Cybersecurity Home Lab: Remote Access Trojan Deployment & Post-Exploitation

# Overview

This report documents a hands-on cybersecurity exercise conducted in a controlled lab environment using Kali Linux and a vulnerable Windows 7 virtual machine. The objective was to simulate a Remote Access Trojan (RAT) deployment and demonstrate post-exploitation capabilities using Meterpreter.

# Objective

Gain a Meterpreter shell on a Windows 7 system by exploiting a bind shell payload using Metasploit, and perform keystroke logging and screen sharing to simulate intelligence gathering during a post-exploitation phase.

# Lab Setup

- Kali Linux VM as the attacker

- Windows 7 VM (IE8 version) as the victim

- Oracle VirtualBox configured with Host-only Adapter for internal networking

- Metasploit Framework used for exploitation

- Payload used: windows/meterpreter/bind\_tcp

# Attack Execution

1. Set payload to windows/meterpreter/bind\_tcp

2. Set RHOST to the IP address of the Windows 7 target machine (e.g., 10.0.2.6)

3. Execute exploit to establish a reverse Meterpreter shell

4. Once Meterpreter session was opened, proceed with post-exploitation commands

# Post-Exploitation

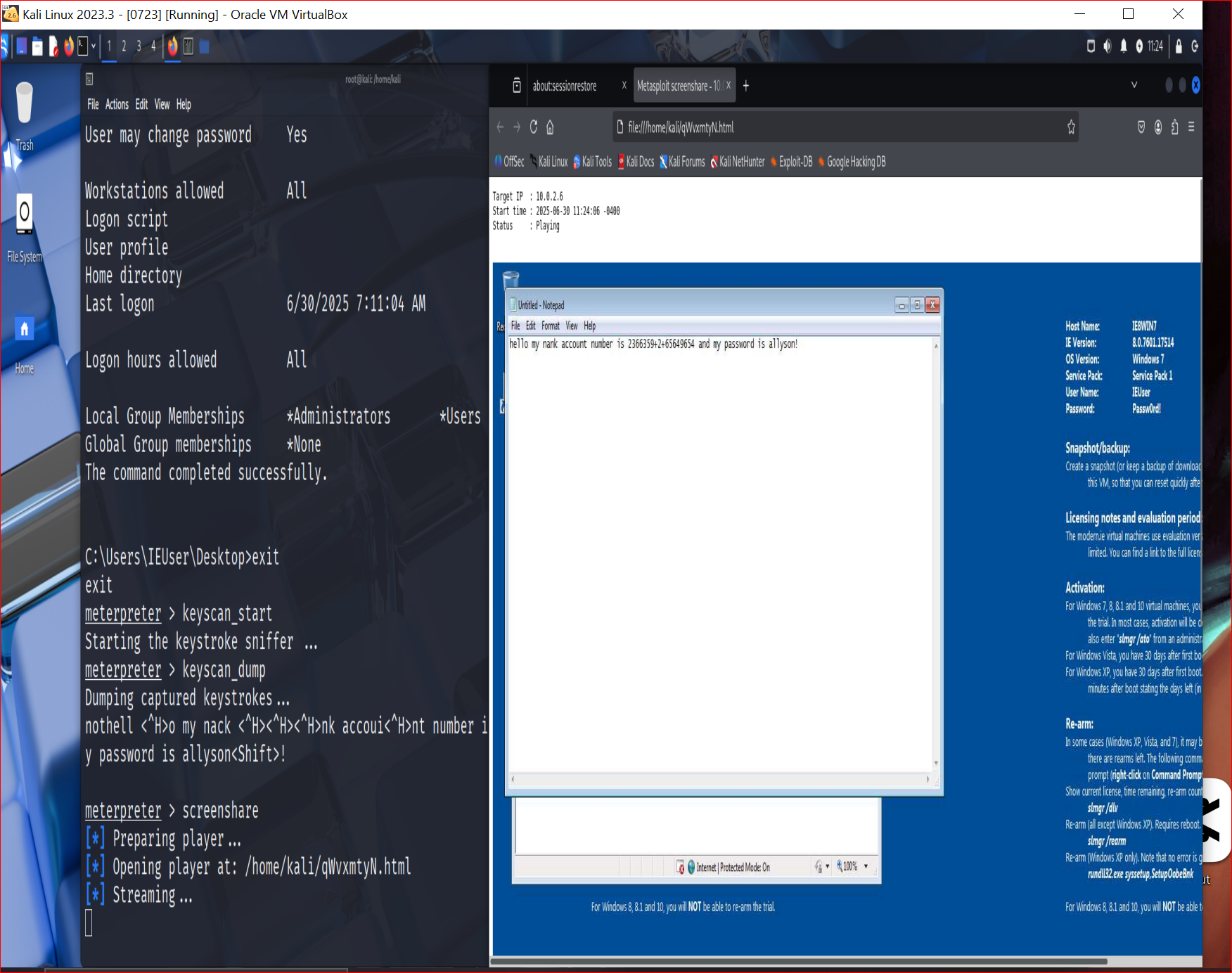
1. Used 'sysinfo' to gather system details

