Guide: Installing and Configuring a Honeypot with PentBox on Kali Linux

This guide will walk you through the process of installing and configuring a basic honeypot using **PentBox** on **Kali Linux**. A honeypot is a security mechanism that lures attackers by simulating vulnerabilities. PentBox is a lightweight security tool used to set up various security scenarios, including honeypots, which can help detect potential intrusions in an enterprise network.

Table of Contents

---

1. Introduction to Honeypots

A **honeypot** is a decoy system or resource that is deliberately made vulnerable to entice cyber attackers. By monitoring the interactions with a honeypot, administrators can detect unauthorized access attempts and gather intelligence about attack methods. This information can be useful for strengthening your enterprise network security.

---

2. What is PentBox?

PentBox is a security suite written in Ruby that offers various tools for network analysis and penetration testing. One of its most useful features is the ability to create a simple **honeypot** to detect network intrusions. While PentBox is not as advanced as some other honeypot solutions, it is easy to install and configure, making it ideal for lightweight honeypot implementations.

---

3. Prerequisites

Before you begin, ensure the following:

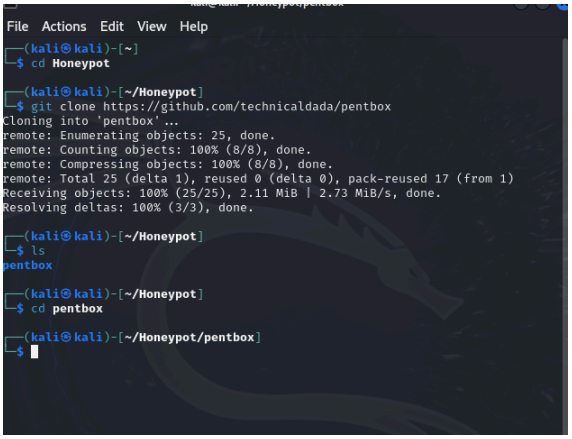
- You have **Kali Linux** installed on your system.
- You have **root access** or appropriate privileges to install software.
- **Ruby** is installed on your Kali Linux (it comes pre-installed on most Kali versions).
- Basic understanding of networking and Linux commands.

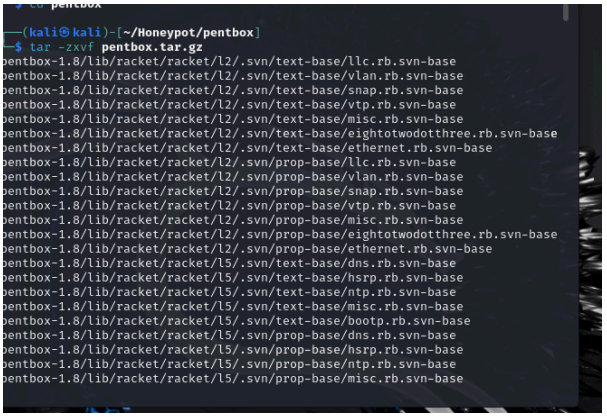
---

4. Step-by-Step Guide: Installing and Configuring PentBox Honeypot

Step 1: Update Your Kali Linux

Before installing PentBox, it's a good practice to update the system to ensure that you are running the latest packages. sudo apt update && sudo apt upgrade -y





Step 2: Install PentBox on Kali Linux

You can download PentBox directly from GitHub or clone it to your system using the following command:

git clone https://github.com/technicaldada/pentbox.git

cd pentbox

cd pentbox-1.8

Step 3: Configuring the Honeypot

To configure a honeypot in PentBox, follow these steps:

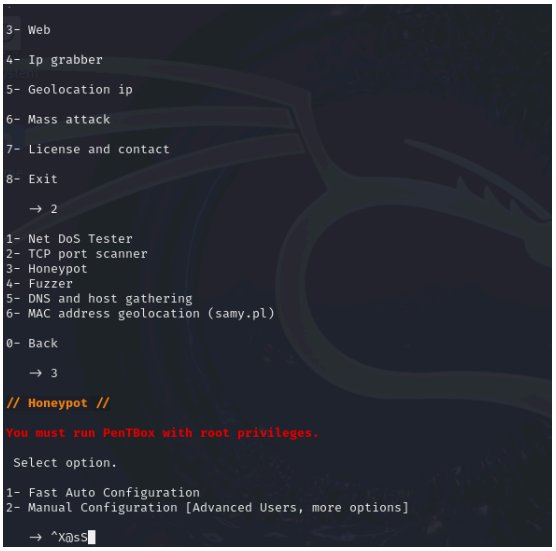
./pentbox.rb

Select the Network tools section from the Pentbox menu by typing:

