

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):**

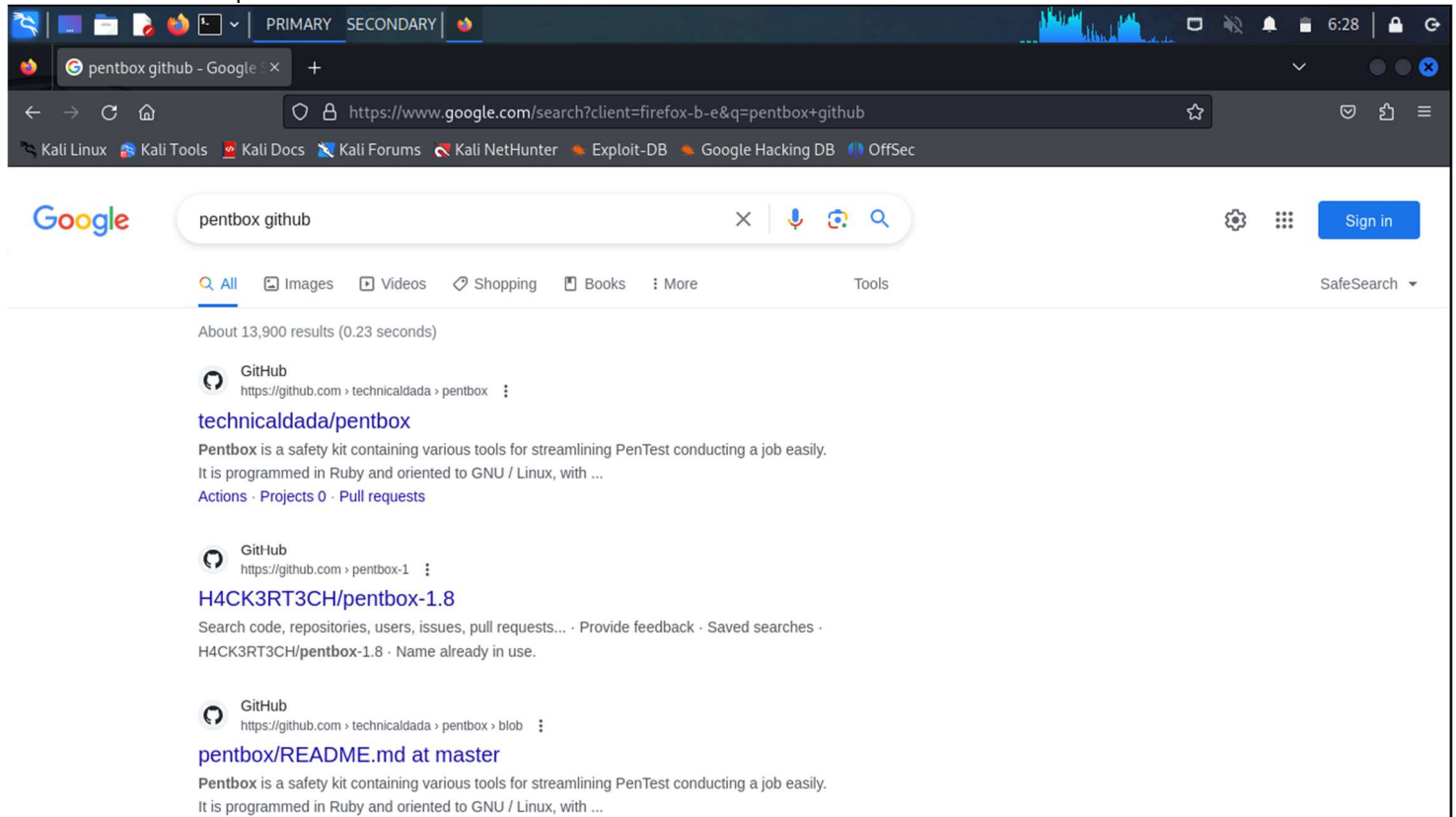
Type: High-Interaction Honeypot Framework

Description: Facilitates the deployment and management of high-interaction honeypots, supporting various honeypot technologies.

