Information Security IA

Implementation of Honeypot using PenTbox

Sidharth Nair - 16010120032
Rahi Patil - 16010120038

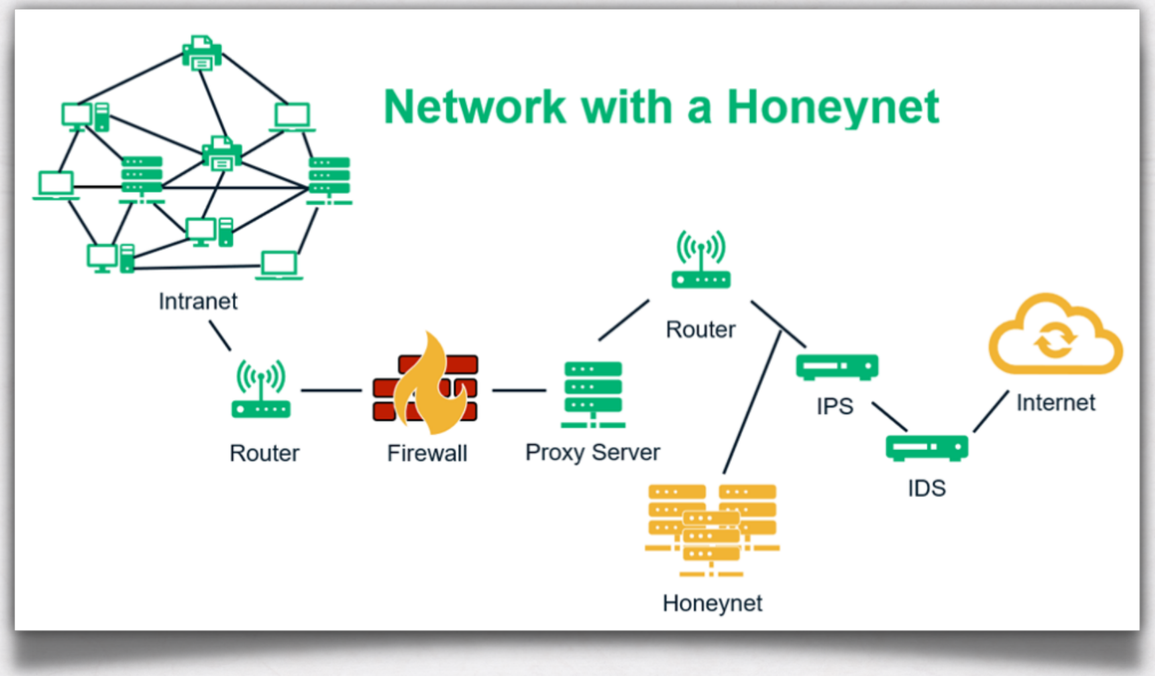
Index

Introduction

- A Linux distribution with Debian roots called Kali Linux is made for penetration testing and digital forensics. Offensive Security oversees and provides maintenance for it.
- Kali Linux offers 600 penetration-testing applications, including Armitage, Nmap, Wireshark, John the Ripper, sqlmap, Aircrack-ing, Burp, and OWASP ZAP.
- It was created by Offensive Security employees Mati Aharoni and Devon Kearns through the rewriting of BackTrack, a Linux distribution they had previously used for information security testing and which was based on Knoppix. The Hindu deity Kali served as the name's inspiration.

