

FIREWALL

A firewall is a computer network security system that restricts internet traffic in, out, or within a private network.

This software or dedicated hardware-software unit functions by selectively blocking or allowing data packets. It is typically intended to prevent anyone inside or outside a private network from engaging in an unauthorized web activities and to help prevent malicious activity. It can be viewed as gated borders or gateways that manage the travel of permitted and prohibited web activitys in a private network**.** It is also used in both personal and enterprise settings, and many devices come with one built-in, including Mac, Windows, and Linux computers. They are widely considered as an essential component of network security.

# Why firewall is important

Networks without protection are vulnerable to any traffic that is trying to access your system. Harmful or not, network traffic should always be vetted.

Hacking, identity theft, malware, and online fraud are common threats users could face when they expose themselves by linking their computers to a network or the internet. Once discovered by a malicious actor, your network and devices can easily be found, rapidly accessed, and exposed to repeated threats. Around the clock internet connections elevate the risk of this.

[Proactive protection](https://www.kaspersky.co.in/security-cloud) is critical when using any sort of network. Users can protect from the very worst dangers by erecting an invisible wall to filter out those threats. Fortunately, an invisible wall already exists - it is known as a firewall.

# How Does firewall work

As mentioned before, firewalls filter the network traffic within a private network. It analyses that which traffic should be allowed or restricted based on a set of rules. Think of the firewall like as a gatekeeper at your computer’s entry point which only allows

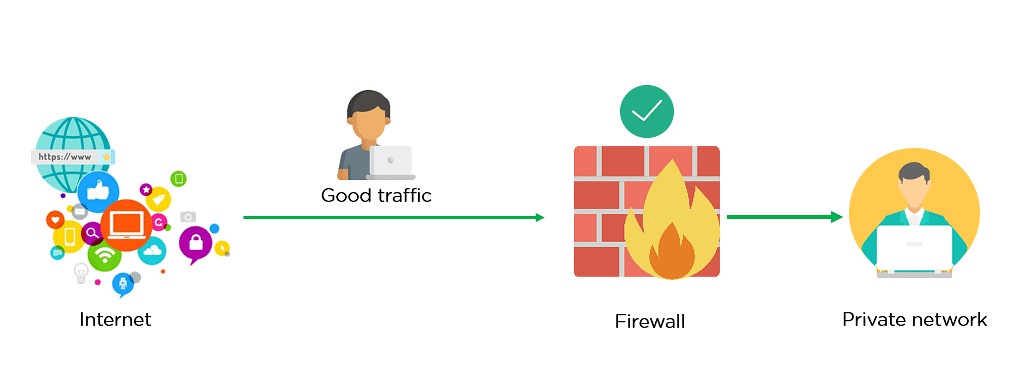
trusted sources, or IP addresses, to enter your network.

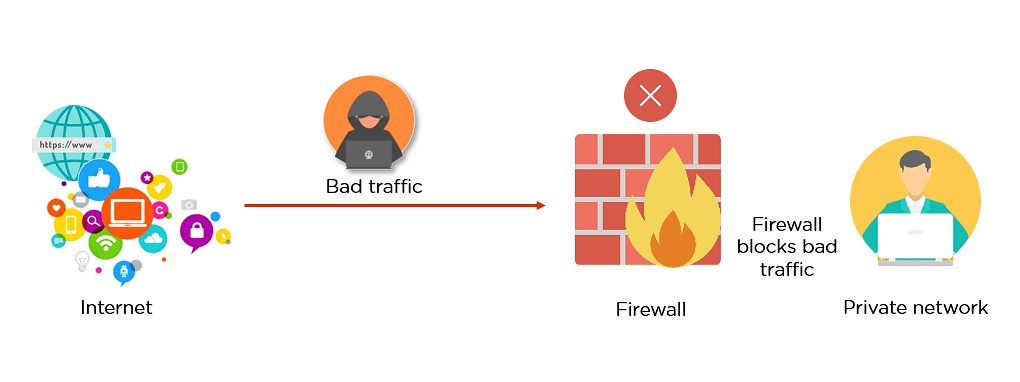
A firewall welcomes only those incoming traffic that has been configured to accept. It distinguishes between good and malicious traffic and either allows or blocks specific data packets on pre-

established security rules.

These rules are based on several aspects indicated by the packet data, like their source, destination, content, and so on. They block

traffic coming from suspicious sources to prevent cyberattacks.