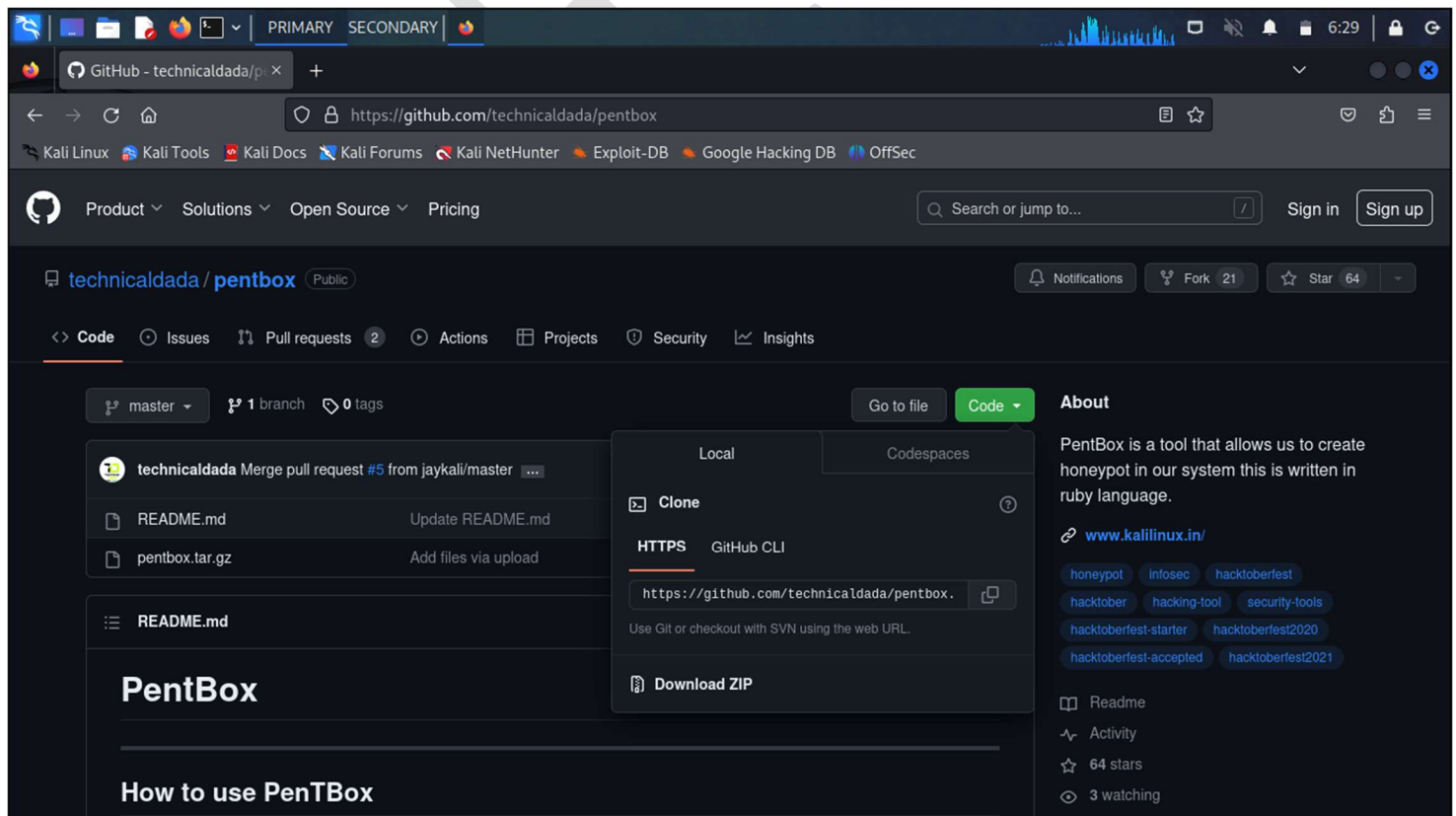
IMPLEMENTATION:

TOOL: PENTBOX

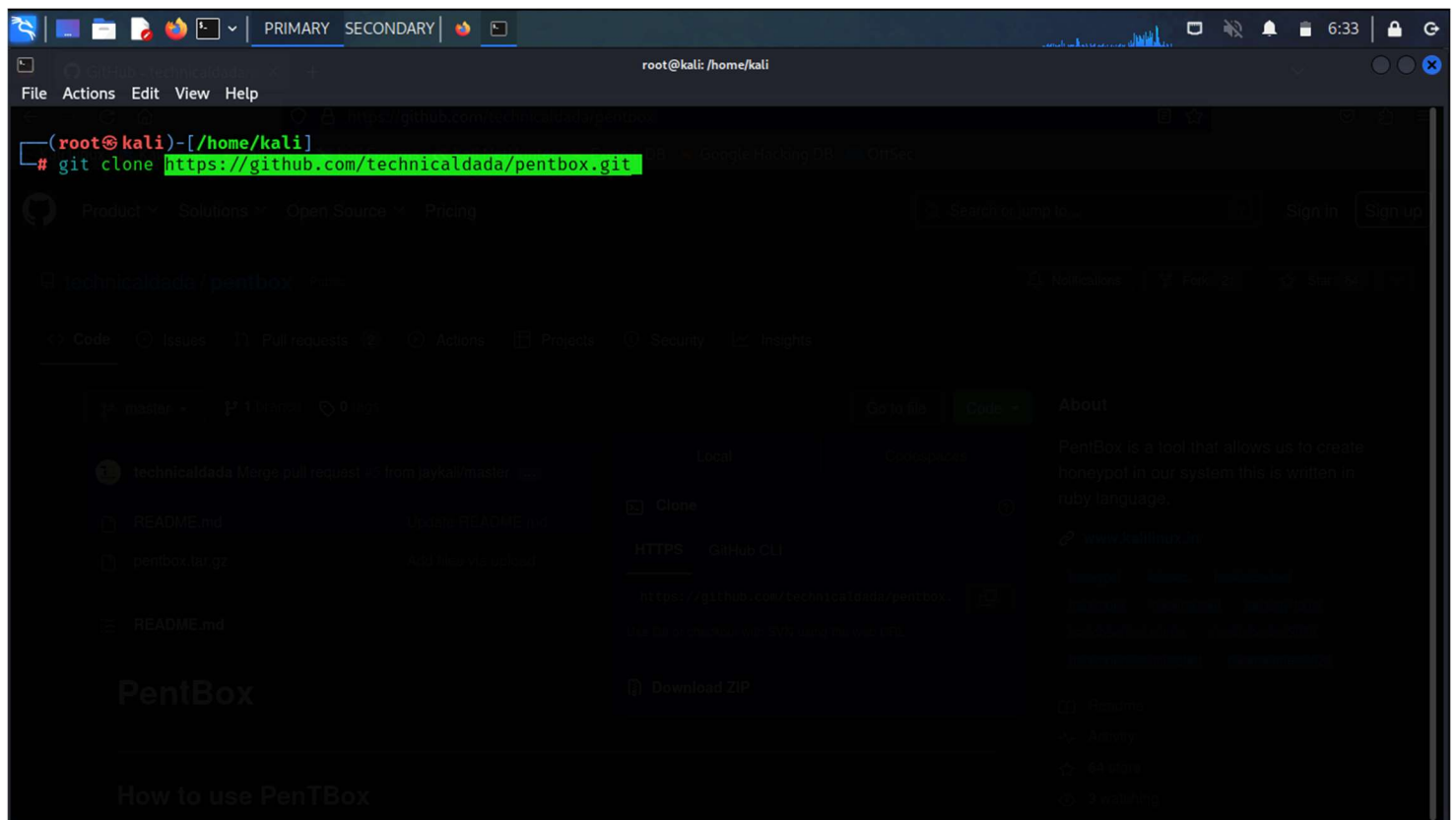
1. Search for the tool pentbox for installation