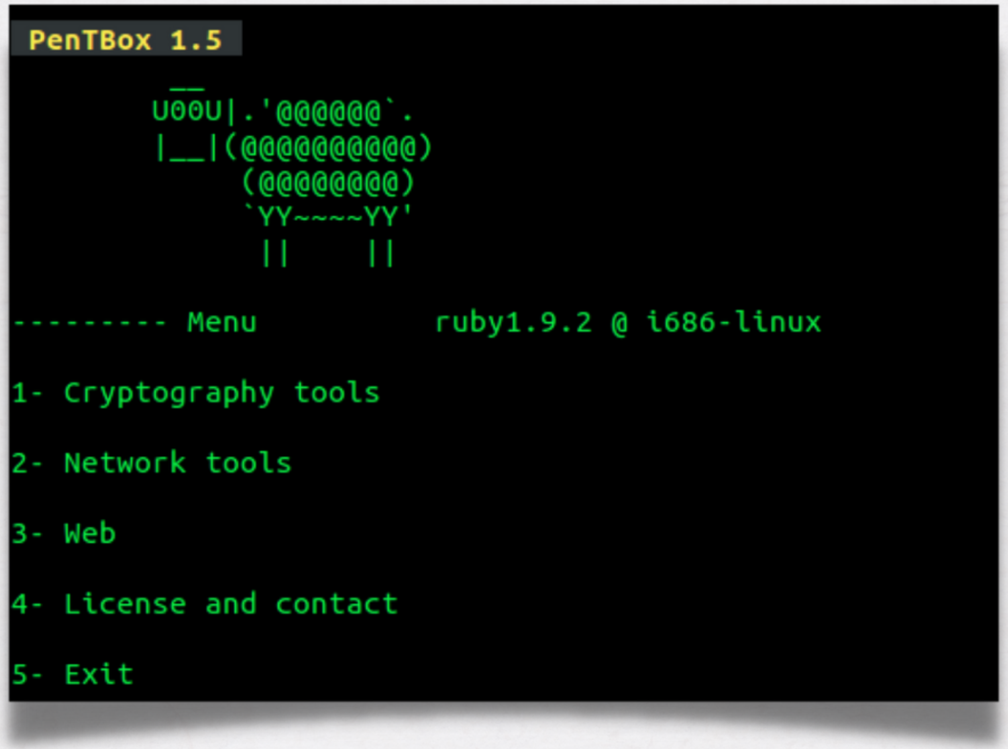
Honeypot

Honeypots are network-attached systems used by hackers to identify and research tactics and types of attacks. Large businesses and cybersecurity-related organisations are the main users, but crooks may use them to hoodwink researchers and disseminate false information.



