**🧪 Cybersecurity Portfolio**

**Perform Enumeration with Nmap**

**🧠 Objective:**

The purpose of this lab is to scan the network to determine the operating systems of devices and identify any openly shared folders. This helps assess potential vulnerabilities within the internal network.

**🧰 Tools Used:**

* **Zenmap (Nmap GUI)**
* **Windows Command Prompt / PowerShell**
* **File Explorer**

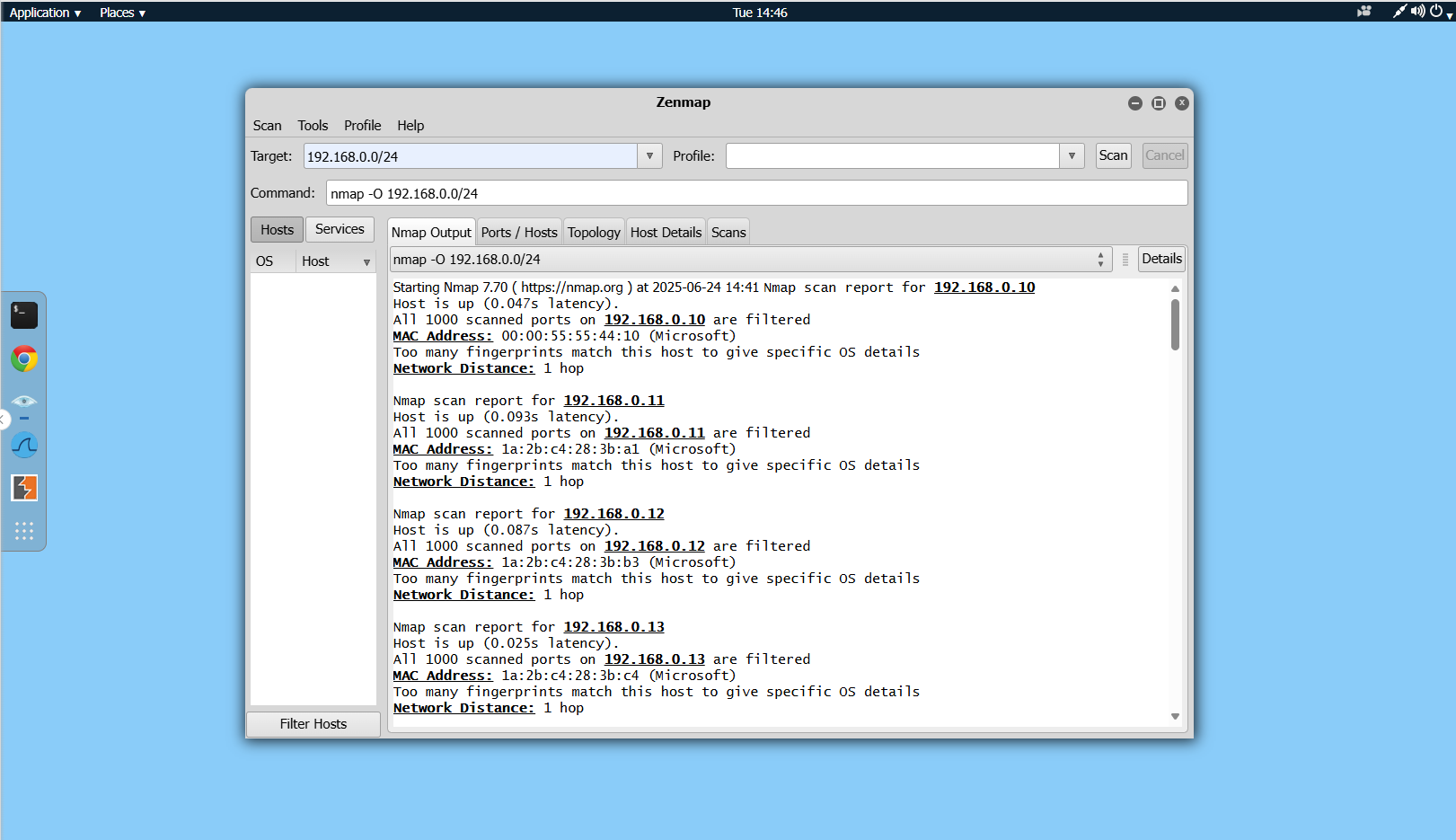
**🧪 Lab Steps and Results:**

**🔍 Part 1 – Identify Operating Systems with Zenmap**

1. Launched **Zenmap** on the **IT-Laptop**.
2. Entered the command below in the "Command" field:

nmap -O 192.168.0.0/24

1. From the scan results, the following IP addresses were determined to be running **Linux**:
   * 192.168.0.22
   * 192.168.0.30
   * 192.168.0.46
   * 192.168.0.47
   * 192.168.0.48

