HONEY POTS

A honeypot is a security mechanism designed to mimic real systems, applications, or networks with the goal of attracting and detecting malicious activity. It acts as a decoy, luring attackers into an environment that simulates legitimate systems, services, and data. The primary purpose of honeypots is to gather information about attackers, their tactics, techniques, and procedures (TTPs), and to enhance overall cybersecurity by improving threat intelligence.

Types of Honeypots:

➢ Low-Interaction Honeypots:

Emulate a limited set of services and protocols without fully replicating the actual operating system.
Simulate the presence of vulnerabilities to attract attackers.
Less resource-intensive and easier to deploy.

➢ Medium-Interaction Honeypots:

Emulate a broader range of services and protocols, providing a more realistic environment for attackers.
Balance between realism and resource efficiency.
Suitable for capturing more sophisticated attack behaviors.

➢ High-Interaction Honeypots:

Fully replicate real systems, including the operating system, services, and applications.
Provide a highly realistic environment for attackers to interact with.
Most resource-intensive but offers the most accurate insights into attacker behavior.

Honeypot Tools:

➢ Honeyd:

Type: Low-Interaction Honeypot
Description: Allows emulation of multiple operating systems and services.

➢ Dionaea:

Type: Medium-Interaction Honeypot
Description: Captures and analyzes attacks targeting various services like SMB, FTP, and HTTP.

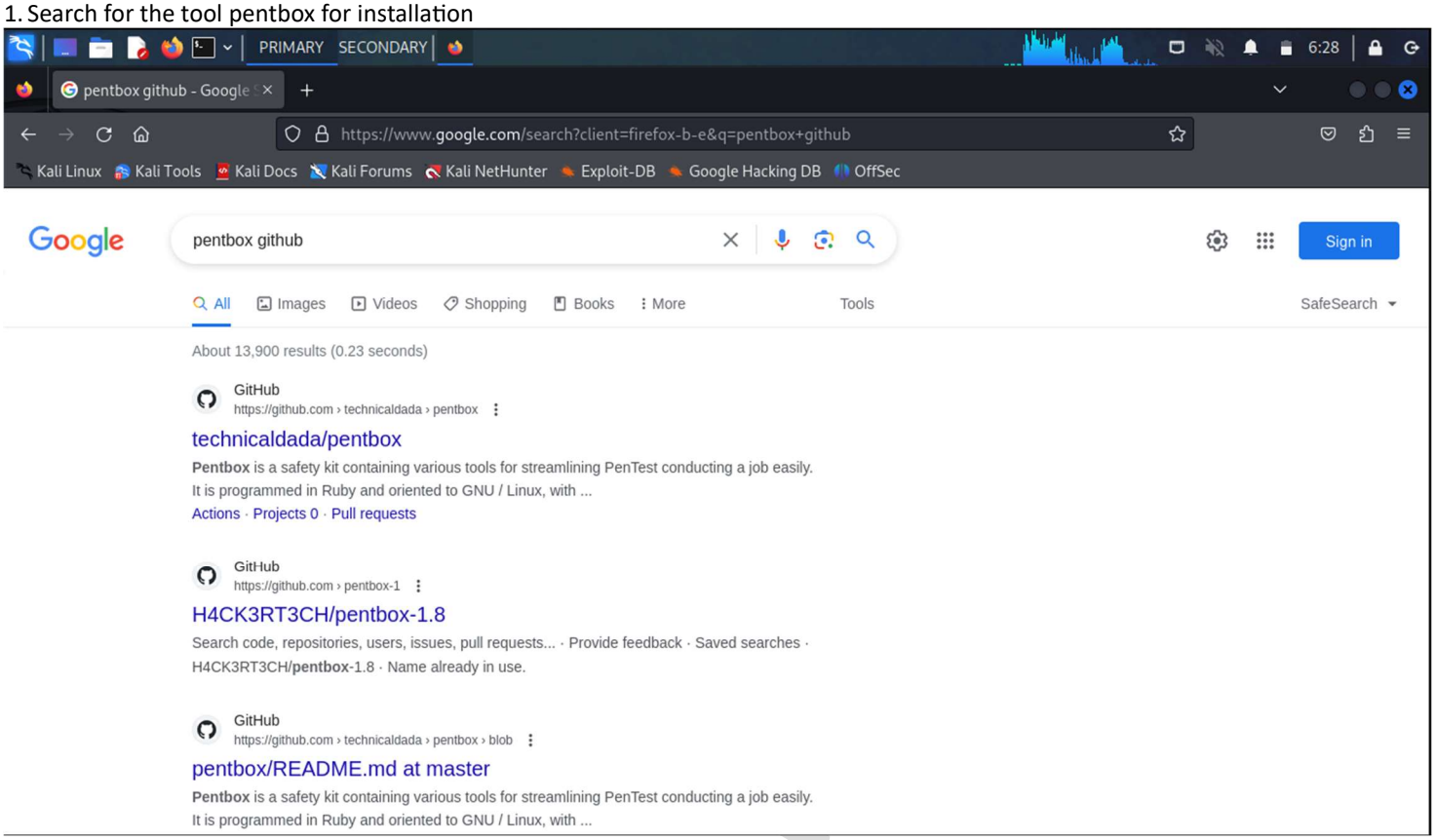
➢ Modern Honey Network (MHN):

Type: High-Interaction Honeypot Framework
Description: Facilitates the deployment and management of high-interaction honeypots, supporting various honeypot technologies.