2. Executed 'keyscan\_start' and 'keyscan\_dump' to capture live keystrokes from the victim

3. Activated 'screenshare' module to spy on the victim's desktop in real-time

# Screenshots

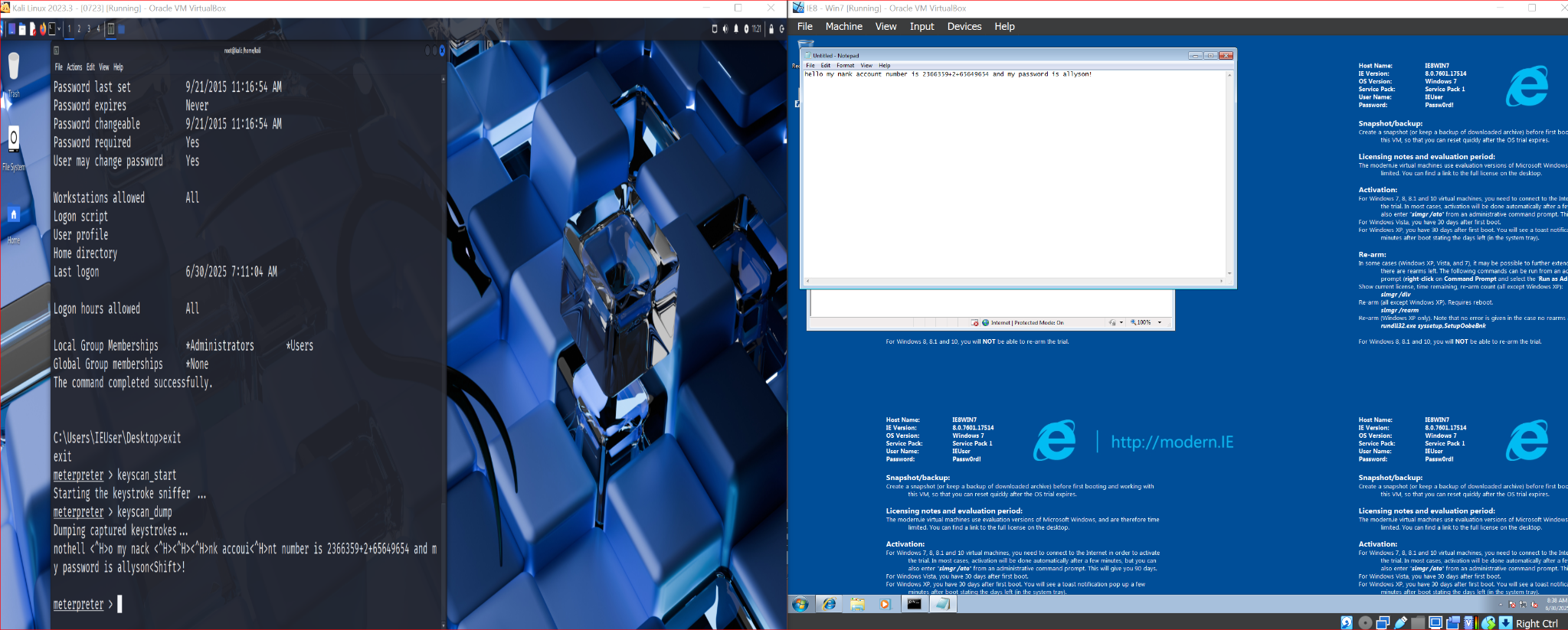
1. Live screen view of Windows 7 host while the attack was active:



2. Meterpreter session opened and keylogging output:



3. Dumped keystrokes revealing sensitive information:



# Conclusion

This exercise demonstrates how attackers can deploy and leverage a Remote Access Trojan for system reconnaissance, data collection, and persistent access. It reinforces the importance of endpoint protection, user awareness, and network segmentation in defending against real-world threats.