2

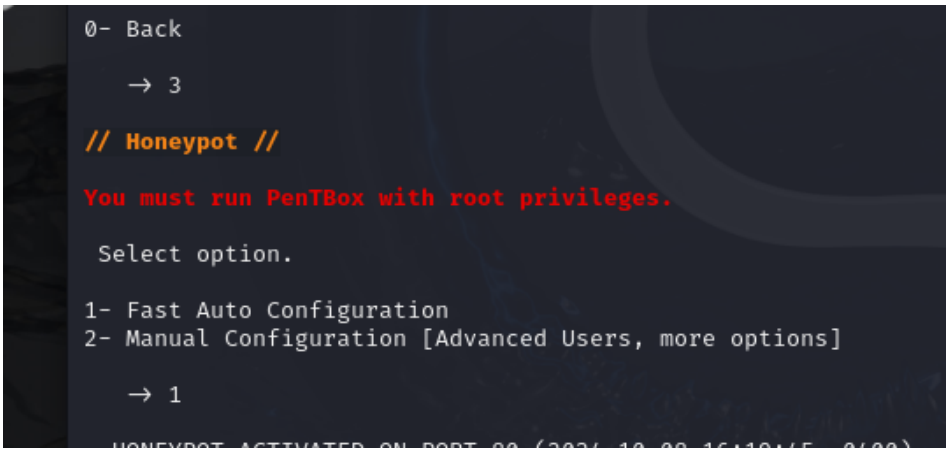
You will see a menu with several options. Select the Honeypot option by typing its corresponding number, 3(Honeypot option) in PentBox's menu:

3



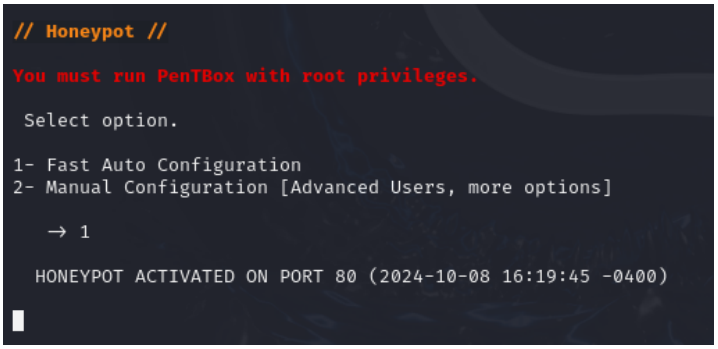
select the Fast Auto Configuration option, on the run Pentbox screen, type:

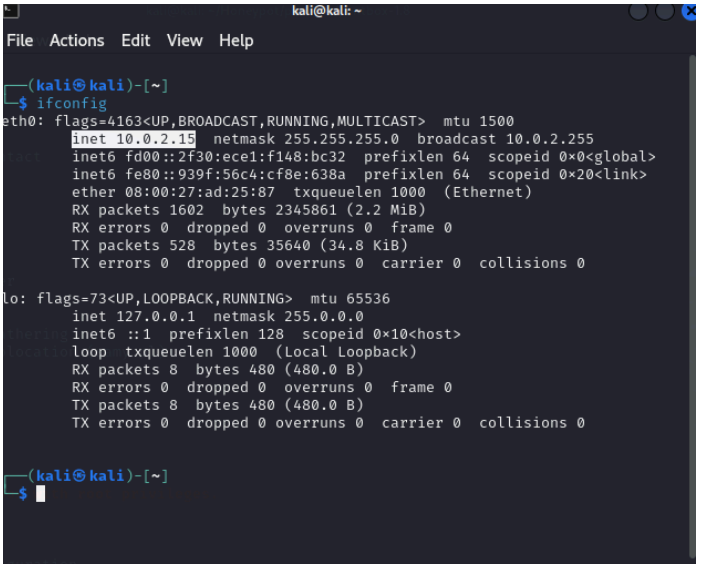
1



The next screen will ask you to configure the port you want the honeypot to listen on. Common ports targeted by attackers include 22 (SSH), 23 (Telnet), or 80 (HTTP).