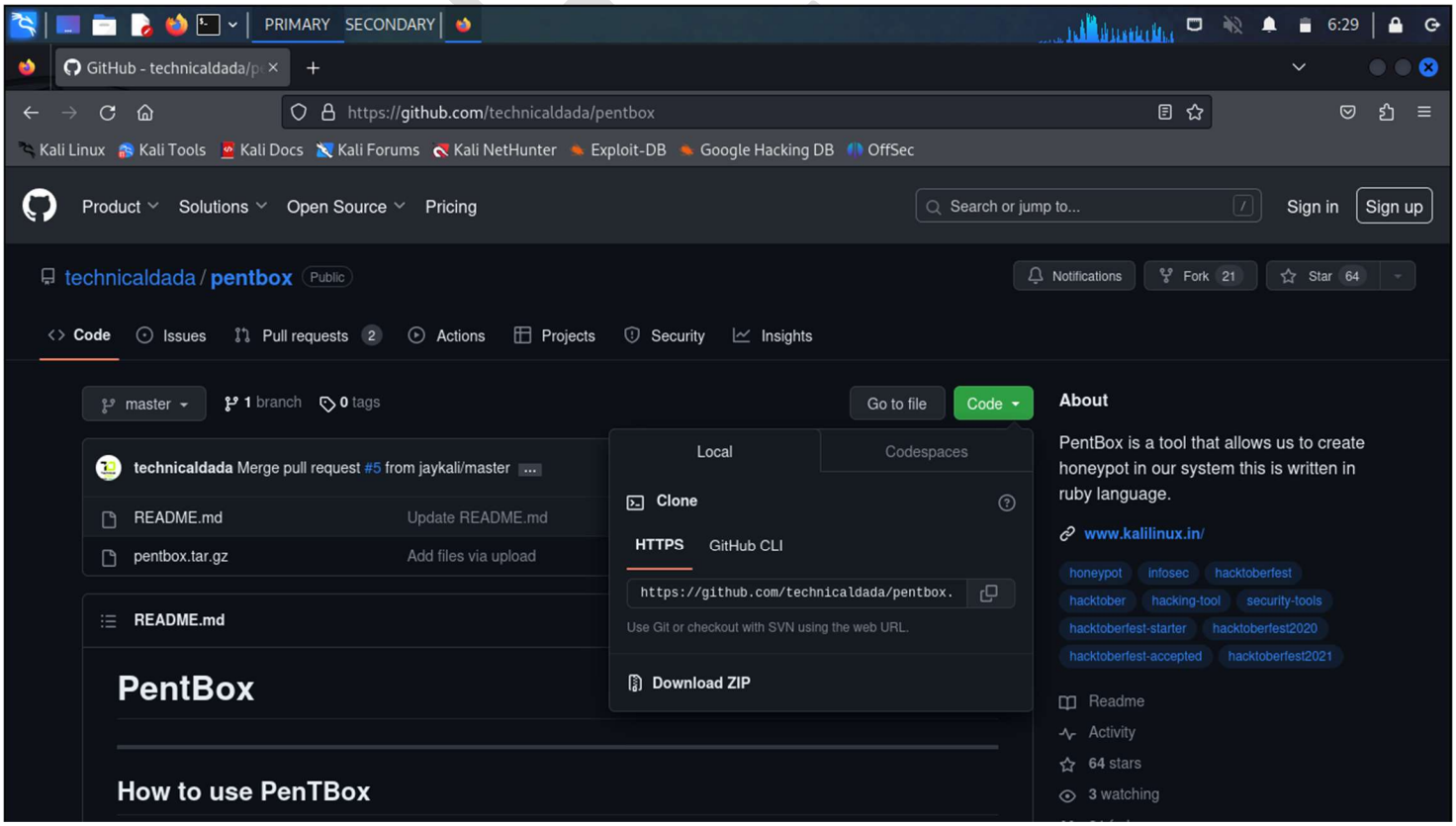
IMPLEMENTATION:

