

STUDY GUIDE FOR MODULE NO. LAB 05**Honeypot: Invasion Detection Using Pentbox****MODULE OVERVIEW**

A honeypot is a cybersecurity technique that involves setting up decoy systems or resources within a network to attract and trap malicious actors. These decoy systems mimic legitimate targets, such as servers or applications, but are isolated and closely monitored. This module explores the world of honeypots, a security mechanism designed to attract and analyze cyber threats and intrusions. It dives into the practical application of honeypots and leverages the Pentbox framework for creating, deploying, and managing honeypots to detect and understand malicious activities on a network.

The primary function of a honeypot is to collect valuable data on potential risks and the methods, strategies, and tools used by attackers. It acts as an early detection mechanism, aiding organizations in enhancing their ability to identify and react to security breaches with greater efficiency. Honeypots come in various forms, from low-interaction honeypots that simulate services to high-interaction honeypots that use real systems. While they can be a powerful asset for threat detection and research, their deployment requires careful planning to minimize risks and ensure they do not become a security liability themselves.

For this module, using pentbox as honeypot mimics the available ports or services in an ip address wherein it is monitored if an intruder attacks those mimic ports.

**MODULE LEARNING OUTCOMES**

By the end of this module, participants should be able to:

- Acquire fundamental knowledge about Honeypots as a tool used in the field of cyber security.
- Comprehend the sequential procedures involved in Honeypot deployment.
- Establish a basic understanding of the key functionalities and capabilities of Honeypots.
- Develop insights into the realm of portable cyber security assessment tools.
- Demonstrate the ability to set up and configure a honeypot in a controlled environment.
- Develop skills in monitoring honeypot activity and identifying suspicious or malicious behaviour.

**LEARNING CONTENT**

The following steps provide instructions for the configuration of a honeypot laboratory:

➤ **Hardware/Software Requirement**

Acquire the essential hardware/software elements required for setting the Honeypot.

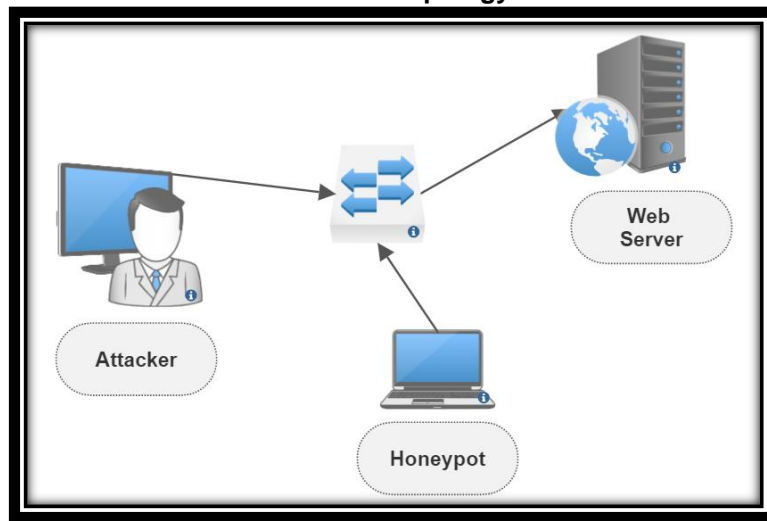
- *Raspberry Pi (with compatible model and hardware)*
- *MicroSD card (8GB or larger recommended)*
- *MicroSD card reader*
- *Computer with an SD card reader*
- *Power supply*
- *Display/Monitor*
- *Keyboard and Mouse*

In this network topology as shown in figure 1 below, a central hub switch forms the core of the network, connecting three key components: an attacker, a honeypot, and a web server. The hub switch is a simple networking device that broadcasts incoming data to all connected devices, lacking the traffic management sophistication of more advanced switches. Within this setup, the attacker is a potentially malicious entity seeking to compromise the network's security, while the honeypot acts as a decoy, intentionally attracting and monitoring the attacker's activities. The web server, on the other hand, serves as a genuine component of the network, hosting websites or web applications and catering to legitimate user requests. This topology is



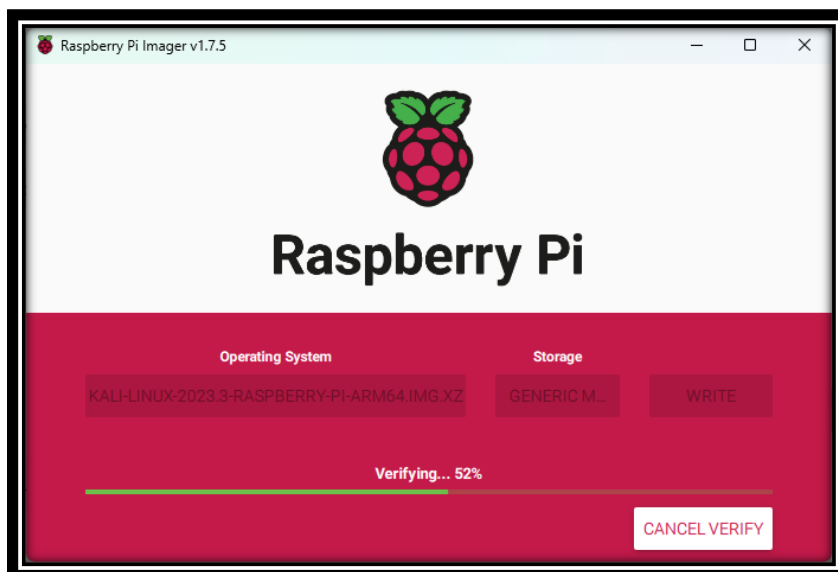
noteworthy for its capacity to facilitate security monitoring and threat detection. The attacker's actions, primarily directed at the web server, are closely observed by the honeypot, allowing network administrators to gain insights into attack methodologies and potential vulnerabilities.

Network Topology



Part I: Format the microSD Card using the downloaded Raspberry Pi Imager

In this part, we will guide you through the process of formatting the microSD card using the Raspberry Pi Imager you've downloaded.



Setting Up Your Raspberry Pi for Kali Linux

Step 1: To install Kali Linux on a Raspberry Pi, you must follow several vital steps. First, ensure you have all the necessary materials including a compatible Raspberry Pi model, a microSD card (8GB or larger is recommended), a microSD card reader, a computer with an SD card reader, and an internet connection.

- 1.1 Next, visit the official Kali Linux website's download page for Raspberry Pi and select the appropriate Raspberry Pi model. Download the Kali Linux image file in .img format.

Study Guide in (Elective 1 – Systems and Network Administration 1)

Module No. Lab 05

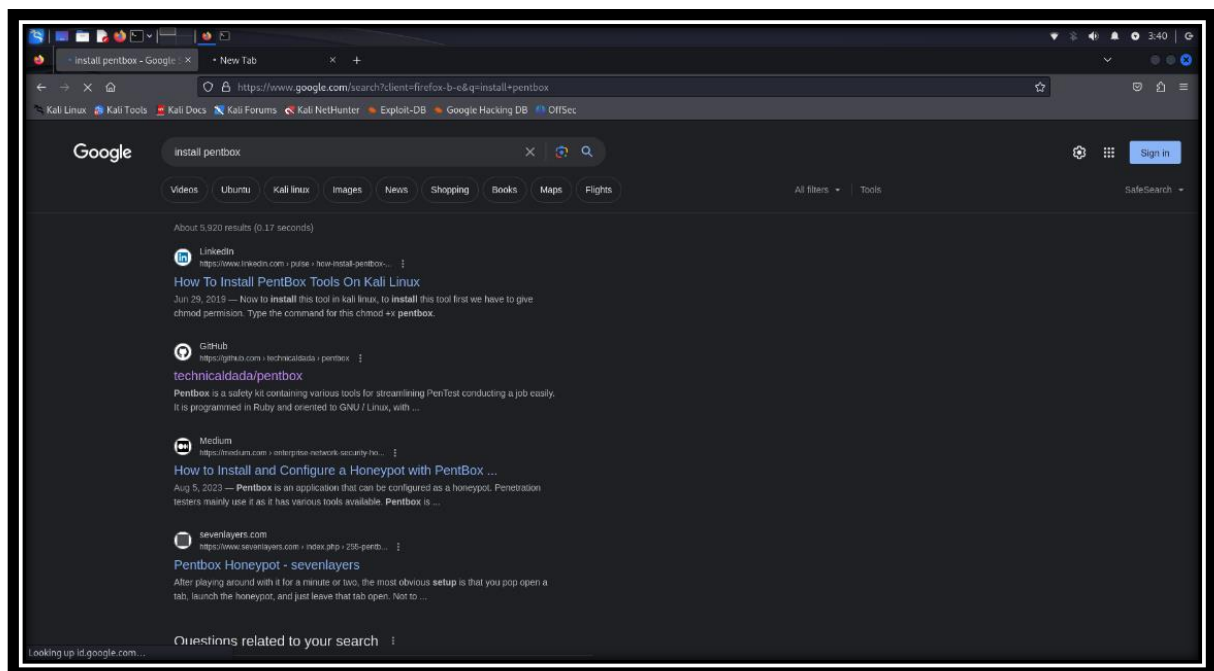
- 1.2 With the microSD card inserted into your computer's card reader, use a tool like Balena Etcher or Raspberry Pi Imager to write the Kali Linux Image to the microSD card. Follow the instructions provided by the tool.
- 1.3 Enabling SSH access is also optional. To accomplish this, generate a blank file titled "ssh" (without any file extension) at the root directory of the microSD card.
- 1.4 Ensure the microSD card is properly removed from your computer, place it into your Raspberry Pi, and initiate the Raspberry Pi by connecting it to a compatible micro-USB cable and power adapter. The Raspberry Pi should boot into Kali Linux.
- 1.5 Upon the initial boot, use the default login credentials (username: "kali" and password: "kali"). It's essential to change the default password for security reasons.
- 1.6 Ensure the Kali Linux system is up to date.
- 1.7 Refresh Package Listings: In a terminal, execute the command 'sudo apt update' to refresh the package listings.
- 1.8 Upgrade Packages: Run sudo apt upgrade to upgrade installed packages to their latest versions.

Part II: Setting up a Honeypot

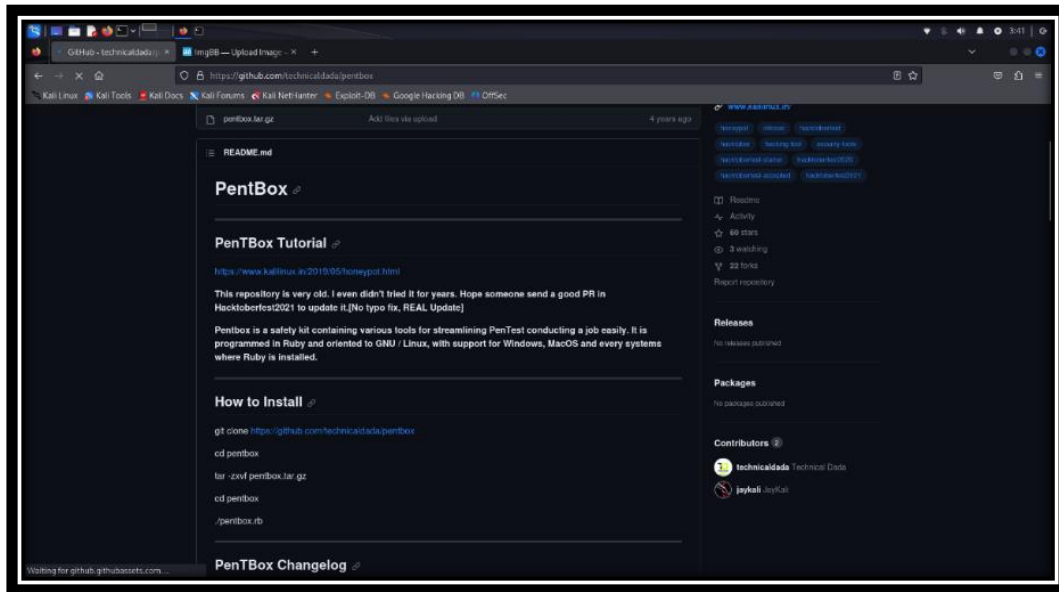
This part will guide you through the process of setting up a honeypot environment specifically tailored for use within the Kali Linux operating system.

