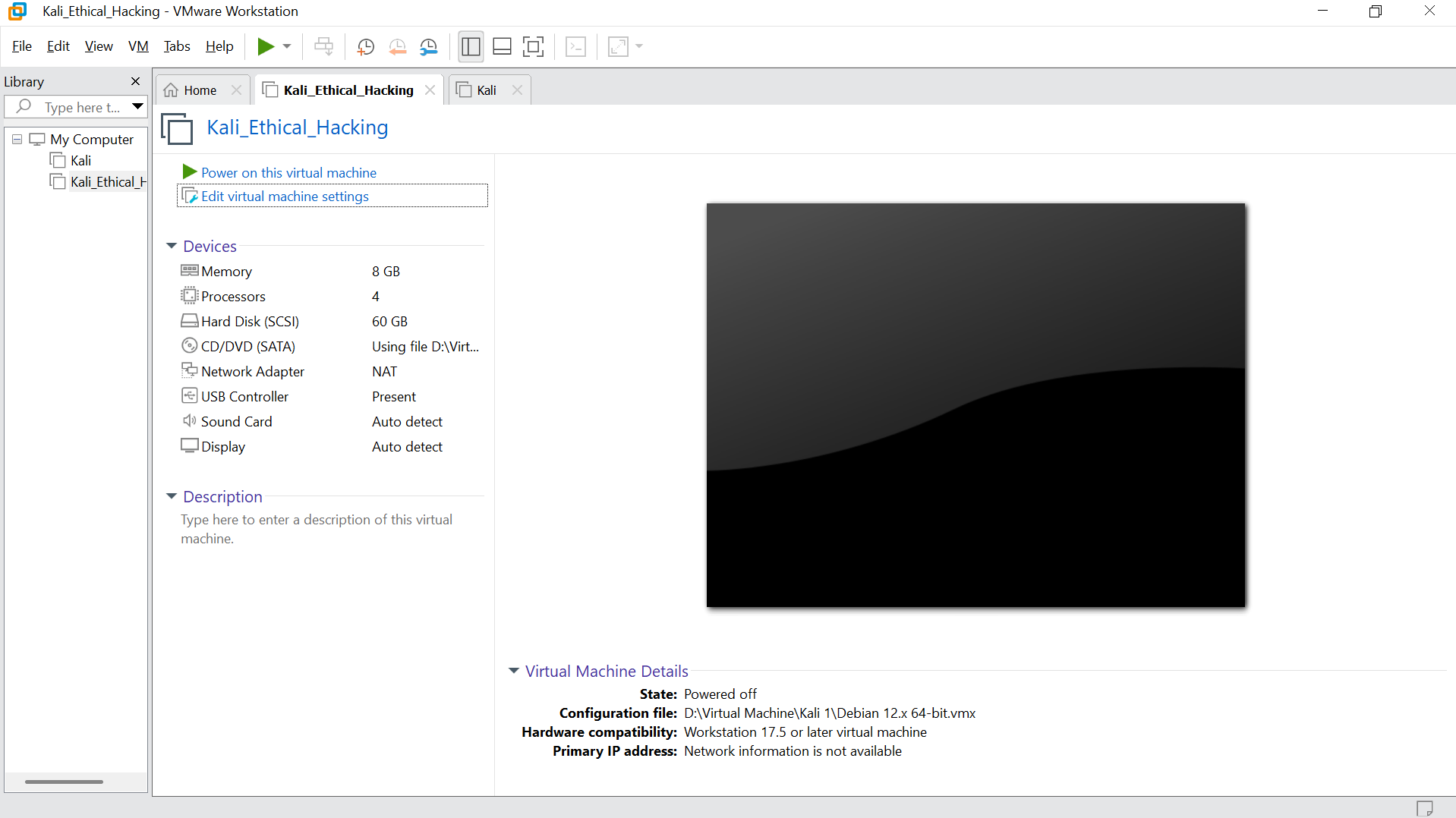
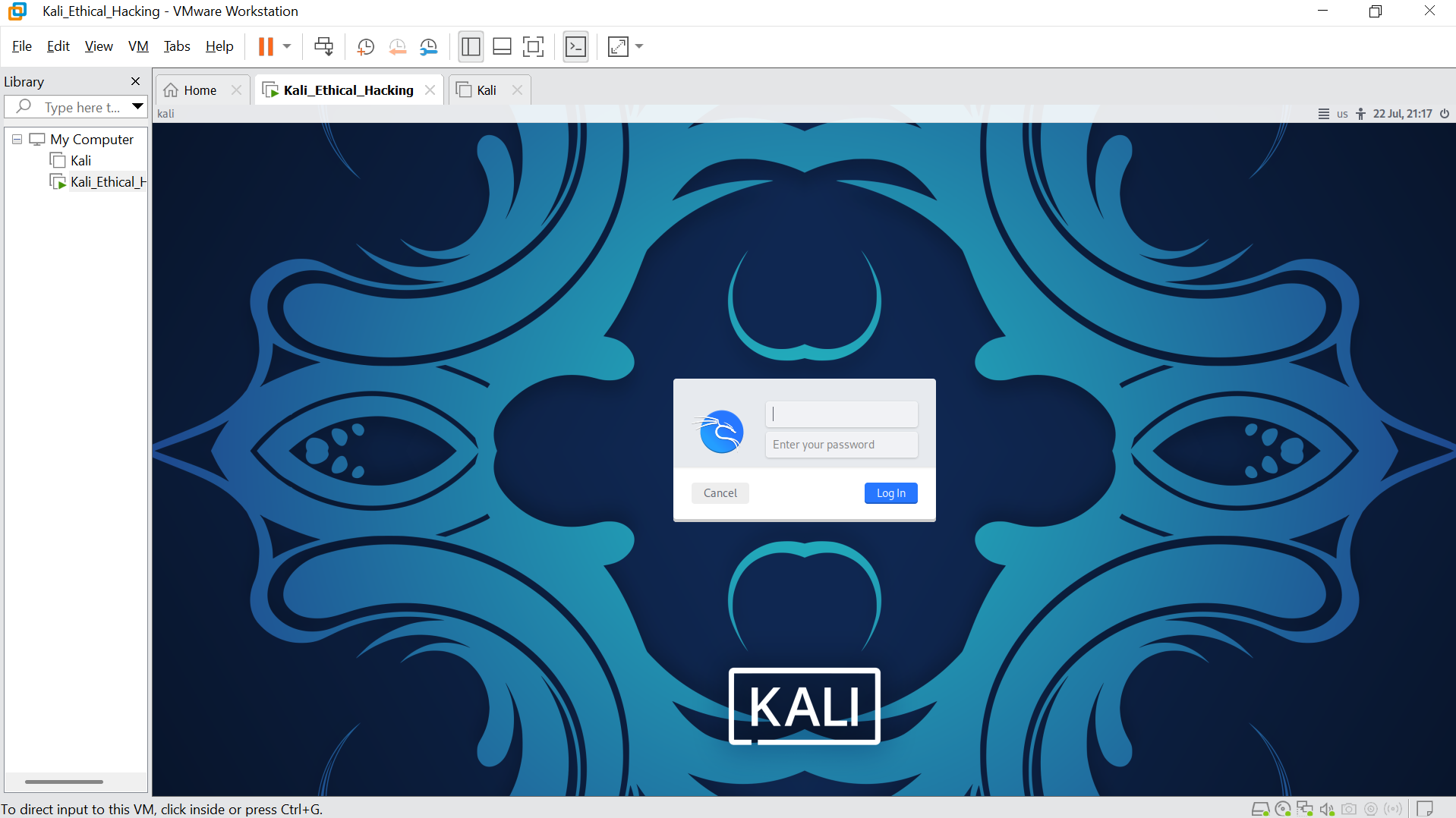
**MODULE 1-4**