TOOL: PENTBOX

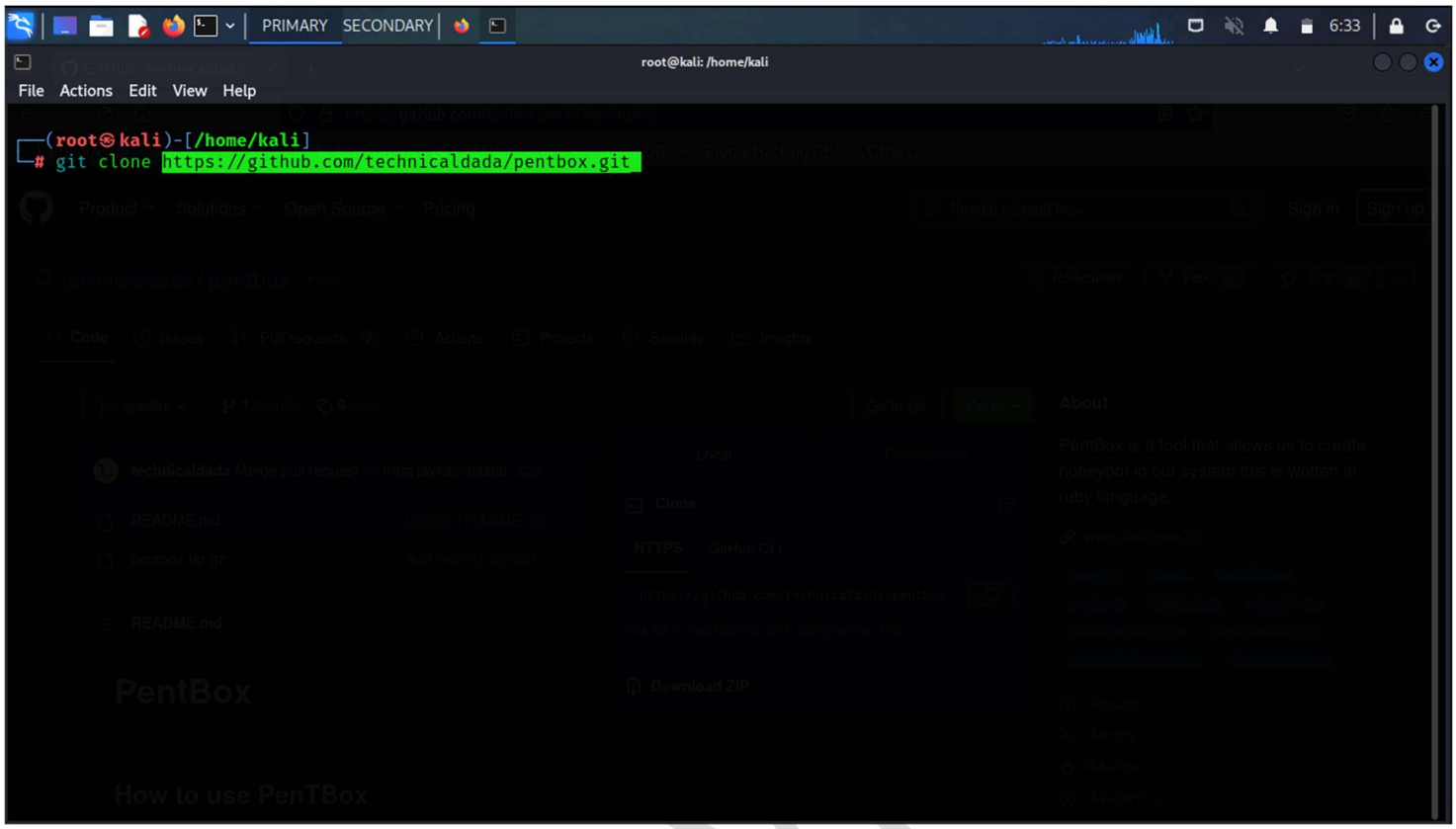
1. Search for the tool pentbox for installation



