**Task Report**

**Name:- Kundan Keshav Gawande**

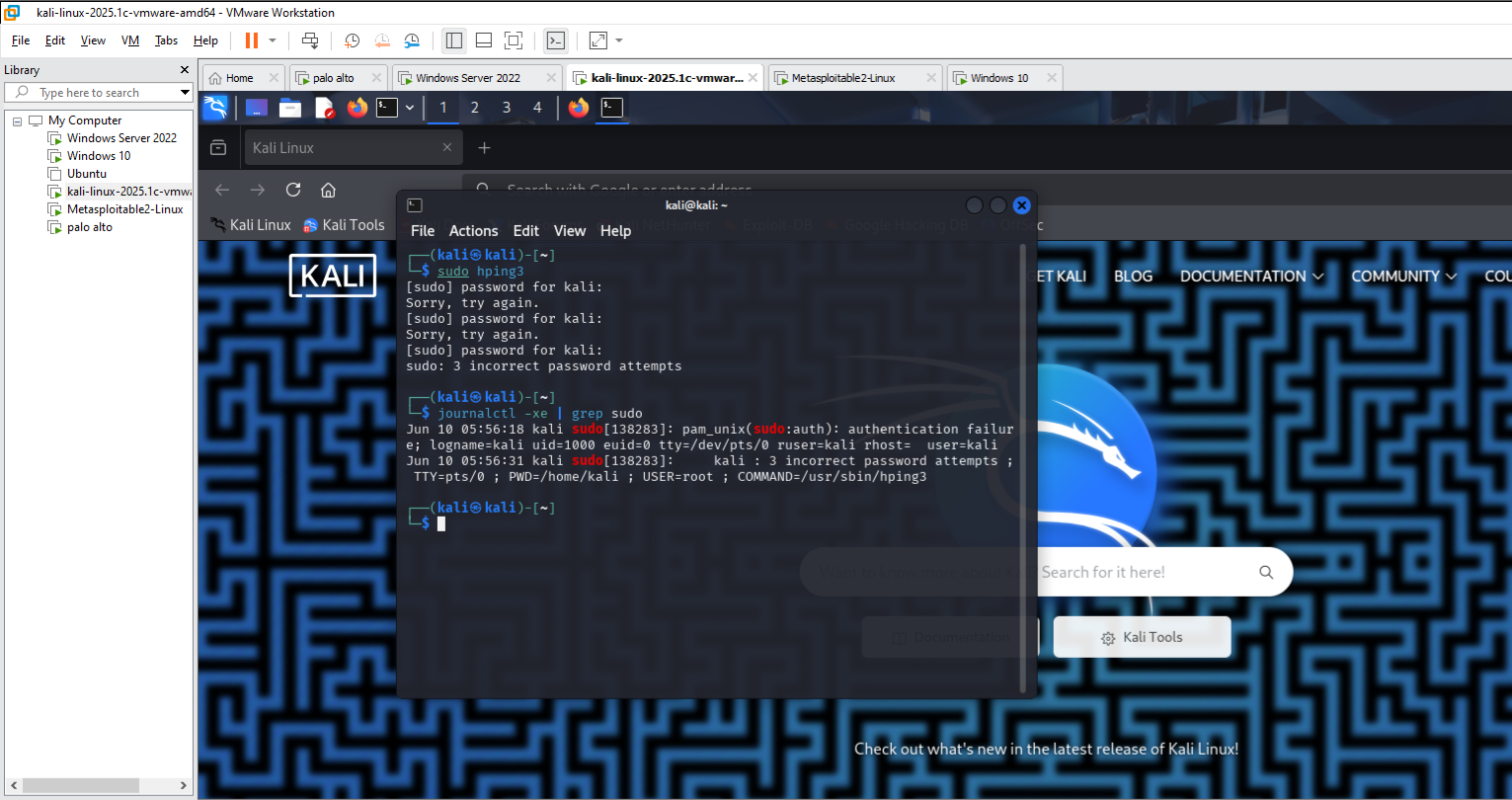
**ID:- 28806**

**Week-4, Day-2**

**Date- 10/06/2025**

**Task-1 Students to attempt anunauthorized Sudo attempt and observe the logs**

* **Step No.1:-** **Open Kali Linux in a Virtual Machine**, **Start your Kali Linux system within your virtual environment (like VirtualBox or VMware).**
* **Step No.2:- Launch the Terminal,Once Kali has booted, open the Terminal from the applications menu or by right-clicking on the desktop.**
* **Step No.3:- Run the command: sudo hping3 (or any sudo command)**
* **Step No.4:- Enter the Wrong Password Multiple Times, When prompted for your password, intentionally type the wrong password two or three times to simulate failed authentication attempts.**
* **Step No.5:- After failed attempts, run: journalctl -xe | grep sudo**
* **Step No.5:- Review the Logs, The output will display recent log entries, including the failed sudo attempts, along with timestamps and system messages**.