**1.** Install VirtualBox or VMware. Set up a virtual machine with any Linux distribution (preferably Kali Linux).

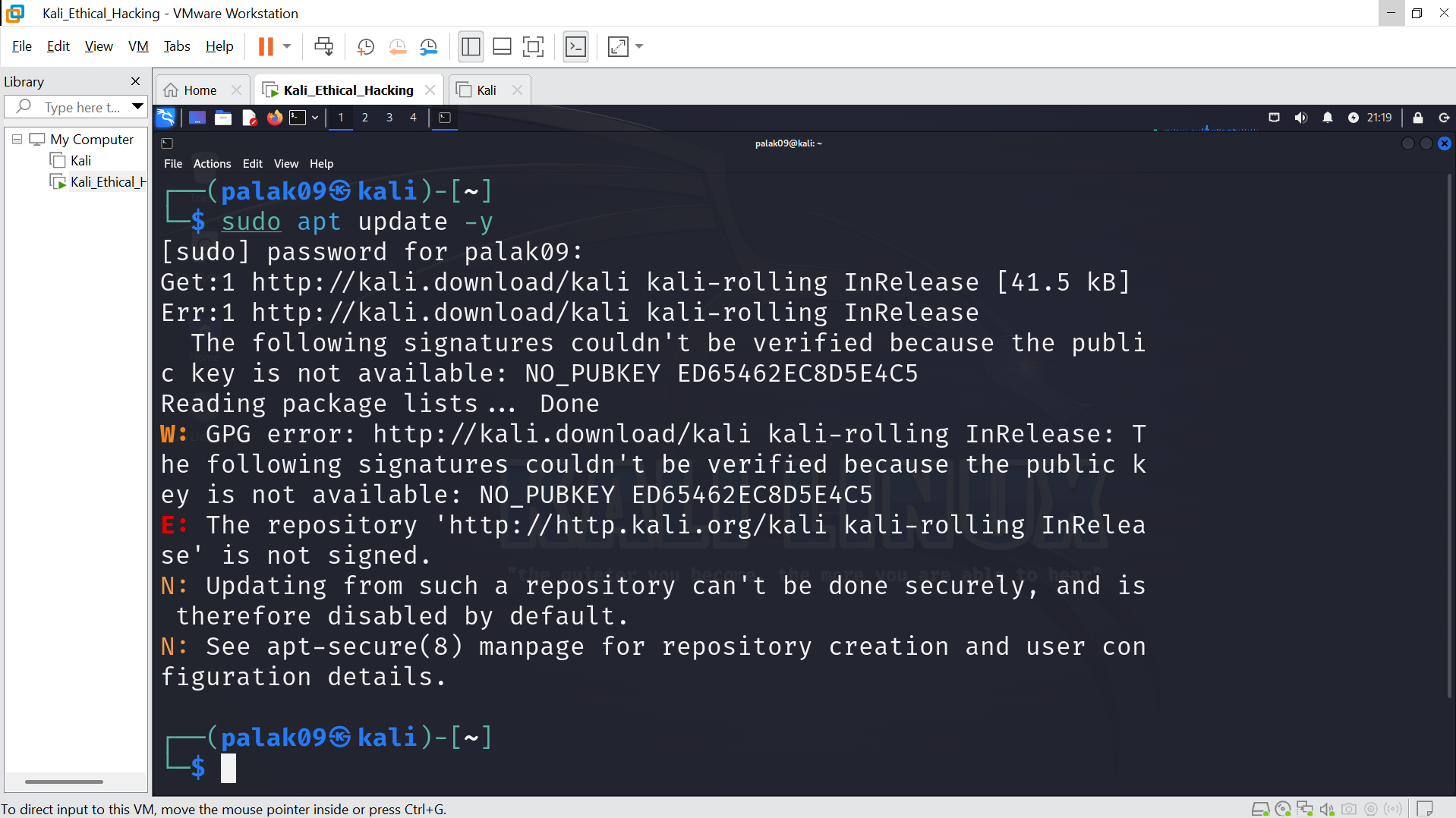
* **Screenshot Submission:** Screenshot of VirtualBox/VMware with the virtual machine running.



****

**2.**  Install Kali Linux in your virtual machine and update it..

* **Screenshot Submission:** Screenshot of the terminal showing the completion of the update.



**3.** Explore the applications menu in Kali Linux. List 5 tools and their purpose.

**Screenshot Submission:** Screenshot of the applications menu.

Step 1: Explore the Applications Menu

Click on the “Applications” menu on the top-left of the Kali Linux desktop.