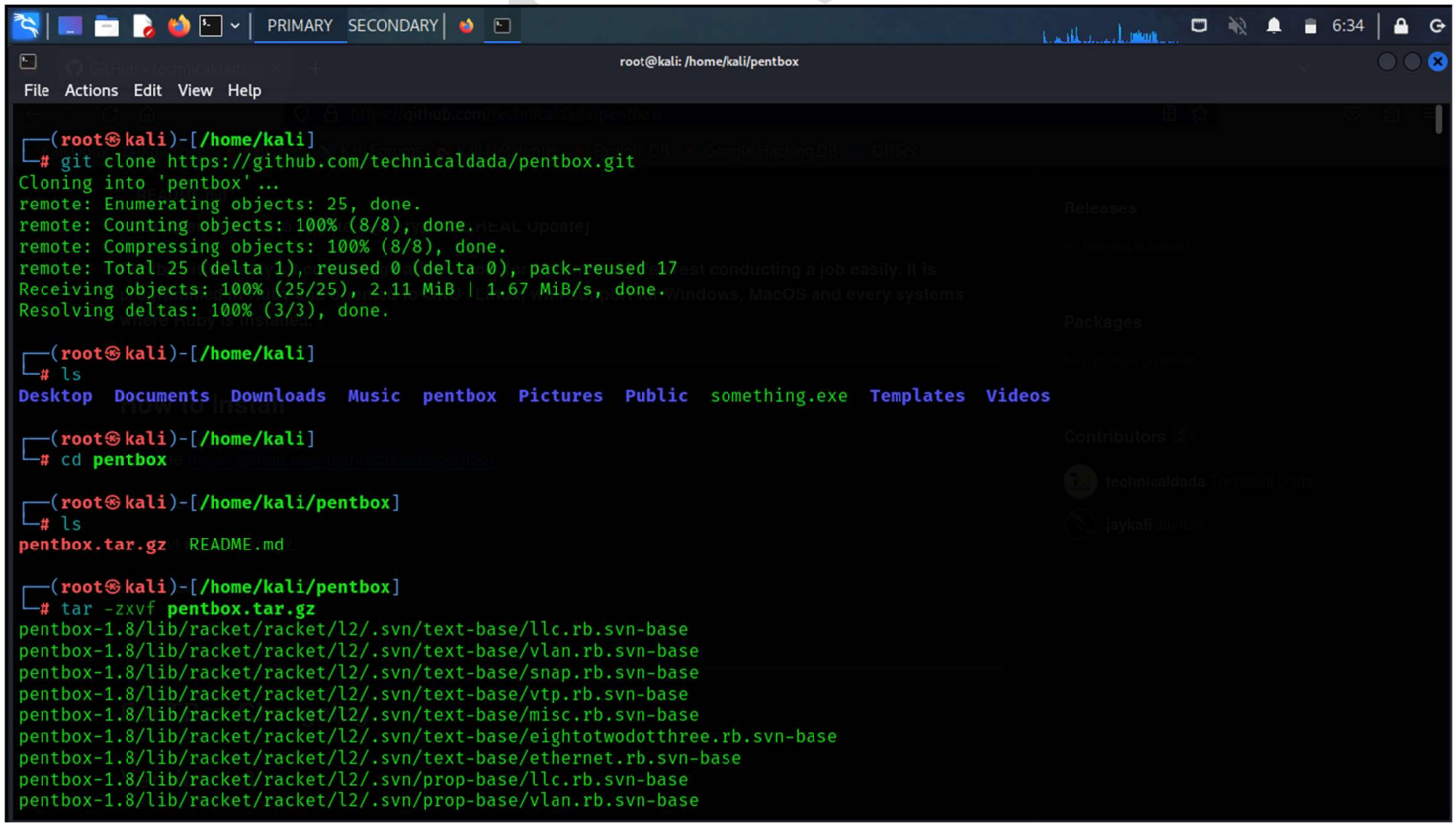
2. Open GITHUB and copy the code for the repository