➤ Installation of Pentbox

Step 1: Install Pentbox from GitHub on Google



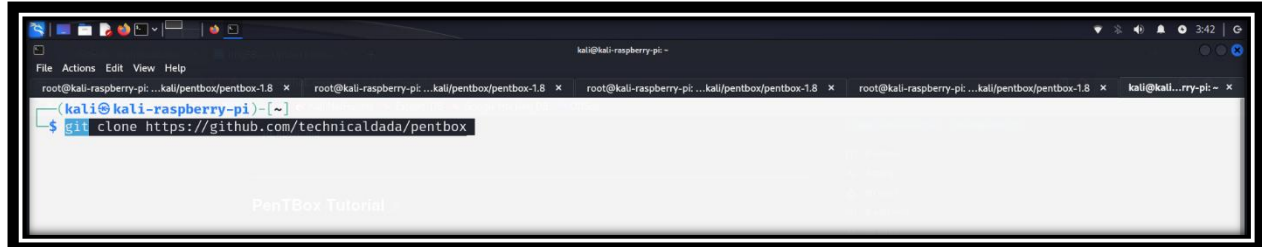
- 1.1 Access the GitHub website and review all the essential instructions and repositories that need to be employed.



1.1 Clone the Pentbox Repository:

To obtain the Pentbox repository from GitHub, employ the “git clone” command. Once the repository is cloned, proceed to the destination directory where you intend to set up Pentbox, and execute the necessary commands.

Step 2: Install Dependencies



2.1 Exploring folders within PentBox.

2.2 In the command line, you begin in your home directory by default. You can use commands like pwd to display your current directory by specifying its path.

2.3 Pentbox may have specific dependencies that need to be installed. Refer to the Pentbox documentation or the README file in the cloned repository for details on any required packages or libraries.

2.4 Unzip the tar.gz File. Utilize the 'cd' command to switch your current directory to the place where the tar.gz file is situated.

2.5 To unzip the tar.gz file, you can use the tar command. After running the command, tar will extract the

contents of the tar.gz file into the current directory. You can verify the extraction by listing the files in the directory with the ls command. This will display the files and directories that were extracted.^[5]

```

kali@kali-raspberry-pi-1:~/pentbox/pentbox-1.8$ git clone https://github.com/technicaldada/pentbox\
fatal: destination path 'pentbox' already exists and is not an empty directory.

kali@kali-raspberry-pi-1:~/pentbox/pentbox-1.8$ ls
Desktop  Documents  Downloads  log_honeypot_port23.txt  Music  pentbox  Pictures  Public  Templates  Videos

kali@kali-raspberry-pi-1:~/pentbox/pentbox-1.8$ cd pentbox
kali@kali-raspberry-pi-1:~/pentbox$ ls
pentbox-1.8  pentbox.tar.gz  README.md

kali@kali-raspberry-pi-1:~/pentbox$ cd pentbox-1.8
kali@kali-raspberry-pi-1:~/pentbox/pentbox-1.8$ ls
changelog.txt  COPYING.txt  lib  other  pb_update.rb  pentbox.rb  readme.txt  todo.txt  tools

```

2.6 Exploring the folder structure within the extracted zip file

Once you've successfully explored the contents of the extracted file within a specific folder, your next step is to launch PentBox and choose the Network Tools option by pressing the number 2.

```

kali@kali-raspberry-pi-1:~/pentbox/pentbox-1.8$ sudo su
root@kali-raspberry-pi-1:/home/kali/pentbox/pentbox-1.8# ls
changelog.txt  COPYING.txt  lib  other  pb_update.rb  pentbox.rb  readme.txt  todo.txt  tools

root@kali-raspberry-pi-1:/home/kali/pentbox/pentbox-1.8# ./pentbox.rb

PentBox 1.8
-----
Menu
1- Cryptography tools
2- Network tools
3- Web
4- Ip grabber
5- Geolocation ip
6- Mass attack
7- License and contact

PentBox Changelog
Version 1.8

```

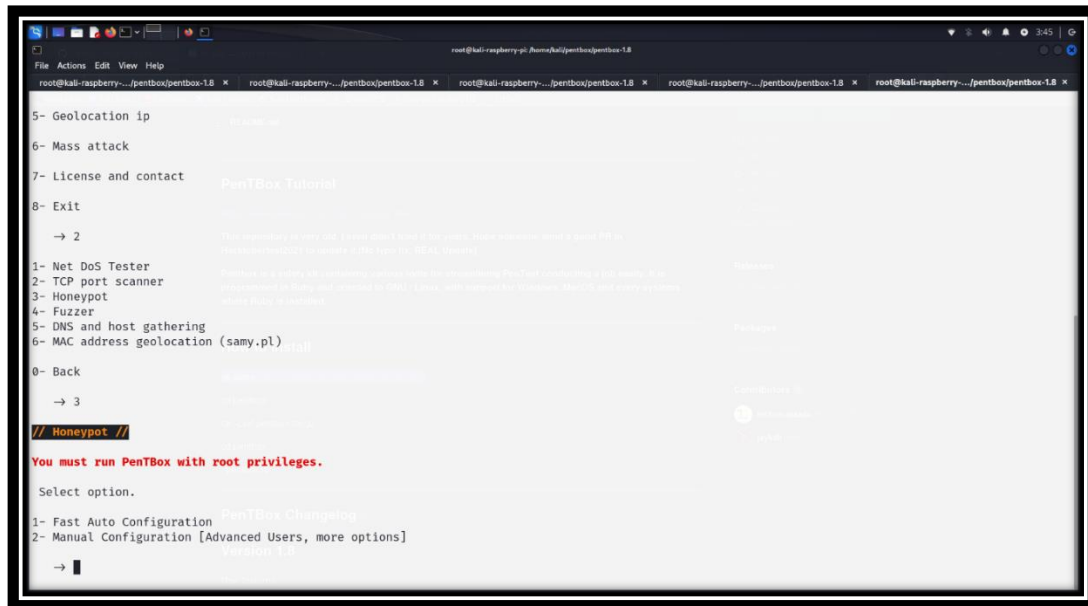
Step 3: Selecting the Honeypot

3.1 Open the Honeypot by pressing the number 3.

3.2 Select the Fast Auto Configuration option by pressing the number 1.

Part III: Testing and Validation using Honeypot

In this concluding part, we delve into the crucial testing and validation phase within the context of honeypot deployment on a Kali Linux environment.



Step 1: View Network Interfaces

The command `ifconfig` will display a list of network interfaces, such as "eth0" for wired Ethernet connections or "wlan0" for wireless connections. This is to identify the interface that is connected to the network where you want to deploy the honeypot.



Step 2: Identification of Vulnerabilities

Honeypots are intentionally set up to attract and deceive attackers, essentially acting as decoy systems. By using the `nmap -sS` command on the IP address of a honeypot, you are attempting to identify potential vulnerabilities or open ports that might attract attackers. The SYN scan is particularly useful because it sends SYN packets to initiate a TCP connection, and the response (or lack thereof) can reveal which ports are open,

closed, or filtered.



```

root@kali:~/kali
# sudo nmap -ss 192.168.1.16
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-22 23:53 EDT
Nmap scan report for 192.168.1.16
Host is up (0.023s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
MAC Address: E4:5F:01:F2:B0:DD (Raspberry Pi Trading)

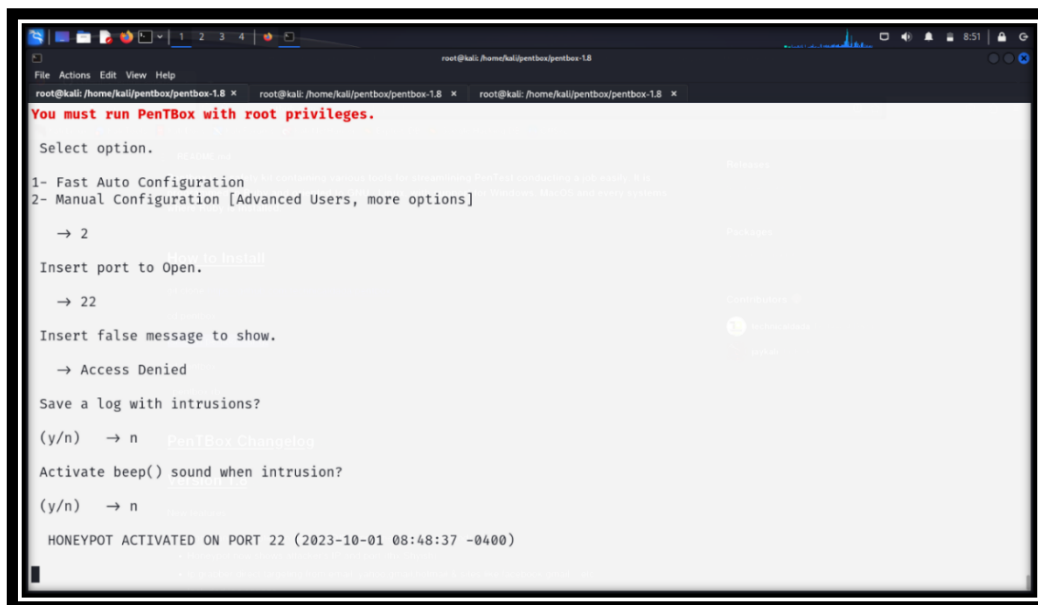
Nmap done: 1 IP address (1 host up) scanned in 5.40 seconds

root@kali:~/kali
#
  
```

Step 3: Setting up Listeners

Setting up listeners on ports 22, 23, and 80 in Kali Linux, especially in the context of a honeypot, can be a valuable security practice for detecting and analyzing potentially malicious activity.

3.1: Port 22 (SSH) is commonly associated with SSH (Secure Shell) services. SSH is used for secure remote access to systems and is a common target for attackers looking to gain unauthorized access.



```

You must run PentBox with root privileges.

Select option.
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
→ 2

Insert port to Open.
→ 22

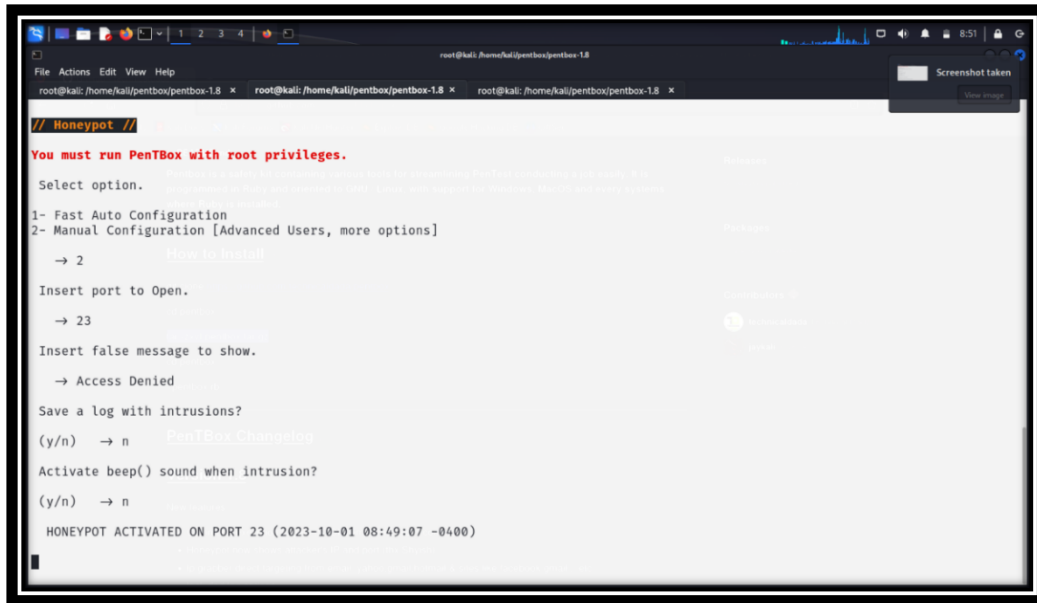
Insert false message to show.
→ Access Denied

Save a log with intrusions?
(y/n) → n

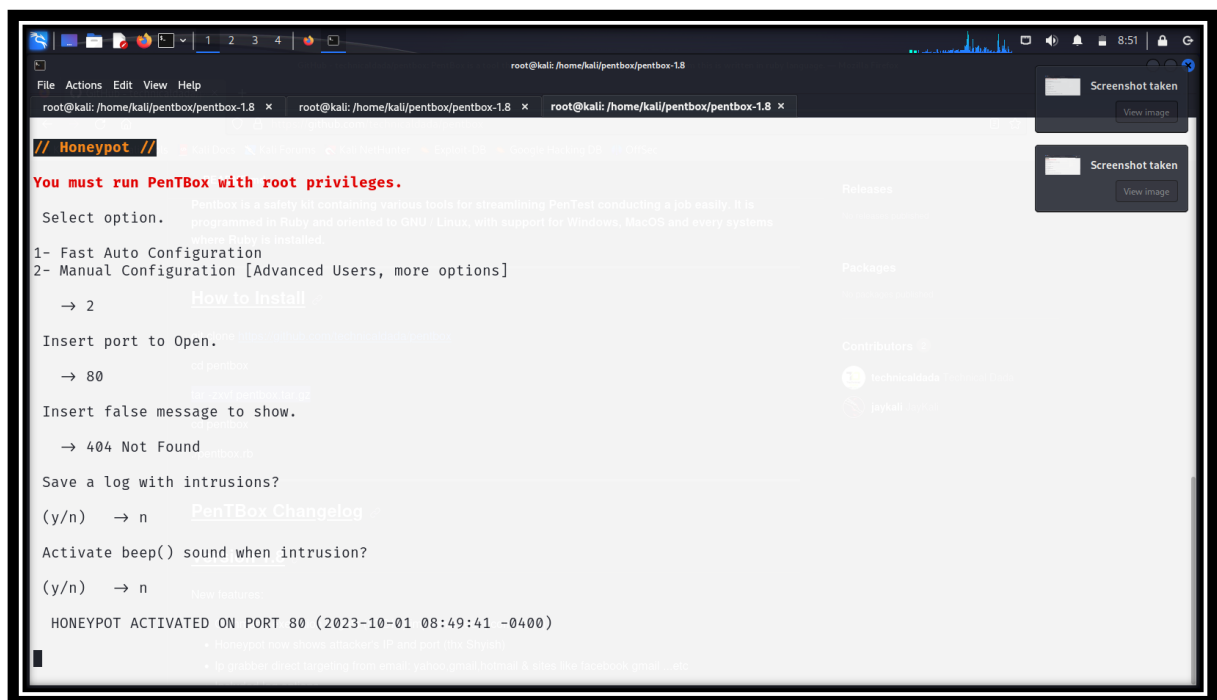
Activate beep() sound when intrusion?
(y/n) → n

HONEYPOT ACTIVATED ON PORT 22 (2023-10-01 08:48:37 -0400)
  