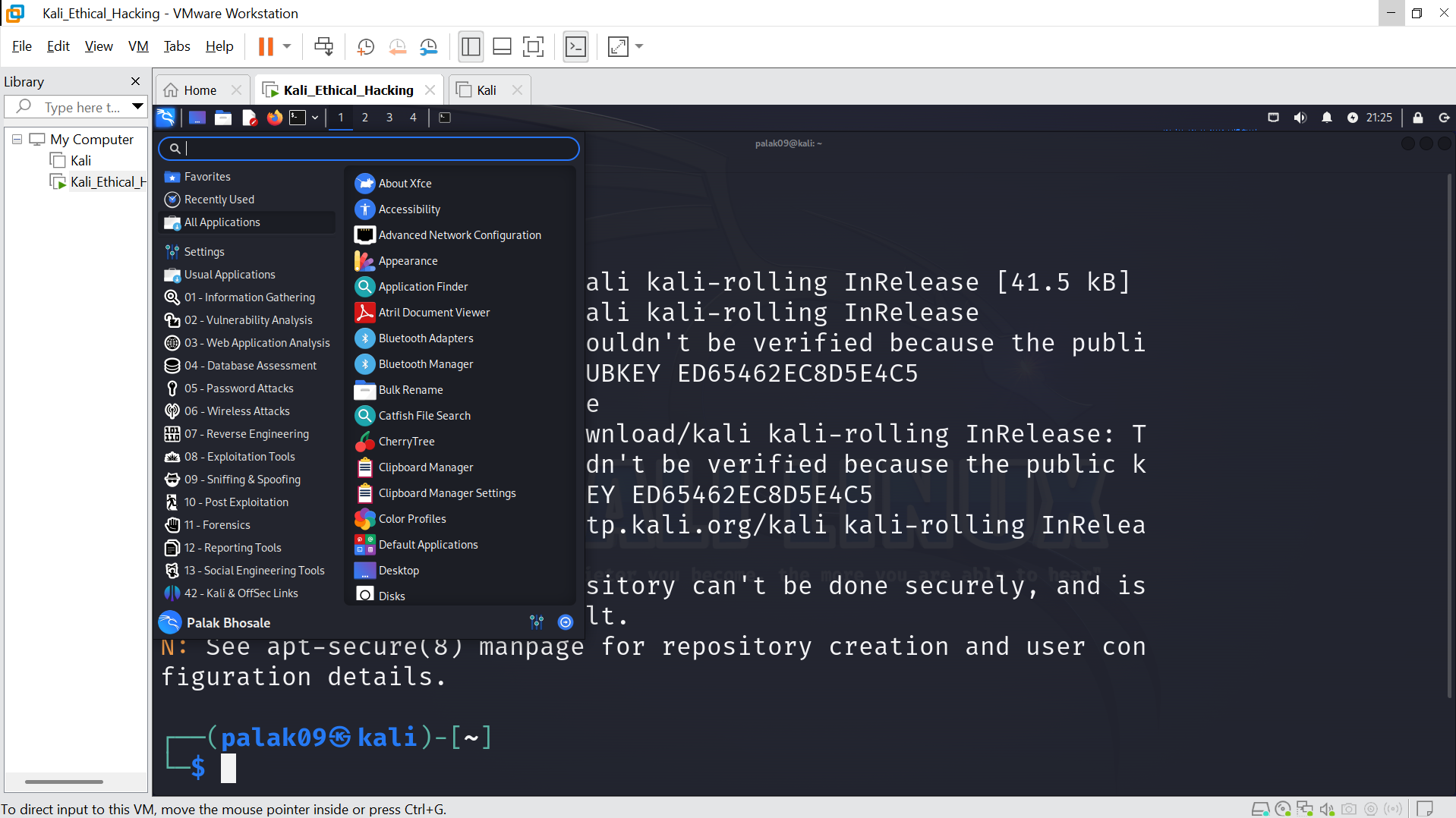
Navigate to “Kali Linux” → you’ll see different categories such as:

* Information Gathering
* Vulnerability Analysis
* Web Application Analysis
* Exploitation Tools
* Forensics, etc.