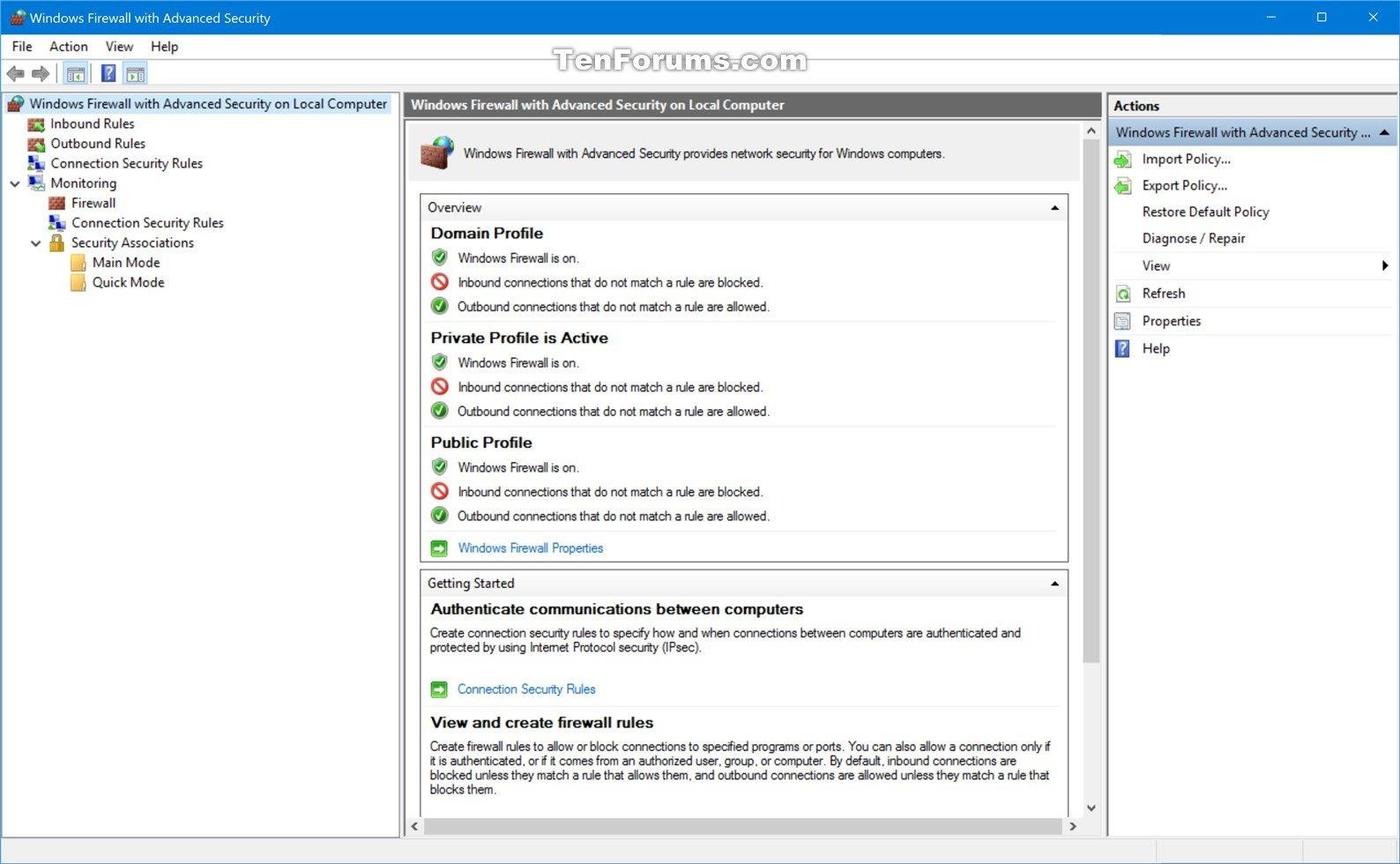


This way, a firewall carries out quick assessments to detect

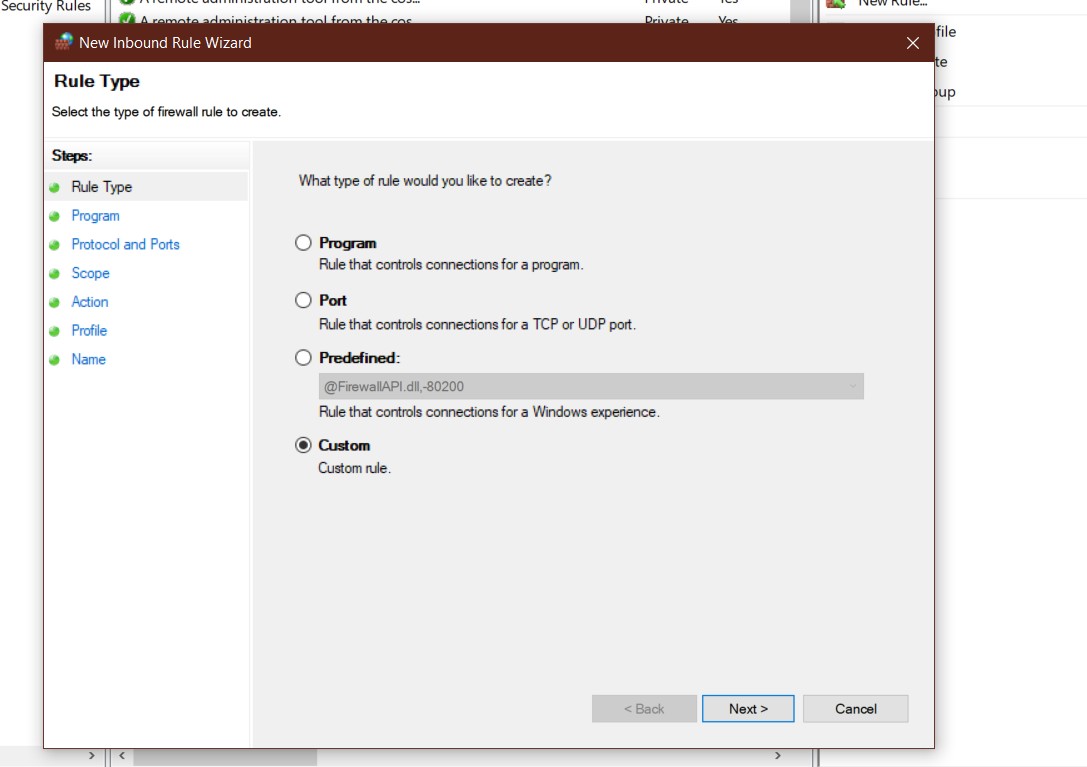
malware and other suspicious activities.

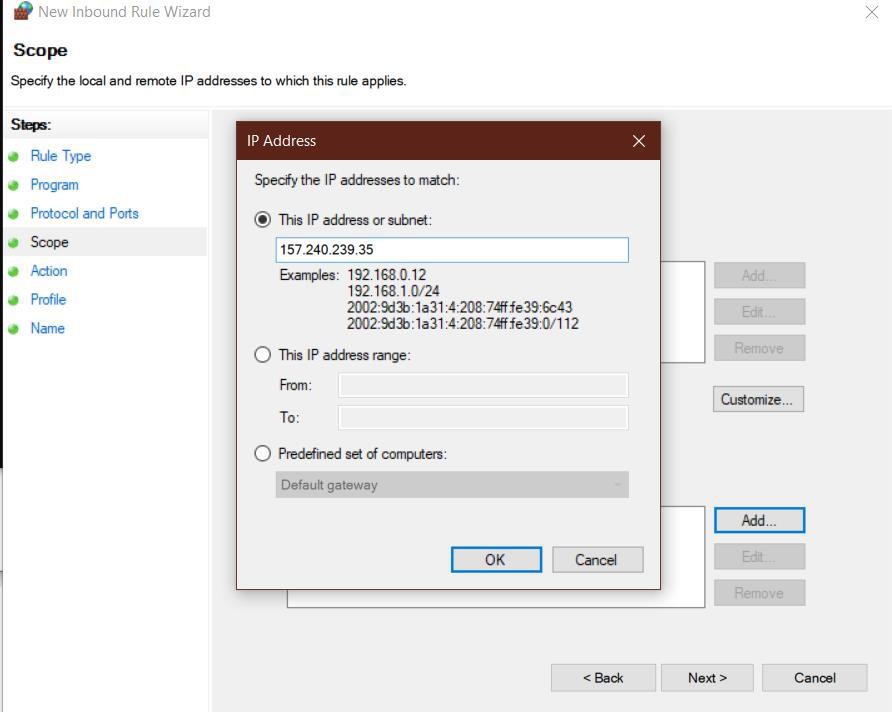
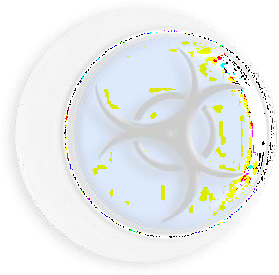
## Blocking Or Allowing IP:

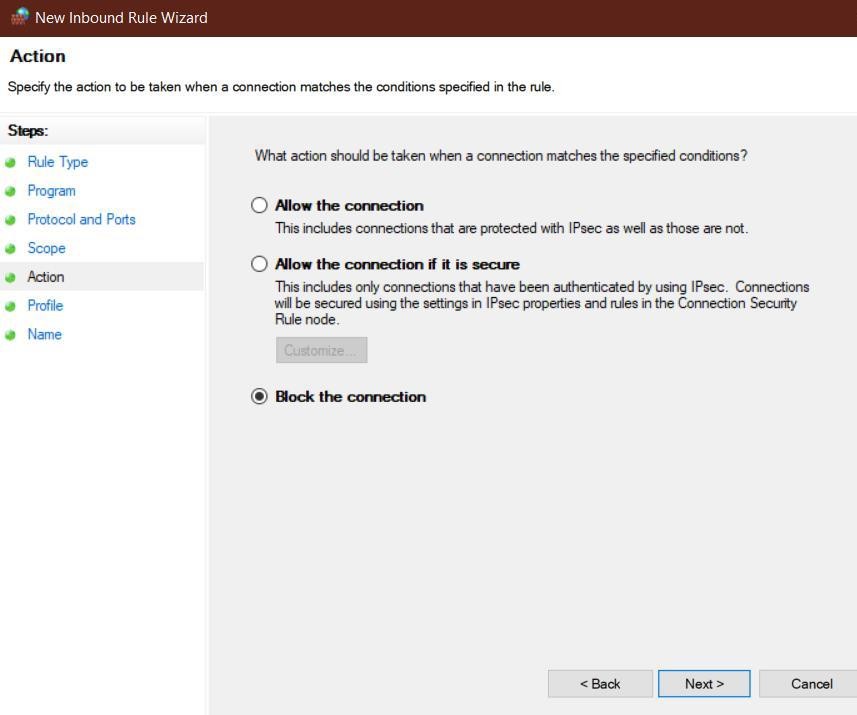
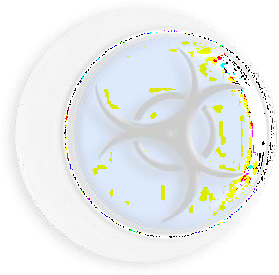
**Step1-** Open Advanced Windows Firewall Settings.