```


3.2: Port 23 (Telnet) is typically associated with Telnet, which is an older, unencrypted remote access protocol. It's less secure than SSH and often targeted by attackers.

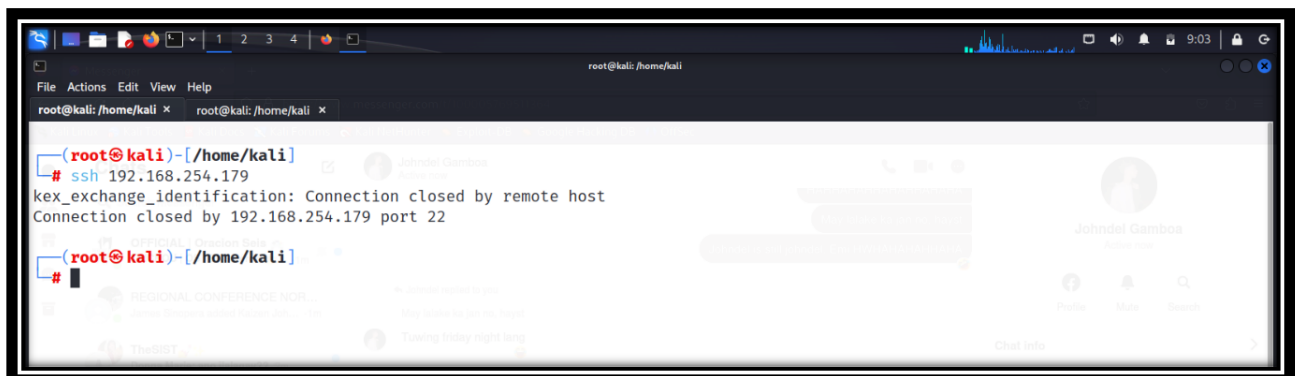


3.3: Port 80 (HTTP) is associated with HTTP (Hypertext Transfer Protocol), which is used for web traffic. Running an HTTP honeypot can help detect web-based attacks and malicious traffic.^[6]

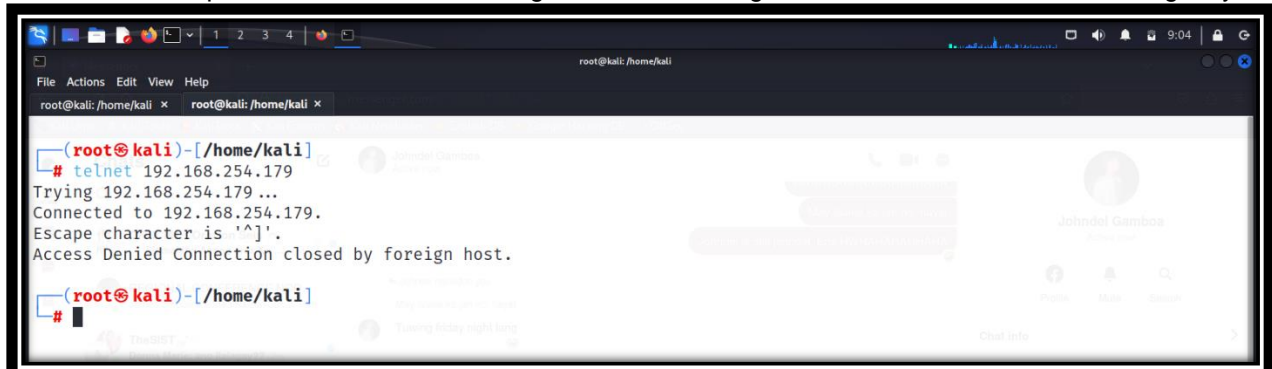


Step 4: Attacking

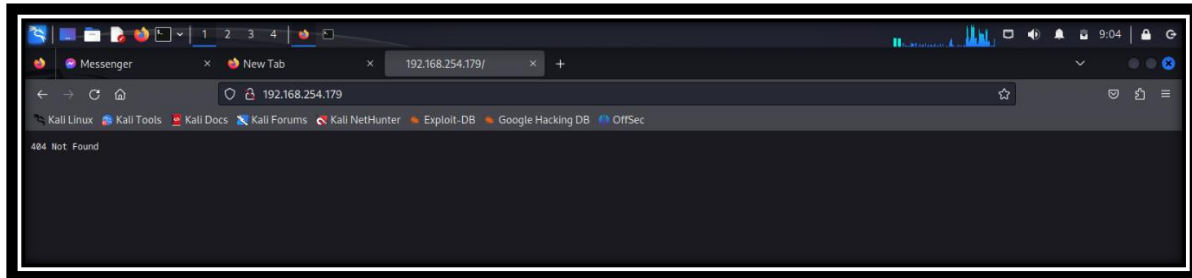
4.1: Attempting to attack using the command "ssh <ip add>" in Kali Linux in the context of a honeypot typically involves an attacker trying to gain unauthorized access to a remote system using the SSH (Secure Shell) protocol.



4.2: The attacker uses "telnet <ip add>" in Kali Linux, they are attempting to establish a telnet connection to a specific IP address, indicating their intention to gain unauthorized access to the target system.



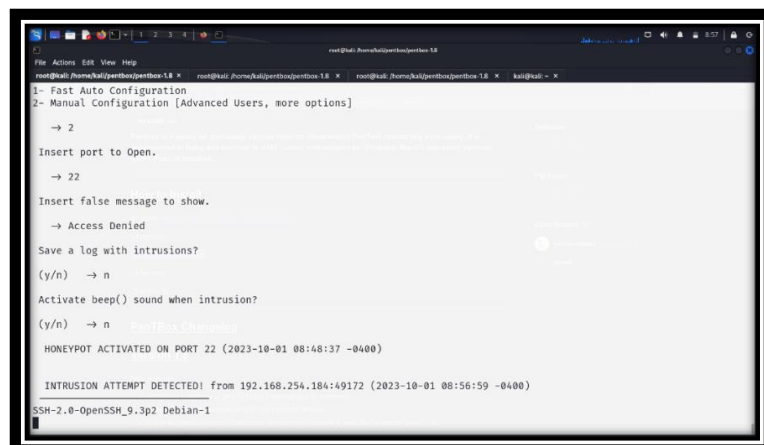
4.3: The purpose of configuring the honeypot HTTP server to respond with a "404 Not Found" error is to create a believable but ultimately unproductive interaction for the attacker. This response might discourage further exploration of the server or lead the attacker to believe they've stumbled upon an uninteresting or poorly configured system. In reality, the honeypot is logging the attacker's activities, including the IP addresses, the types of requests made, and any potential attack patterns.



Step 5: Detecting Intrusion Attempt

The message "HoneyPot activated on port 22, 23, and 80 detecting intrusion attempt detected! with displaying IP address, current date and time" signifies that a security honeypot, set up on network ports 22, 23, and 80, has observed an unauthorized intrusion attempt. HoneyPots are intentionally deployed decoy systems that attract potential attackers. In this case, the honeypot has captured the IP address of the source and recorded the exact date and time when the intrusion attempt occurred. This information is essential for network administrators and security teams, enabling them to identify the source of the threat, analyze the attack, and take appropriate security measures to protect the network from potential risks. It underscores the critical role honeypots play in cybersecurity by actively monitoring and deterring malicious activities while providing valuable insights into the tactics and sources of potential attackers.^{[7][8]}

5.1: Port 22



5.1: Port 23

```

root@kali:~/honeypot# ./honeypot.py
Select option.
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
→ 2
Insert port to Open.
→ 23
Insert false message to show.
→ Access Denied
Save a log with intrusions?
(y/n) → n
Activate beep() sound when intrusion?
(y/n) → n
HONEYPOT ACTIVATED ON PORT 23 (2023-10-01 08:49:07 -0400)

INTRUSION ATTEMPT DETECTED! from 192.168.254.184:56854 (2023-10-01 08:57:57 -0400)
=====

```

5.1: Port 80

```

root@kali:~/honeypot# ./honeypot.py
Select option.
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
→ 2
Insert port to Open.
→ 80
Insert false message to show.
→ Access Denied
Save a log with intrusions?
(y/n) → n
Activate beep() sound when intrusion?
(y/n) → n
HONEYPOT ACTIVATED ON PORT 80 (2023-10-01 08:49:41 -0400)

INTRUSION ATTEMPT DETECTED! from 192.168.254.184:46838 (2023-10-01 08:59:05 -0400)
GET / HTTP/1.1
Host: 192.168.254.179
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 192.168.254.184:46842 (2023-10-01 08:59:09 -0400)
GET /favicon.ico HTTP/1.1
Host: 192.168.254.179
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://192.168.254.179/

```

**LEARNING ACTIVITY 1**

Name: Cerujano, Erman Ace M. Due date: March 4, 2024

Create a detailed step-by-step method with pictures and detailed description on how you installed a Honeypot in your Raspberry Pi.

PART I: Installing rpi-imager and installing kali linux on bootable device.

Step 1: Download and install rpi imager (<https://www.raspberrypi.com/software/>)

The screenshot shows a web browser displaying the Raspberry Pi Imager website. The page title is "Install Raspberry Pi OS using Raspberry Pi Imager". The text describes the Imager as a quick and easy way to install Raspberry Pi OS and other operating systems to a microSD card. It provides instructions on downloading and installing the Imager to a computer with an SD card reader. Below the text are three download links: "Download for Windows", "Download for macOS", and "Download for Ubuntu for x86". A code block shows the command to install the Imager on Raspberry Pi OS: `sudo apt install rpi-imager`. To the right of the text is a screenshot of the Raspberry Pi Imager v1.8.1 application interface, which shows three tabs: "Raspberry Pi Device", "Operating System", and "Storage". Each tab has a "CHOOSE" button. A "NEXT" button is at the bottom right of the application window. The browser's address bar shows the URL "raspberrypi.com/software/". The Windows taskbar at the bottom shows the time as 8:05 PM on 3/1/2024.

Install Raspberry Pi OS using Raspberry Pi Imager

Raspberry Pi Imager is the quick and easy way to install Raspberry Pi OS and other operating systems to a microSD card, ready to use with your Raspberry Pi.

Download and install Raspberry Pi Imager to a computer with an SD card reader. Put the SD card you'll use with your Raspberry Pi into the reader and run Raspberry Pi Imager.

[Download for Windows](#)

[Download for macOS](#)

[Download for Ubuntu for x86](#)

To install on **Raspberry Pi OS**, type `sudo apt install rpi-imager` in a Terminal window.