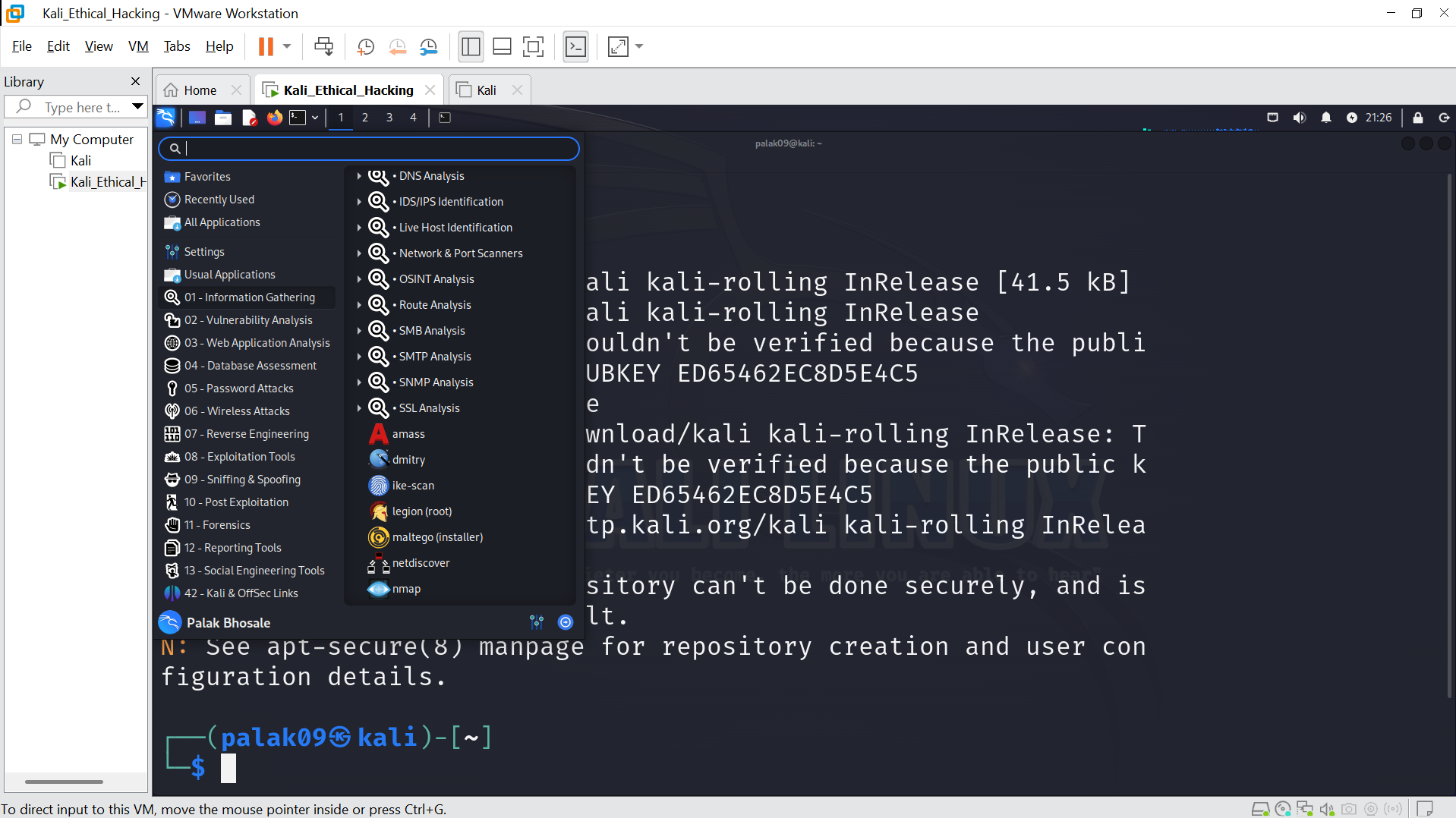
Step 2: List 5 Tools and Their Purpose

| Tool Name | Category | Purpose |
| --- | --- | --- |
| Nmap | Information Gathering | Network scanner used to discover hosts, services, and open ports on a network. |
| Wireshark | Sniffing & Spoofing | Captures and analyzes network traffic in real-time. Useful for deep protocol inspection. |
| Burp Suite | Web Application Analysis | Intercepts and manipulates web traffic for penetration testing of web applications. |
| Metasploit | Exploitation Tools | Framework for developing and executing exploit code against a remote target machine. |
| John the Ripper | Password Attacks | Password cracker used to perform dictionary attacks on encrypted passwords. |

