Cybersecurity 701

Honeypot Lab

Honeypot Materials

- Materials needed
  - Kali Linux Virtual Machine

- Software tool used
  - PenTBox

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 1.2 – Summarize fundamental security concepts.
    - Deception and disruption technology
      - Honeypot
      - Honeyfile
      - Honeynet
      - Honeytoken

What is a Honeypot?

- A honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems
- In this lab, you will create and test a honeypot.

```
 INTRUSION ATTEMPT DETECTED! from 10.1.37.69:59672 (2021-04-30 13:55:06 +0000)
 ----------------------------
GET /favicon.ico HTTP/1.1
Host: 10.1.36.106
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/90.0.4430.93 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://10.1.36.106/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

A honeypot detecting an intrusion attempt

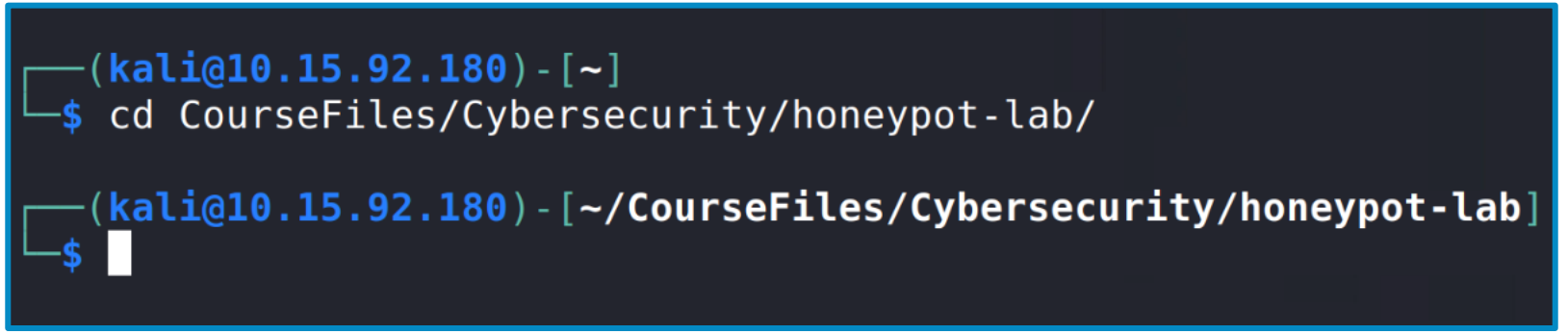
Honeypot Lab Overview

1. Locate PenTBox
2. Run PenTBox with Root Privileges
3. Create the Honeypot
4. Test the Honeypot
5. Investigate Honeypot Findings

Locate PenTBox

Locate and use PenTBox to create a honeypot

- Open a terminal
- Navigate to the honeypot-lab folder:
  - **`cd CourseFiles/Cybersecurity/honeypot-lab`**

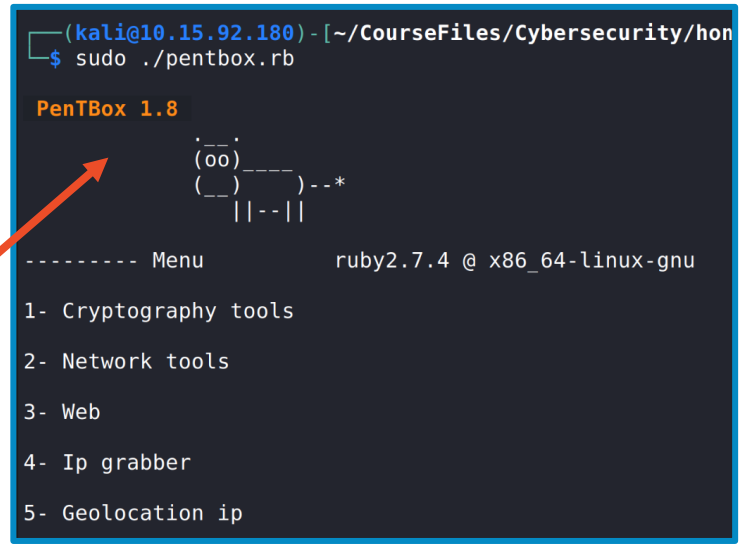


Run PenTBox with Root Privileges

You can use PenTBox with basic user privileges, but to create the honeypot, we need root privileges.

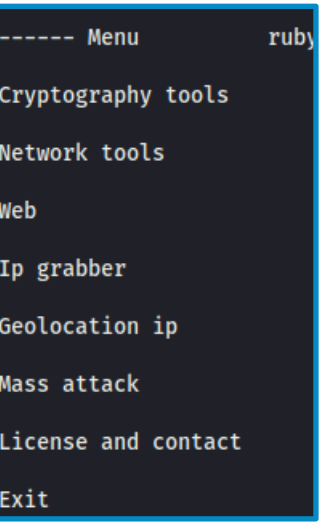
- Navigate into the PenTBox directory:
  - **`cd pentbox-1.8/`**
- Start PenTBox with root privileges:
  - **`sudo ./pentbox.rb`**

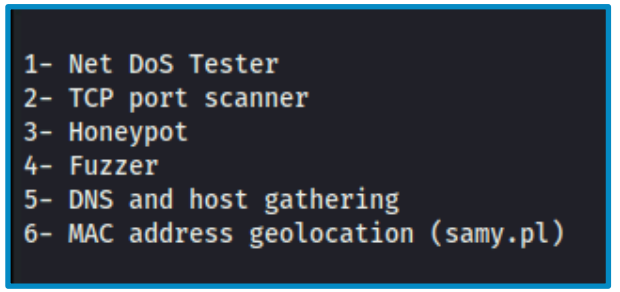
You should see PenTBox open in the Terminal

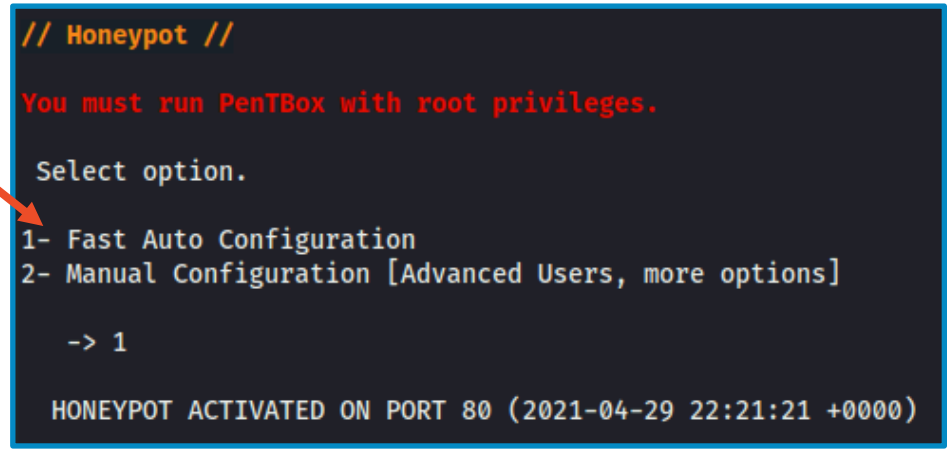