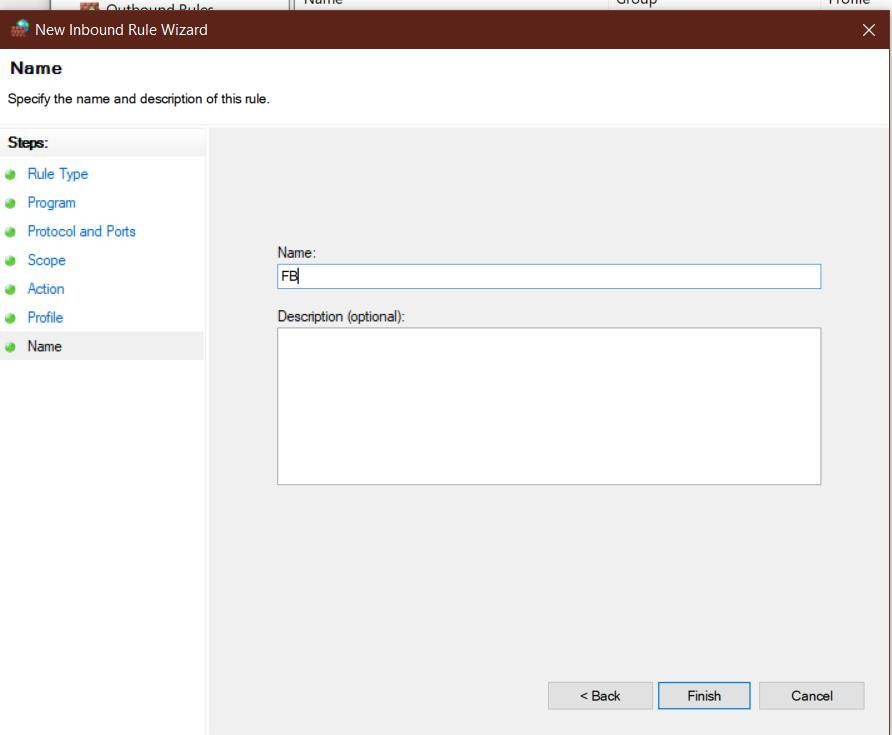
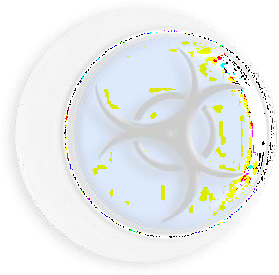


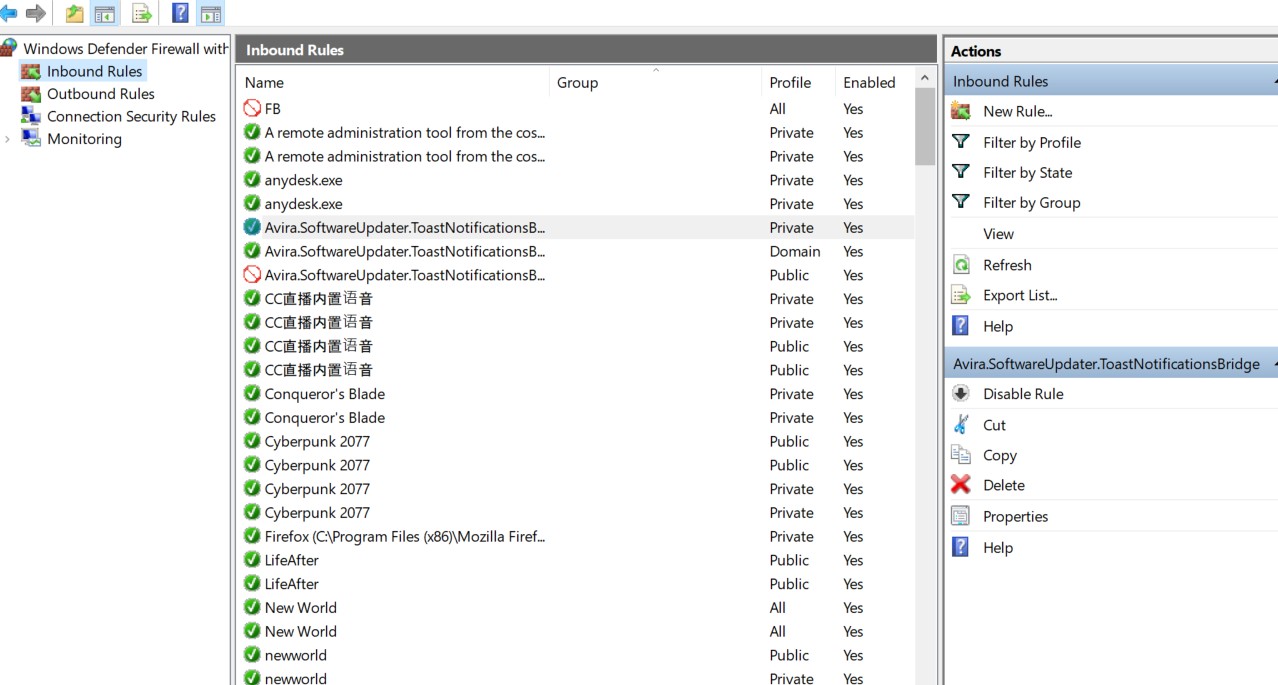
**Step2-** Making New Inbound Rule

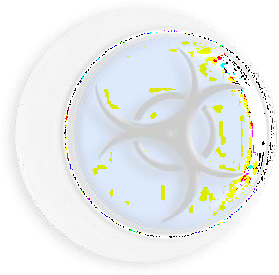


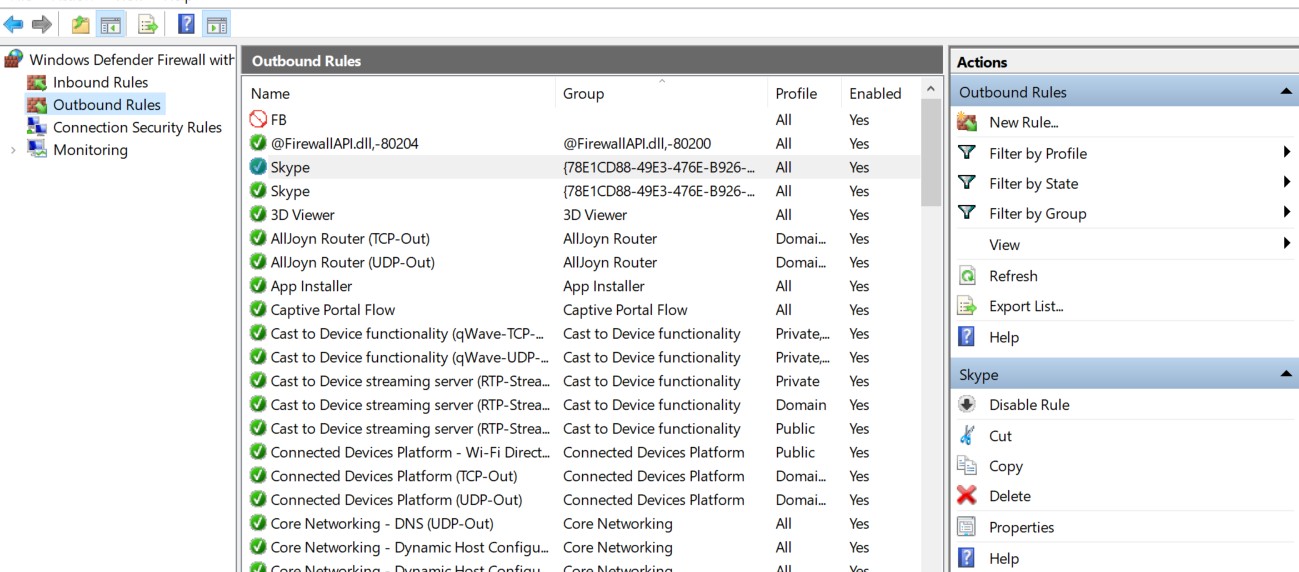
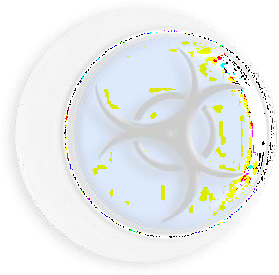