Raspberry Pi Imager v1.8.1

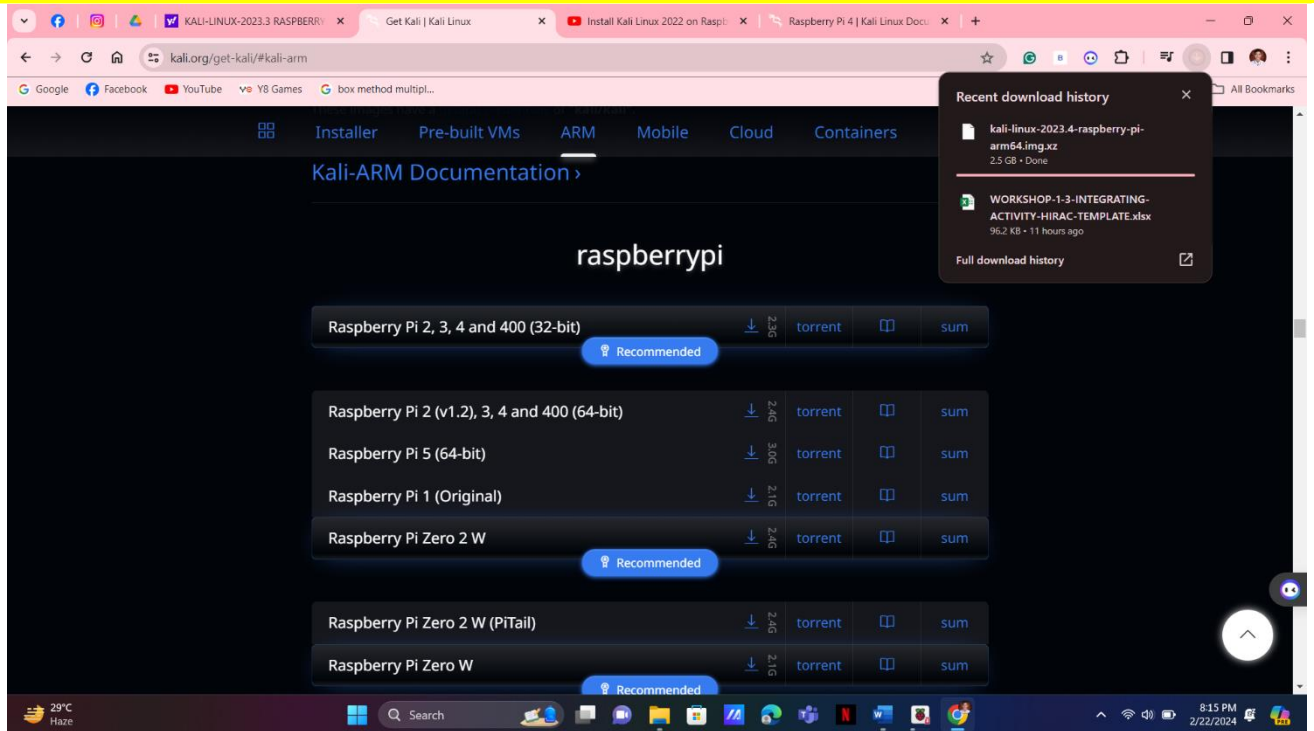
Raspberry Pi

Raspberry Pi Device | Operating System | Storage

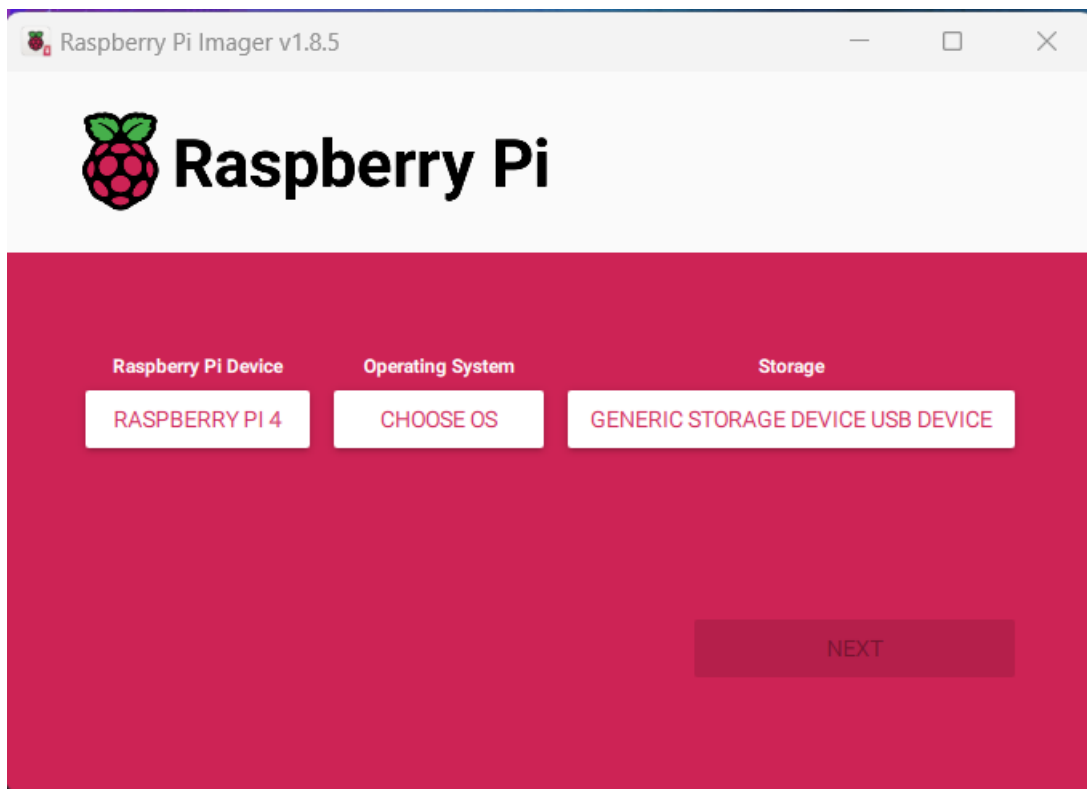
CHOOSE DEVICE | CHOOSE OS | CHOOSE STORAGE

NEXT

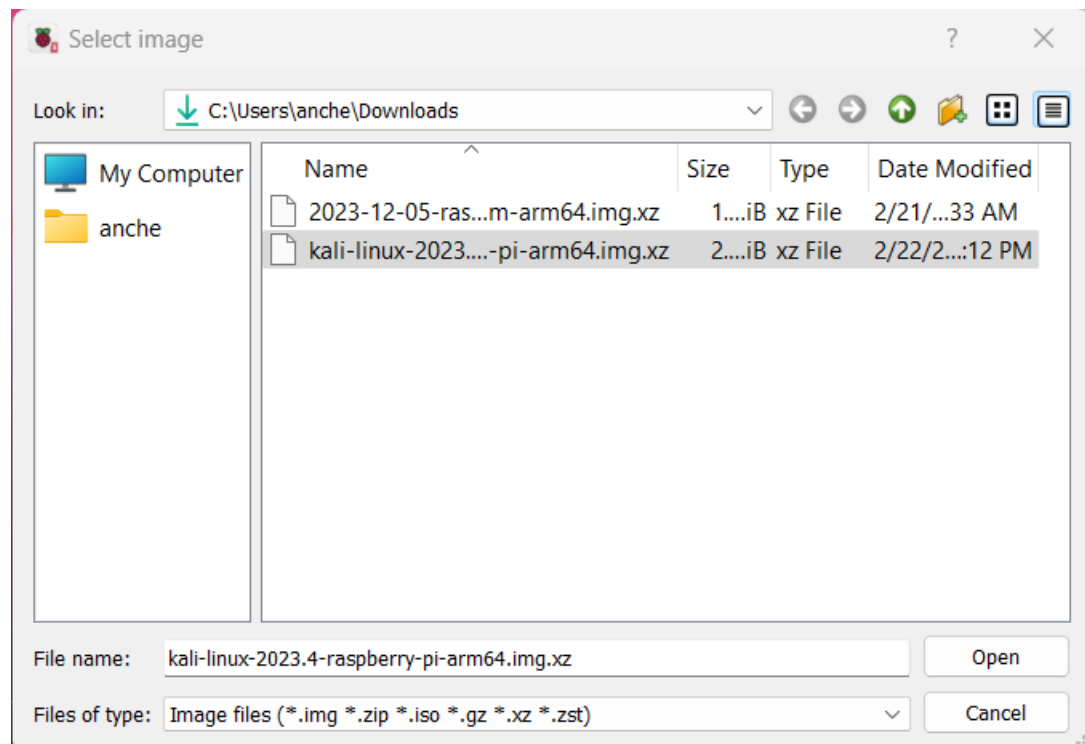
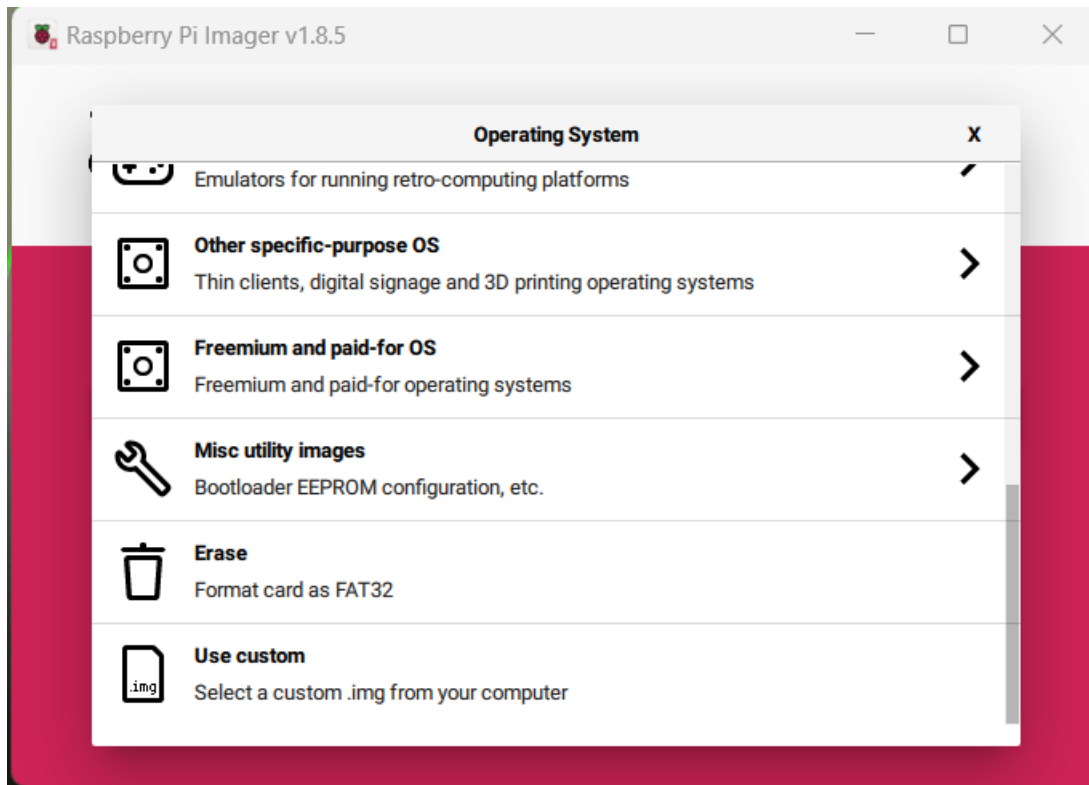
- 1.1:** Next, visit the official Kali Linux website's download page for Raspberry Pi and select the appropriate Raspberry Pi model. Download the Kali Linux image file in .img format.



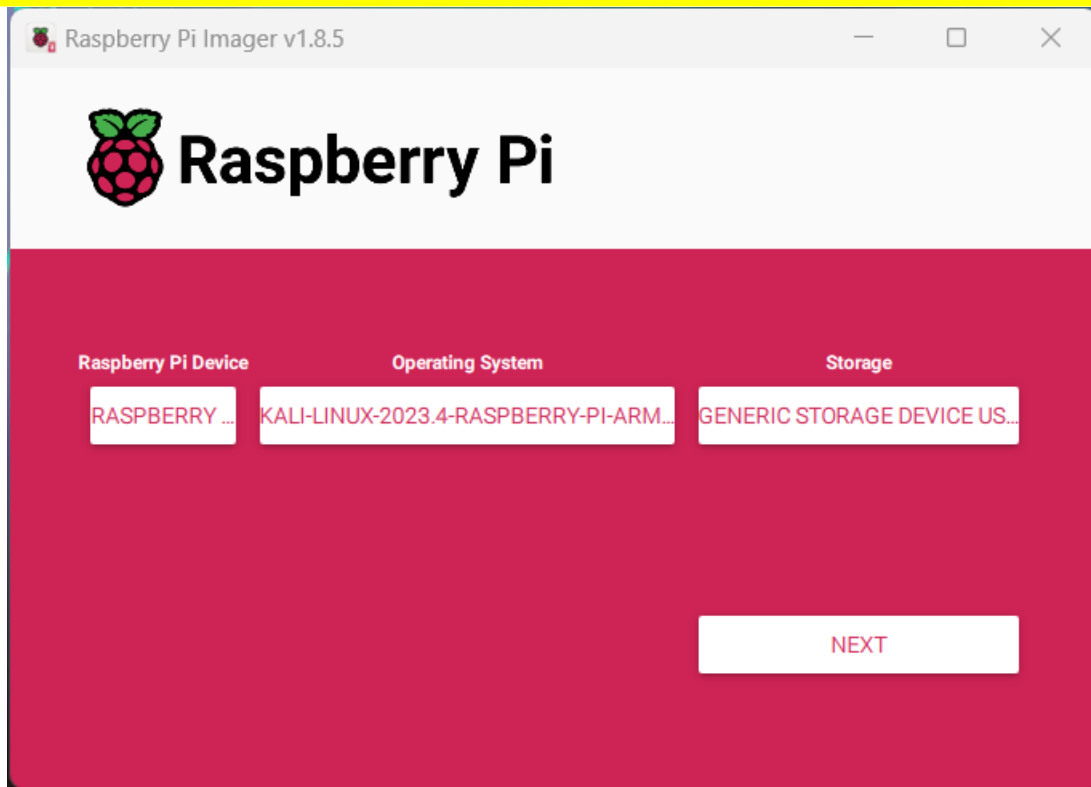
1.2: Open rpi-imager and install the kali linux in a bootable sd card. Under Raspberry Pi Device pick the version you are going to use. In my case I am using RASPBERRY PI 4.



