**Title: Data Stealing using DNS tunneling**

**Learning Objectives:** This exercise is focused on data stealing using DNS tunneling. You will learn to understand and simulate the DNS tunneling technique using the iodine tool, covertly exfiltrate various types of data through DNS queries and responses, and implement effective mitigation strategies to prevent data theft through DNS tunneling.

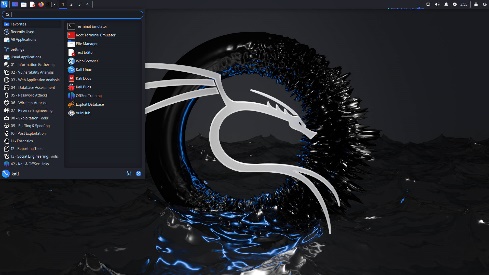
**Description:** Data stealing using DNS tunneling is a method that exploits the DNS protocol to covertly exfiltrate sensitive information from compromised systems. By leveraging DNS queries and responses, attackers can bypass traditional network security measures, making detection challenging. This method demonstrates how the iodine tool facilitates the setup of DNS tunnels, enabling the transmission of various types of data through seemingly innocuous DNS traffic.

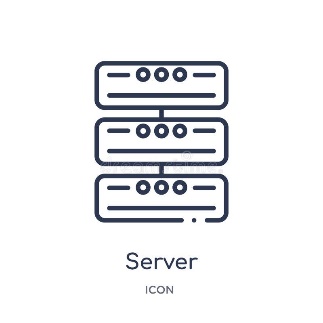
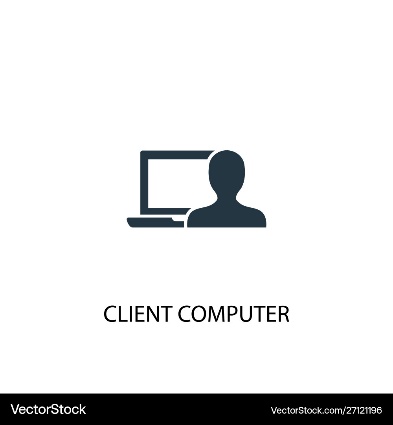
**Instructions to Follow Before Executing the Exercise:**

1. Set up isolated virtual environment for client and server setups.
2. Ensure iodine can be installed and operated on chosen OS versions.
3. Install and Configure iodine on both client and server systems.
4. Configure DNS Settings: Set up DNS records and server for tunneling domain.
5. Adjust Firewall Rules: Configure firewalls to permit UDP traffic on iodine's port.
6. Prepare Monitoring Tools: Set up tools to monitor and log DNS traffic during the exercise.
7. Plan for post-exercise cleanup and system restoration to revert any changes made during the exercise.

**About the Exercise lab infrastructure:**

For this exercise, you need one Kali Linux virtual machine where both the DNS tunneling server and client will be simulated. Ensure iodine is installed and the machine has network access configured for both server and client roles.