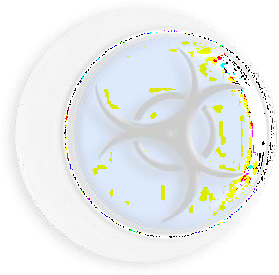


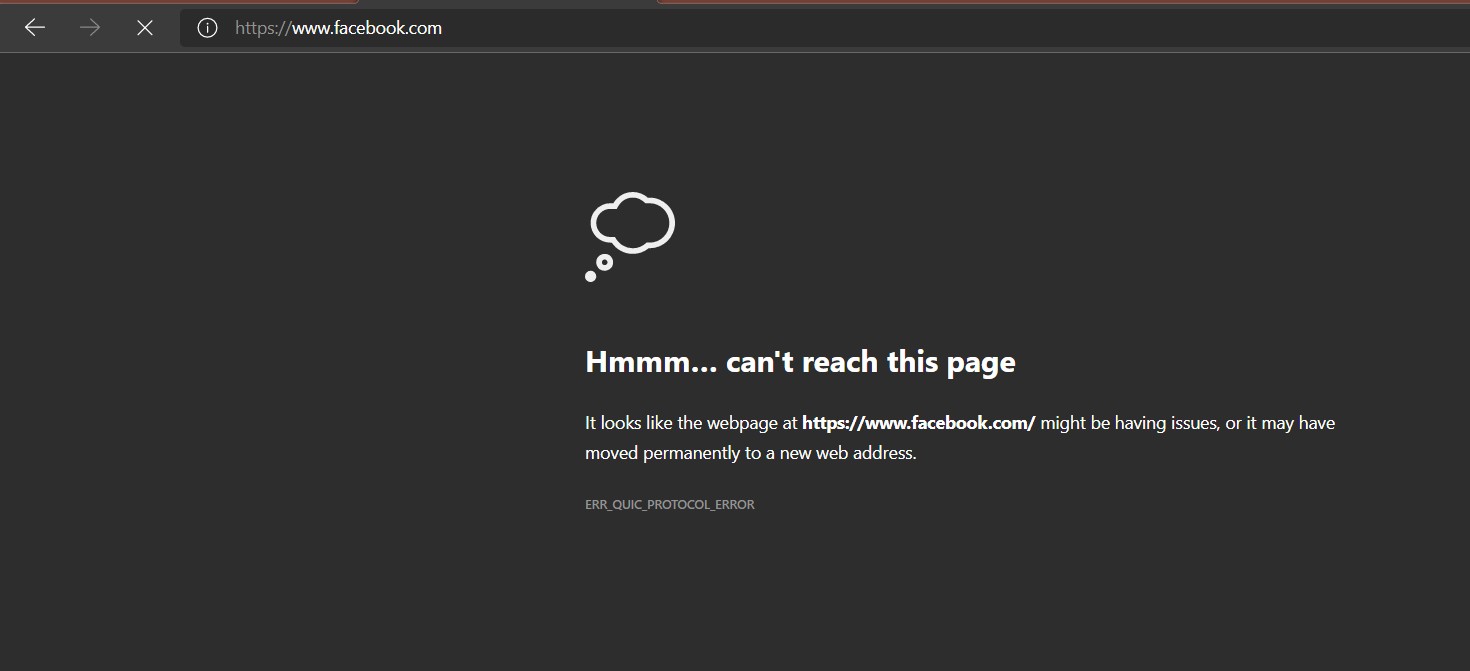




**Step3-** After making an inbound rule, we will make an outbound rule just like we did for inbound rule and the listed IP would be blocked.



Now if we visit these Ip Addresses we will get this



**Honeypot**

Honeypots is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempt at unauthorized use of information systems . Generally, a honeypot consists of data that appears to be a legitimate

part of the site and contain information or resources that are beneficial for attackers. It is actually isolated, monitored, and capable of blocking or analyzing the

attackers.

Honeypots are a type of deception technology that allows you to understand attacker’s behavior patterns. Security teams can use honeypots to investigate cybersecurity breaches to collect intel on how cybercriminals operate.

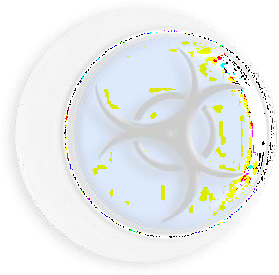
They also reduce the risk of false positives, comparison of traditional cybersecurity measures, because they are unlikely to attract legitimate activity.

Honepots are mostly used by large companies and organizations involved in cybersecurity. It helps cybersecurity researchers to learn about the different type of cyber attacks. It is suspected that even the cybercriminals use these honeypots to as a decoy for spreading wrong information.

The cost of a honeypot is high because it requires specialized skills and resources to implement in a system. In such a way that it appears to provide an organization’s

resources but in truth it protects the acess of system from the back.

## Types of Honeypots

**Production honeypots**—serve as decoy systems inside fully operating networks and servers, often as part of an intrusion detection system (IDS). They deflect criminal attention from the real system while analyzing malicious activity to help mitigate vulnerabilities.

**Research honeypots**—used for educational purposes and security enhancements. They contain trackable data that you can trace when stolen to analyze the attack.