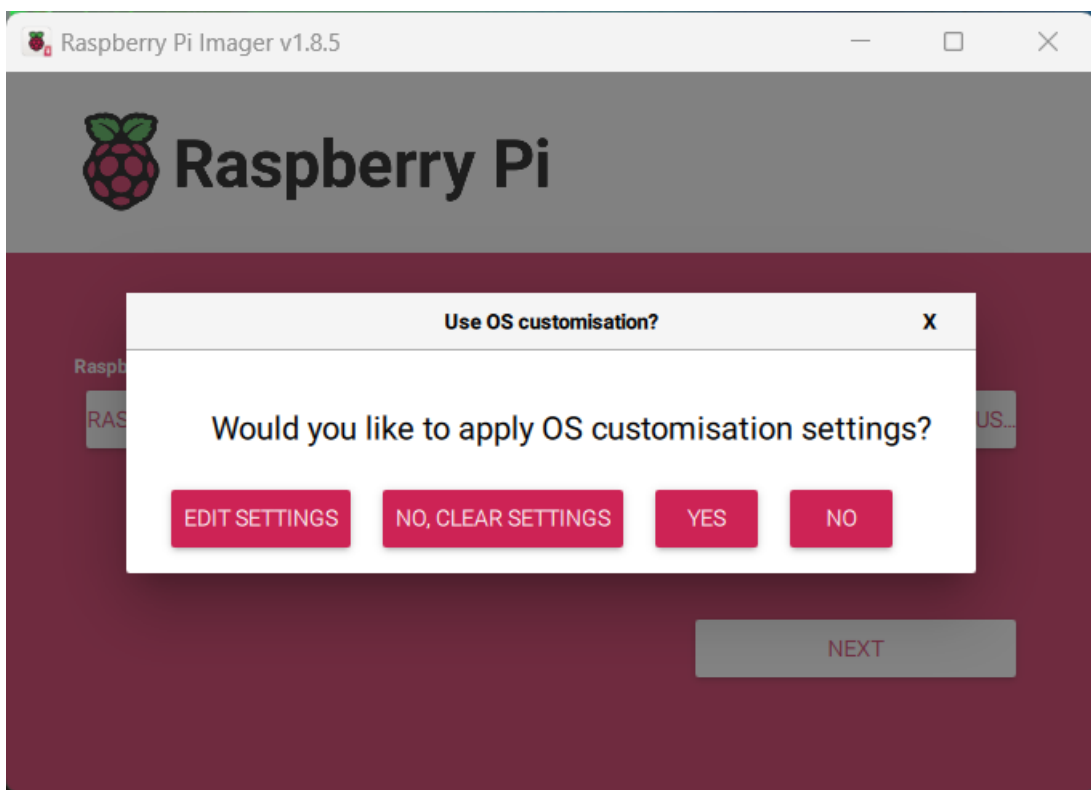
1.3: Click on use custom and pick the kali linux file



1.4: Chose storage device.



1.5: Click next and set-up the OS customization setting. Edit according to your preferences.



OS Customisation

GENERAL SERVICES OPTIONS

☒ Set hostname: floyd22.local

☒ Set username and password

Username: floyd

Password: ●●●●●●●●●●●●●●●●

☐ Configure wireless LAN

SSID: HUAWEI-5G-B69v

Password: ●●●●●●●●●●●●●●●●

☐ Show password ☐ Hidden SSID

Wireless LAN country: GB

☐ Set locale settings

Time zone: Asia/Shanghai

Keyboard layout: us

SAVE

Use OS customisation? X

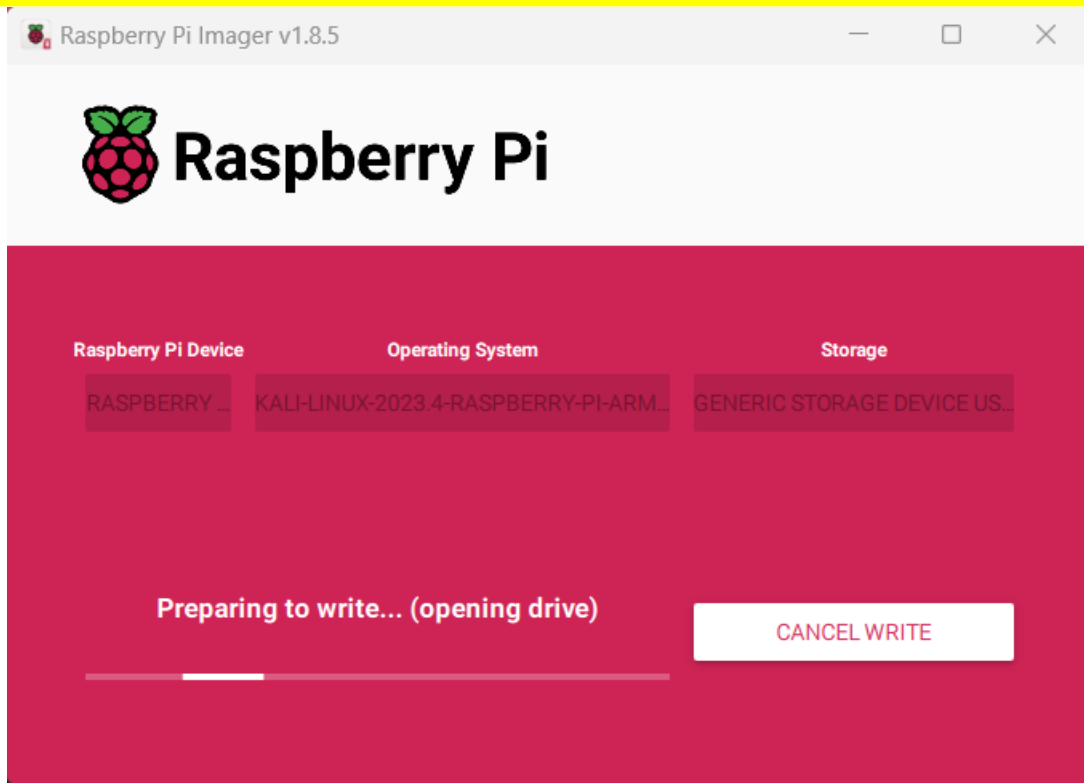
Would you like to apply OS customisation settings?

EDIT SETTINGS NO, CLEAR SETTINGS YES NO

Warning X

All existing data on 'Generic STORAGE DEVICE USB Device' will be erased.
Are you sure you want to continue?

NO YES



1.5: After installing, insert the sd card to your rpi. Power up your rpi, connect the micro to hdmi chord to tv / monitor to start booting.

PART II: Installing pentbox on kali Linux.

2.1: After booting, setup kali Linux by updating, upgrading, installing and configuring some utilities and settings.

```

kali@kali-raspberry-pi: ~
File Actions Edit View Help

(kali@kali-raspberry-pi)-[~]
$ ping www.google.com
PING www.google.com (142.251.221.4) 56(84) bytes of data.
64 bytes from mnl08s02-in-f4.1e100.net (142.251.221.4): icmp_seq=1 ttl=55 time=7.45 ms
64 bytes from mnl08s02-in-f4.1e100.net (142.251.221.4): icmp_seq=2 ttl=55 time=7.44 ms
^C
— www.google.com ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 7.441/7.447/7.454/0.006 ms

(kali@kali-raspberry-pi)-[~]
$ sudo date -s "2024-02-29 16:55:00"
Thu Feb 29 04:55:00 PM UTC 2024

(kali@kali-raspberry-pi)-[~]
$ █

```

```

(kali@kali-raspberry-pi)-[~]
$ sudo apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main arm64 Packages [19.7 MB]
Get:3 http://http.re4son-kernel.com/re4son kali-pi InRelease [10.4 kB]
Get:4 http://http.re4son-kernel.com/re4son kali-pi/main arm64 Packages [17.7 kB]
Get:5 http://kali.download/kali kali-rolling/main arm64 Contents (deb) [46.5 MB]
Get:6 http://http.re4son-kernel.com/re4son kali-pi/main arm64 Contents (deb) [2,460 kB]
Get:7 http://kali.download/kali kali-rolling/contrib arm64 Packages [104 kB]
Get:8 http://kali.download/kali kali-rolling/contrib arm64 Contents (deb) [179 kB]
Get:9 http://kali.download/kali kali-rolling/non-free arm64 Packages [152 kB]
Get:10 http://kali.download/kali kali-rolling/non-free arm64 Contents (deb) [839 kB]
Get:11 http://kali.download/kali kali-rolling/non-free-firmware arm64 Packages [32.2 kB]
Get:12 http://kali.download/kali kali-rolling/non-free-firmware arm64 Contents (deb) [16.1 kB]
Fetched 70.1 MB in 25s (2,839 kB/s)
█

```

```

(kali@kali-raspberry-pi)-[~]
$ sudo apt upgrade █

```

```

kali@kali-raspberry-pi: ~
File Actions Edit View Help

speech-dispatcher-espeak-ng sphinx-rtd-theme-common sqlite3 sqlmap ssh
ssldump sslh sslscan statsprocessor strongswan strongswan-charon
strongswan-libcharon strongswan-starter stunnel4 subversion sudo swaks
sysstat systemd systemd-dev systemd-sysv systemd-timesyncd sysvinit-utils
tar taskset taskset-data tcl tcl8.6 tdb-tools telnet texlive-base
texlive-binaries texlive-fonts-recommended texlive-latex-base
texlive-latex-extra texlive-latex-recommended texlive-pictures
texlive-plain-generic theharvester thunar thunar-archive-plugin tk tk8.6
tk8.6-blt2.5 traceroute tree triggerhappy tshark tumble tldata
tldata-legacy udev udisks2 unrar upower upx-ucl usb-modeswitch-data
usb.ids usbmuxd usbutils usr-is-merged usrmerge util-linux
vboot-kernel-utils vboot-utils vim vim-common vim-runtime vim-tiny wfuzz
wireshark winexe wireless-tools wireplumber wireshark-common
wpasupplicant xbrlapi xdg-desktop-portal xdotool xfce4-battery-plugin
xfce4-cpufreq-plugin xfce4-cpugraph-plugin xfce4-datetime-plugin
xfce4-diskperf-plugin xfce4-fsguard-plugin xfce4-genmon-plugin
xfce4-netload-plugin xfce4-notifyd xfce4-places-plugin
xfce4-power-manager xfce4-power-manager-data xfce4-power-manager-plugins
xfce4-pulseaudio-plugin xfce4-systemload-plugin xfce4-timer-plugin
xfce4-verve-plugin xfce4-wavelan-plugin xfce4-whiskermenu-plugin
xfce4-xkb-plugin xfconf xkb-data xml-core xserver-common xserver-xephyr
xserver-xorg-core xserver-xorg-legacy xvfb xz-utils yelp zenity
zenity-common zlib1g zlib1g-dev zsh zsh-common zutty
1496 upgraded, 59 newly installed, 0 to remove and 18 not upgraded.
Need to get 1,697 MB of archives.
After this operation, 459 MB of additional disk space will be used.
Do you want to continue? [Y/n] -y

```

2.2: Open your browser and go to <https://github.com/technicaldada/pentbox> to start installing pentbox.

README

PentBox

How to use PentBox

<https://www.kalilinux.in/2019/05/honeybot.html>

This repository is very old. I even didn't tried it for years. Hope someone send a good PR in Hacktoberfest2021 to update it.[No typo fix, REAL Update]

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 systems where Ruby is installed.