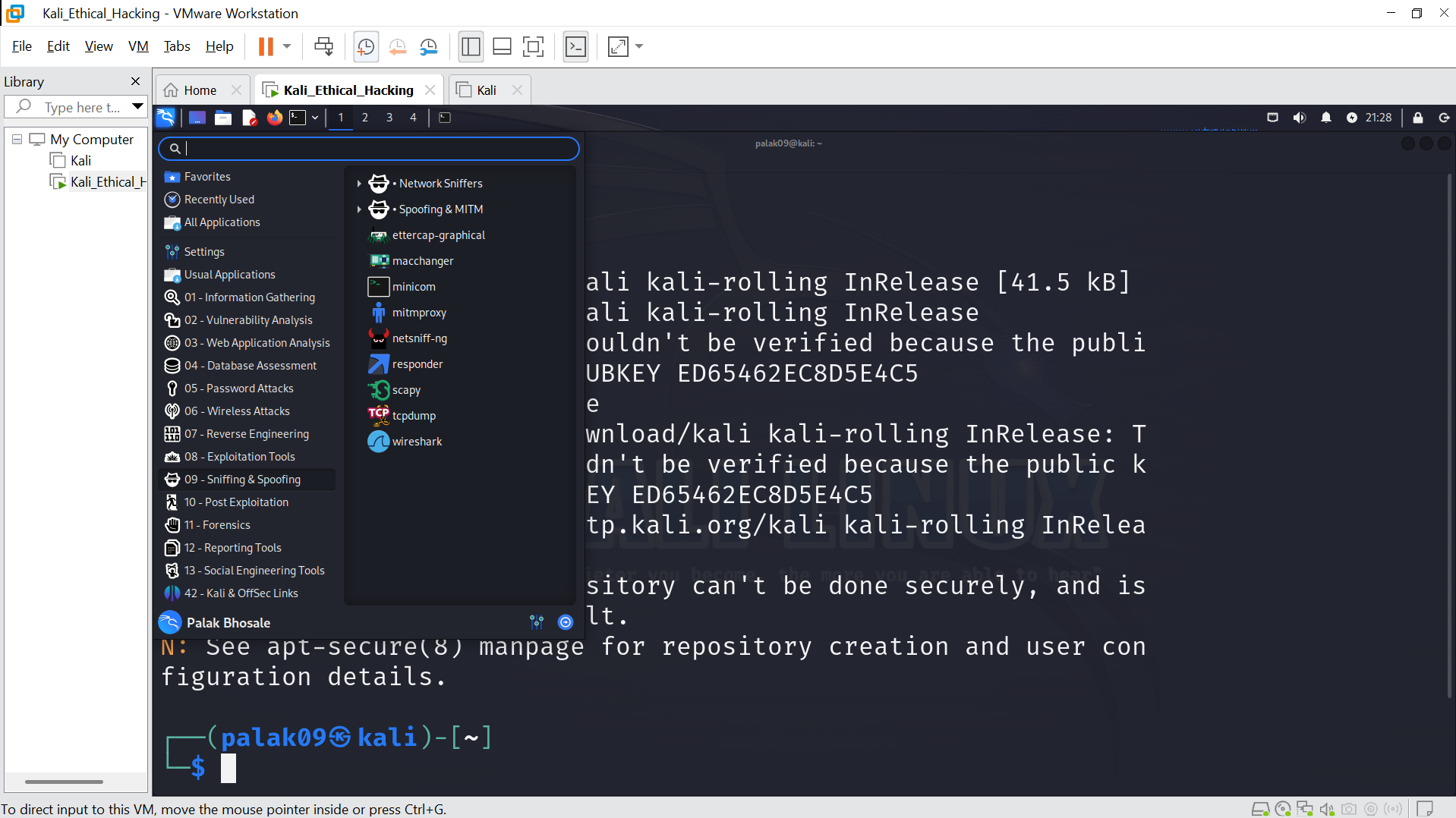
**Applications**



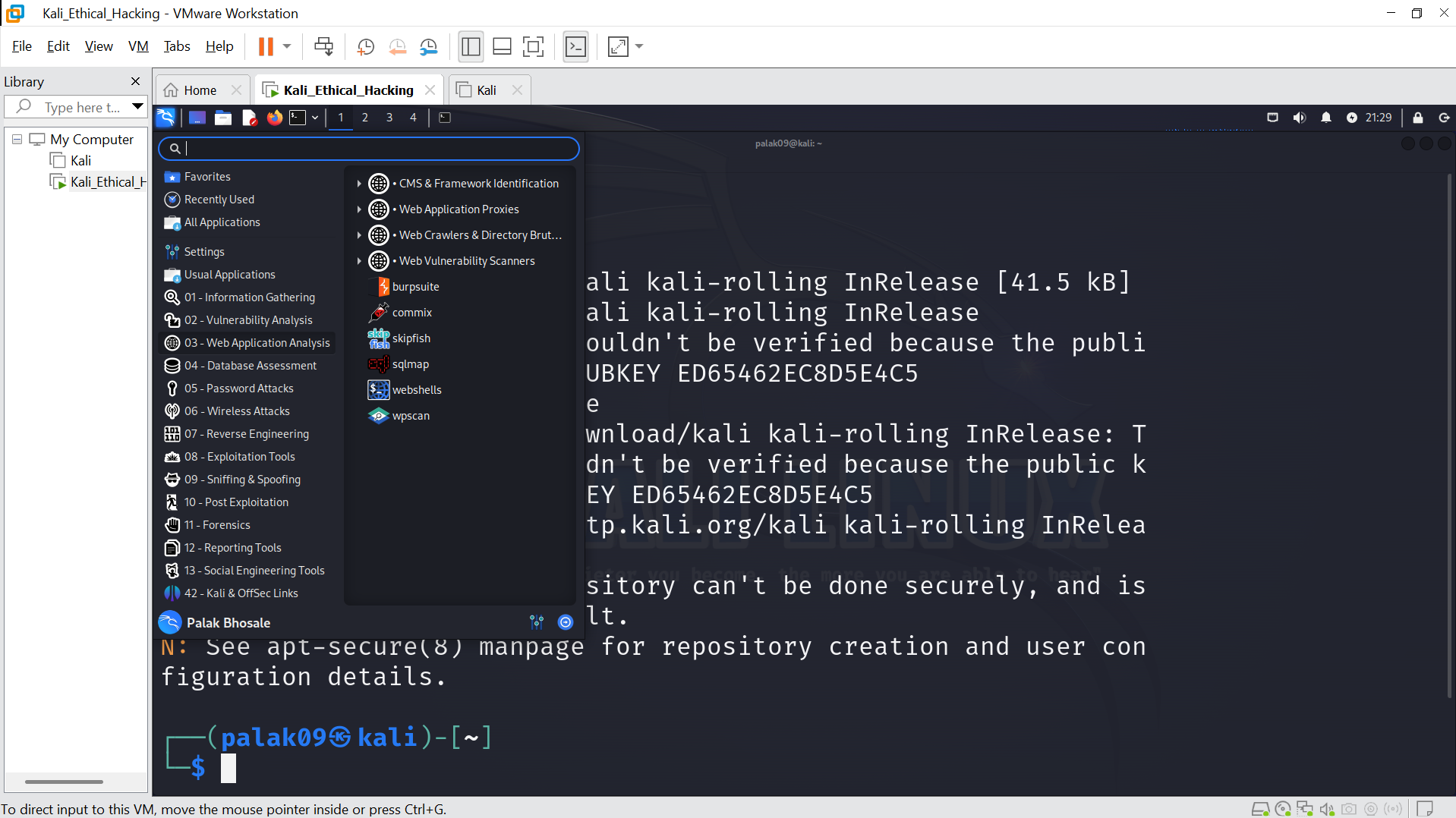
**nmap**



**Wireshark**

