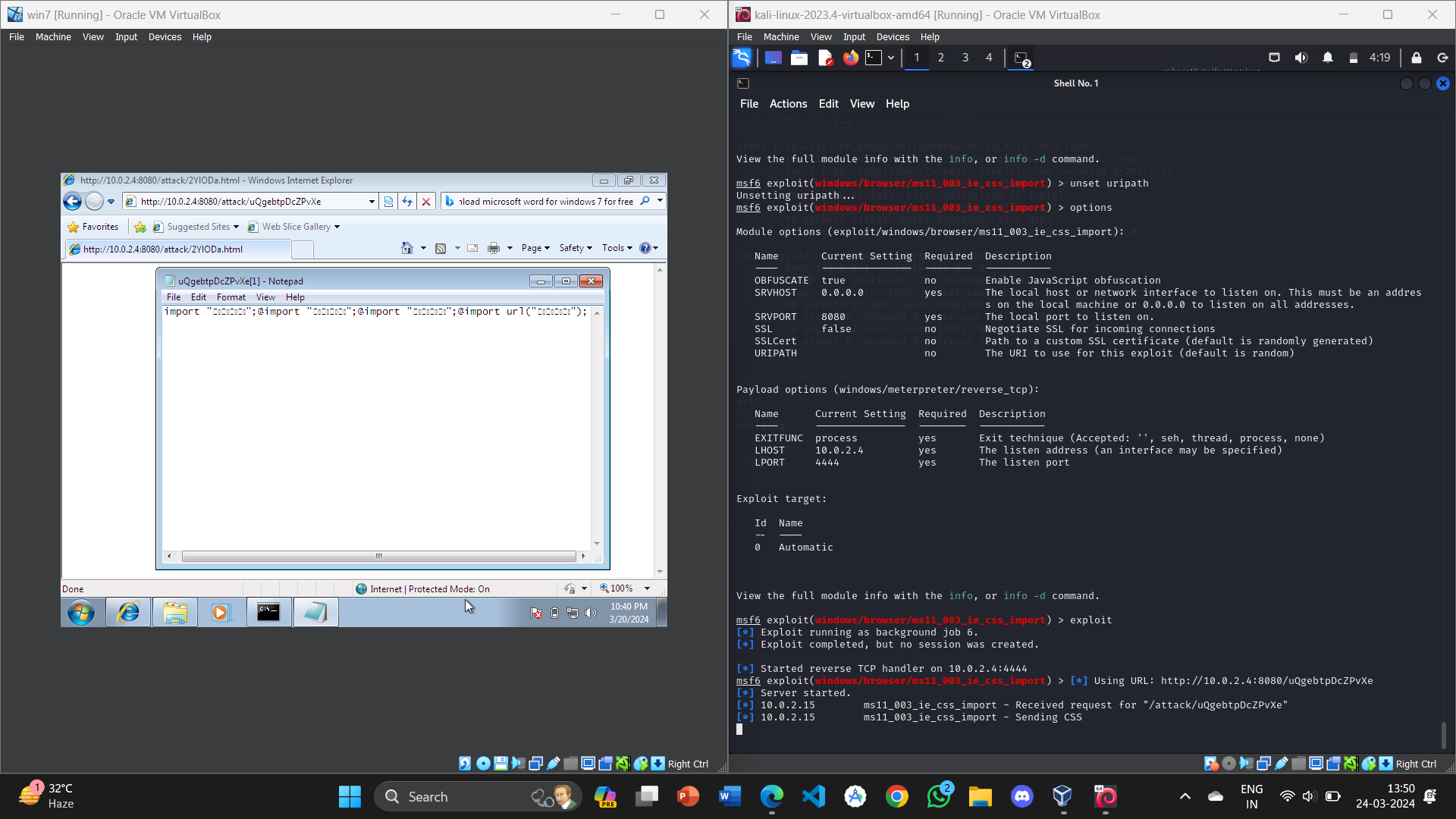
### Ethical Hacking

**Lab5: Exploiting Client side vulnerabilities**