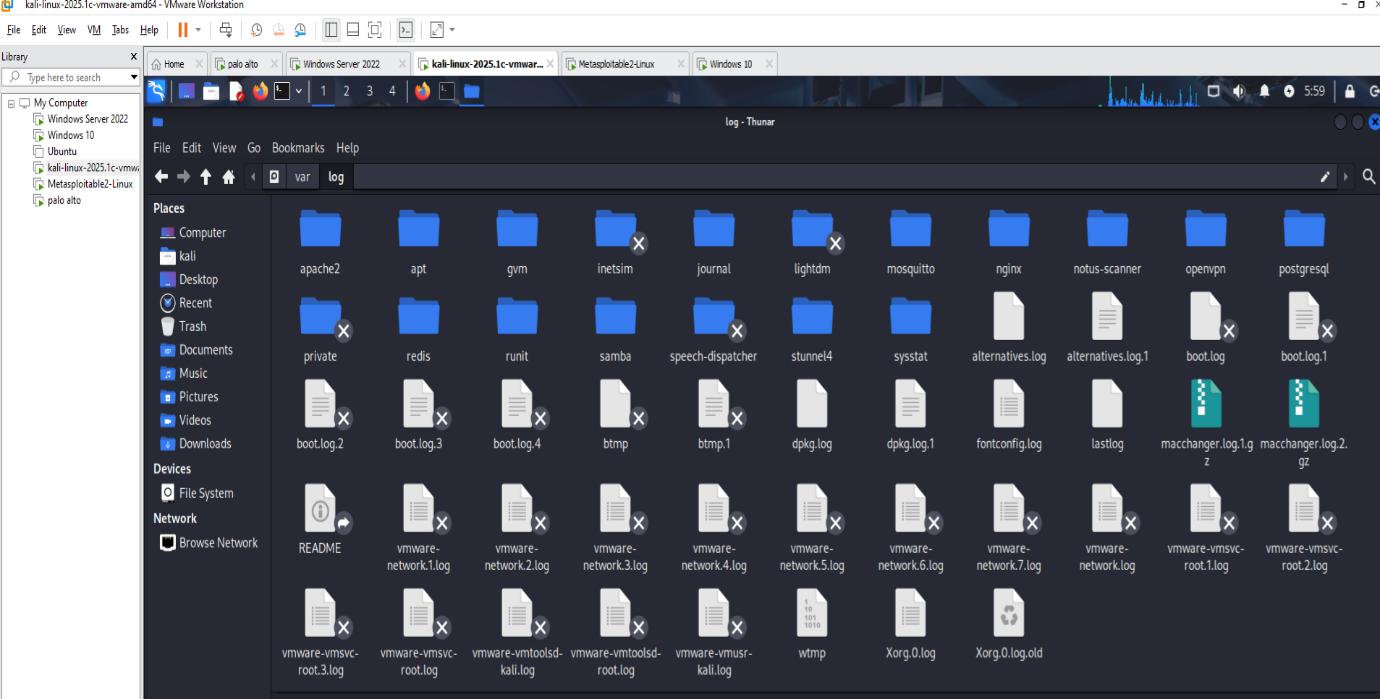
**2nd method used for Observing the logs**