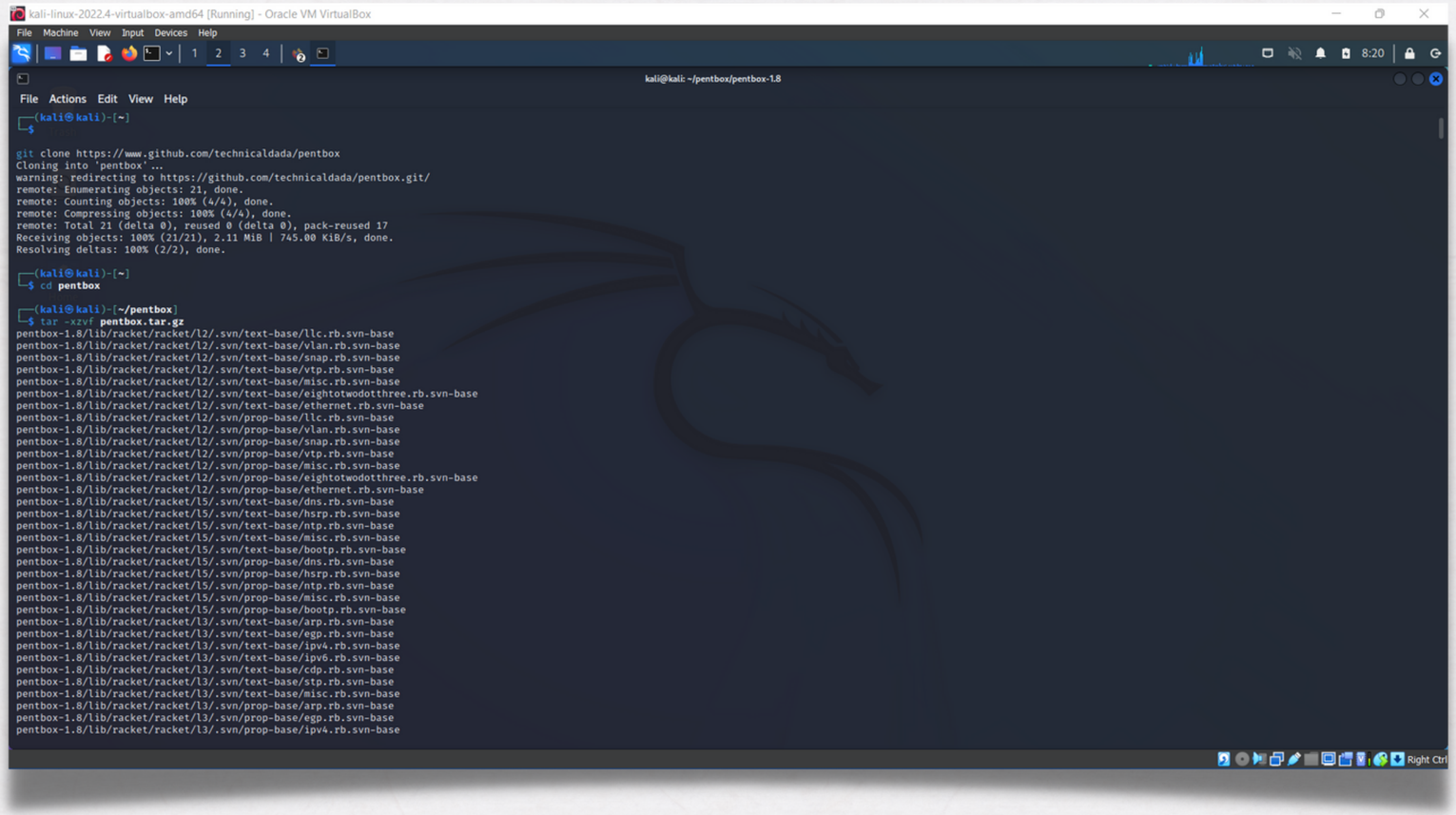
PenTbox

PenTBox is a security suite that can be used in penetration testing engagements to perform a variety of activities.Specifically these activities include from cracking hashes,DNS enumeration and stress testing to HTTP directory brute force.