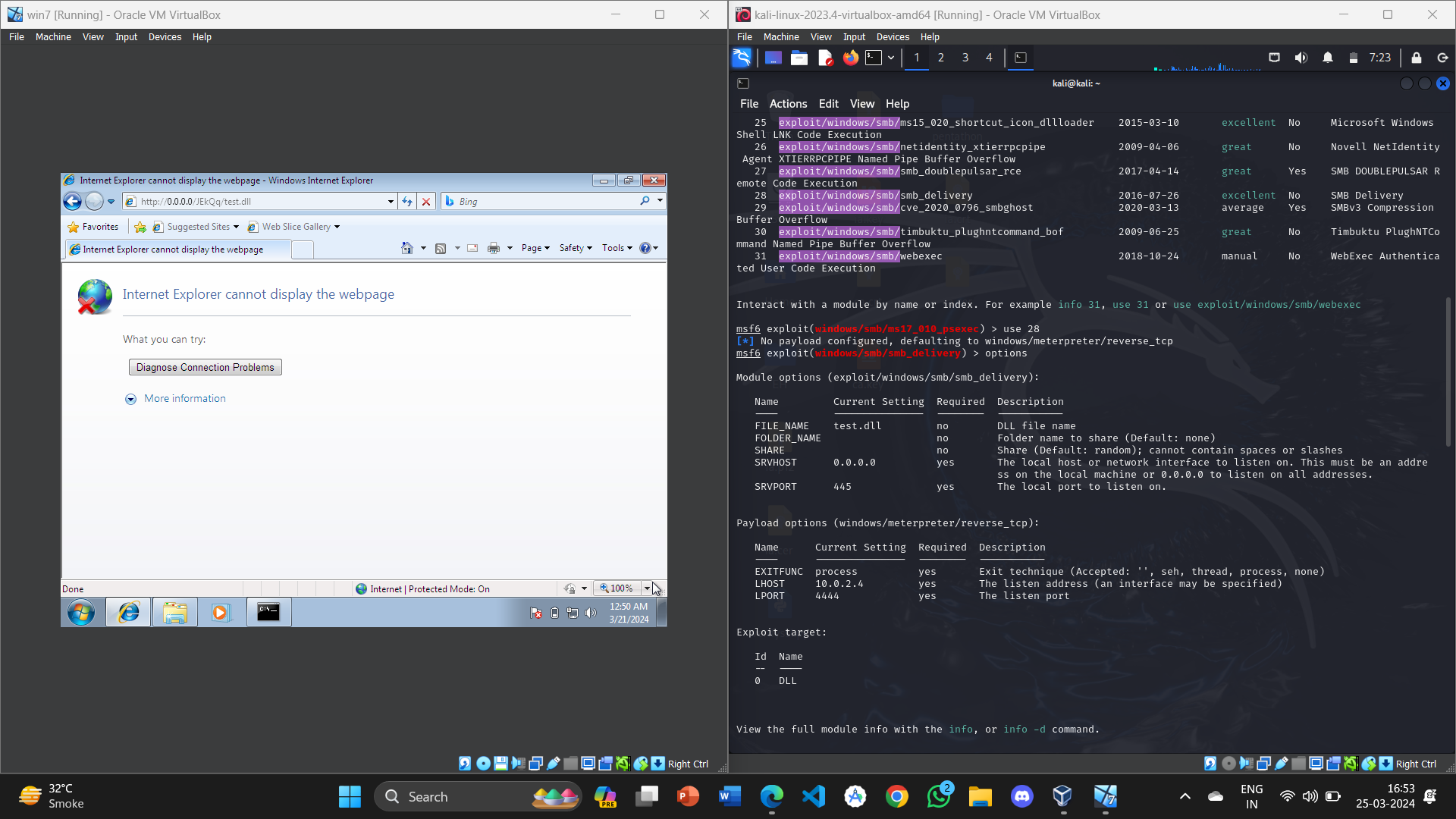
Student Name: Adwait Purao Sem: VI Date: 15/04/2024