**Step-1 Open Folder**

**Step-2 Open File System(Root Directory)**

**Step-3 Then Open var Folder**

**Step-4 Then you can see logs over there**



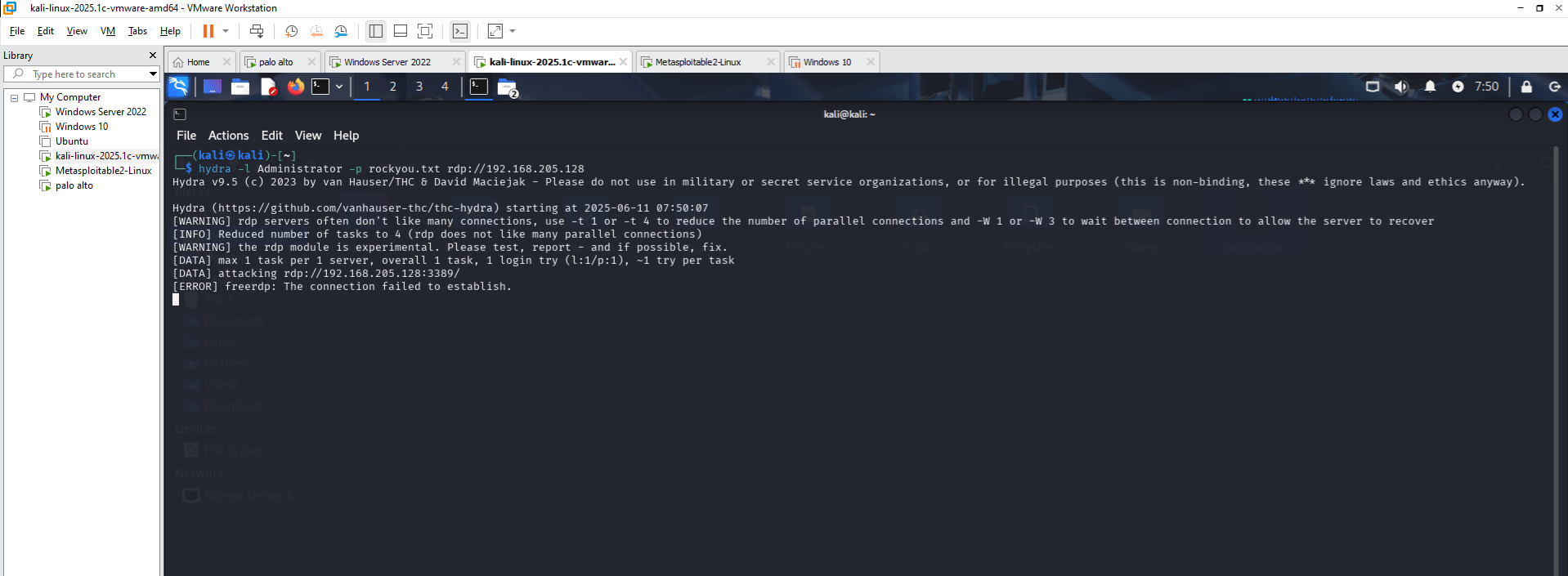
**Task-2 Students to launch a bruteforceattack using Kali Linux and observethe events in the event viewer.**

**Step-1First you have to download the rockyou.txt file from browser.**

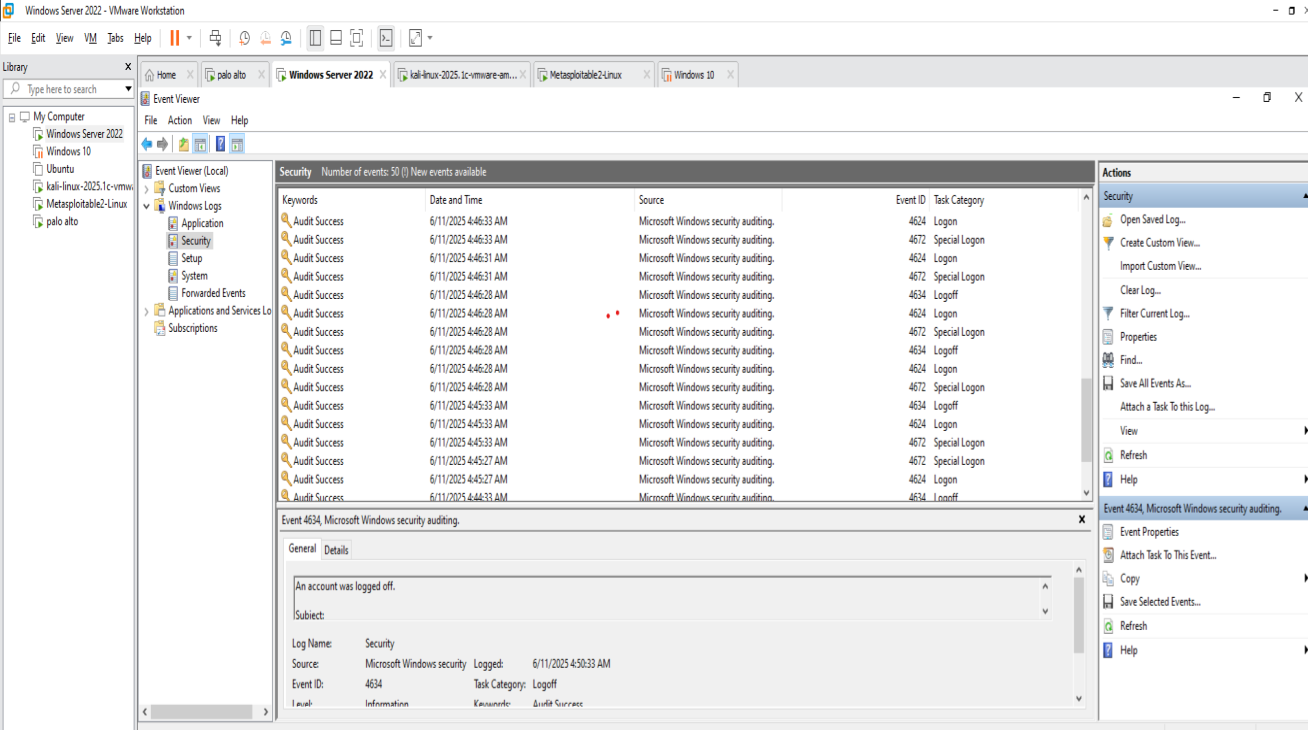
**Step-2 Then Save it in your Root Directory in kali linux**