## Advantages of Honeypot

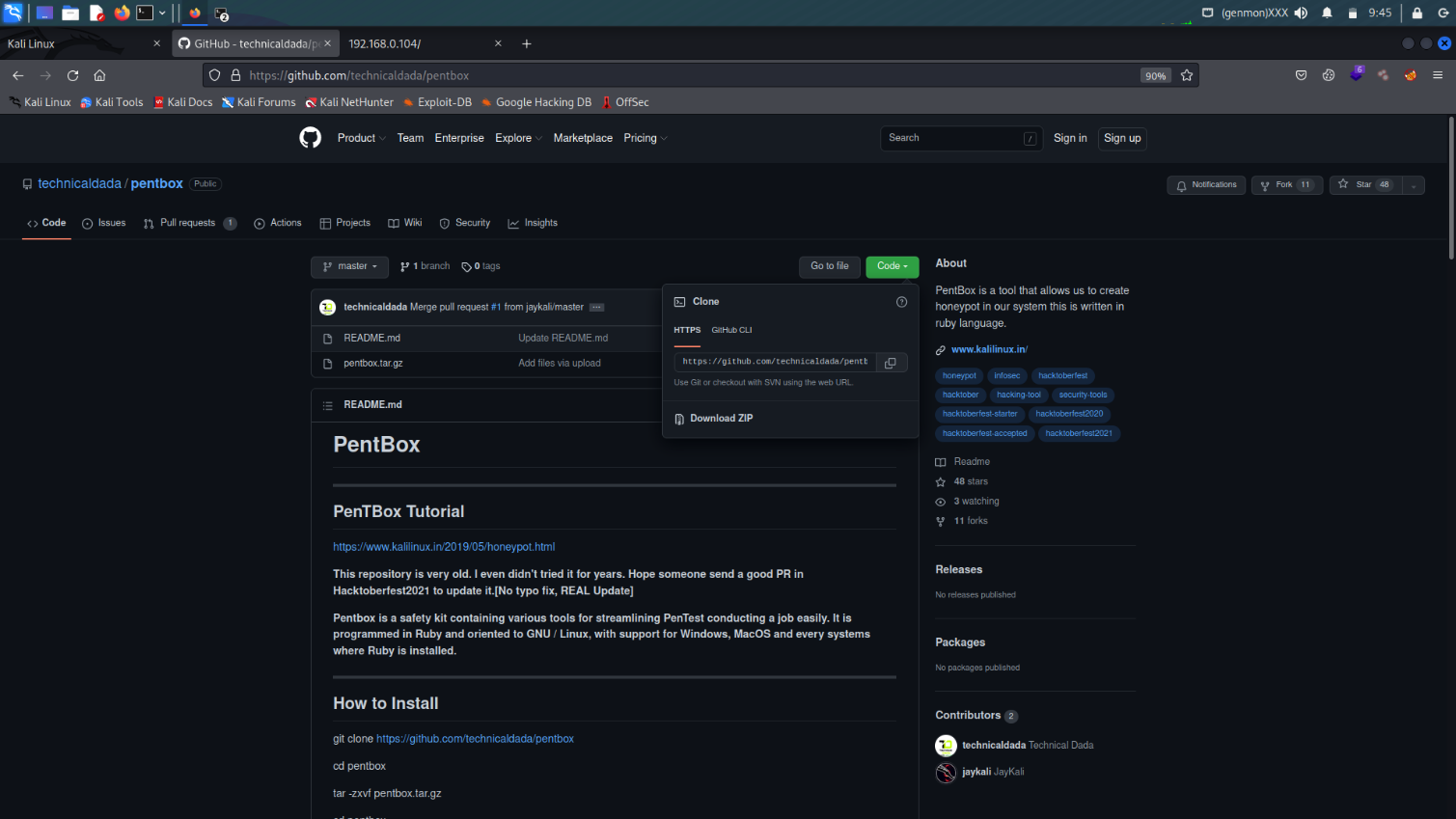
* Acts as a rich source of information and help to collect real time data.
* Identifies malicious activity even if encryption is used.
* Wastes hackers time and resources
* Improves security.

## Disadvantages of Honeypot

* Being distinguishable from production system, it can be easily identified by experienced attackers.
* Having a narrow field of view can only identify direct attacks.
* A honeypot once attacked can be used to attack other systems.
* Fingerprinting (an attacker can identify the true identity of honeypot)

# Practical Of Honeypot Tool

Download The tool From the github For Creating the Honeypot name “Pentbox”