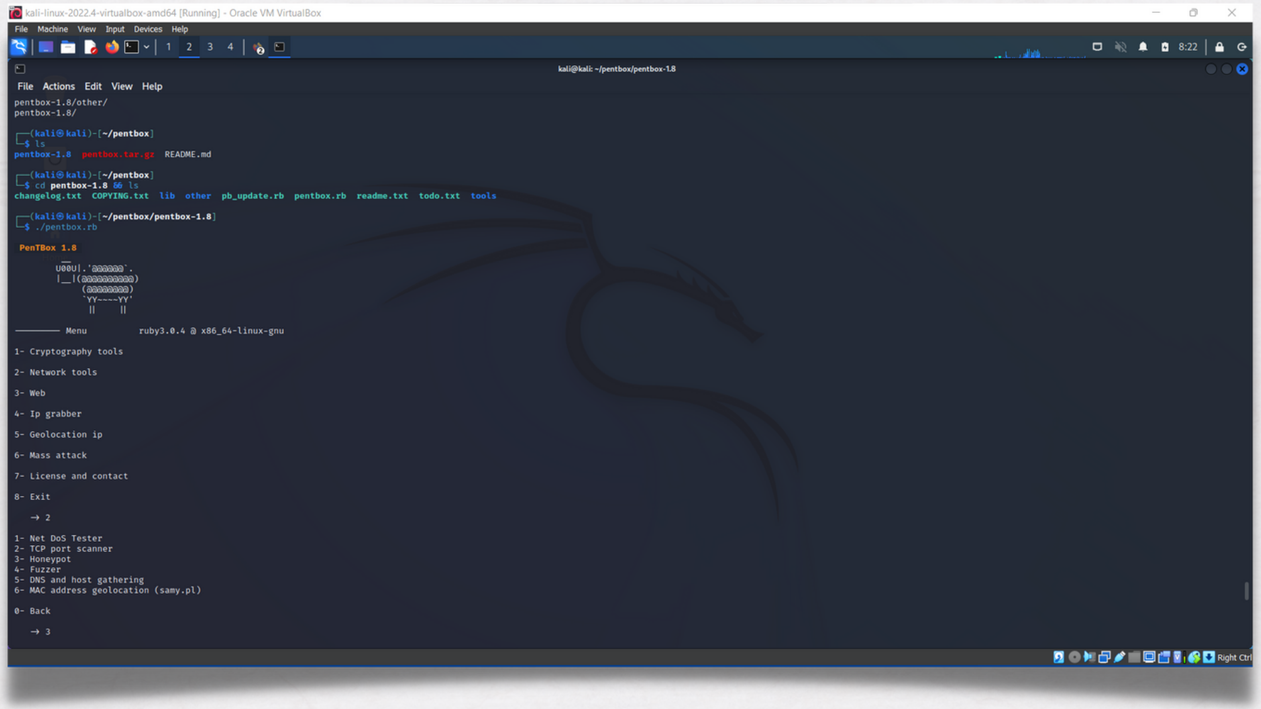
Stepwise Demonstration

- To set up a honeypot in our Kali Linux system we need to download a tool from GitHub it called **Pentbox**. This tool is written in ruby language. To download this we use the following command:



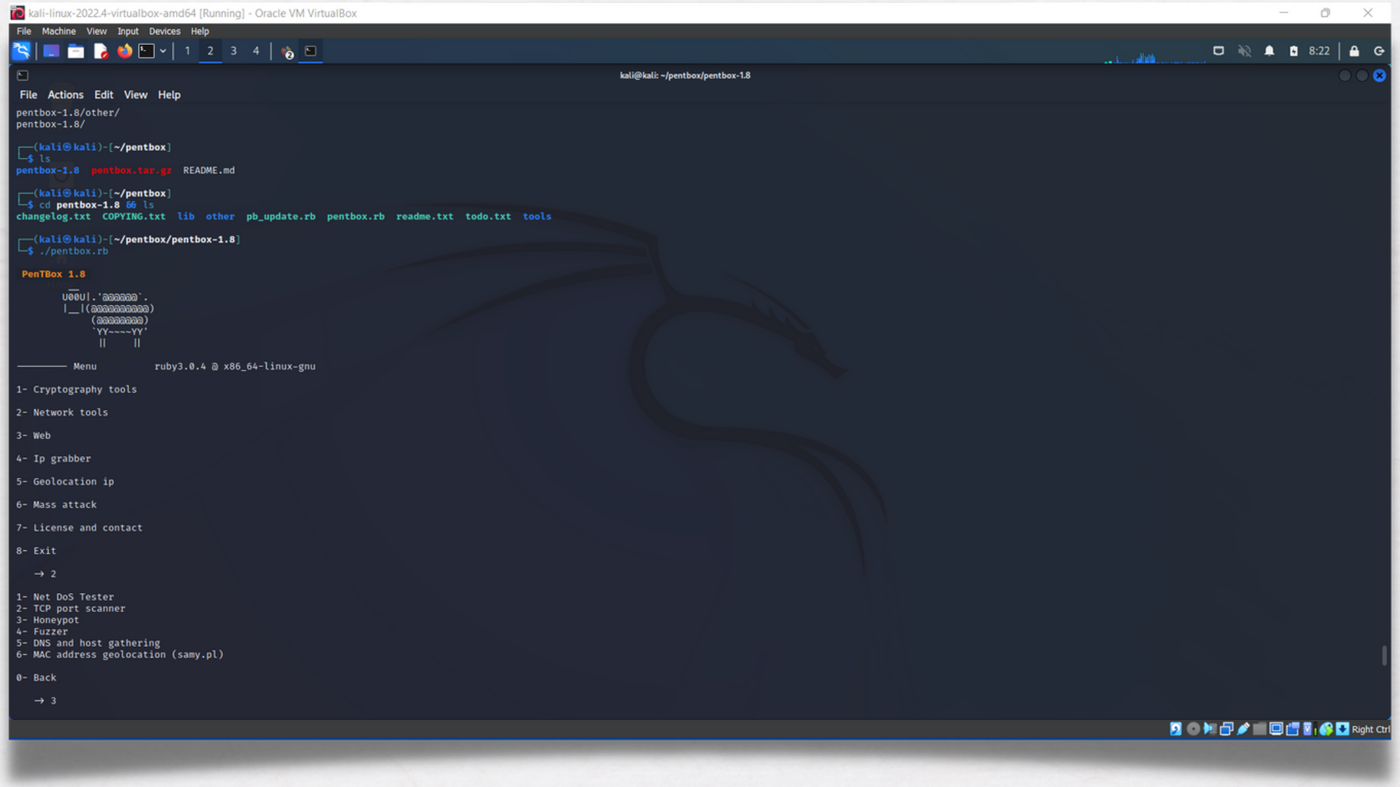
Stepwise Demonstration

- Then we need to go into the pentbox folder by using cd command. Here we have a compressed file named pentbox.tar.xz and to extract it. Then we run this ruby tool by using simple command as following: ./pentbox.rb