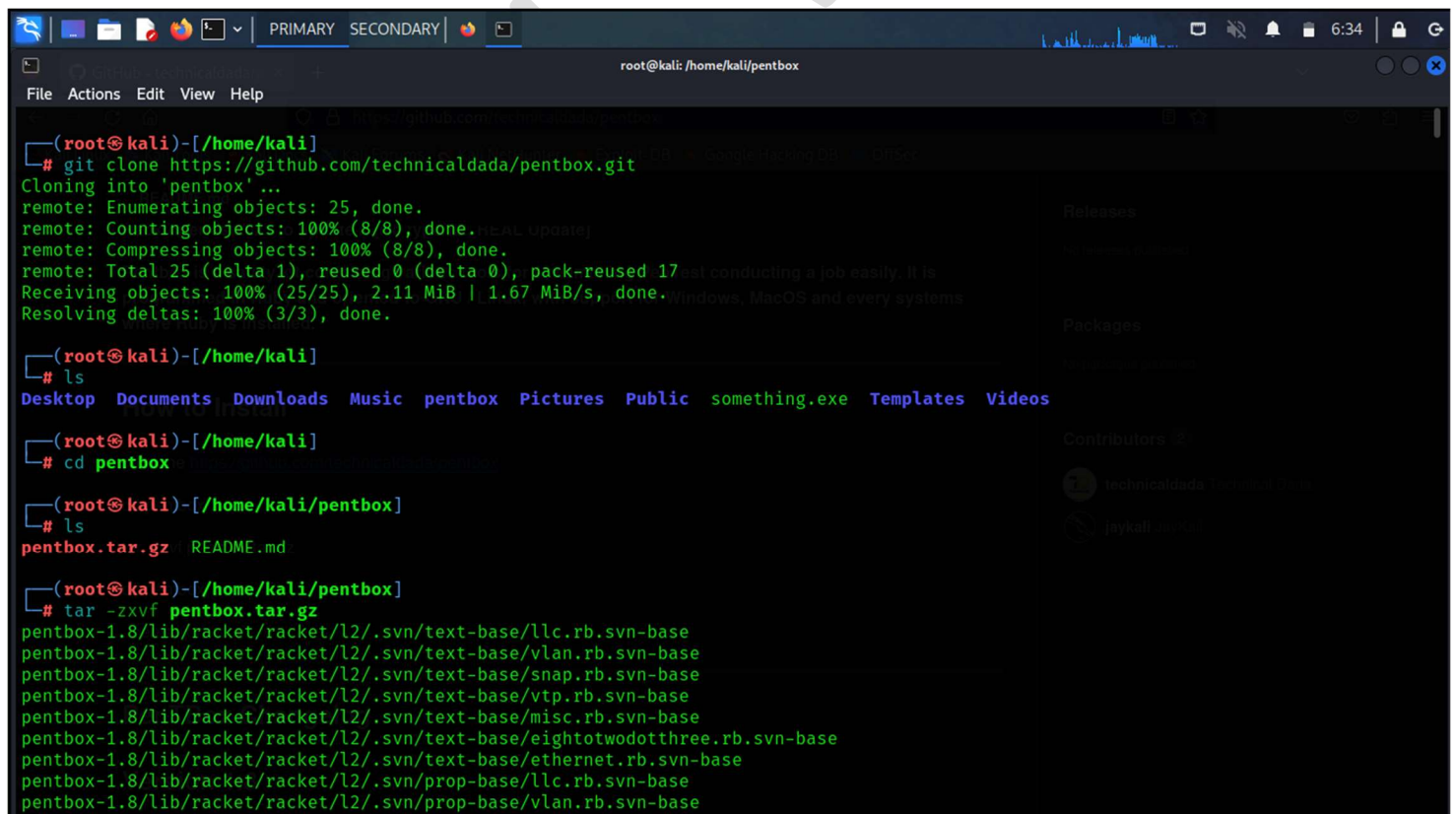
2. Open GITHUB and copy the code for the repository