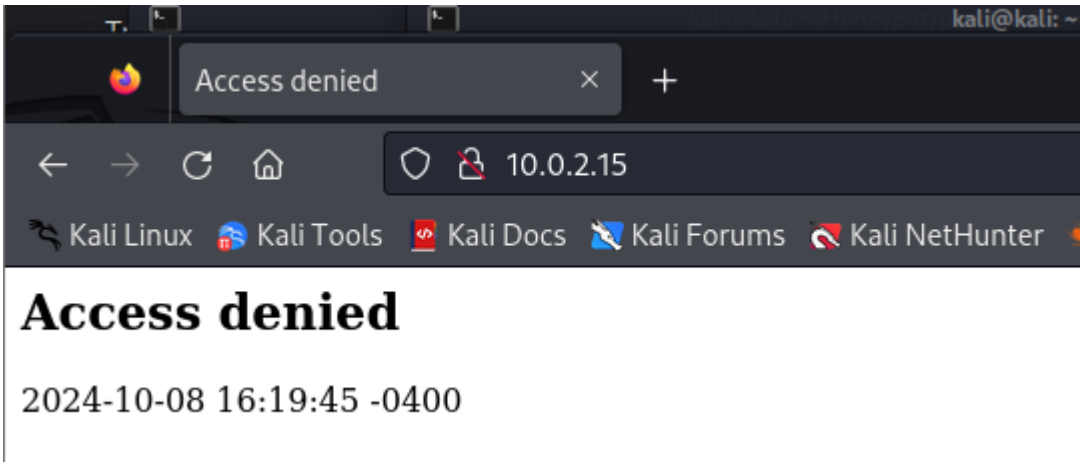
You will get a notification that the HONEYPOT ACTIVATED ON PORT 80.





Test Honeypot Fast Auto Configuration Functionality with a new Kali Linux tab: ifconfig

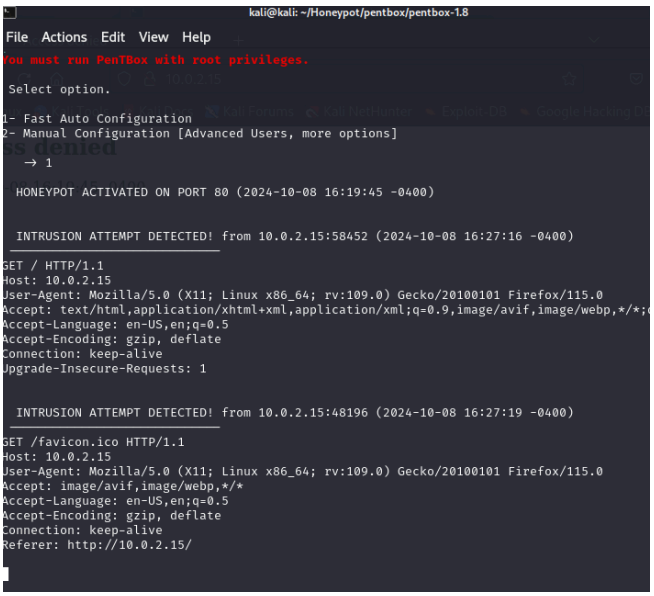
Open Firefox on the Kali Linux machine, click on the address bar, and type: which will be different for each, mine is 10.0.2.15 then enter. An “Access denied” message appears on the web page.



The Kali terminal window displays INTRUSION ATTEMPT DETECTED from 10.0.2.15:50061.

Note that the port numbers may vary.

In a real scenario, the system administrator where the honeypot is deployed can take the appropriate measures to strengthen a computer system’s defenses.

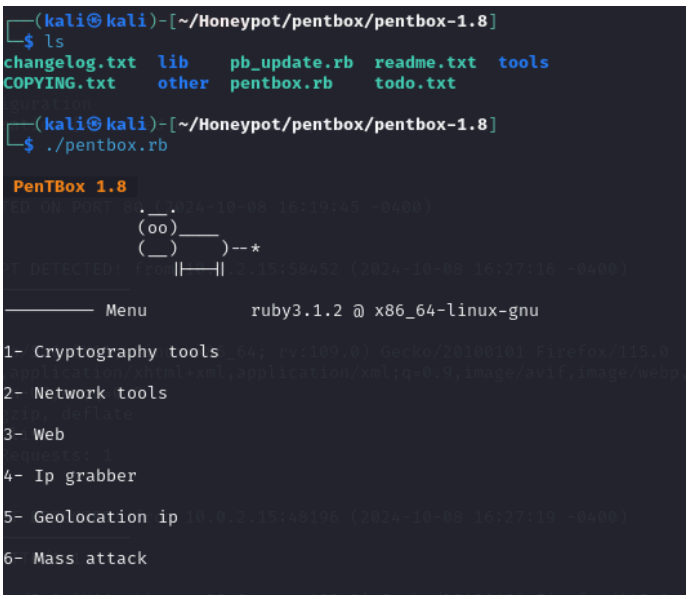


Test Honeypot Manual Configuration Functionality with Parrot.