Create the Honeypot

- Choose "Network tools"
  - 2
- Choose "Honeypot"
  - 3
- Choose "Fast Auto Configuration"
  - 1







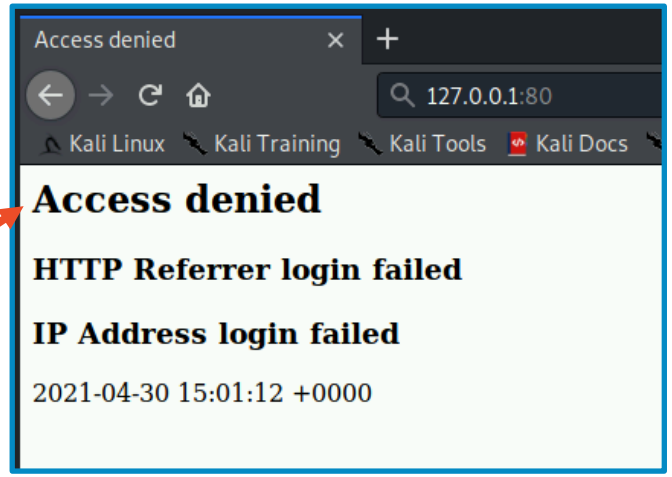
Test the Honeypot

Now that the honeypot is created, we need to see how it works.

- Open a web browser and navigate to:

  `127.0.0.1:80`

Notice that access is denied when attempting to access the webpage



Refresh the webpage multiple times to see multiple intrusion attempts

*Please Note: If trying to access from a different system (like the Windows VM), you would enter the URL <KALI_IP_ADDRESS>

Investigate Honeypot Findings

- Go back to your terminal with PenTBox running

Notice that PenTBox has notified the Kali user of an Intrusion attempt

```
  INTRUSION ATTEMPT DETECTED! from 10.15.13.250:49193 (2023-07-05 13:13:58 +0000)
 ------------------------------
GET / HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, i
mage/pjpeg, application/x-ms-xbap, */*
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; S
LCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.
0; .NET4.0C; .NET4.0E)
Accept-Encoding: gzip, deflate
Host: 10.15.92.180
Connection: Keep-Alive


  INTRUSION ATTEMPT DETECTED! from 10.15.13.250:49194 (2023-07-05 13:14:01 +0000)
 ------------------------------
GET /favicon.ico HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; S
LCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.
0; .NET4.0C; .NET4.0E)
Host: 10.15.92.180
Connection: Keep-Alive
```

What all information is captured by the honeypot about each intrusion attempt?

Food for Thought

- What information can you gather from PenTBox?
- How would you implement this in the real world?
- Once there is an attempt to access the honeypot, what actions would you take?