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].

```

root@kali: /home/kali/pentbox/pentbox-1.8
File Actions Edit View Help
# cd pentbox-1.8
# ls
changelog.txt COPYING.txt lib other pb_update.rb pentbox.rb readme.txt todo.txt tools
# ./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
  
```

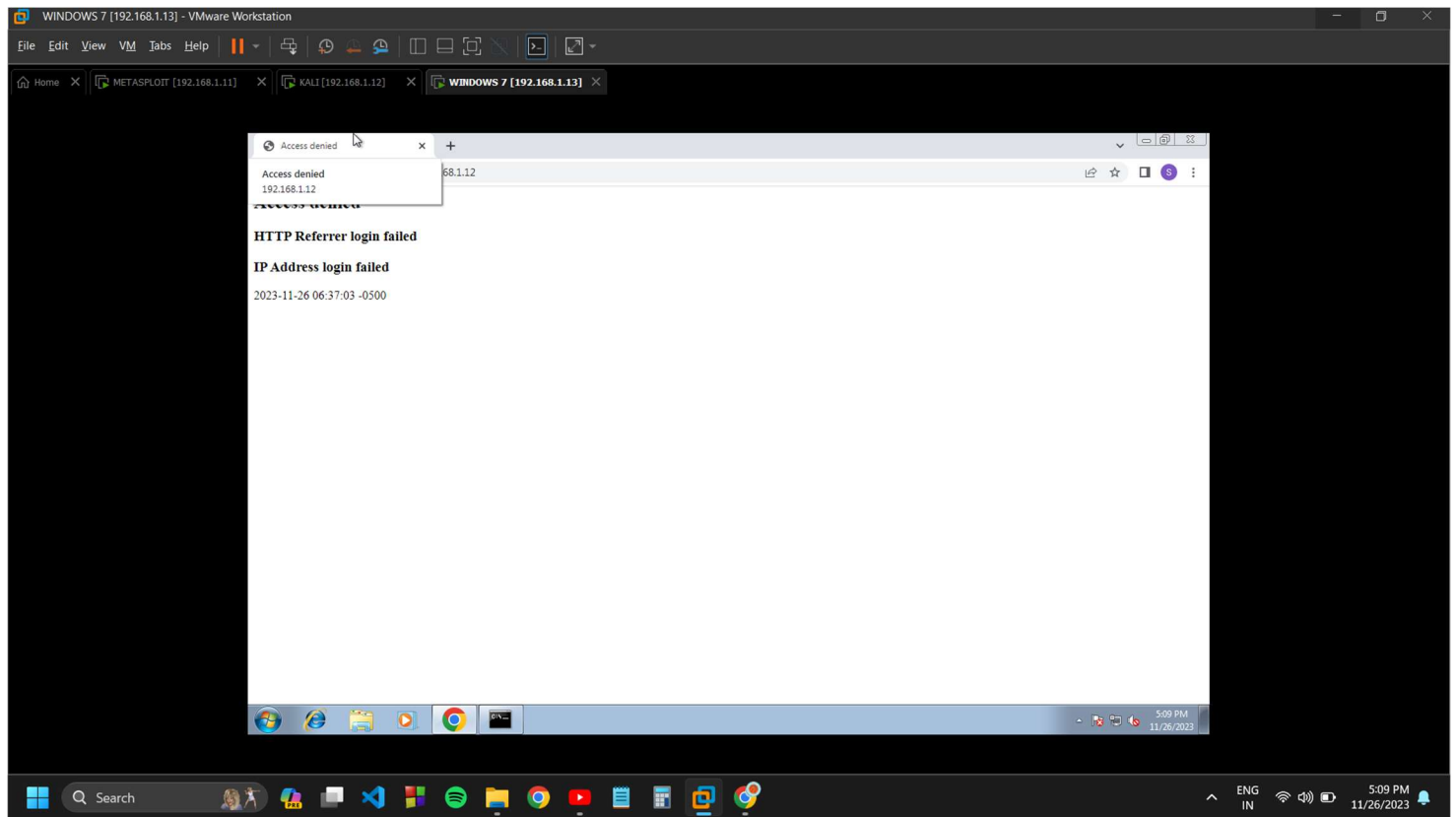
[Fast Auto Configuration]

