# Pooh’s Pentbox HoneyPot

Contents

[Pentbox HoneyPot 1](#_Toc179108085)

[Pentbox 1](#_Toc179108086)

[What is a HoneyPot? 1](#_Toc179108087)

[Install Penbox 2](#_Toc179108088)

[Setup the HoneyPot 2](#_Toc179108089)

[Use the Honeypot 3](#_Toc179108090)

[Lessons Learned 3](#_Toc179108091)

[Assignment Submission 4](#_Toc179108092)

Time required: 60 minutes

# Pentbox

**Objective:** Download and install Pentbox.

**Description:** In this activity, you download and install Pentbox to create a HoneyPot. Pentbox is a safety kit containing various tools for streamlining PenTest conducting a job easily. It is programmed in Ruby and oriented to GNU / Linux, with support for Windows, MacOS and every system where Ruby is installed.

# What is a HoneyPot?

It has nothing to do with Winnie the Pooh, except that Winnie the Pooh is attracted to honey. A honeypot is a cybersecurity trap, like a fake system, designed to attract and study hackers, helping experts understand their tactics to enhance overall online security.

* **Threat Intelligence**: Gathers information on emerging threats, aiding in the development of effective countermeasures.
* **Incident Response Preparation**: Helps prepare and refine incident response strategies through simulated attack scenarios.
* **Training Environment**: Provides a safe space for security personnel to enhance their skills in dealing with cyber threats.

# Install Pentbox

**OS:** Kali Linux

1. Open a terminal session.
2. Run the following command to clone pentbox to your local system.

|  |
| --- |
| git clone https://www.github.com/technicaldada/pentbox  # Change to the pentbox directory  cd pentbox  # Extract the pentbox files  tar -xzvf pentbox.tar.gz  # List contents of the folder  ls |

1. You should see a pentbox-1.8 folder.

# Setup the HoneyPot

|  |
| --- |
| # Change to the program folder  cd pentbox-1.8  # Run the pentbox ruby script  sudo ./pentbox.rb |

1. You should see the pentbox menu.
2. Type **2** to go to Network tools.
3. Type **3** to go to Honeypot.
4. Type **1** for Fast Auto Configuration.
5. The Honeypot is activated and running on port 80.
6. Test the Honeypot by using a web browser to go to [127.0.0.1:80](https://www.blogger.com/127.0.0.1:80)
7. The message in your browser will say there isn’t a connection. That is how this is supposed to work. The Honeypot program captured your information.
8. Insert a screenshot.

Click or tap here to enter text.

1. Go back to the Honeypot terminal. You should see your activity logged to the screen.
2. Insert a screenshot.

Click or tap here to enter text.

# Use the Honeypot

This will be how a Honeypot is typically used, to capture information about a computer trying to connect to a website on a network.

1. Set your Kali Linux machine to a Bridged Adapter.
2. Use **ip a** to find your ip address.
3. From another computer go to a web browser and access the ip address of the Kali machine.
4. The message in your browser will say there isn’t a connection. That is how this is supposed to work. The Honeypot program captured your information.
5. Insert a screenshot.

Click or tap here to enter text.

1. Go back to Kali Linux to the Honeypot terminal. Your activity is logged to the screen.
2. Insert a screenshot.

Click or tap here to enter text.

# Lessons Learned

A honeypot is a security tool used to attract and detect cyberattacks. It works by simulating a vulnerable system or network that looks like a real target to attackers. When a hacker tries to breach the honeypot, their actions are monitored and recorded. This helps cybersecurity professionals learn about attack methods and improve defenses.

Key points for beginners:

* It’s a decoy, not a real system.
* It gathers data about attackers, such as techniques and tools used.
* It helps improve security without exposing real systems to harm.

In the case of this tutorial, it was a website that didn’t appear to work.

## Assignment Submission

Attach this completed document to the assignment in Blackboard.