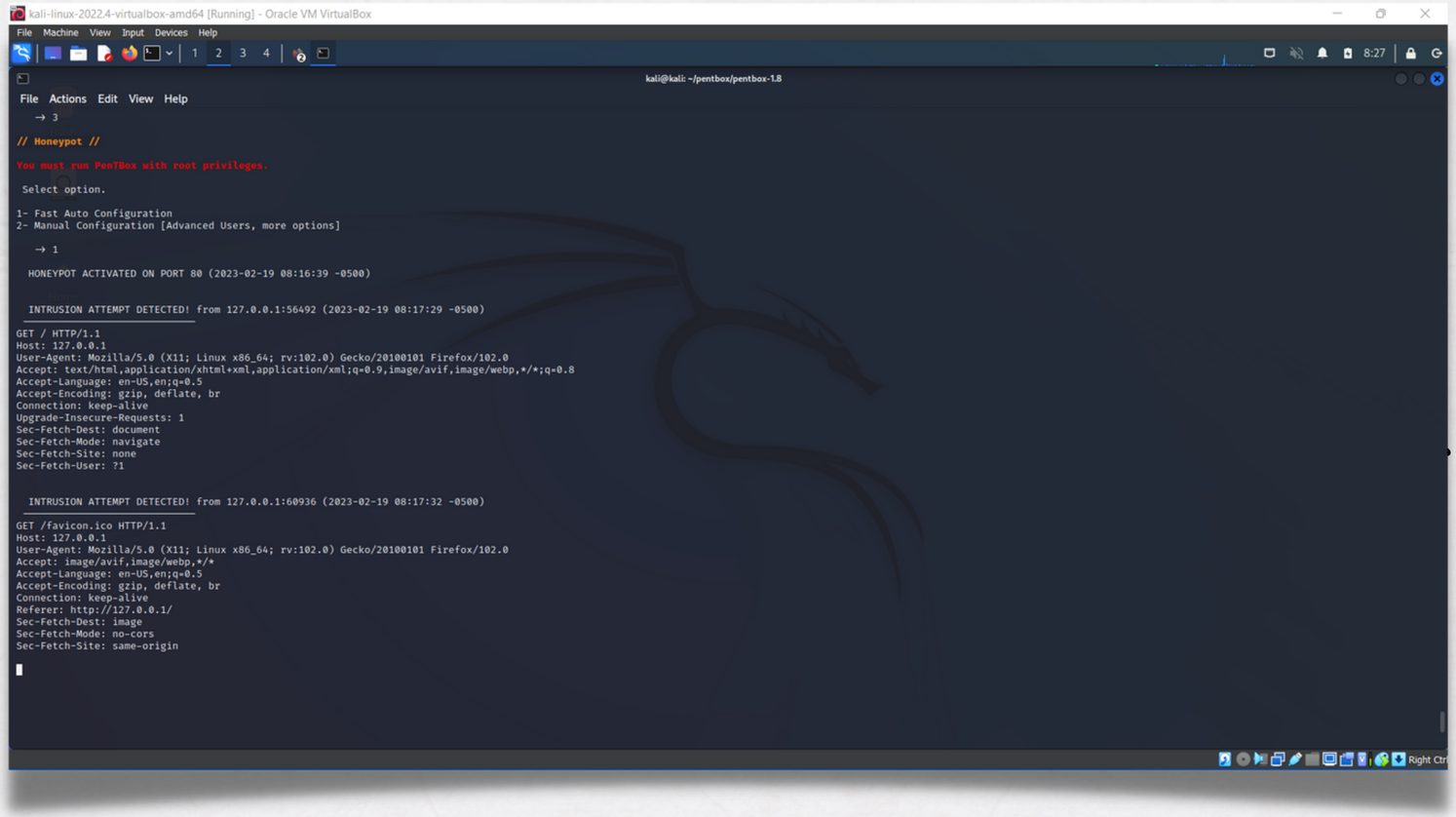
Stepwise Demonstration

- Then this tool will open. Here we need to go to the Network tools option. Then we can see the Honeypot option.



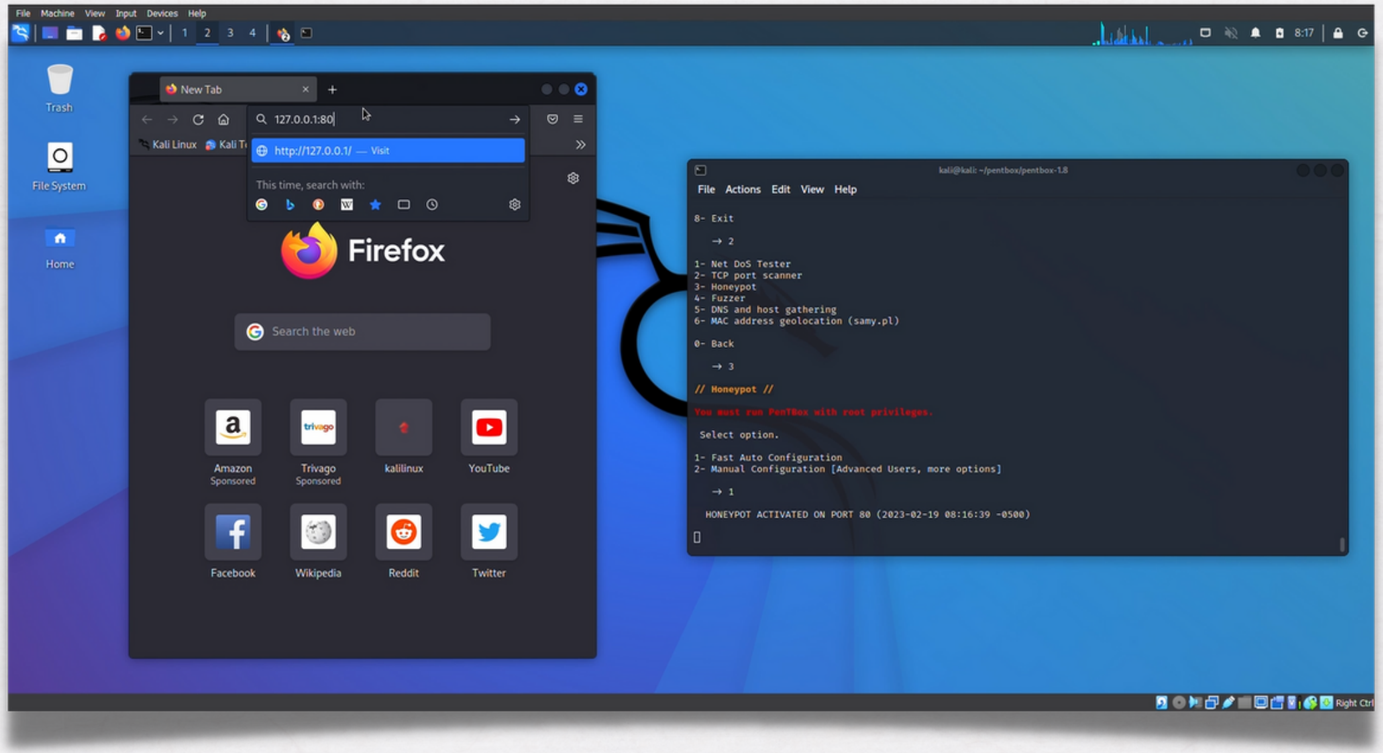
Stepwise Demonstration

- Here we can choose 1 for auto configuration this will be fast or we can choose 2 for manual configuration. Manual configuration contains more options but it is for advanced users.