Link :- <https://github.com/technicaldada/pentbox>

Installation process

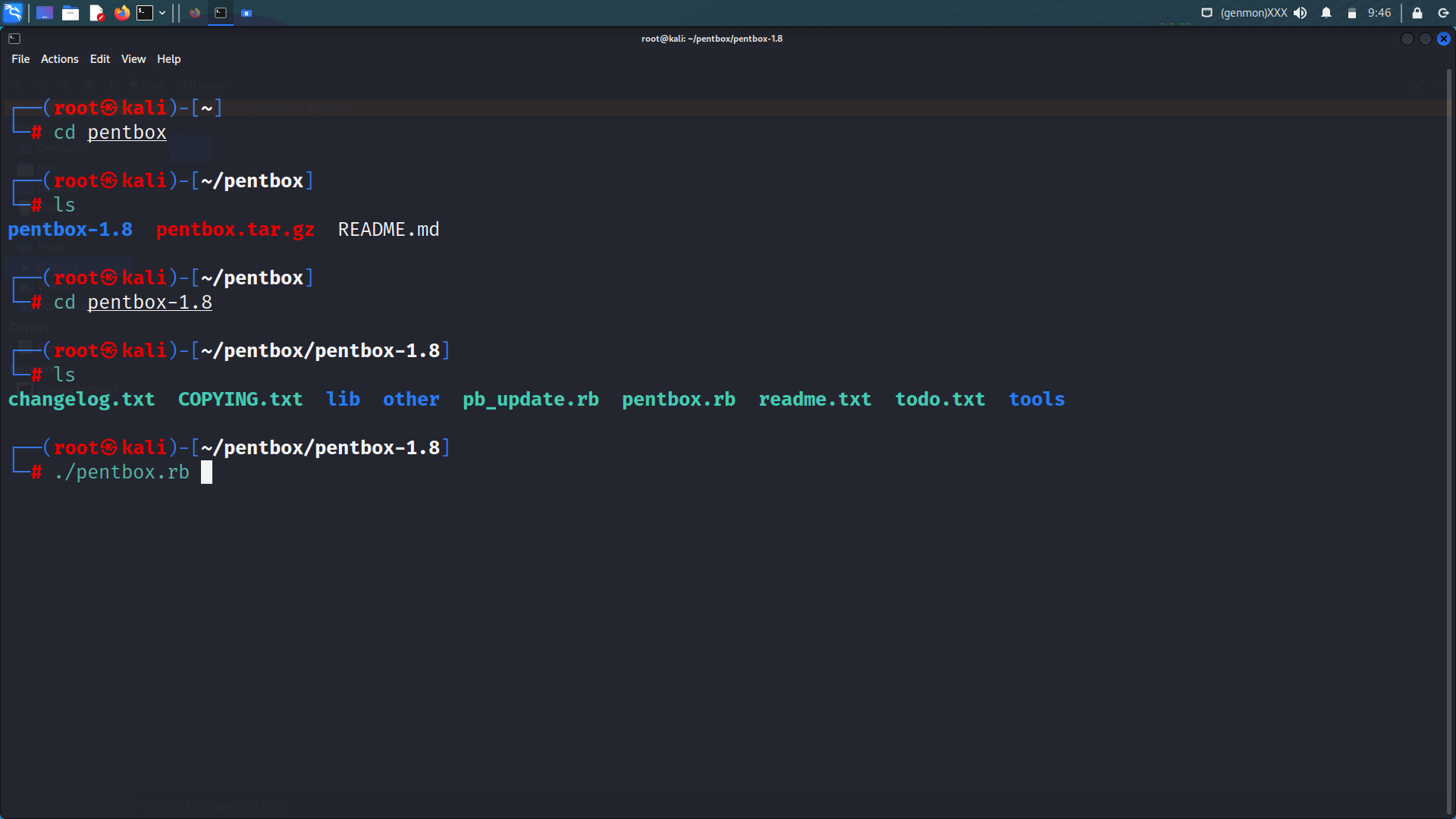
cd pentbox

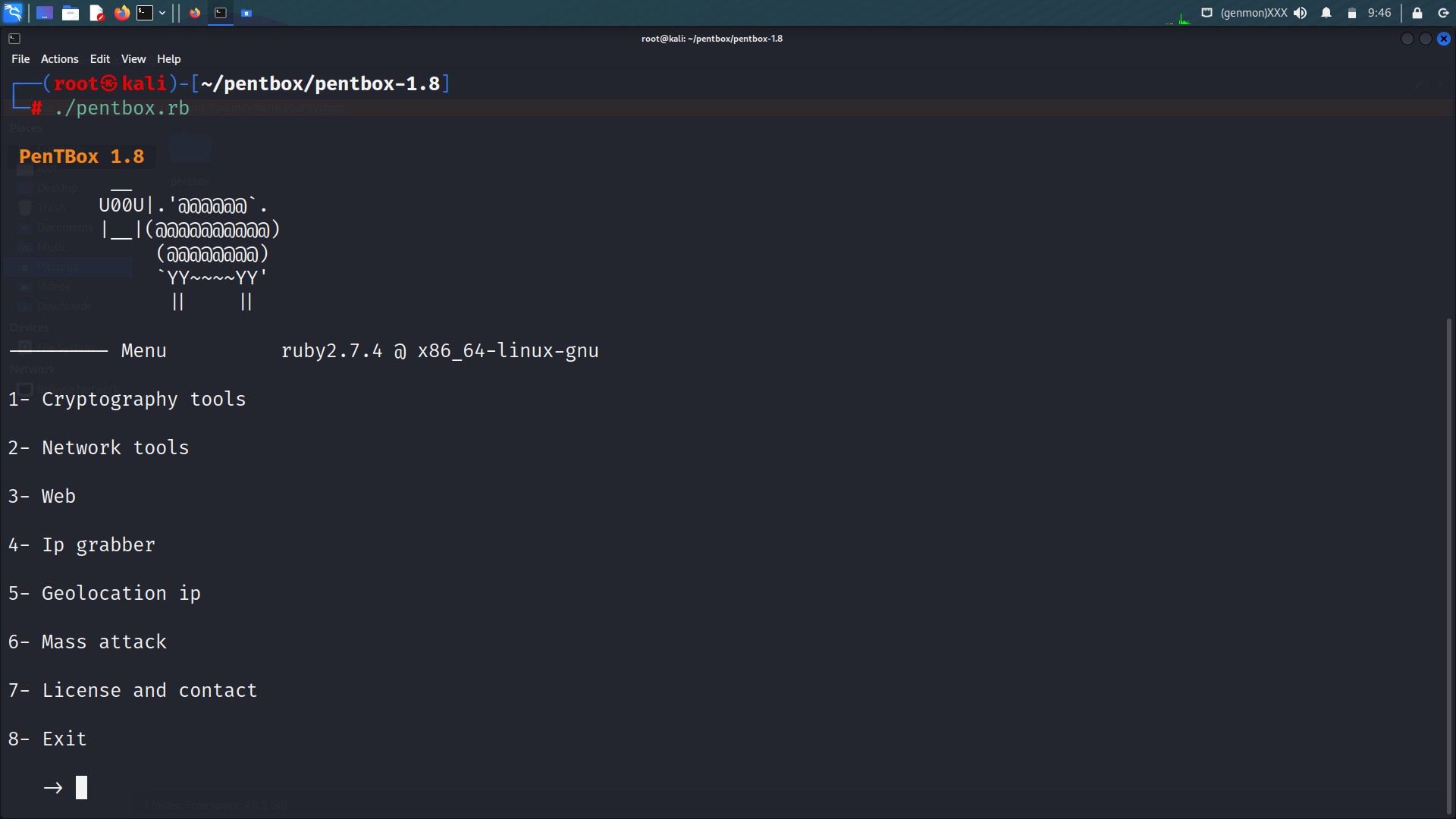
tar -zxvf pentbox.tar.gz

cd pentbox

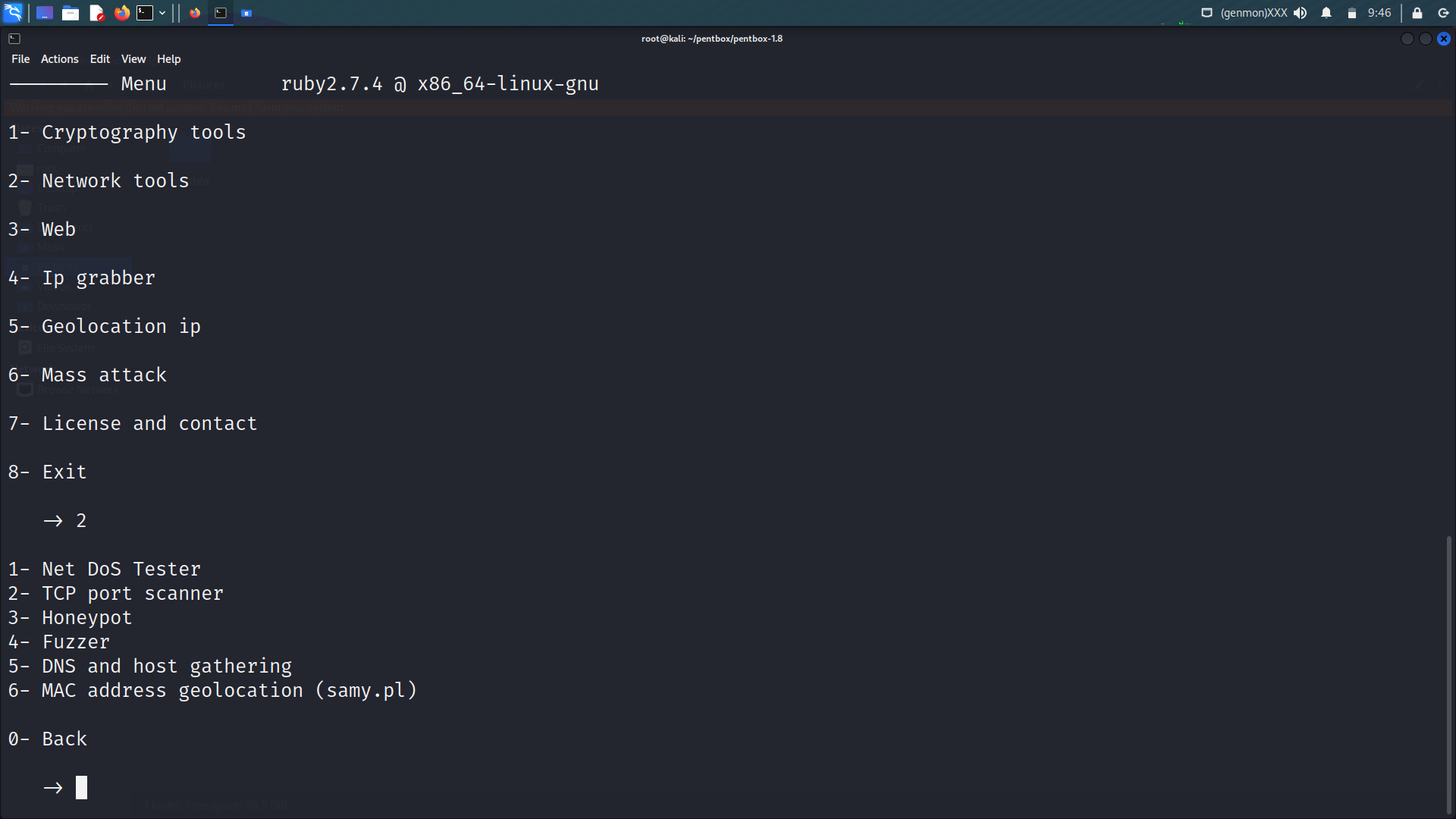