****

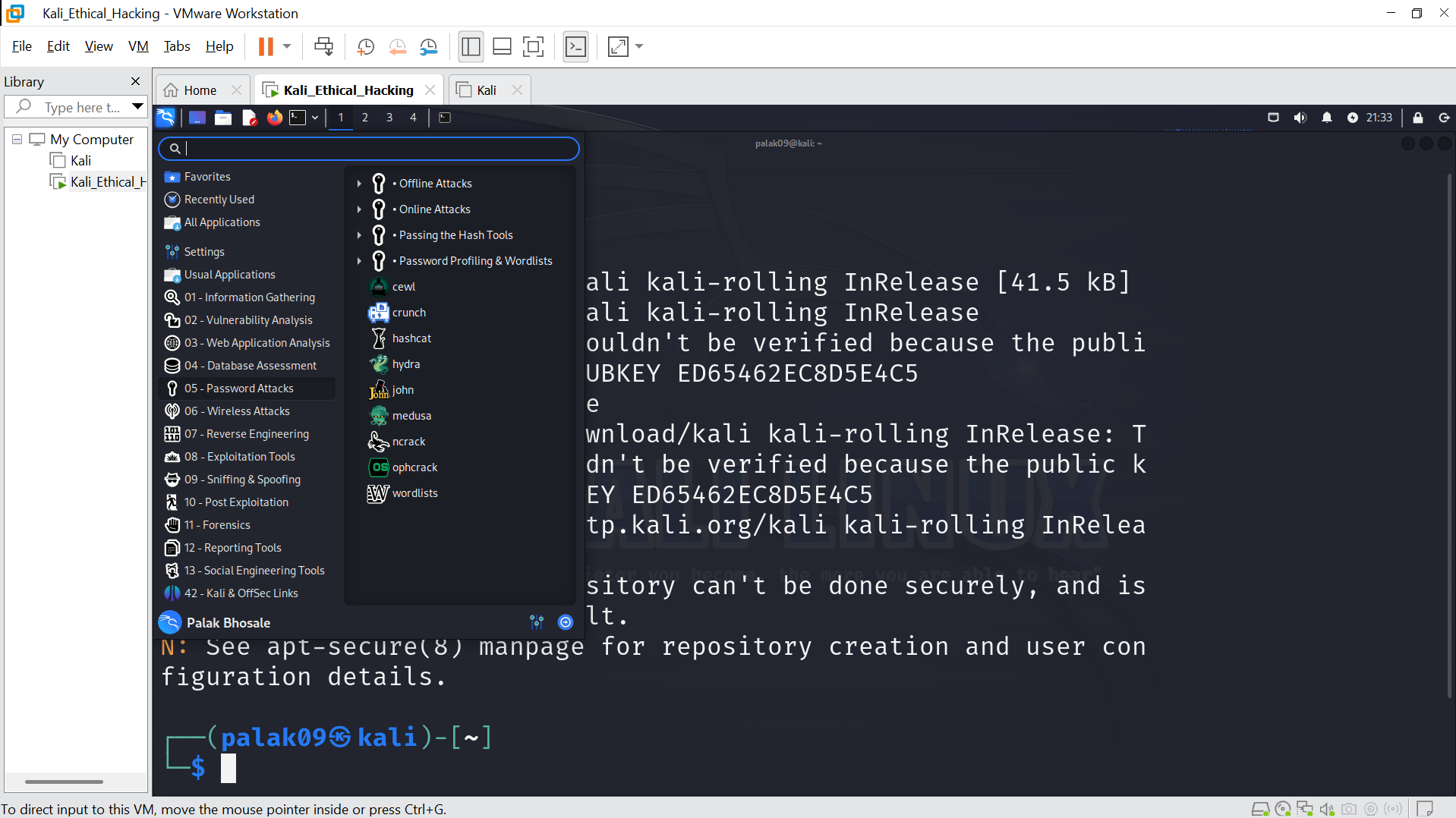
**Burp Suite**

****

**Metasploit**

****

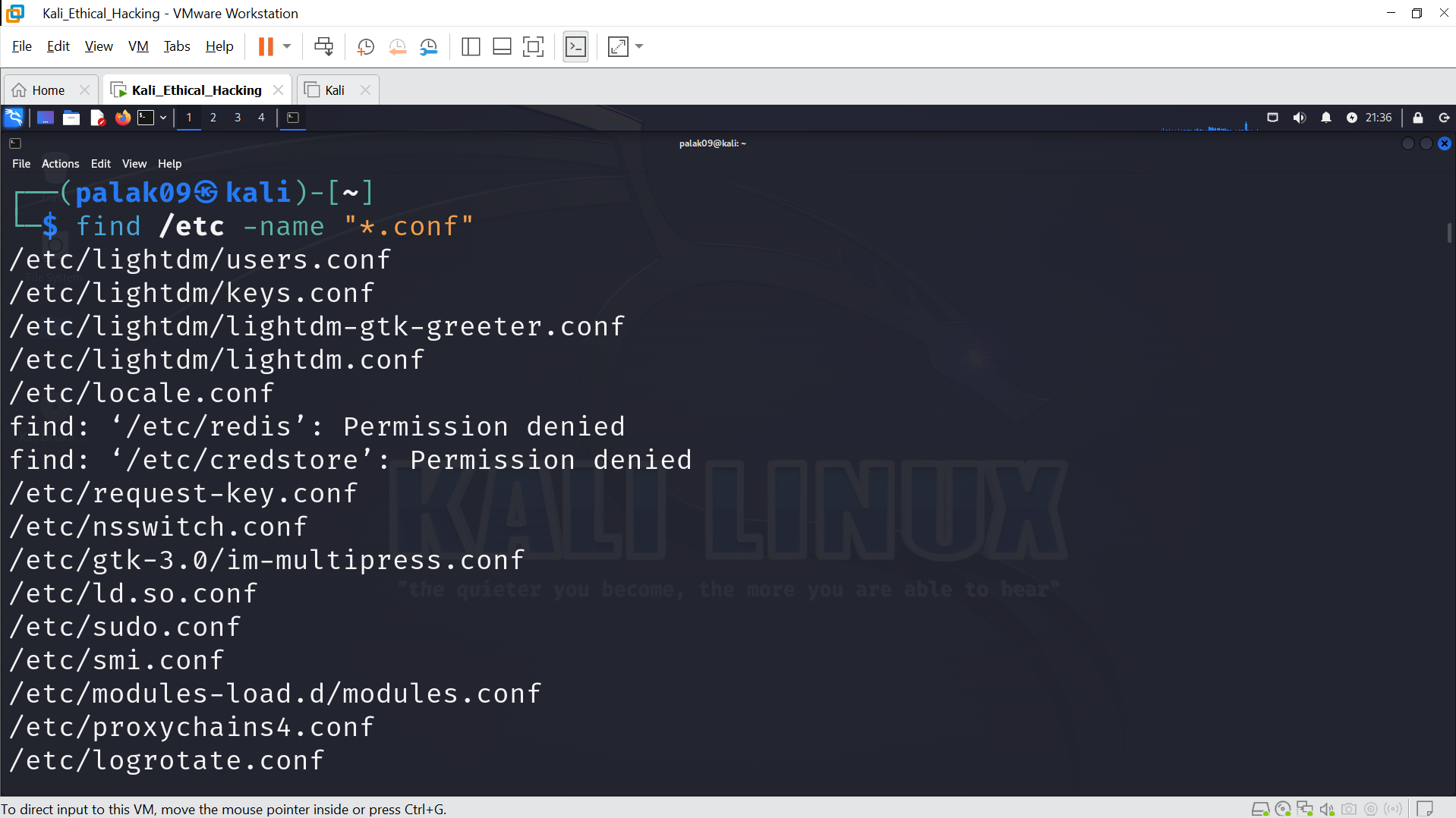