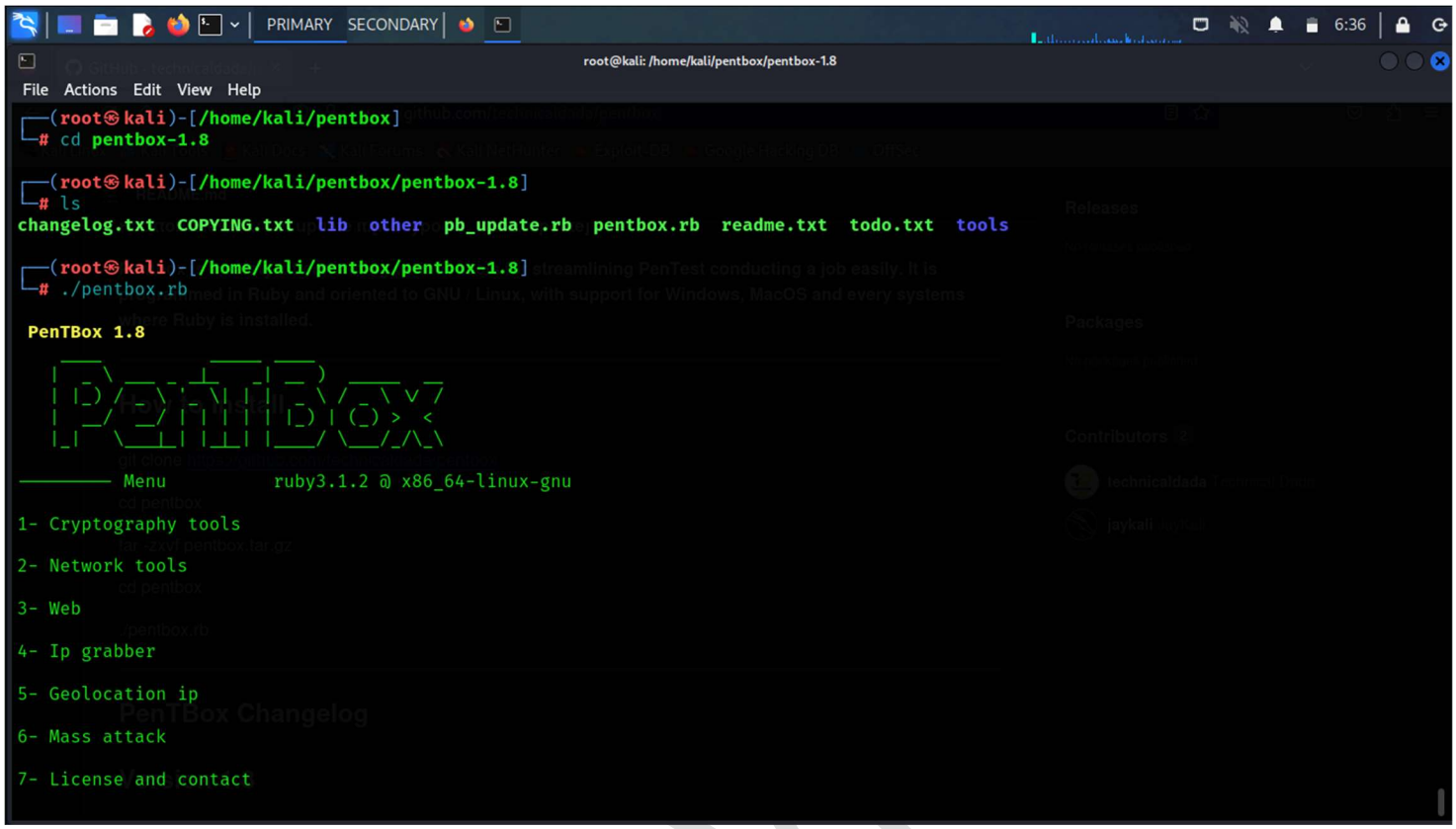
3. Open the terminal and download the tool from the repository