**Step-3 Open Your Terminal in Kali Linux**

**Step-4 Then Type hydra -l Administrator -P rockyou.txt rpd://192.168.205.128**



**Step-5 Go to your system which IP address you have assigned in command and see the event viewer**



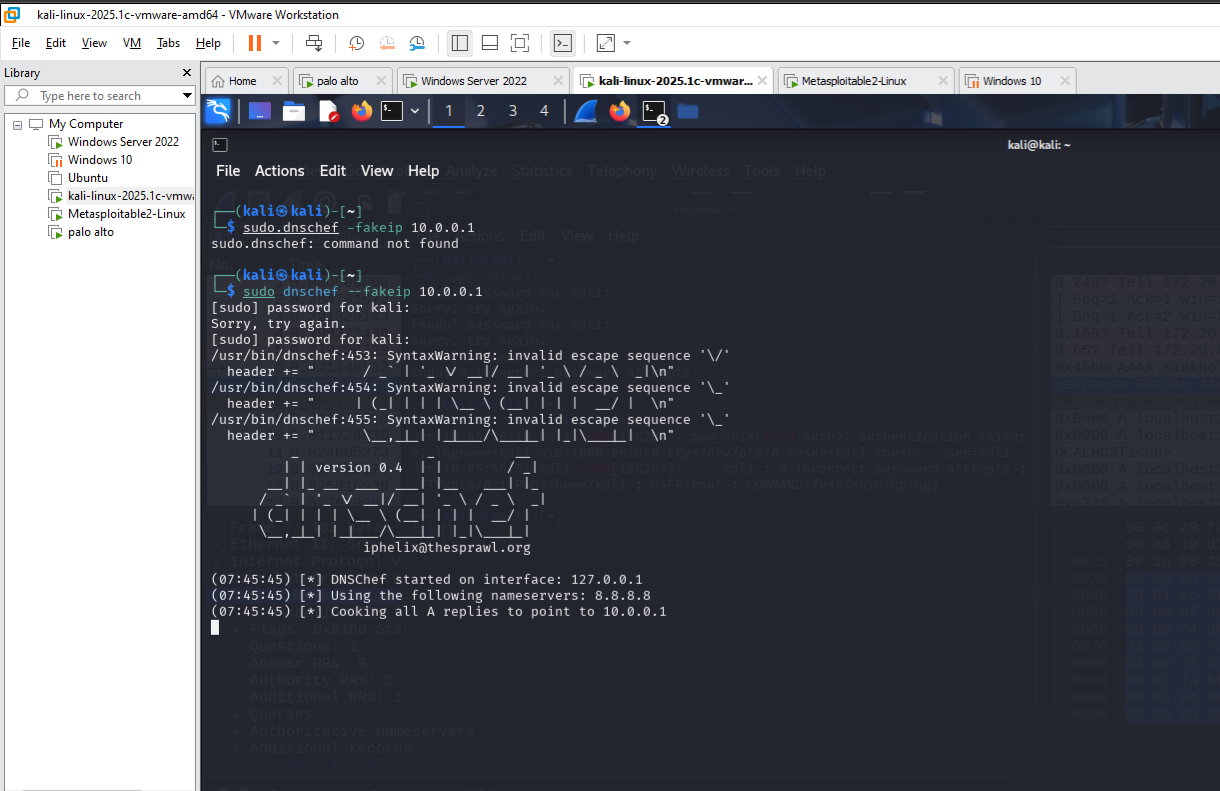
**Task-3: Students to launch DNS basedattacks and explore the results.**

**** **Step 1: First, open your Kali Linux operating system and make sure it is fully booted up and ready to use.**

 **Step 2: After the system has loaded, open the Terminal by clicking on the Terminal icon or using the right-click menu.**

** Step 3: In the Terminal, type the following command to start dnschef with a fake IP address:**

**sudo dnschef --fakeip 10.0.0.1**



**Step 4: Now, open Wireshark, a network analysis tool, and start capturing traffic. Look specifically at the DNS response packets to observe how dnschef is replying with the fake IP address.**