IP Address of Parrot machine: 10.0.2.15

Run Pentbox in Kali Linux: ./pentbox.rb

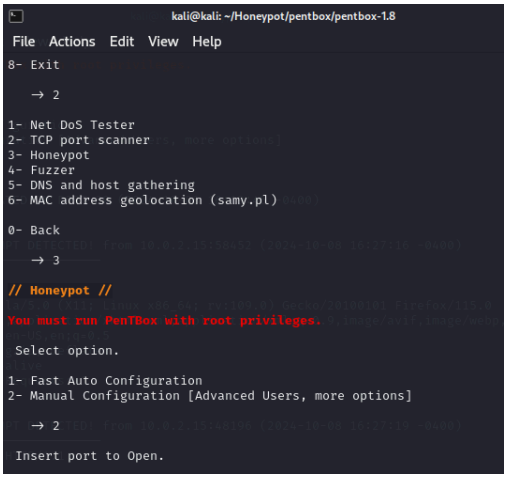
Select the network tools section: 2

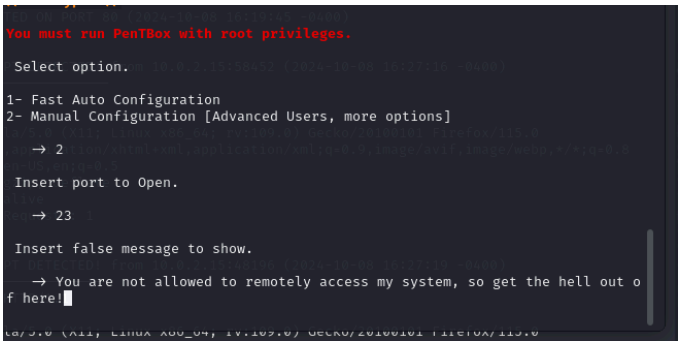


On the next menu screen, type: 3

Then select the Manual Configuration option on the run Pentbox screen by typing: 2

Set up the manual configurations with the following commands, Port number: 23





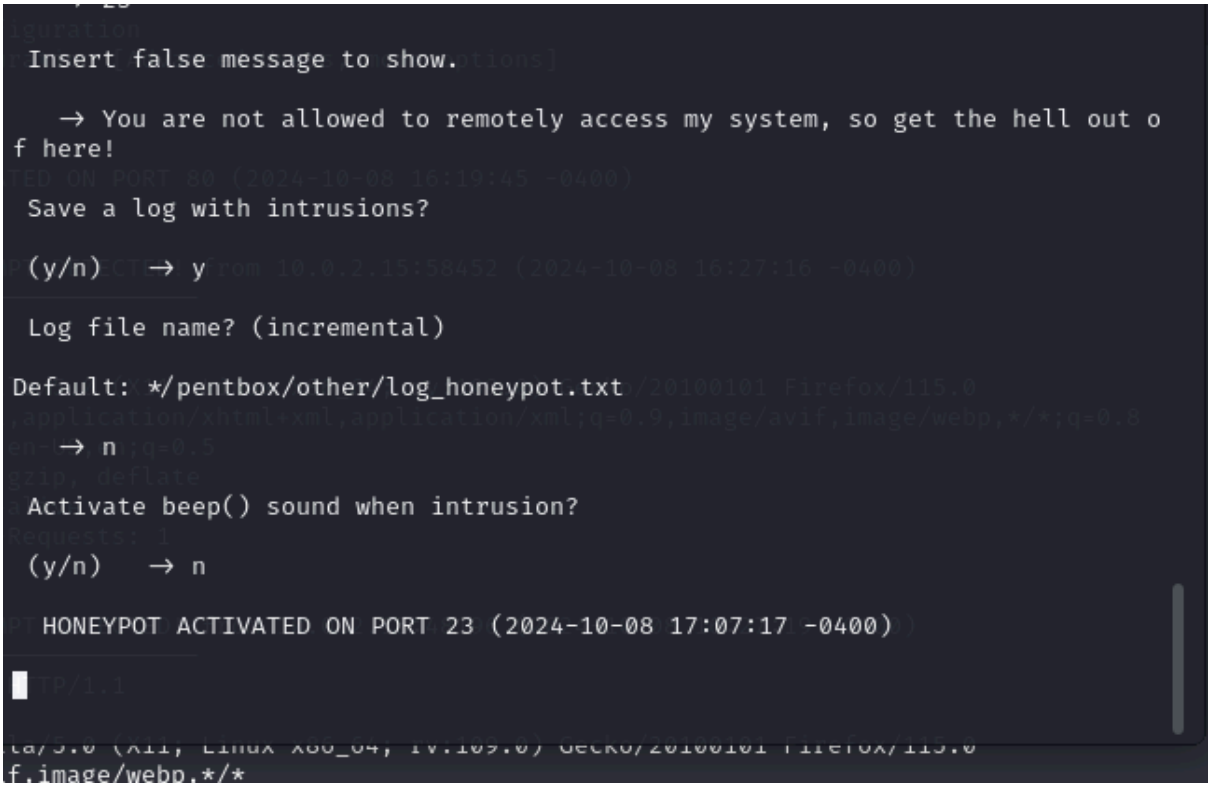
Insert false message to show: “You are not allowed to remotely access my system, so get the hell out of here!”