4. Navigate to the downloaded repository and unarchive the tool.

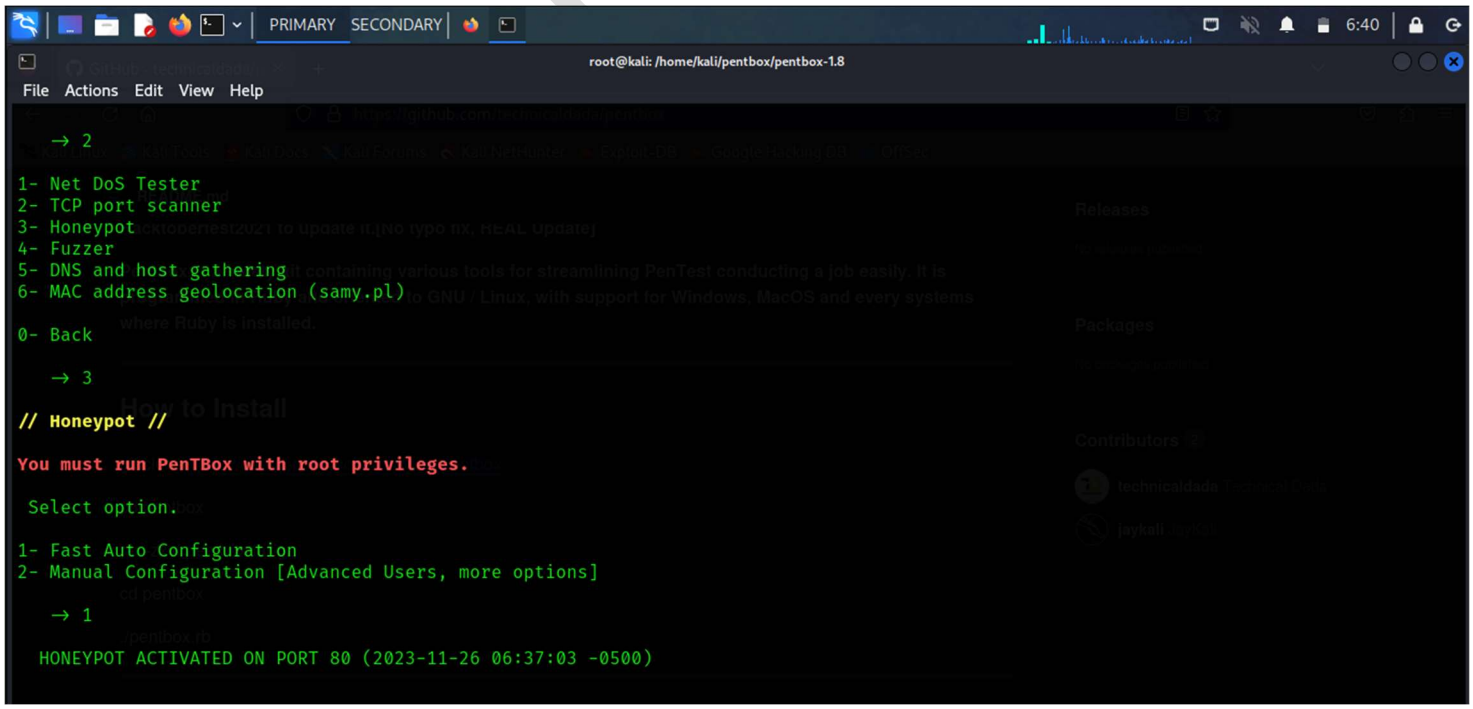


5. Now run the script named as pentbox.rb [RUBY SCRIPT].

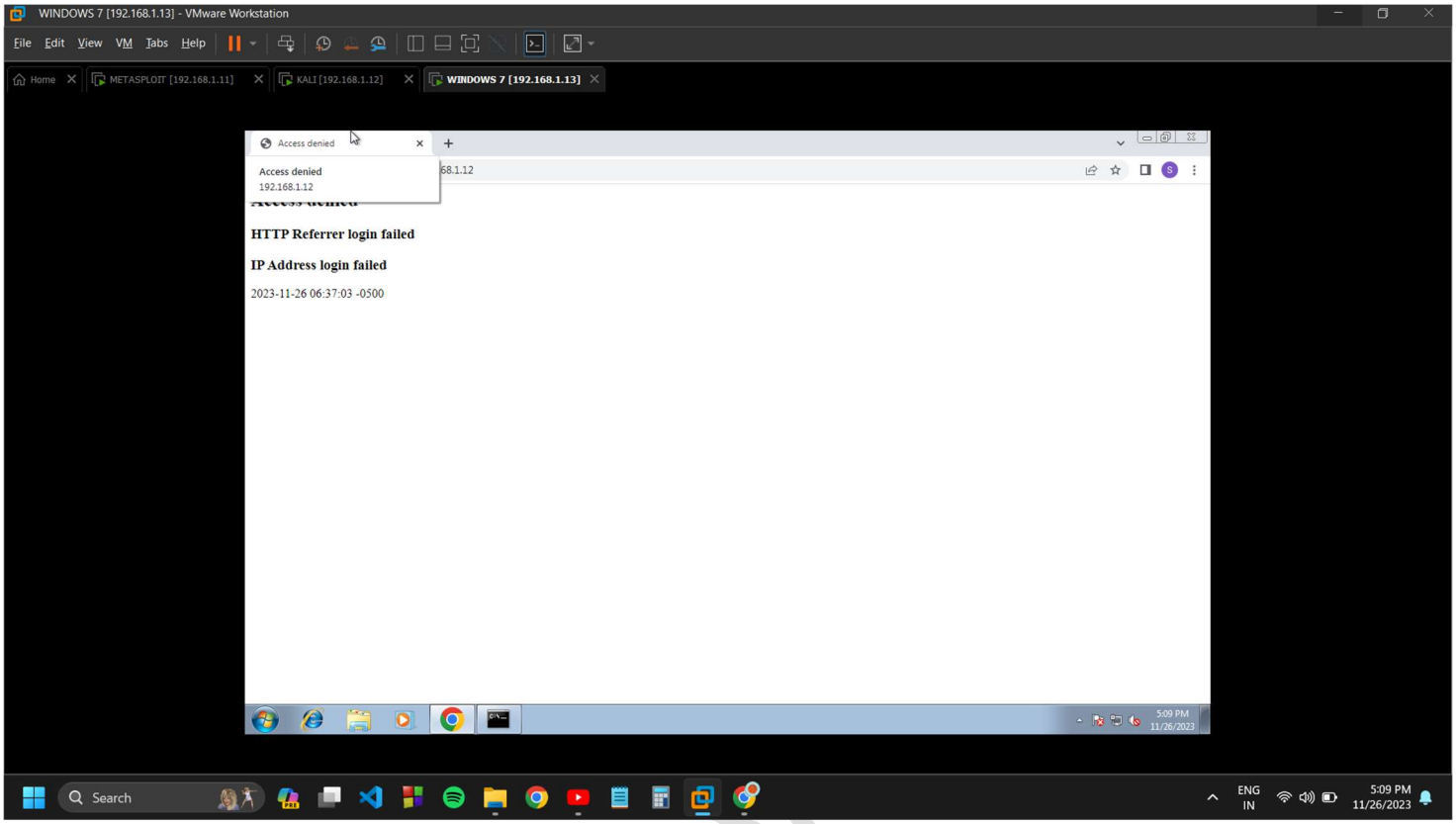


[Fast Auto Configuration]

