-03-13 00:00:06 +0800)
  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:34902 (2025-03-13 00:00:51 +0800)
  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:48198 (2025-03-13 00:28:40 +0800)
  INTRUSION ATTEMPT DETECTED! from 192.168.100.172:46586 (2025-03-13 00:29:32 +0800)
```

Figure 33

This gives a clearer picture of recurring intrusion attempts by filtering and extracting only the log entries about the IP 192.168.100.172. The findings support several attempts at unauthorized connections in a brief period of time, raising the possibility of reconnaissance or brute-force attacks.

4.0 Conclusion

As an integral part of cybersecurity, honeypots enable preliminary threat detection, attack evaluation, and deception-based security. Honeypots enable security personnel to analyze the attacker's activities in greater detail and construct more advanced defensive measures against an attack by redirecting the attacker's attention from vital infrastructure to non-essential systems. Organizations can stay ahead of changing threats due to the varying levels of insight into attacker behaviors that can be obtained from a variety of types of honeypots, such as low and high interaction, email, and malware honeypots.

However, the use of honeypots comes with a set of inherent problems. Through distinctive fingerprinting, attackers are able to identify honeypots and then proceed to launch denial-ofservice attacks and then compromise and exploit the system for further attacks. Analyzing honeypot data requires skilled personnel, and in addition to proper isolation and frequent updating, these systems also need sophisticated personnel to effectively interpret the data. Despite these limitations, Microsoft's IoT honeypot experiment is a real-world example that shows how honeypots are invaluable in the detection of botnets, malware campaigns, and attempted intrusions.

Organisations must adhere to best practices like appropriate network segmentation, secure logging, real-time monitoring, and deception techniques in order to optimise the efficiency of honeypots. Honeypots are a useful addition to current security infrastructures when they are integrated with firewalls, intrusion detection systems (IDS), and security information and event management (SIEM) programs.

In summary, honeypots are an essential part of a larger cybersecurity strategy and should not be utilized as a stand-alone security measure. When properly deployed, they improve proactive security measures, offer vital intelligence on new threats, and fortify an organization's overall defense posture against cybercriminals. The strategic placement of honeypots will continue to be a potent instrument for cybersecurity research, network defense, and cyber threat intelligence collection as long as cyber threats continue to change.

5.0 References

What is a honeypot? meaning, types, benefits, and more | Fortinet. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-honeypot

Vaideeswaran, N. (2025, January 16). *Honeypots in cybersecurity explained*. Crowdstrike. https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/honeypots/

Wikipedia contributors. (2024, November 8). *Honeypot (computing)*. Wikipedia. https://en.wikipedia.org/wiki/Honeypot_(computing)

Disadvantages of honeypots | The value of honeypots | InformIT. (n.d.). https://www.informit.com/articles/article.aspx?p=30489&seqNum=2

Baig, Z., Choo, K.-K. R., & Salah, K. (2017). Forensic Investigation of Cyber Harassment and Online Threats Using Honeypots. *Proceedings of the IEEE Trustcom/BigDataSE/ICESS* , 501–508. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.251

Thakkar, M. (2022, July 28). *Security Honeypot: 5 tips for setting up a honeypot - InfoSec Insights*. InfoSec Insights. https://sectigostore.com/blog/security-honeypot-5-tips-for-setting-upa-honeypot/

Lutkevich, B. (2021, March 31). *How to build a honeypot to increase network security*. WhatIs. https://www.techtarget.com/whatis/feature/How-to-build-a-honeypot-to-increase-networksecurity

Grant, D. (2024, July 19). New honeypot techniques for addressing targeted attacks. *Security Magazine*. https://www.securitymagazine.com/articles/100865-new-honeypot-techniques-foraddressing-targeted-attacks

UK Cyber Security Ltd. (2025, February 24). *Stopping attacks before they start: Honeypot Best practices for Enterprises*. UK Cyber Security Group Ltd. https://www.ukcybersecurity.co.uk/blog/news-advice/stopping-attacks-before-they-starthoneypot-best-practices-for-enterprises/

Borges, E. (2021, August 25). *Best Honeypots for Detecting Network Threats*. Securitytrails.

https://securitytrails.com/blog/top-honeypots

Ops, A. H. (2023, August 11). Enterprise Network Security — How to Install and Configure a Honeypot with PentBox on Kali Linux to Detect an Intrusion. *Medium*. https://medium.com/@anbuhackops/enterprise-network-security-how-to-install-and-configure-ahoneypot-with-pentbox-on-kali-linux-a1caf7441639