**John the Ripper**

****

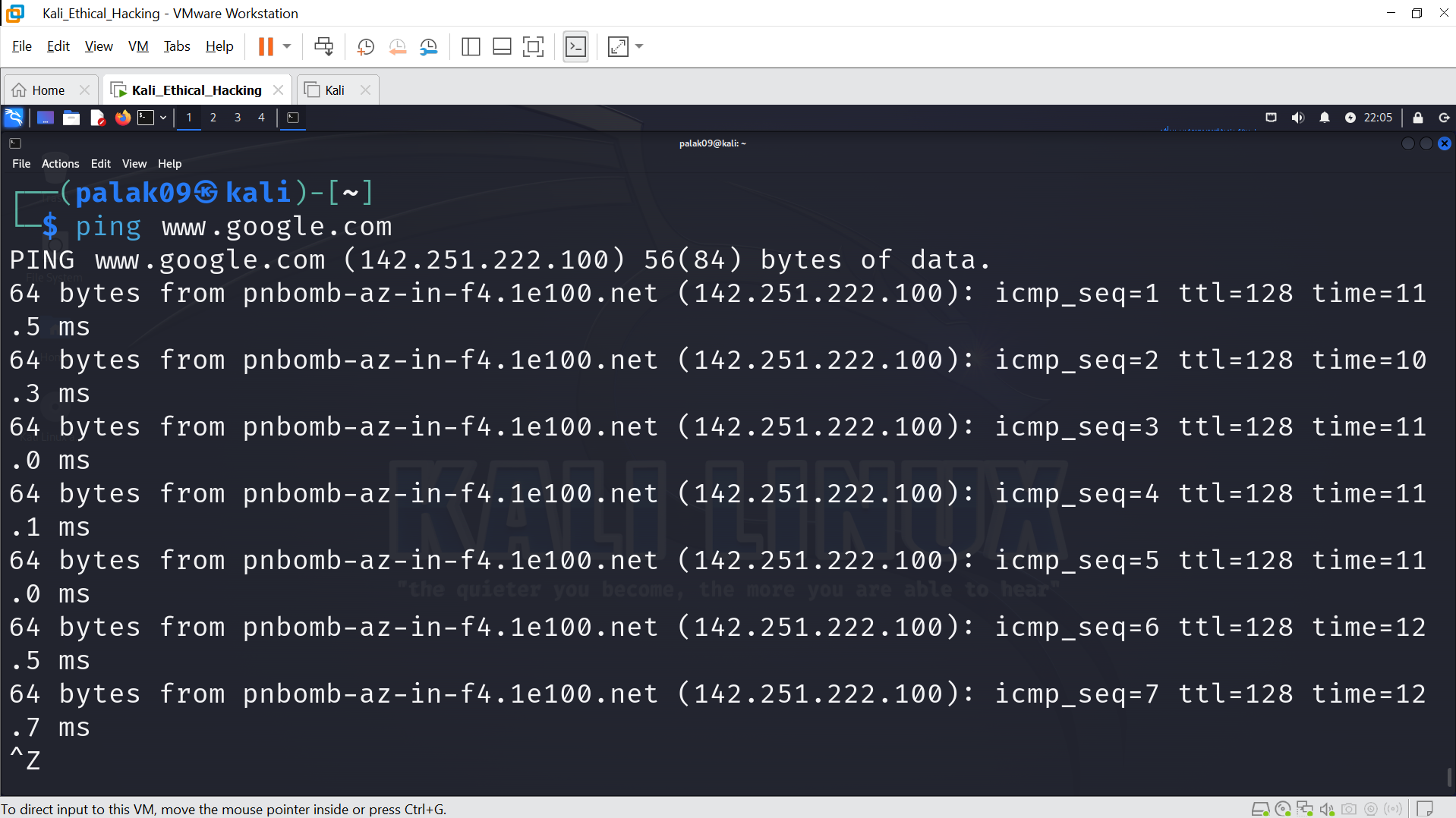
**4. Execute the following Linux commands:**