./pentbox.rb

Git clone for installing the tool in the kali linux

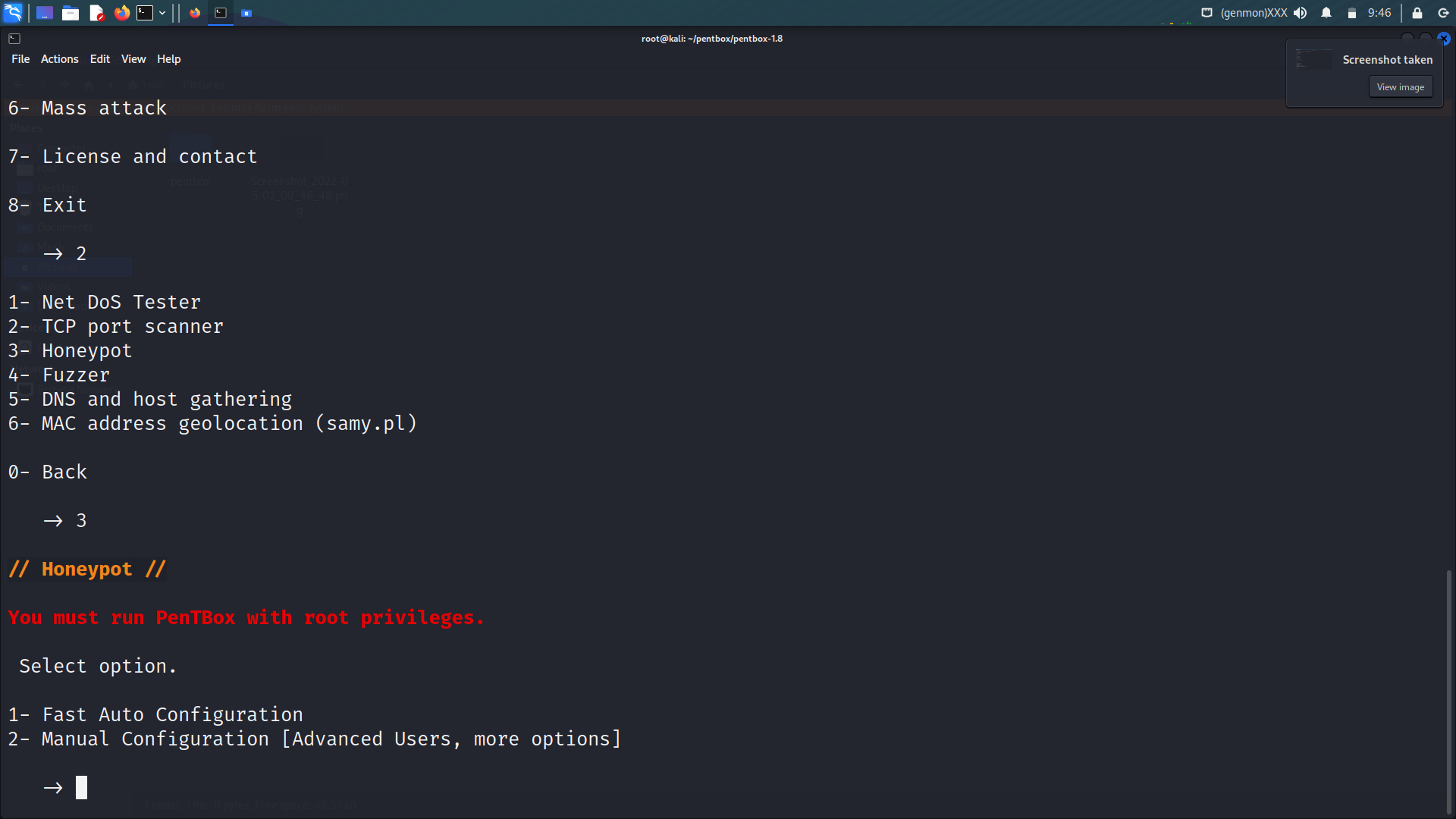




Select the no. 3 “web”

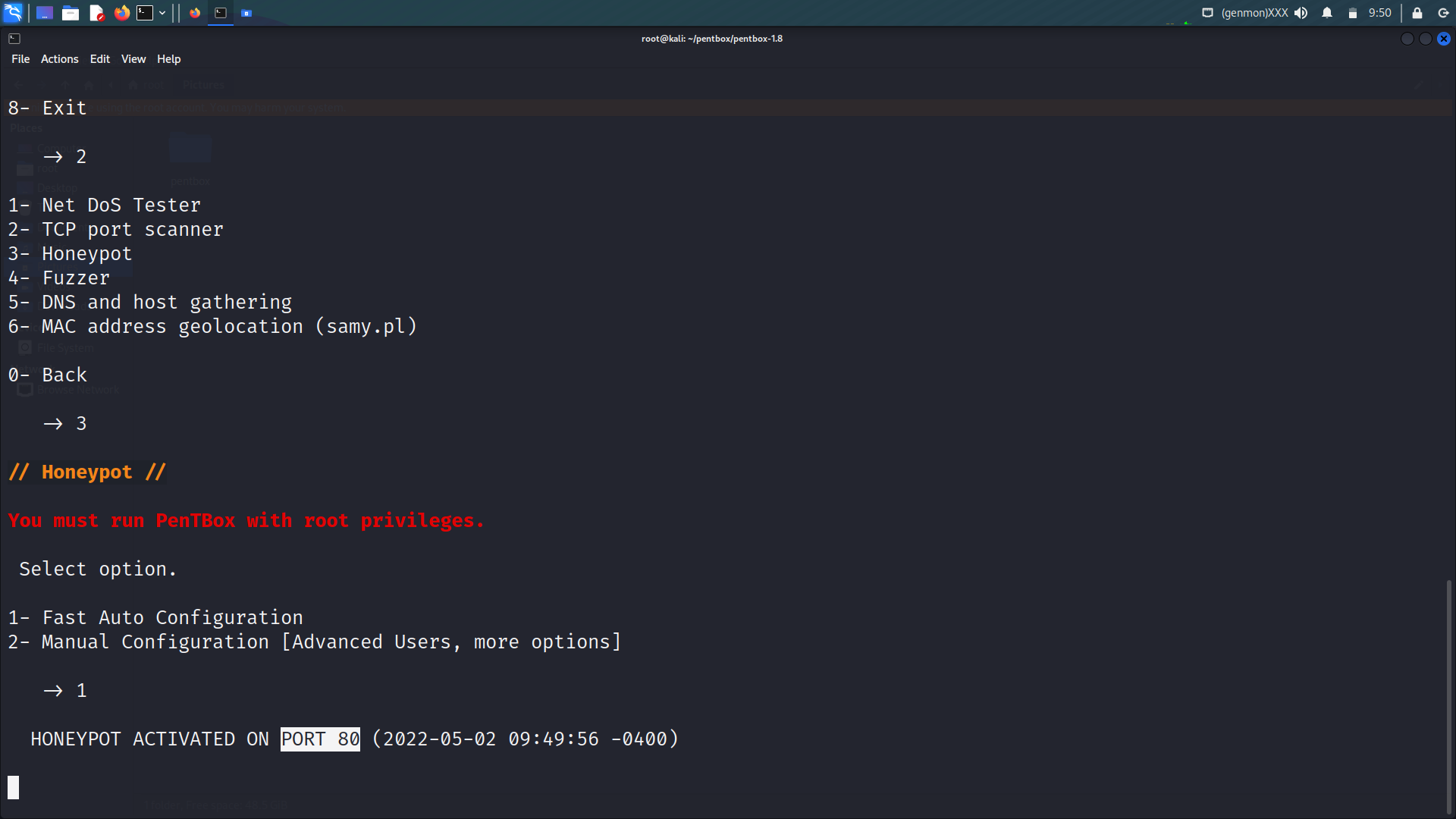


Select the options 3 “Honeypot”