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

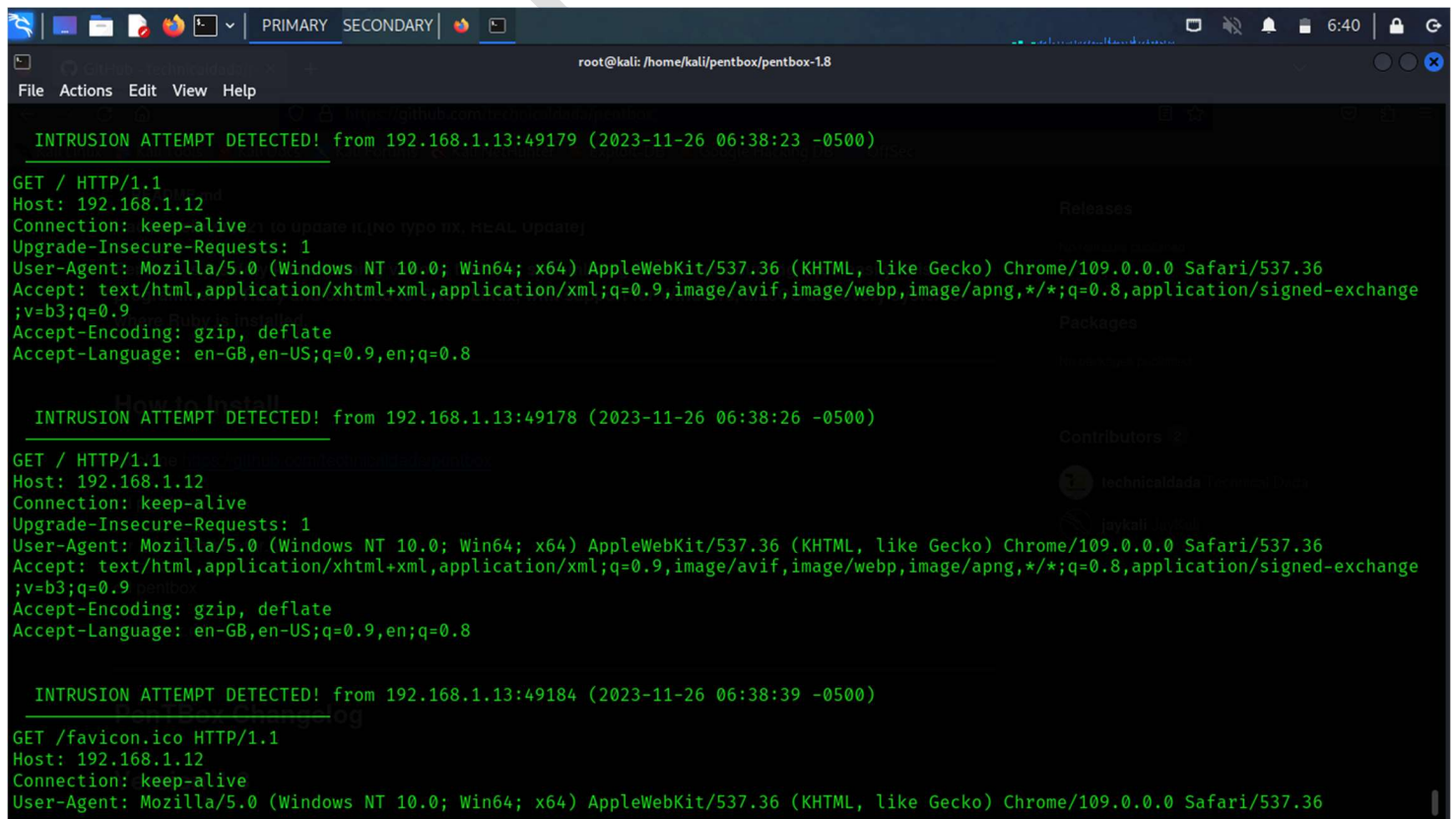
```

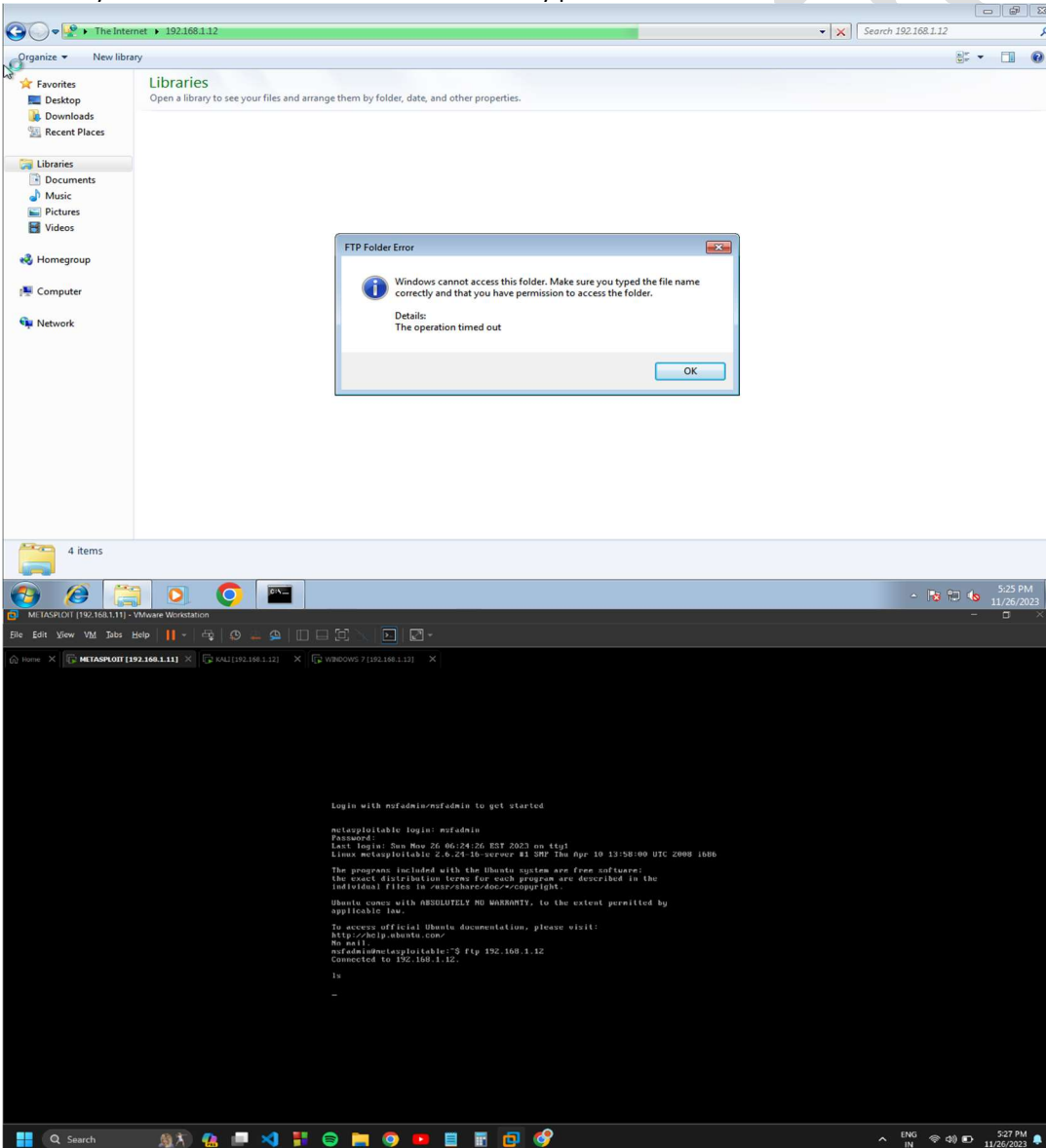
→ 2
1- Net DoS Tester
2- TCP port scanner
3- Honeypot
4- Fuzzer
5- DNS and host gathering
6- MAC address geolocation (samy.pl)
0- Back
→ 3
// Honeypot //
You must run PentBox with root privileges.
Select option.
1- Fast Auto Configuration
2- Manual Configuration [Advanced Users, more options]
→ 1
HONEYPOT ACTIVATED ON PORT 80 (2023-11-26 06:37:03 -0500)
  