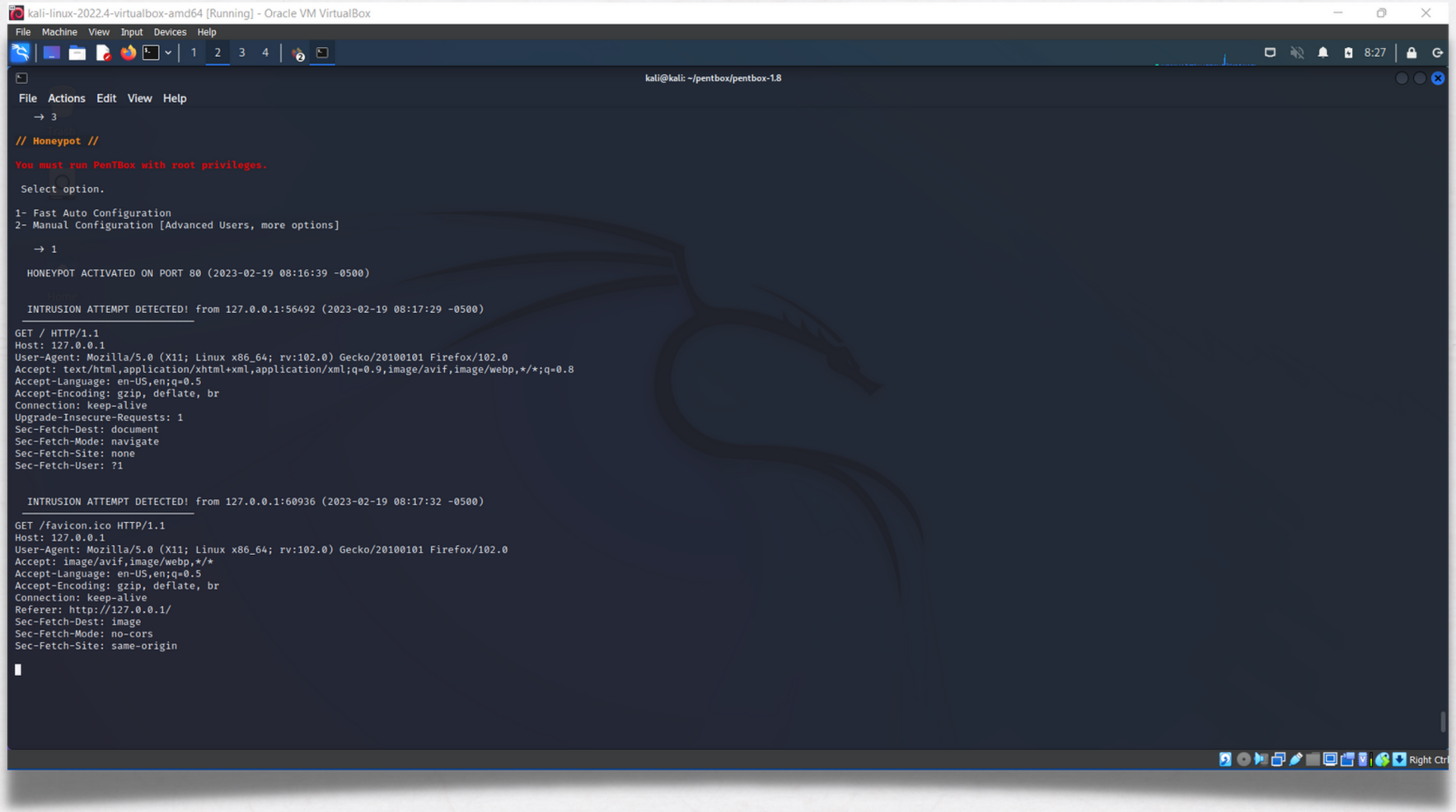


Stepwise Demonstration

- Now we can see that we have successfully run honeypot in our localhost on port 80. To check how it works we can go to browser and check our localhost that is 127.0.0.1:80 and then check in the terminal where we started honeypot



Stepwise Demonstration



Thank You