Save a log with intrusion? Y

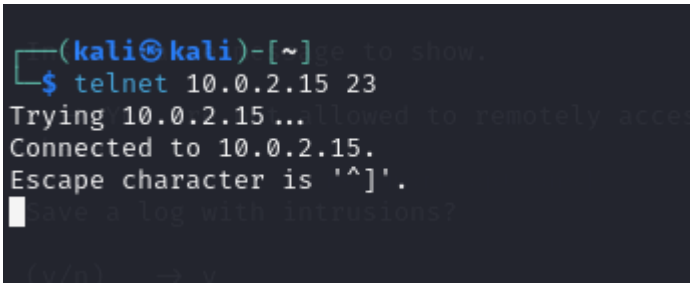
press Enter for Default: */pentbox/other/log_honeypot.txt.

Activate beep sound? N

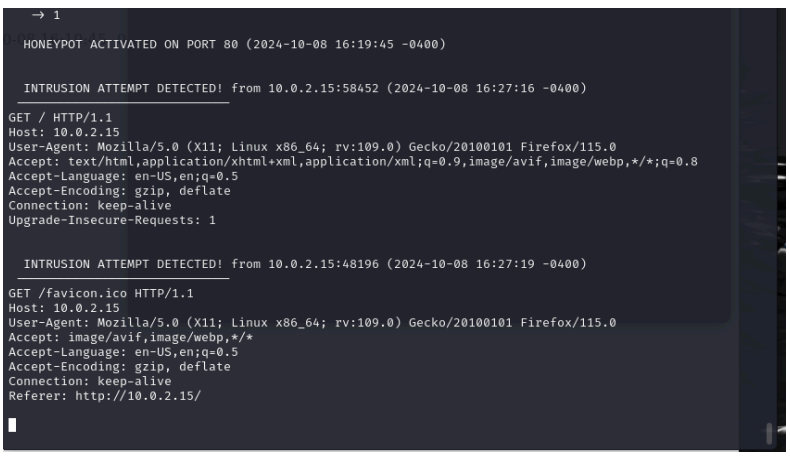
You will be notified that the **HONEYPOT ACTIVATED ON PORT 23,** the Telnet service.



Open a new terminal in Kali Linux or Parrot and run the telnet command followed by the Honeypot host IP address and the port number:



The Kali Linux terminal window displays **INTRUSION ATTEMPT DETECTED from 10.0.2.15:59076.**



Test Honeypot Manual Configuration False message to show Functionality.

Apply the following manual configuration settings.