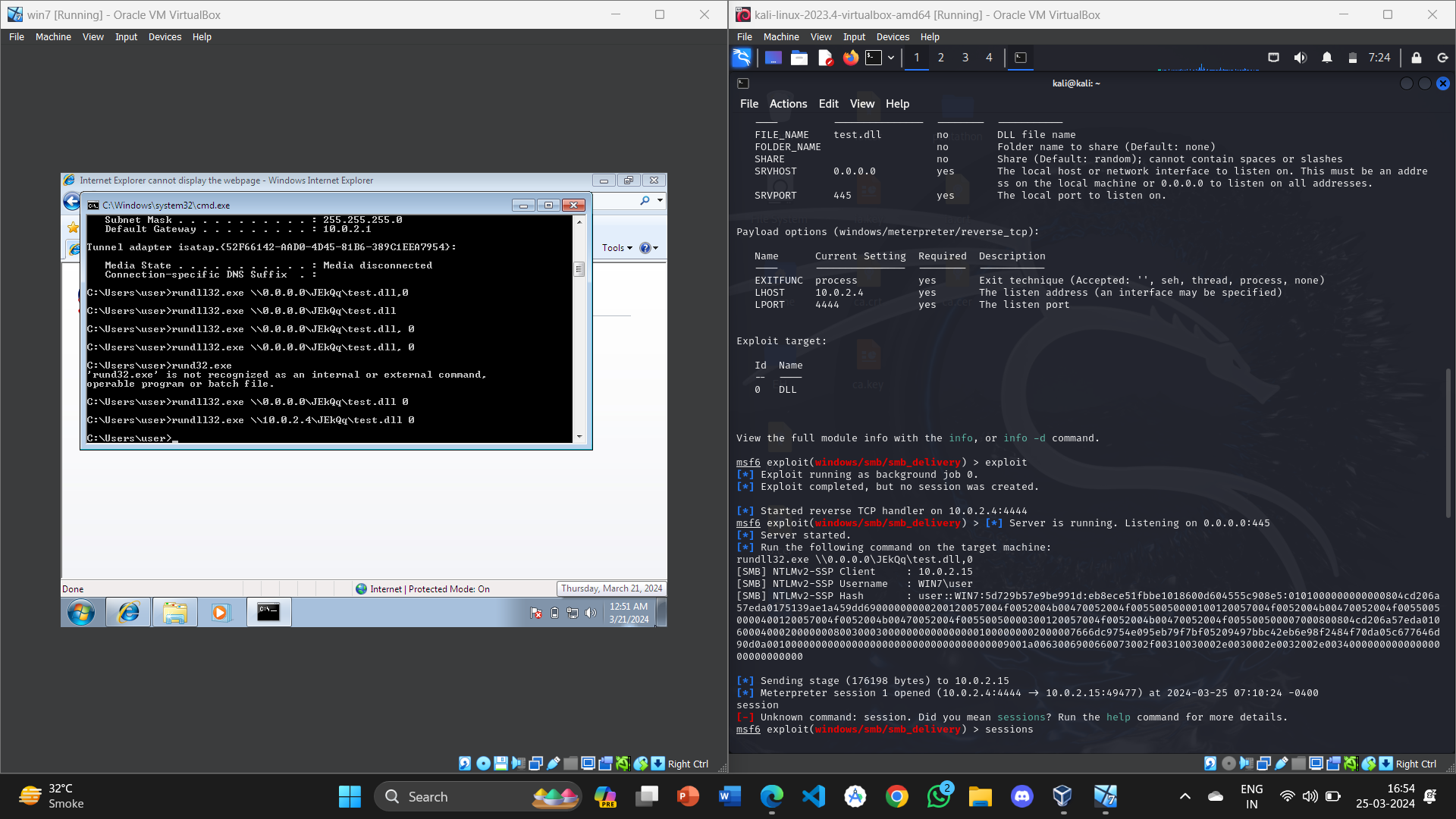
**IP address of windows : 10.0.2.4**

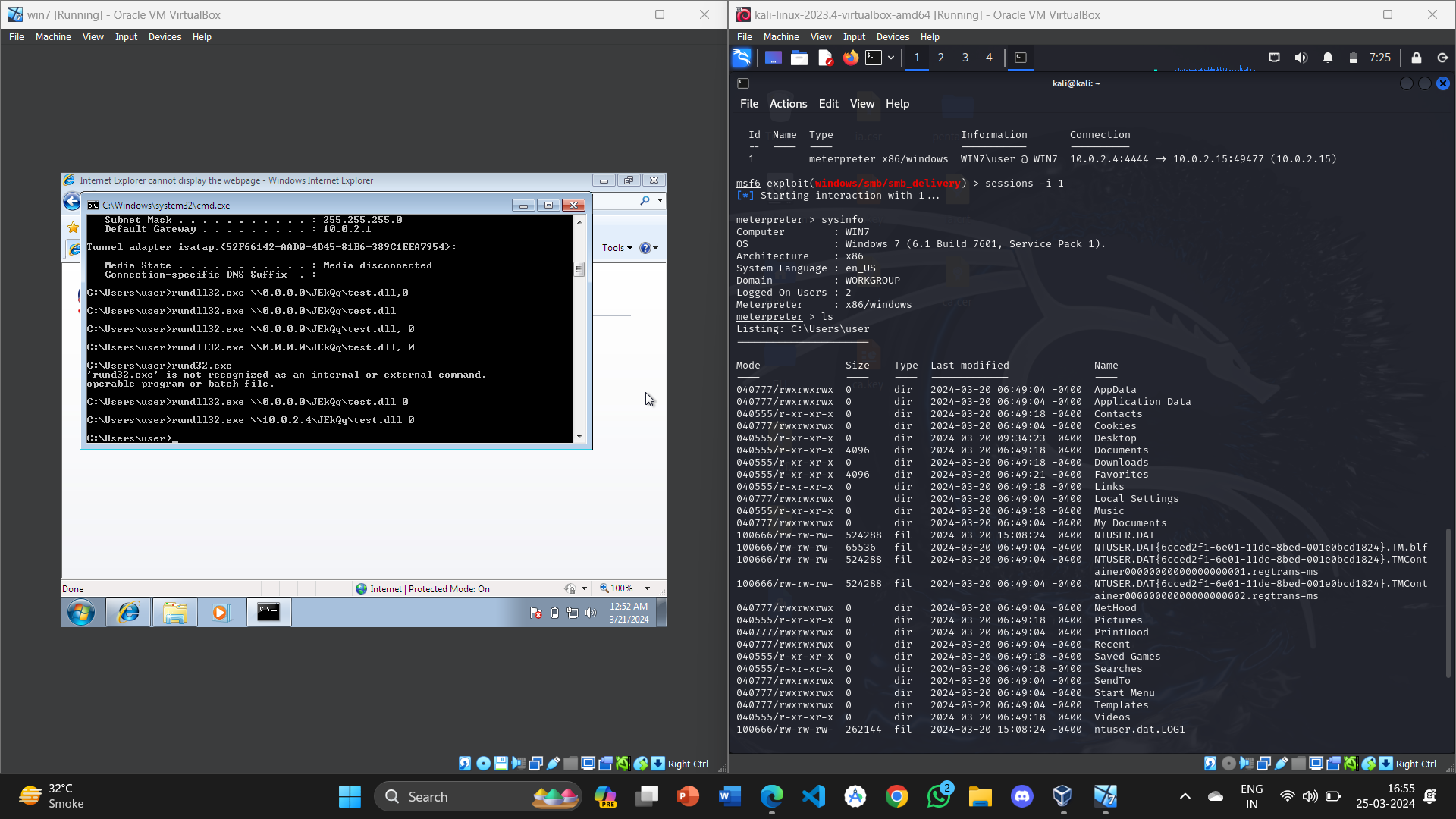
**IP address of Kali: 10.0.2.15**

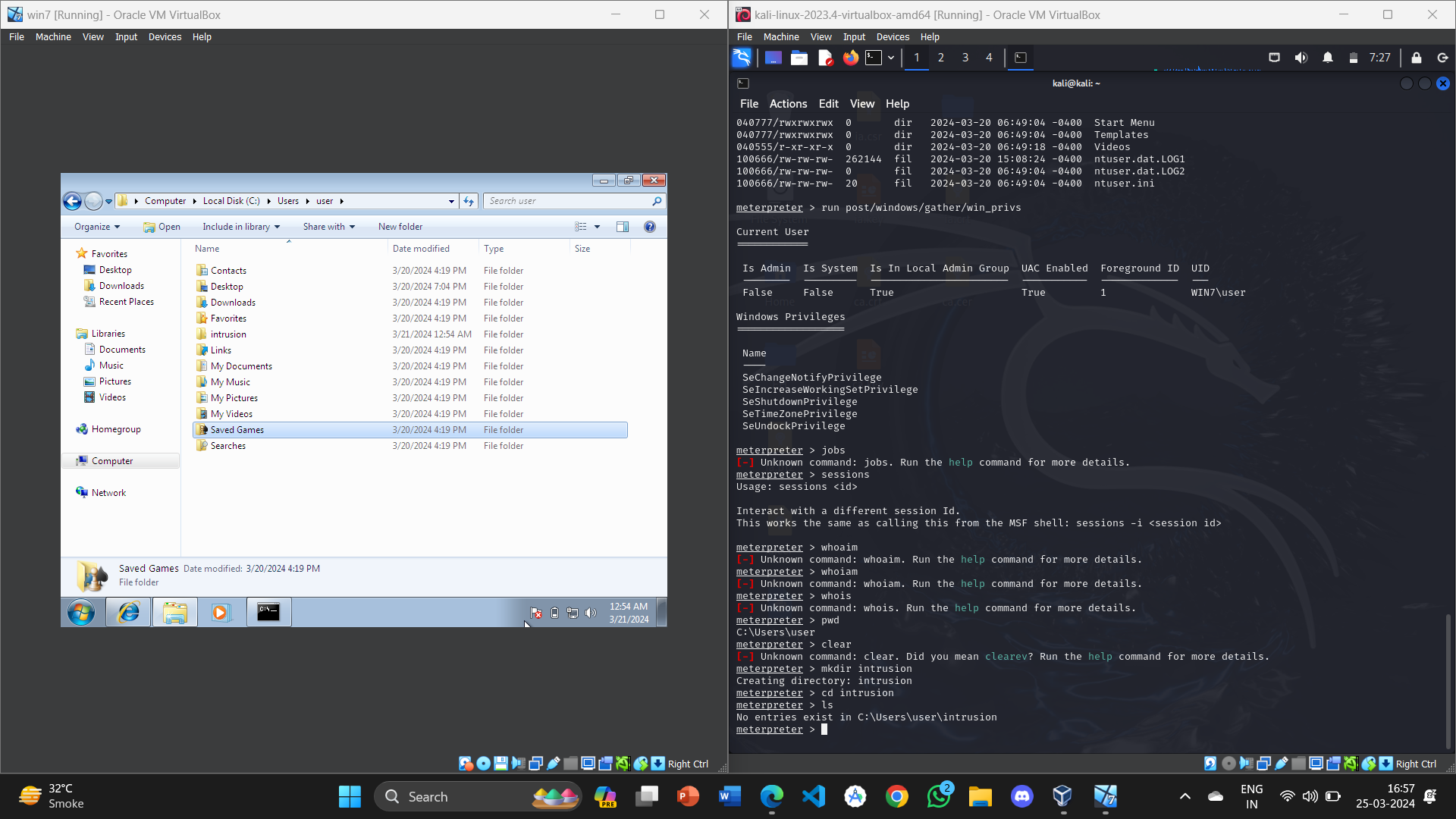
****

**couldn’t exploit ms11\_003 so shifted towards using eternalblue exploits, smb to be more specific.**

****

****

****

****

SMB (Server Message Block) is a network protocol used by Windows-based computers to share files, printers, and other resources across a local network or the internet. It enables communication between client and server systems for various purposes, such as file sharing, remote access, and inter-process communication.

Vulnerability in SMB protocol that was discovered by the U.S. National Security Agency (NSA) and leaked by the Shadow Brokers hacker group in April 2017. It affects the SMBv1 protocol implementation in various versions of Microsoft Windows operating systems.

This vulnerability, tracked as CVE-2017-0144, allows remote attackers to execute arbitrary code on vulnerable Windows systems without authentication. It exploits a flaw in the way SMB version 1 (SMBv1) handles certain requests, specifically related to the processing of SMB packets, allowing an attacker to send specially crafted packets to a vulnerable system and execute malicious code

**Conclusion -**

So we conclude that access to the target system was achieved through exploitation of client-side vulnerabilities, effectively deploying a payload and demonstrating remote control capabilities.