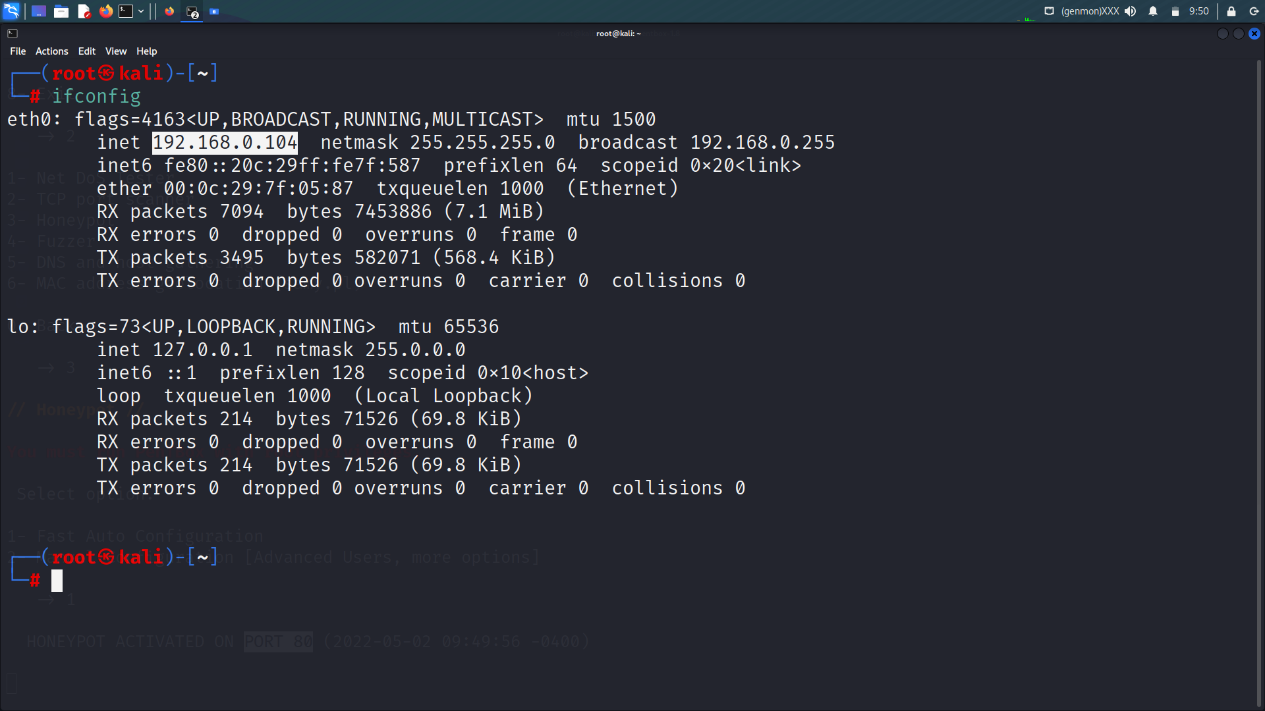
Here we have 2 options

1. Fast auto configuration
2. Manual configuration (Advance Users, options)



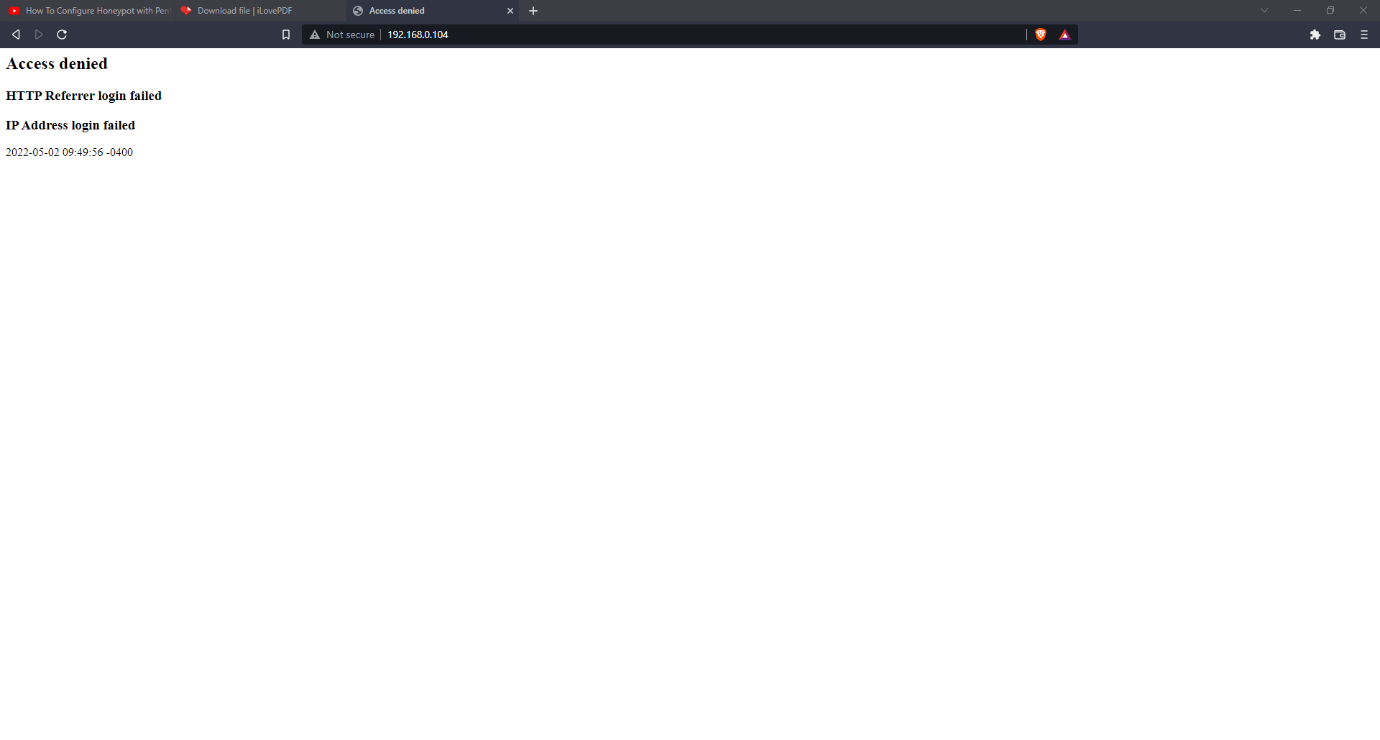
Select the options 1 “Fast Auto Configuration”

Here we see clearly the honeypot is running in the port no. 80 “port 80 is stand for http (hyper text transfer protocol)”



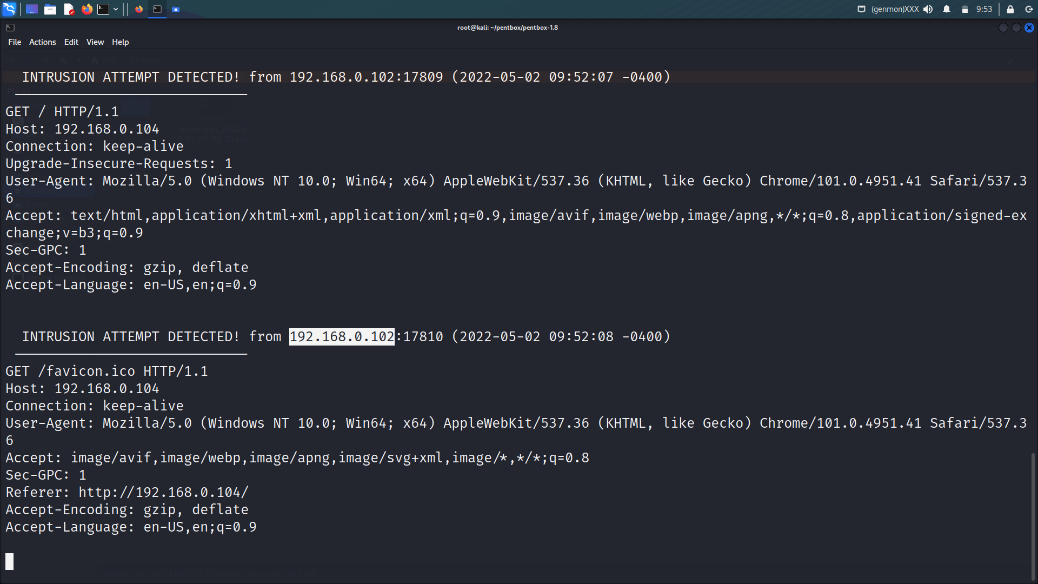
If config command to check the ip address of the kali

Now lets check the power of the honepot tool which we are using “here I am using window os to test the honeypot tool ”



Copy the ip address of the kali linux into the main machine because the tool is running into the port no. 80 and the port no. 80 is strand for hyper text transfer protocol..

Now check the response of the tool in the kali linux



Now here we clearly see the detail of the attacker