* **Find command**
* **Ping command**
* **Traceroute command**
* **Whoami command**
* **Ps command**
* **Screenshot Submission: Screenshot of terminal output for each command.**

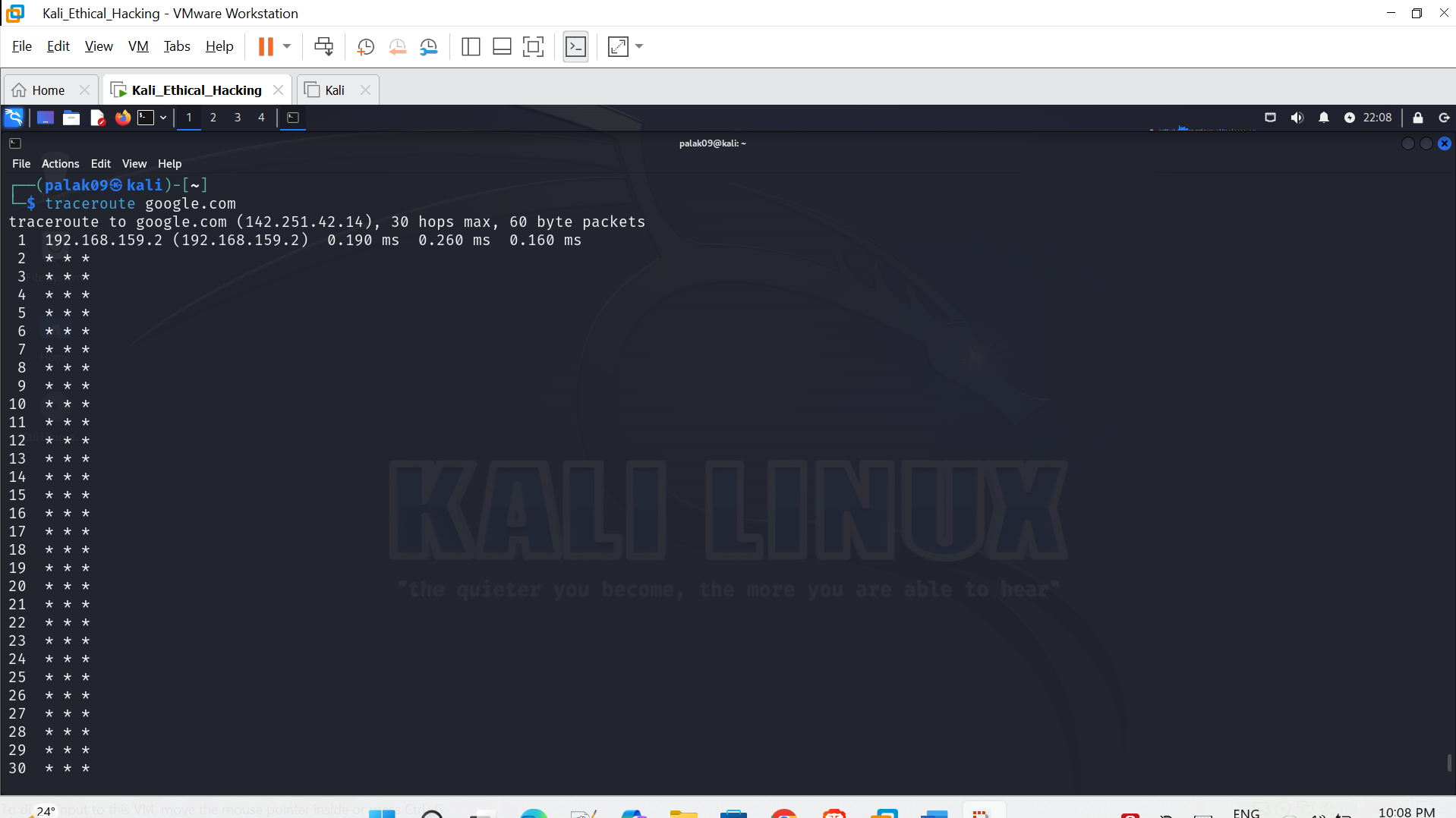
**find**

****

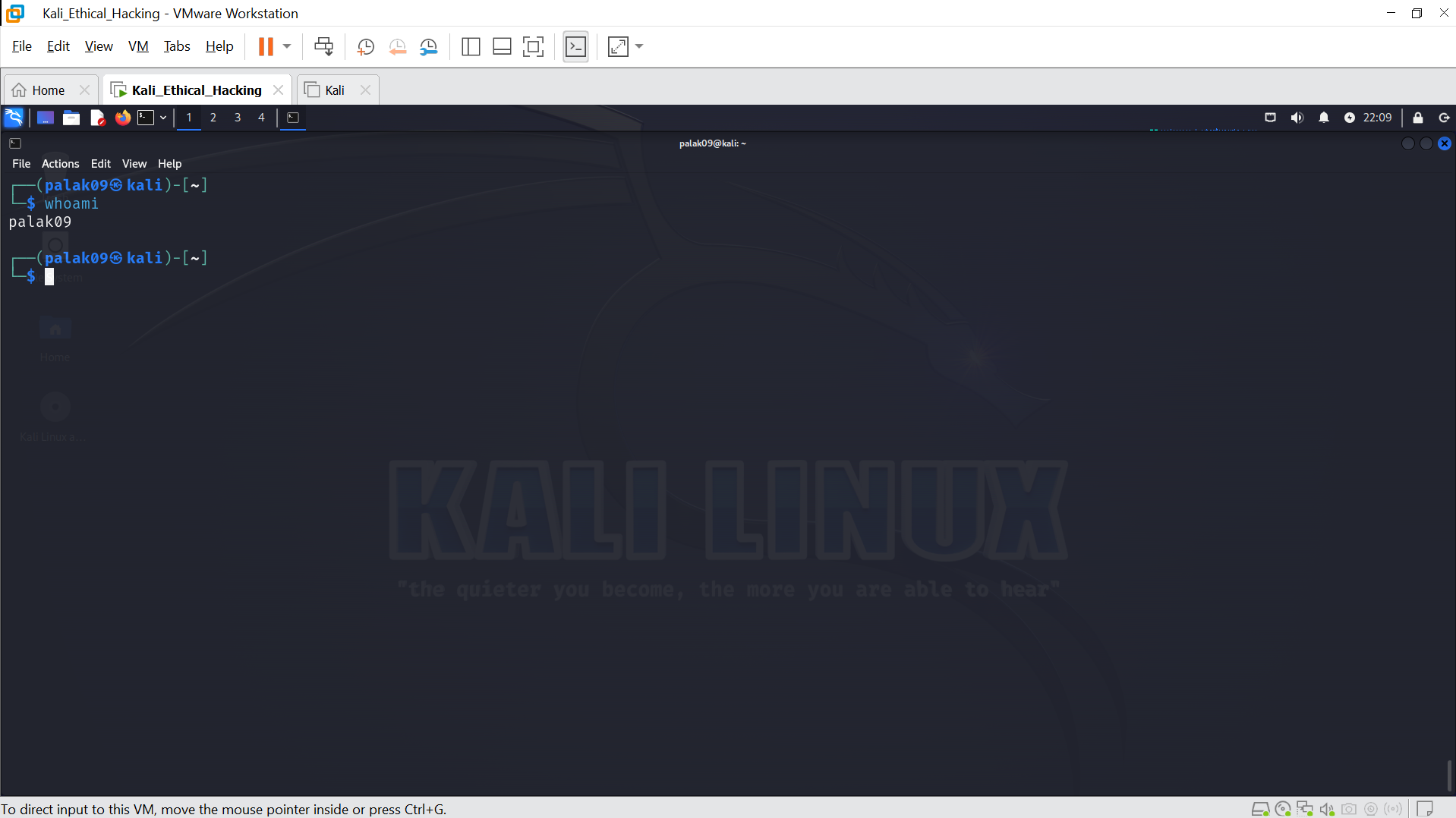
**ping**

****

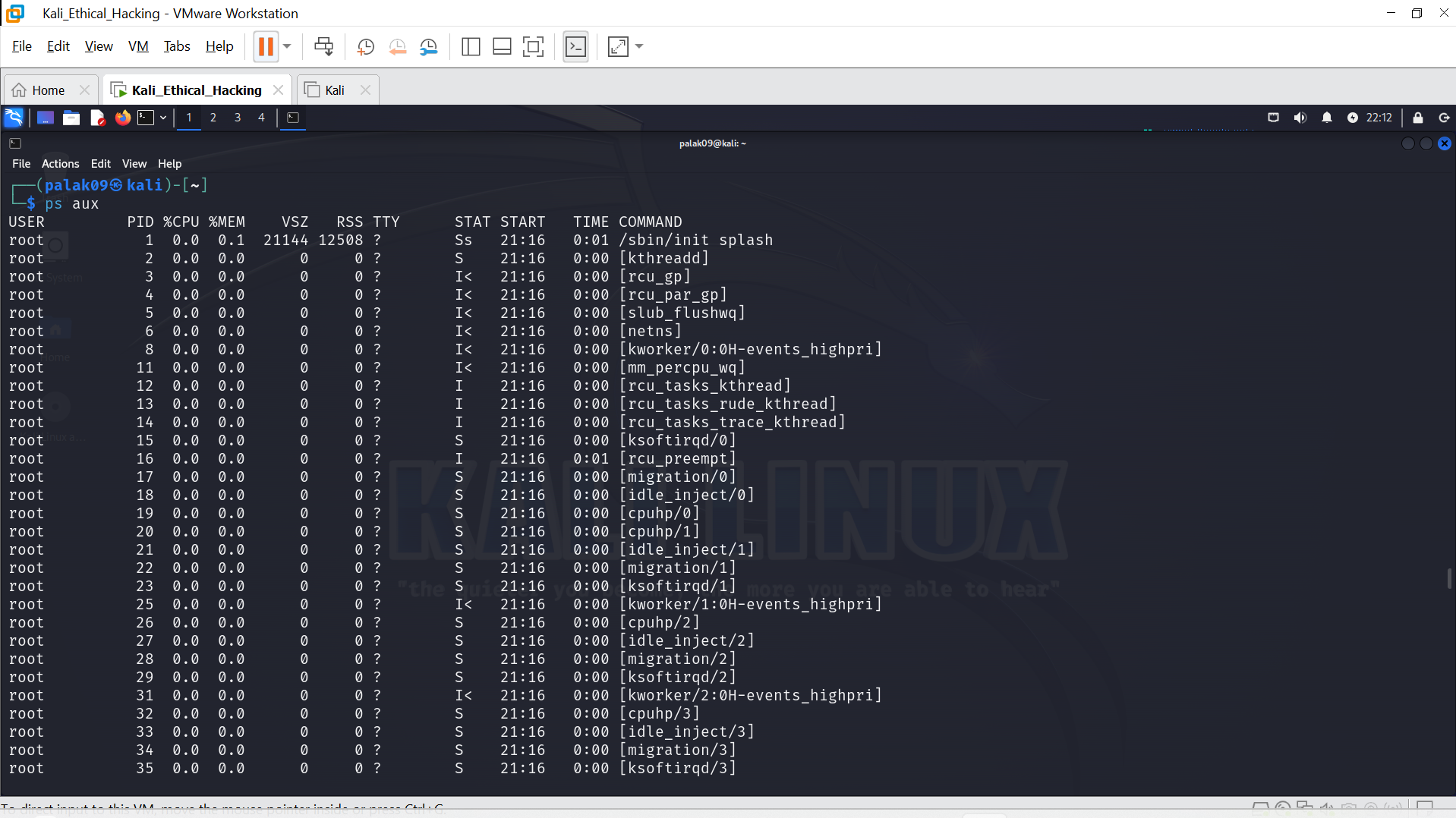
**traceroute**

****

**whoami**

****

**ps**

****