How to Install

```

git clone https://github.com/technicaldada/pentbox
cd pentbox
tar -zxvf pentbox.tar.gz
cd pentbox
./pentbox.rb

```

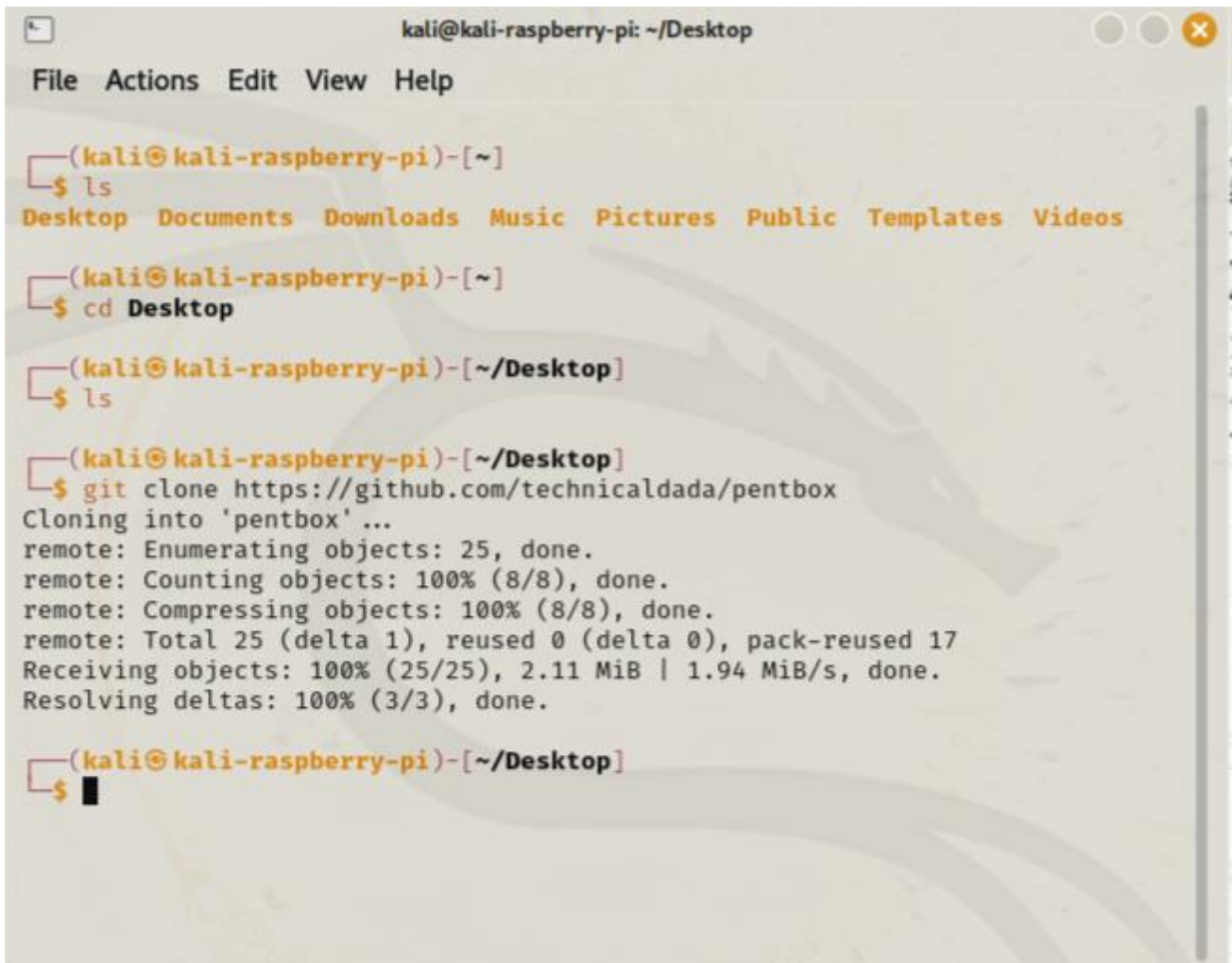
PentBox Changelog

Version 1.8

Contributors

- technicaldada Technical Dada
- jaykali JayKali

2.3: Go to your Desktop directory and start cloning (git clone <https://github.com/technicaldada/pentbox>).



```

kali@kali-raspberry-pi: ~/Desktop
File Actions Edit View Help

(kali@kali-raspberry-pi)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos

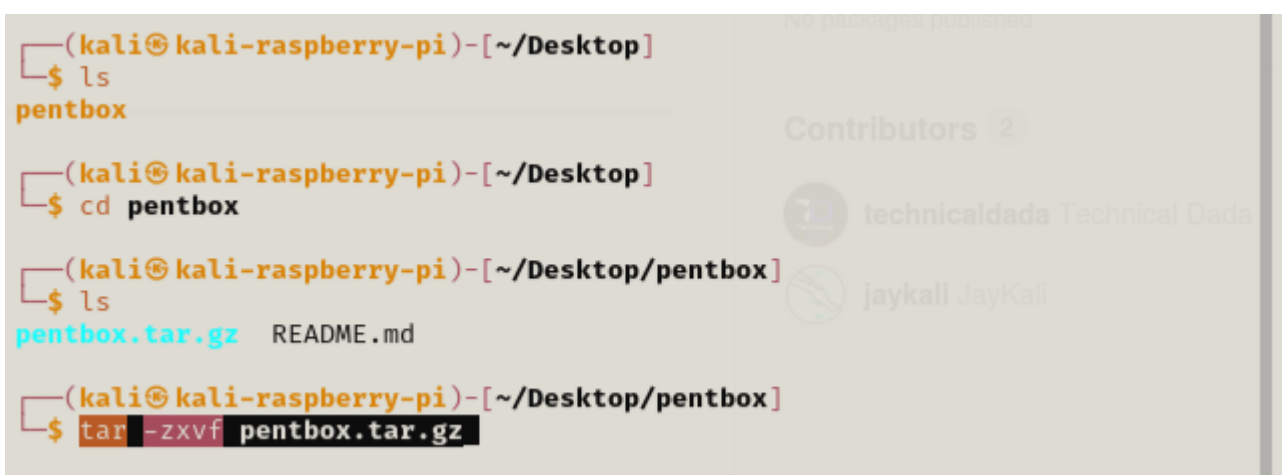
(kali@kali-raspberry-pi)-[~]
$ cd Desktop

(kali@kali-raspberry-pi)-[~/Desktop]
$ ls

(kali@kali-raspberry-pi)-[~/Desktop]
$ git clone https://github.com/technicaldada/pentbox
Cloning into 'pentbox' ...
remote: Enumerating objects: 25, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 25 (delta 1), reused 0 (delta 0), pack-reused 17
Receiving objects: 100% (25/25), 2.11 MiB | 1.94 MiB/s, done.
Resolving deltas: 100% (3/3), done.

(kali@kali-raspberry-pi)-[~/Desktop]
$ █
  
```

2.4: Go to the pentbox directory and unzip the file pentbox.tar.gz (tar -zxvf pentbox.tar.gz).



```

(kali@kali-raspberry-pi)-[~/Desktop]
$ ls
pentbox

(kali@kali-raspberry-pi)-[~/Desktop]
$ cd pentbox

(kali@kali-raspberry-pi)-[~/Desktop/pentbox]
$ ls
pentbox.tar.gz  README.md

(kali@kali-raspberry-pi)-[~/Desktop/pentbox]
$ tar -zxvf pentbox.tar.gz
  
```

```

kali@kali-raspberry-pi: ~/Desktop/pentbox
File Actions Edit View Help
pentbox-1.8/other/log/.svn/
pentbox-1.8/other/.svn/tmp/
pentbox-1.8/other/.svn/text-base/
pentbox-1.8/other/.svn/prop-base/
pentbox-1.8/other/.svn/props/
pentbox-1.8/lib/racket/
pentbox-1.8/lib/json/
pentbox-1.8/lib/net/
pentbox-1.8/lib/bit-struct/
pentbox-1.8/lib/.svn/
pentbox-1.8/tools/network/
pentbox-1.8/tools/cryptography/
pentbox-1.8/tools/.svn/
pentbox-1.8/tools/web/
pentbox-1.8/other/log/
pentbox-1.8/other/.svn/
pentbox-1.8/lib/
pentbox-1.8/tools/
pentbox-1.8/other/
pentbox-1.8/

```

PART III: Enabling and attacking ports 22, 23, and 80.

3.1: Change directory to pentbox-1.8.

```

(kali@kali-raspberry-pi)-[~/Desktop/pentbox]
$ ls
pentbox-1.8  pentbox.tar.gz  README.md

(kali@kali-raspberry-pi)-[~/Desktop/pentbox]
$ cd pentbox-1.8

(kali@kali-raspberry-pi)-[~/Desktop/pentbox/pentbox-1.8]
$ ls
changelog.txt  lib  pb_update.rb  readme.txt  tools
COPYING.txt   other  pentbox.rb  todo.txt

```

3.2: Enter root using sudo su command. Enter and open pentbox using ./pentbox.rb.

```

root@kali-raspberry-pi: /home/kali/Desktop/pentbox/pentbox-1.8
File Actions Edit View Help

(kali@kali-raspberry-pi)-[~/Desktop/pentbox/pentbox-1.8]
$ sudo su
(root@kali-raspberry-pi)-[/home/kali/Desktop/pentbox/pentbox-1.8]
# ls
changelog.txt  lib      pb_update.rb  readme.txt  tools
COPYING.txt   other    pentbox.rb    todo.txt

(root@kali-raspberry-pi)-[/home/kali/Desktop/pentbox/pentbox-1.8]
# ./pentbox.rb

PentBox 1.8

.!!!!!!:.
~~~~!!!!!!:.
:$$NW$ !! :
$$$$$#WX!:
$$$$$ $$$UX : !! UW$$$$$$$$$ 4$$$$$*
^$$$B $$$ $$$$$$$$$$$$ d$$R*
**$bd$$$$ '$$$$$$$$$$$$o+#
      ****      *****

----- Menu                      ruby3.1.2 @ aarch64-linux-gnu

```

3.3 Now we can see some menu below. Go to Network tools by entering number 2 and pressing enter.

```

----- Menu                      ruby3.1.2 @ aarch64-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

```


3.4: Chose Honeypot by entering number 3 and pressing enter.

```
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

// Honeypot //

You must run PentBox with root privileges.
```

3.5: Select Fast Auto Configuration to activate honeypot on port 80.

```
Select option.

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

→ 1

HONEYPOT ACTIVATED ON PORT 80 (2024-02-29 18:00:15 +0000)

□
```

3.6: Open new terminal and check your Ip address using ifconfig command.