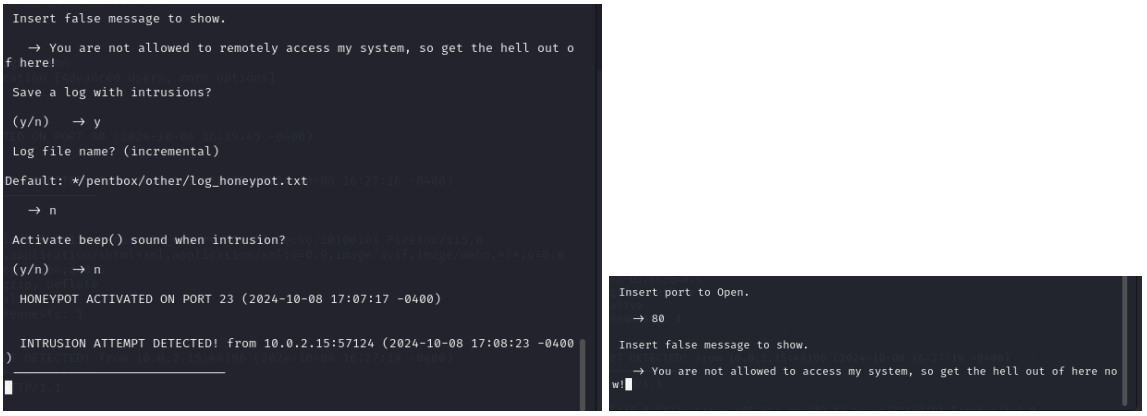
Port Number: 80

Insert false message to show: *You are not allowed to access my system, so get the hell out of here now!*

Save a log with intrusion? Y

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

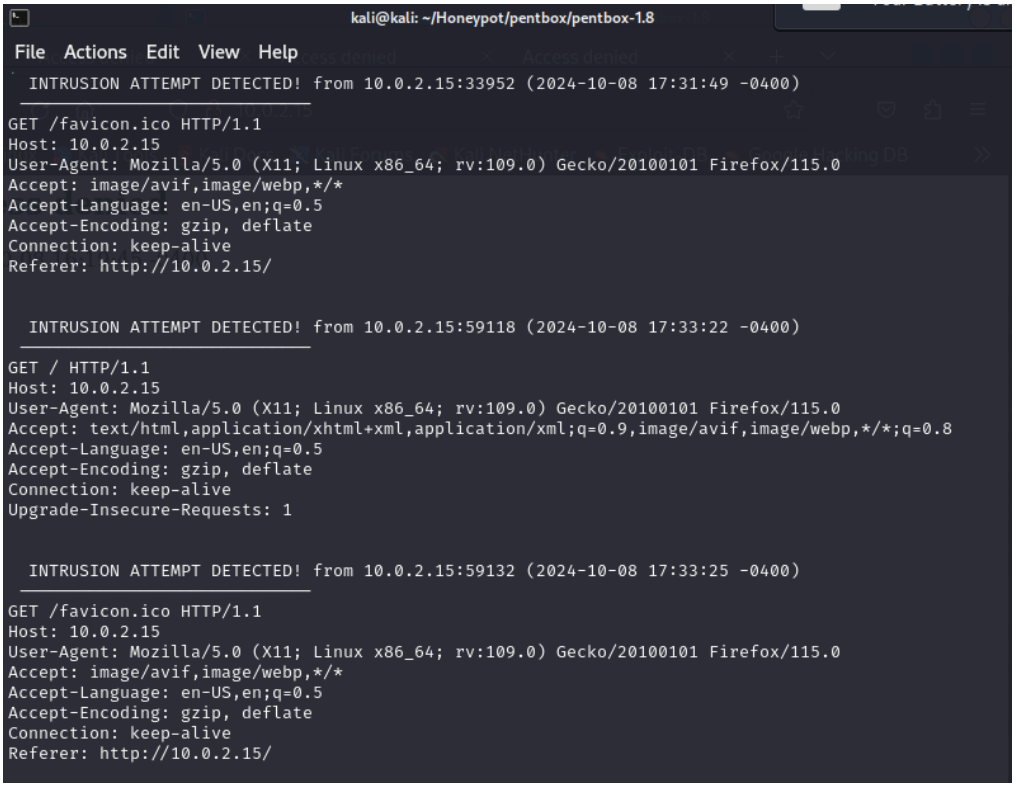
Activate beep sound? N



You will be notified that the **HONEYPOT ACTIVATED ON PORT 80.**

On the Kali machine, on the browser, click on the address bar and type: 10.0.2.15

The previously typed message appears on the web page as the access denied notice


kali@kali: ~/Honeypot/pentbox/pentbox-1.8
File Actions Edit View Help
INTRUSION ATTEMPT DETECTED! from 10.0.2.15:33952 (2024-10-08 17:31:49 -0400)
GET /favicon.ico HTTP/1.1
Host: 10.0.2.15
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://10.0.2.15/
INTRUSION ATTEMPT DETECTED! from 10.0.2.15:59118 (2024-10-08 17:33:22 -0400)
GET / HTTP/1.1
Host: 10.0.2.15
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 10.0.2.15:59132 (2024-10-08 17:33:25 -0400)
GET /favicon.ico HTTP/1.1
Host: 10.0.2.15
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://10.0.2.15/