```

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 the honey pot has been set and observe the intrusions.





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

```

root@kali: /home/kali/pentbox/pentbox-1.8/other
File Actions Edit View Help
(y/n) → y
HONEYPOT ACTIVATED ON PORT 21 (2023-11-26 06:53:28 -0500)

INTRUSION ATTEMPT DETECTED! from 192.168.1.13:49230 (2023-11-26 06:54:16 -0500)

INTRUSION ATTEMPT DETECTED! from 192.168.1.13:49231 (2023-11-26 06:54:46 -0500)

INTRUSION ATTEMPT DETECTED! from 192.168.1.13:49241 (2023-11-26 06:55:18 -0500)

INTRUSION ATTEMPT DETECTED! from 192.168.1.11:33397 (2023-11-26 06:56:31 -0500)
^C
[*] EXITING ...

(root@kali)-[/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)-[/home/kali/pentbox/pentbox-1.8]
# cd ..

(root@kali)-[/home/kali/pentbox]
# ls
pentbox-1.8 pentbox.tar.gz README.md

(root@kali)-[/home/kali/pentbox]
# ls /home/kali/pentbox/pentbox-1.8/other/log

root@kali: /home/kali/pentbox/pentbox-1.8/other
File Actions Edit View Help

(root@kali)-[/home/kali/pentbox]
# ls
pentbox-1.8 pentbox.tar.gz README.md

(root@kali)-[/home/kali/pentbox]
# cd /home/kali/pentbox/pentbox-1.8/other/log

(root@kali)-[/home/./pentbox/pentbox-1.8/other/log]
# ls

(root@kali)-[/home/./pentbox/pentbox-1.8/other/log]
# cd ..

(root@kali)-[/home/kali/pentbox/pentbox-1.8/other]
# ls
hosts.txt http_dirs.txt log log_honeypot.txt pentbox-wlist.txt

(root@kali)-[/home/kali/pentbox/pentbox-1.8/other]
# cat log_honeypot.txt
##### PenTBox Honeypot log

HONEYPOT ACTIVATED ON PORT 21 (2023-11-26 06:53:28 -0500)

INTRUSION ATTEMPT DETECTED! from 192.168.1.13:49230 (2023-11-26 06:54:45 -0500)

INTRUSION ATTEMPT DETECTED! from 192.168.1.13:49231 (2023-11-26 06:55:16 -0500)

INTRUSION ATTEMPT DETECTED! from 192.168.1.13:49241 (2023-11-26 06:55:48 -0500)

(root@kali)-[/home/kali/pentbox/pentbox-1.8/other]
#

```