```

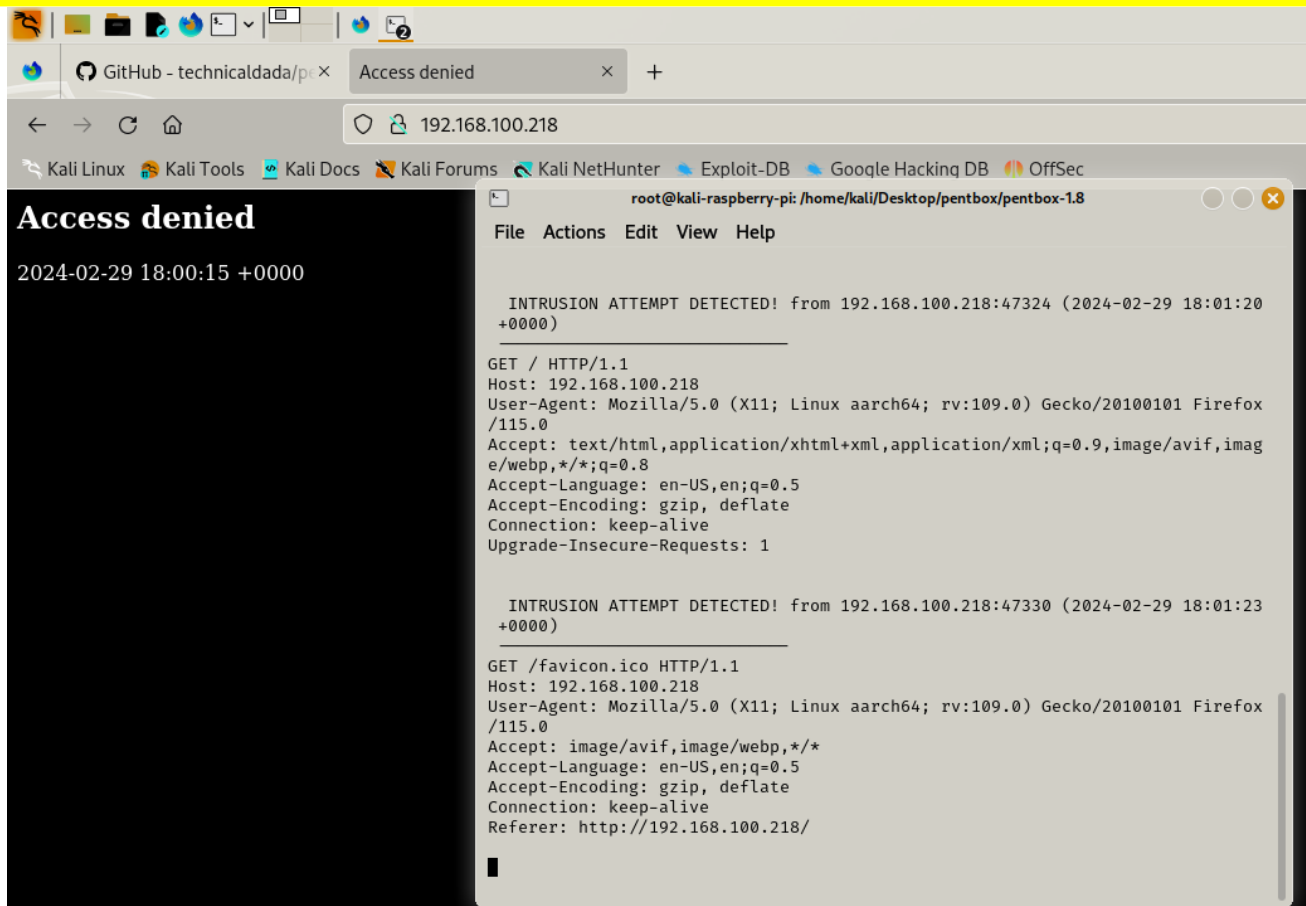
kali@kali-raspberry-pi: ~/Desktop/pentbox/pentbox-1.8
File Actions Edit View Help
(kali@kali-raspberry-pi)-[~/Desktop/pentbox/pentbox-1.8]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.218 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::da3a:ddff:fe27:21a4 prefixlen 64 scopeid 0x20<link>
    ether d8:3a:dd:27:21:a4 txqueuelen 1000 (Ethernet)
    RX packets 1303911 bytes 1882390707 (1.7 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 165631 bytes 12157625 (11.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

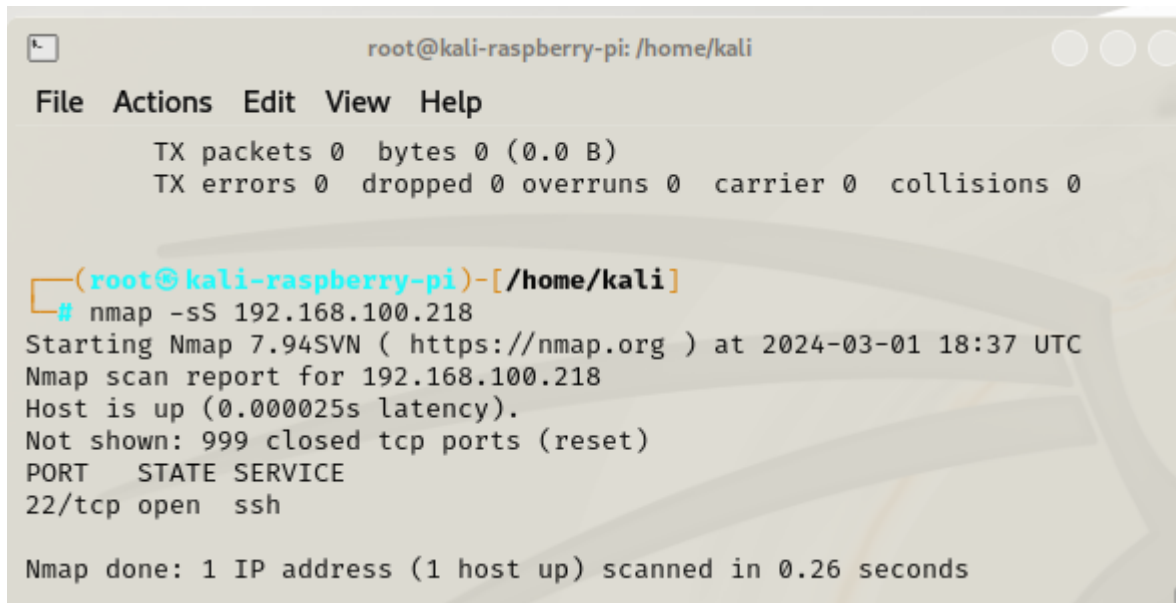
wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 1a:22:28:74:94:ef txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

3.7: Open your browser and enter the Ip address (192.168.100.218). We can see below the message Access denied in the browser and the Intrusion log on the terminal.



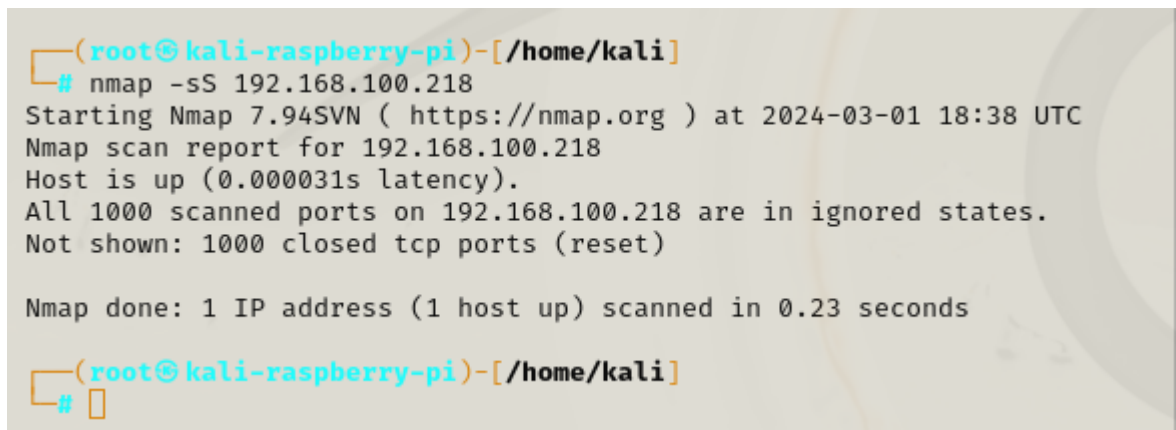
3.8: Now let's close the port and use the manual configuration. First let's check the open ports using the `sudo nmap -sS ip address (192.168.100.218)`.



3.9: Stop the service on port 22 using `sudo service ssh stop`. Check again using the `nmap -sS 192.168.100.218`. if you are not in the root add `sudo` before the `nmap`.



```
kali@kali-raspberry-pi: ~
File Actions Edit View Help
(kali@kali-raspberry-pi)-[~]
$ sudo service ssh stop
(kali@kali-raspberry-pi)-[~]
$
```



```
(root@kali-raspberry-pi)-[/home/kali]
# nmap -sS 192.168.100.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 18:38 UTC
Nmap scan report for 192.168.100.218
Host is up (0.000031s latency).
All 1000 scanned ports on 192.168.100.218 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

(root@kali-raspberry-pi)-[/home/kali]
#
```

3.10: Go to network tools >> honeypot and choose manual configuration. Activate honeypot on port 22.

```

root@kali-raspberry-pi: /home/kali/Desktop/pentbox/pentbox-1.8
File Actions Edit View Help

→ 3

// Honeypot //

You must run PentBox with root privileges.

Select option.

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

→ 2

Insert port to Open.

→ 22

Insert false message to show.

→ Access Denied! Please exit!

Save a log with intrusions?
(y/n) → n

Activate beep() sound when intrusion?
(y/n) → n

HONEYPOT ACTIVATED ON PORT 22 (2024-03-01 18:39:14 +0000)

```

3.11: Check if the port 22 is already open using the nmap command.

```

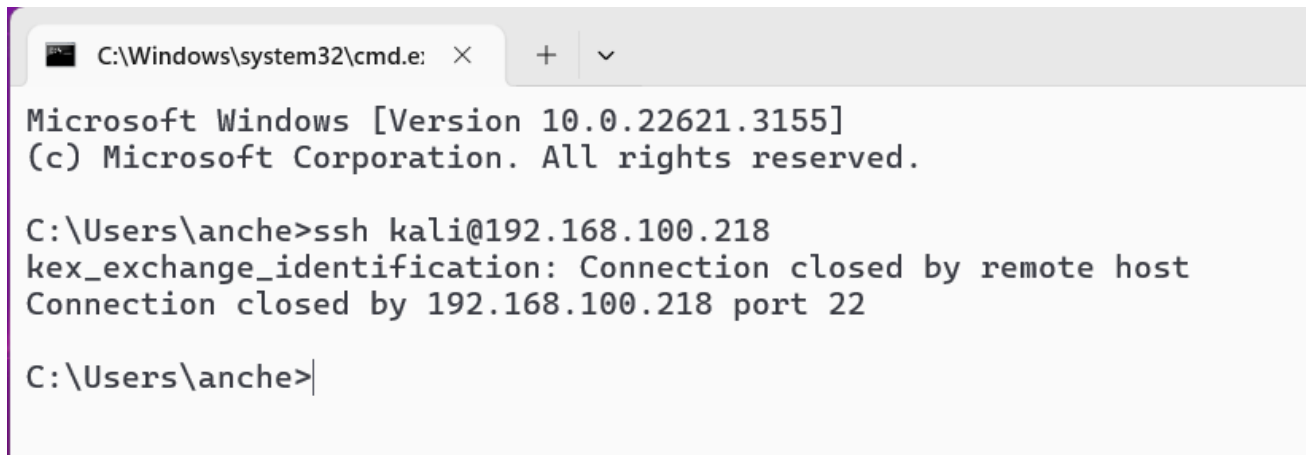
(root@kali-raspberry-pi)-[/home/kali]
# nmap -sS 192.168.100.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 18:39 UTC
Nmap scan report for 192.168.100.218
Host is up (0.000031s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

(root@kali-raspberry-pi)-[/home/kali]
#

```

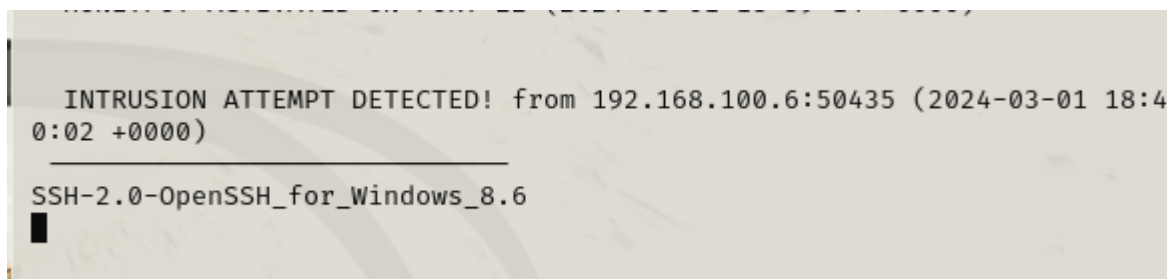
3.12: On your windows terminal ssh kali using the command ssh kali@192.168.100.218. Check the log in your kali Linux terminal. We can see that after trying to ssh the kali, there is a log showing that it has detected some intrusion attempt.



```
C:\Windows\system32\cmd.e: X + v
Microsoft Windows [Version 10.0.22621.3155]
(c) Microsoft Corporation. All rights reserved.

C:\Users\anche>ssh kali@192.168.100.218
kex_exchange_identification: Connection closed by remote host
Connection closed by 192.168.100.218 port 22

C:\Users\anche>|
```



```
INTRUSION ATTEMPT DETECTED! from 192.168.100.6:50435 (2024-03-01 18:4
0:02 +0000)
-----
SSH-2.0-OpenSSH_for_Windows_8.6
█
```

3.13: Next let's open the port 23. Again, go to network tools >> honeypot and choose manual configuration.

```

root@kali-raspberry-pi: /home/kali/Desktop/pentbox/pentbox-1.8
File Actions Edit View Help

→ 3

// Honeypot //

You must run PentBox with root privileges.

Select option.

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

→ 2

Insert port to Open.

→ 23

Insert false message to show.

→ Access Denied! Please Exit

Save a log with intrusions?

(y/n) → n

Activate beep() sound when intrusion?

(y/n) → n

HONEYPOT ACTIVATED ON PORT 23 (2024-03-01 18:41:14 +0000)

```

3.14: Let's check if the port 23 is already open using nmap.

```

(root@kali-raspberry-pi)-[/home/kali]
# nmap -sS 192.168.100.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 18:41 UTC
Nmap scan report for 192.168.100.218
Host is up (0.000032s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

(root@kali-raspberry-pi)-[/home/kali]
#

```


3.15: Now let's access the Ip address (192.168.100.218) using telnet. We can see below the False message we entered. And the other picture shows the log on port 23.