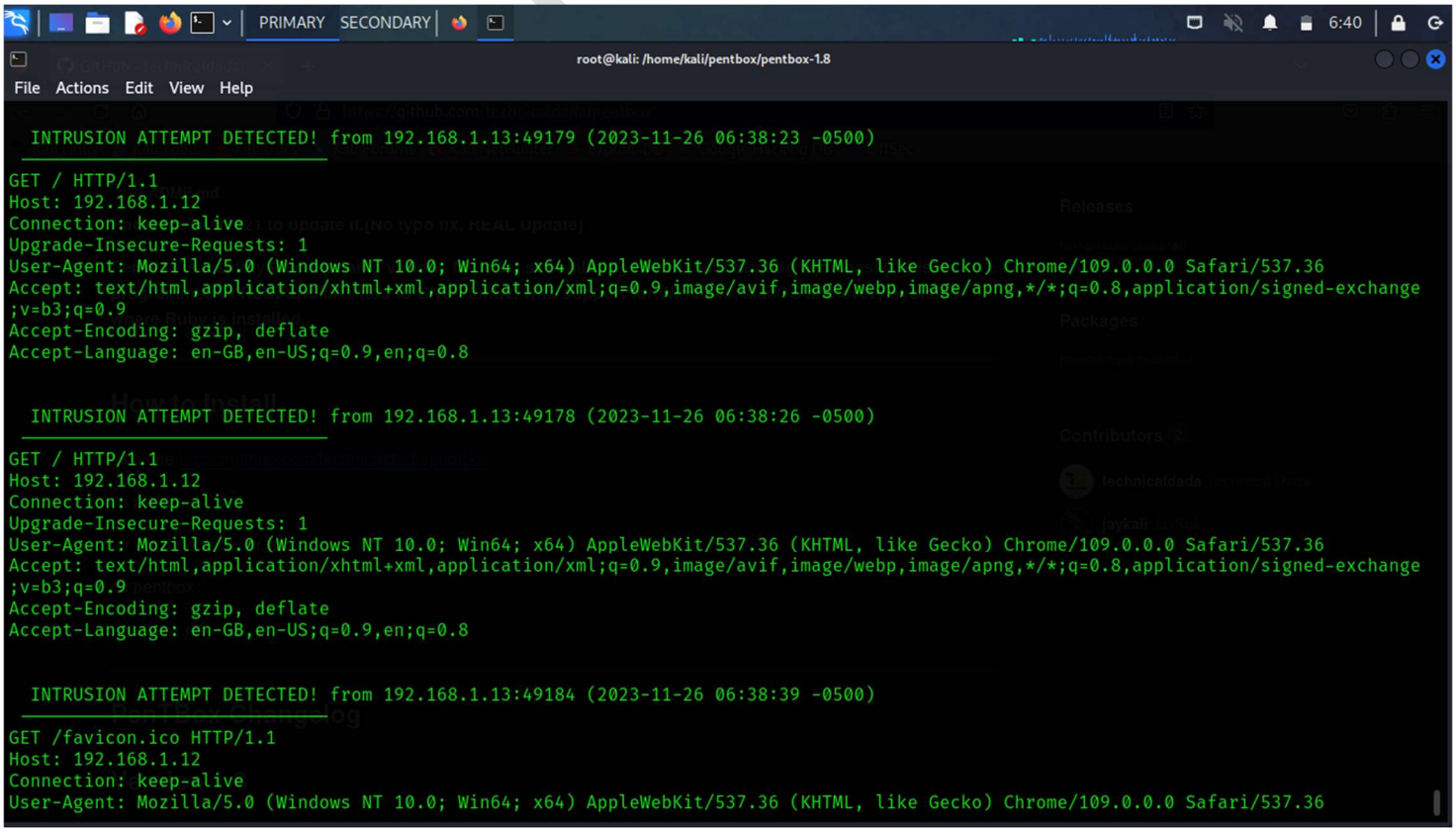
6. Select Network tools from the menu and then select Honeypot and run Fast Auto Configuration.