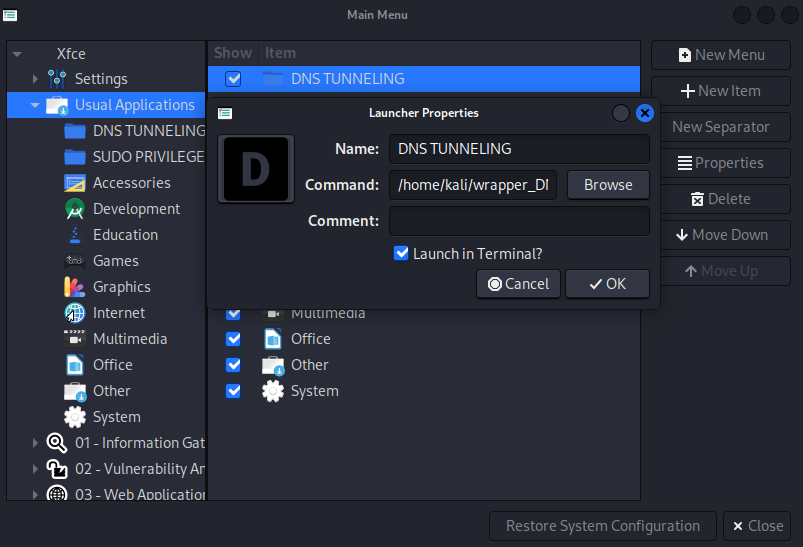


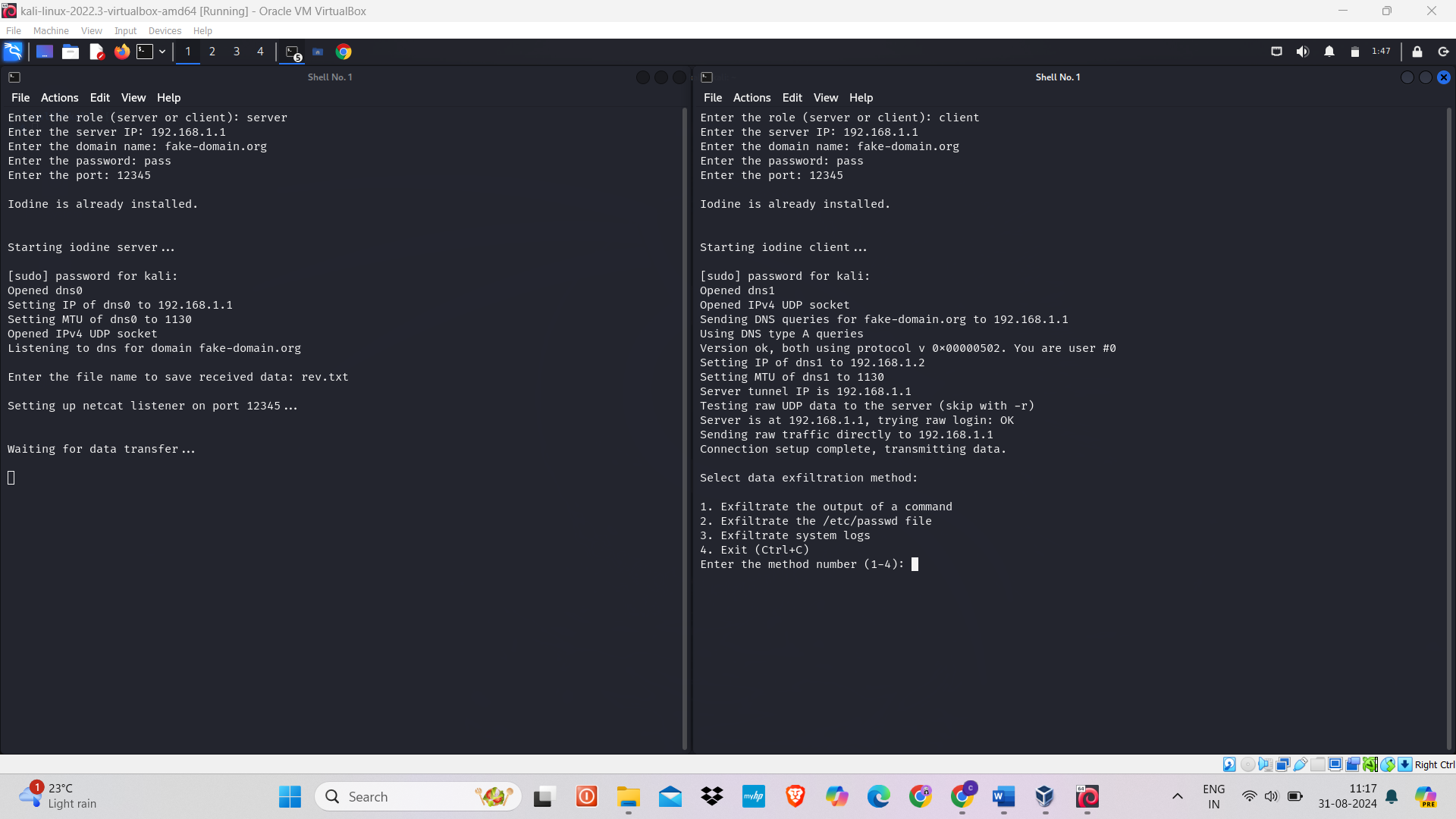


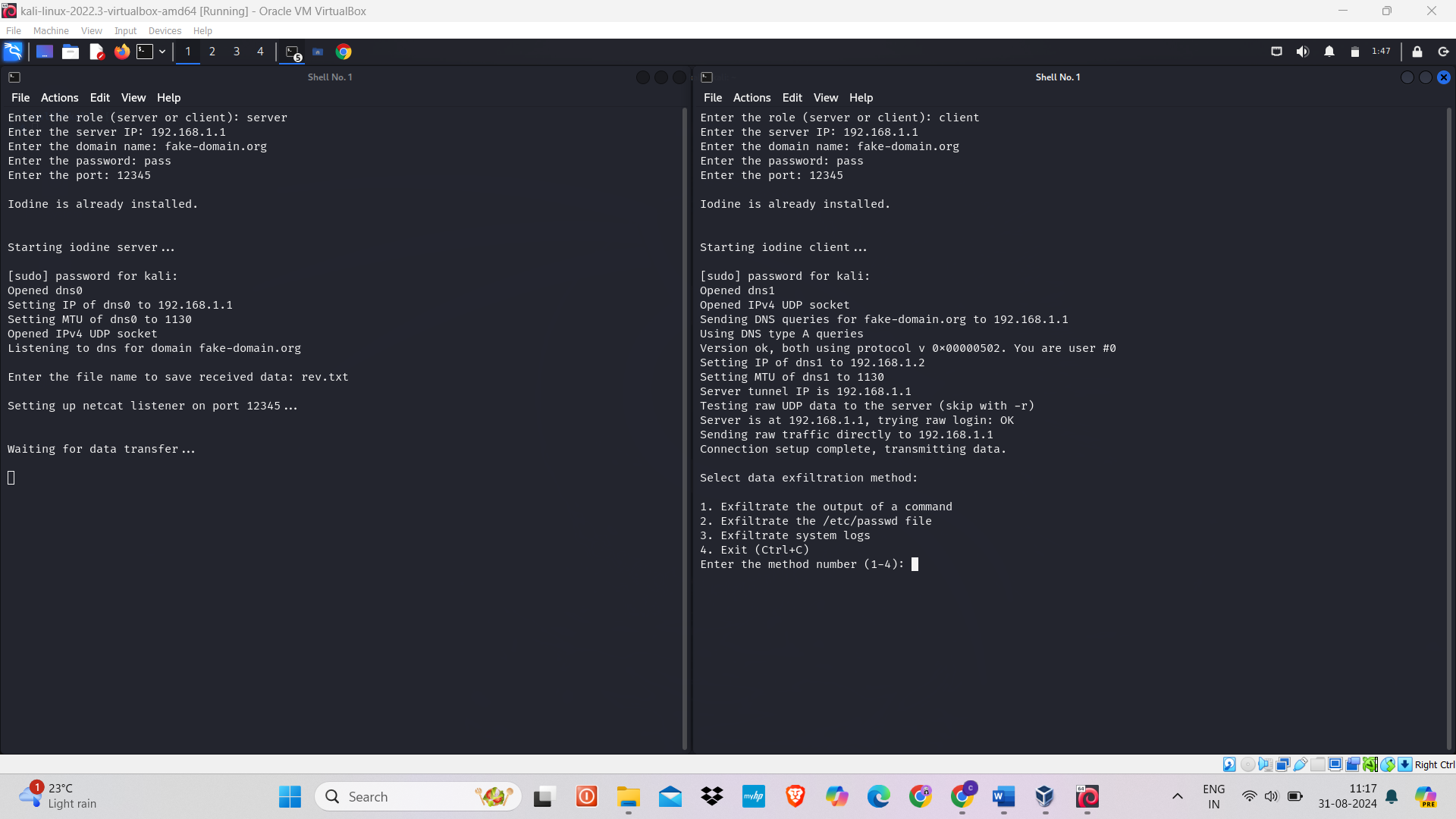
DNS Tunnel

Attacker Victim

Launch Attack by clicking on “DNS TUNNELING” button.

Go to the **Application tab> Usual Applications>DNS TUNNELING** (in Kali machine).





**For detailed instructions, refer to the step-by-step guide provided in the " Data stealing using DNS Tunneling” lab manual.**