The screenshot shows a terminal window with the title bar "kali@kali-raspberry-pi: ~". The menu bar includes "File", "Actions", "Edit", "View", and "Help". The terminal content shows a user prompt "(kali@kali-raspberry-pi)-[~]" followed by the command "\$ telnet 192.168.100.218". The output shows the telnet process attempting to connect to 192.168.100.218, successfully establishing a connection, and then receiving an "Access Denied! Please Exit" message from the remote host. The user prompt is shown again at the bottom of the terminal.

```
kali@kali-raspberry-pi: ~  
File Actions Edit View Help  
(kali@kali-raspberry-pi)-[~]  
$ telnet 192.168.100.218  
Trying 192.168.100.218 ...  
Connected to 192.168.100.218.  
Escape character is '^]'.  
Access Denied! Please Exit  
Connection closed by foreign host.  
(kali@kali-raspberry-pi)-[~]  
$
```

[illegible]

3.16: Lets manually open the port 80. Go to network tools >> honeypot and choose manual configuration.

```

root@kali-raspberry-pi: /home/kali/Desktop/pentbox/pentbox-1.8
File Actions Edit View Help

→ 3

// Honeypot //

You must run PentBox with root privileges.

Select option.

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

→ 2

Insert port to Open.

→ 80

Insert false message to show.

→ Access Denied! Please close tab!

Save a log with intrusions?
(y/n) → n

Activate beep() sound when intrusion?
(y/n) → n

HONEYPOT ACTIVATED ON PORT 80 (2024-03-01 18:43:45 +0000)

```

3.17: Check if port 80 is already open using the nmap command.

```

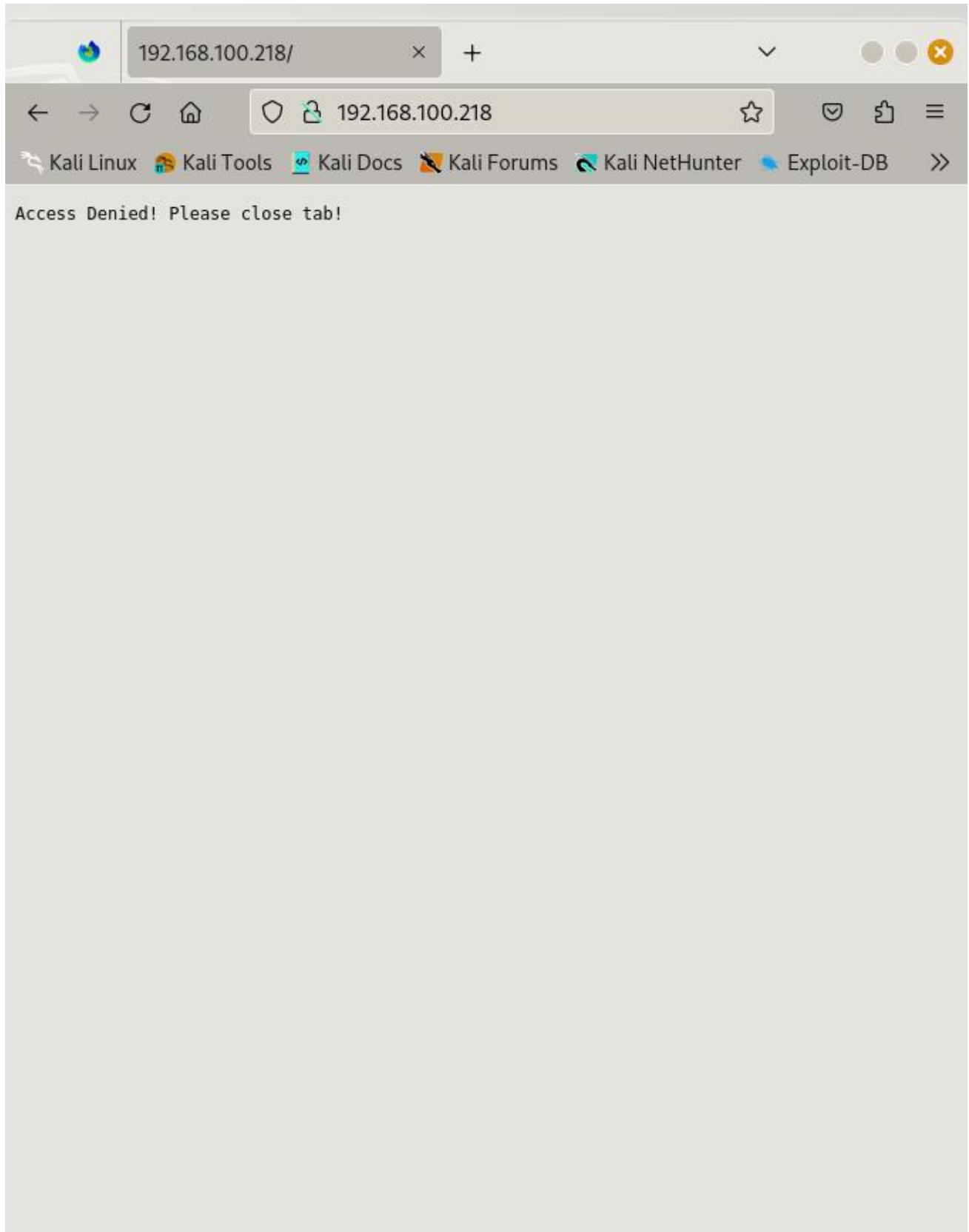
(root@kali-raspberry-pi)-[/home/kali]
# nmap -sS 192.168.100.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 18:43 UTC
Nmap scan report for 192.168.100.218
Host is up (0.000031s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

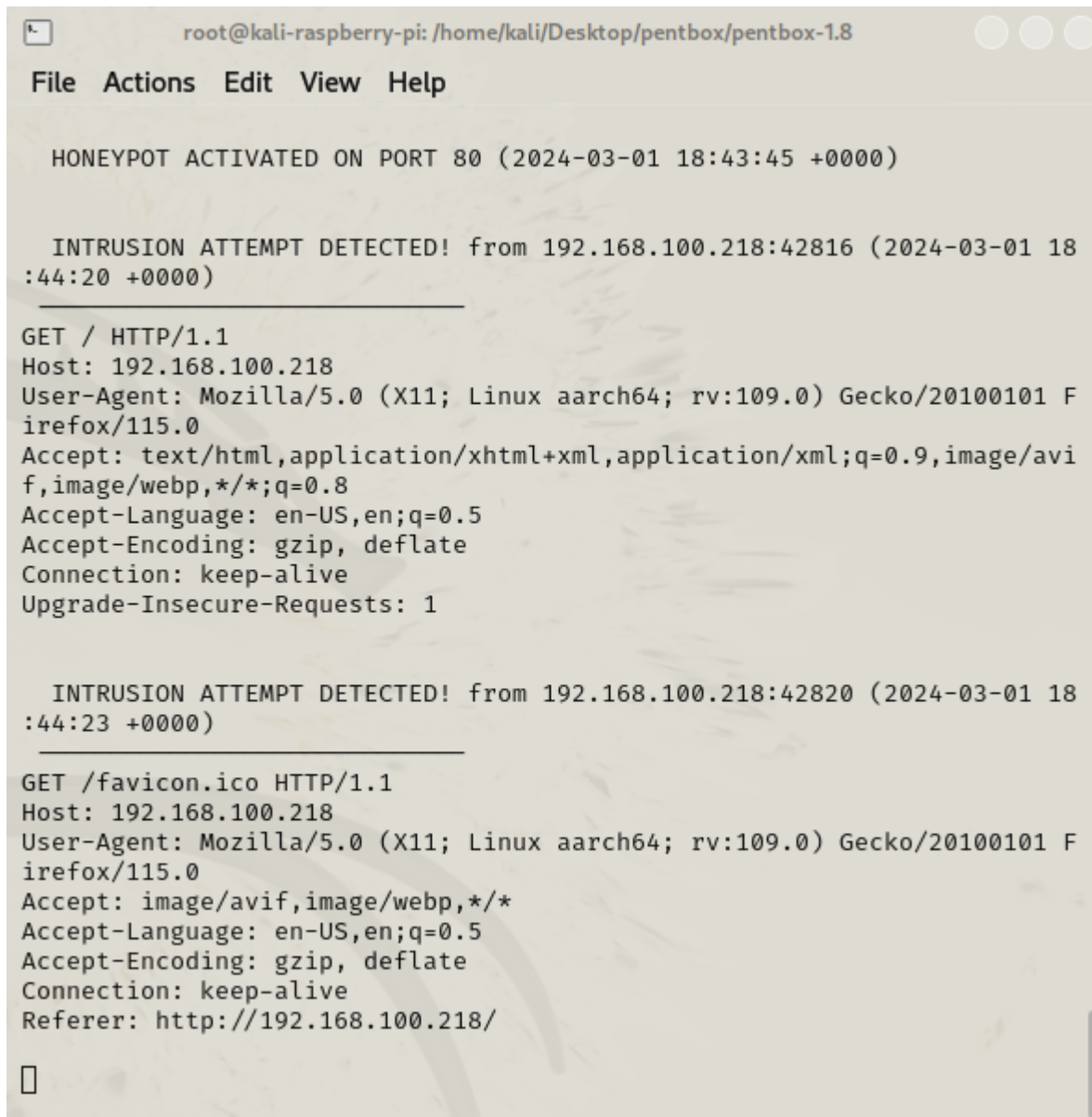
(root@kali-raspberry-pi)-[/home/kali]
#

```

3.18: Now that port 80 is open. Let's open our browser and enter our ip address and add the specific port we just opened (192.168.100.218:80).



3.19: Now let's go back to our terminal to check the log in port 80 that we just accessed.



```
root@kali-raspberry-pi: /home/kali/Desktop/pentbox/pentbox-1.8
File Actions Edit View Help

HONEYPOT ACTIVATED ON PORT 80 (2024-03-01 18:43:45 +0000)

INTRUSION ATTEMPT DETECTED! from 192.168.100.218:42816 (2024-03-01 18:44:20 +0000)
-----
GET / HTTP/1.1
Host: 192.168.100.218
User-Agent: Mozilla/5.0 (X11; Linux aarch64; 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 192.168.100.218:42820 (2024-03-01 18:44:23 +0000)
-----
GET /favicon.ico HTTP/1.1
Host: 192.168.100.218
User-Agent: Mozilla/5.0 (X11; Linux aarch64; 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://192.168.100.218/


```



SUMMARY / CONCLUSION

Throughout this module, we've embarked on a journey into the world of honeypots, gaining valuable insights into their role as pivotal cybersecurity tools. By employing the Pentbox framework, we've not only understood the theoretical concepts behind honeypots but also delved into practical deployment strategies. From formatting microSD cards for Raspberry Pi to configuring honeypots within a Kali Linux environment, each step has been a building block in our understanding of cybersecurity defense mechanisms.

During configuration there are some problems that we encountered where we have difficulty in updating and upgrading. We fixed this issue by configuring the time in the Linux OS. Next is where we cannot manually open the port 22 since it is already running. In order to fix that problem, we forcefully stopped the ssh service and closed the port 22. After that, we can now use the manual configuration to open port 22.

In conclusion, this module has not only provided us with a foundational understanding of honeypots but has also empowered us to become proactive defenders against cyber threats. Armed with the knowledge gained here, we are better prepared to safeguard networks and mitigate potential risks, thus fortifying the resilience of our digital environments against evolving security challenges.

REFERENCES

Bounty Hunter. (2019, December 24). *Detect Intruder (HoneyPot - DDOS)* [Video]. YouTube.

https://www.youtube.com/watch?v=N3vgeJx_h5w

InfoSec Pat. (2020, February 19). *How To Configure Honeypot with PentBox in Kali Linux - 2020* [Video]. YouTube.

<https://www.youtube.com/watch?v=X3J63oGEk7I>

pcap_pirate. (2020, June 18). *Pentbox HoneyPot demo (Install and Run) Kali Linux* [Video]. YouTube.

<https://www.youtube.com/watch?v=YXv3JHoR2ZU>

Wolfgang's Channel. (2020, October 13). *SSH Honeypot in 4 Minutes - Trap hackers in your server* [Video]. YouTube.

<https://www.youtube.com/watch?v=SKhKNUo6rJU>

For your additional References that has been used please use the citation tools on the website

<https://www.scribbr.com/> using APA 7th Edition English, and paste it below.