7. Now try to access the machine in ehich the honey pot has been set from another machine.

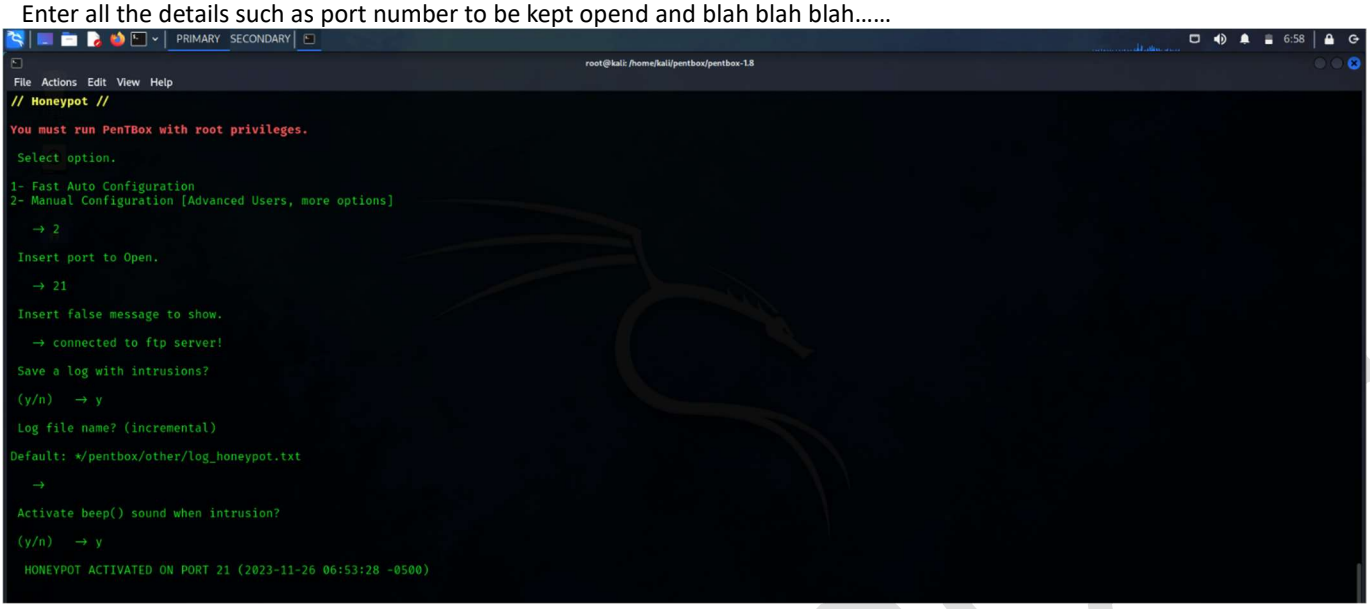


8. Now return to the machine in which the honey pot has been set and observe the intrusions.

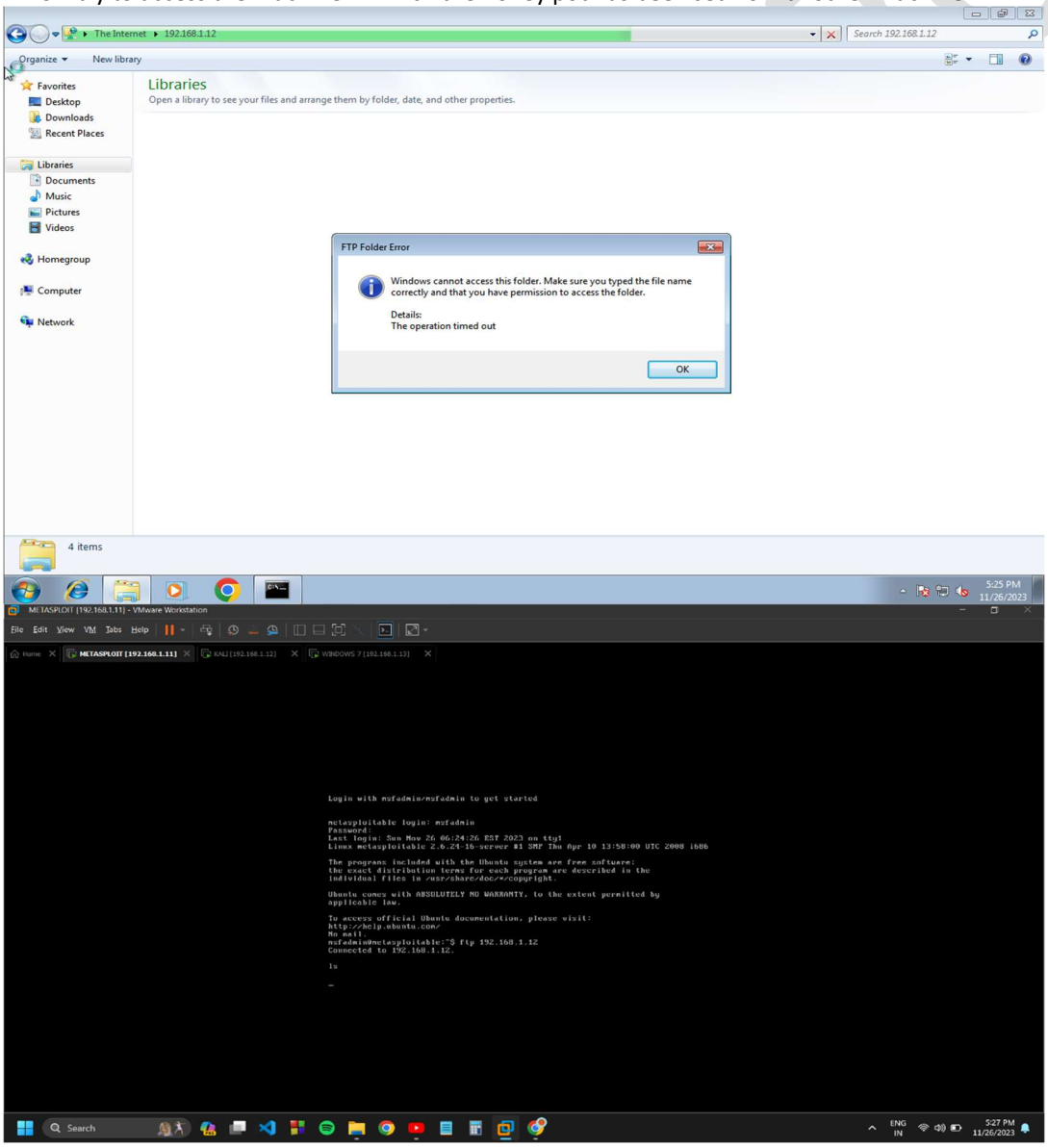


[Manual Configuration]

6.Select Network tools from the menu and then select Honeypot and run Manual Configuration.
Enter all the details such as port number to be kept opend and blah blah blah……



7.Now try to access the machine in which the honey pot has been set from another machine.



8.Now return to the machine in which honey pot has been set and observe the intrusions.