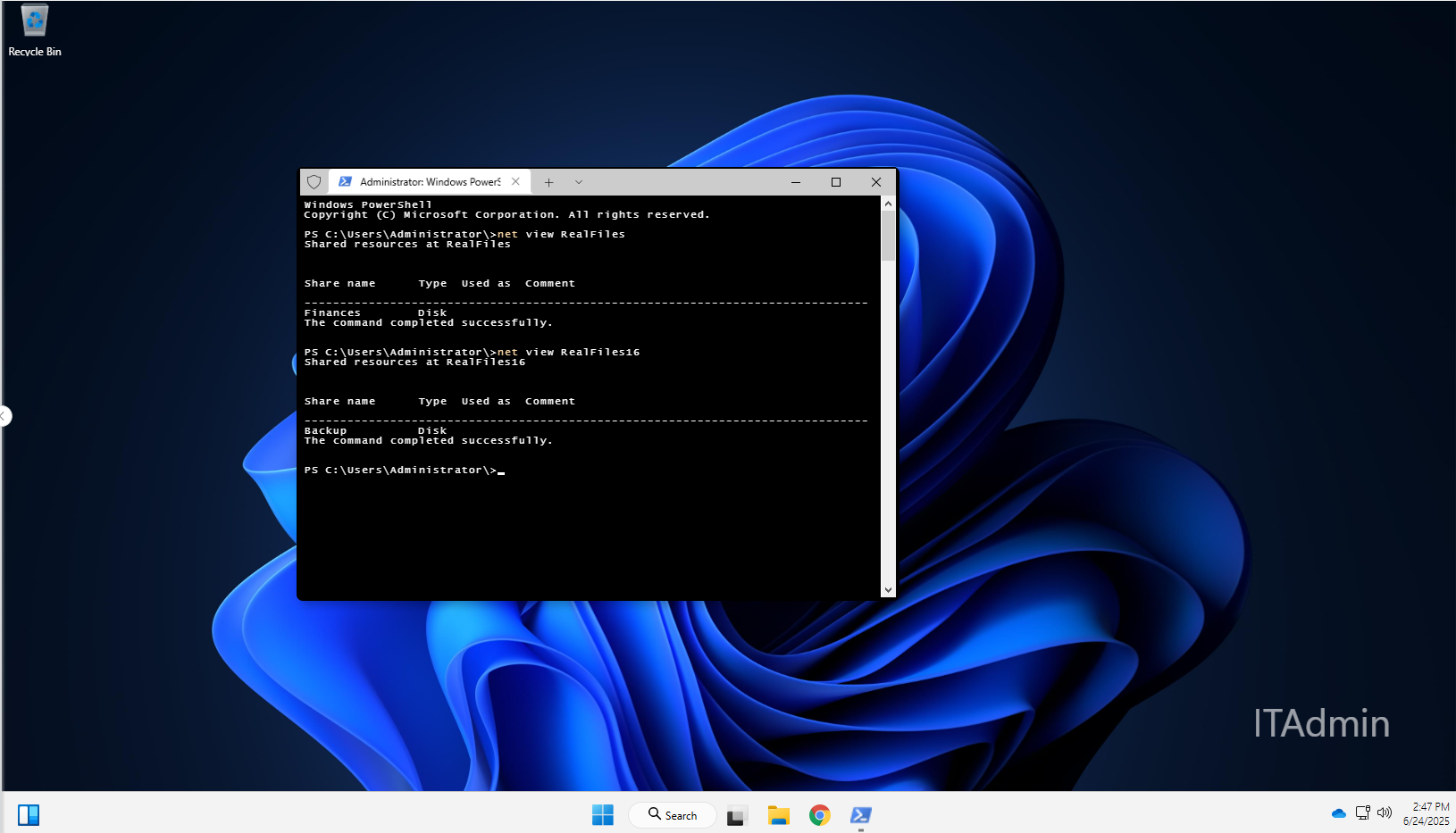


**📁 Part 2 – Check Shared Folders Using net view:**

1. Switched to the **ITAdmin** system.
2. Opened **PowerShell** or **Command Prompt** with admin rights.
3. Executed the following commands:

net view RealFiles

net view RealFiles16



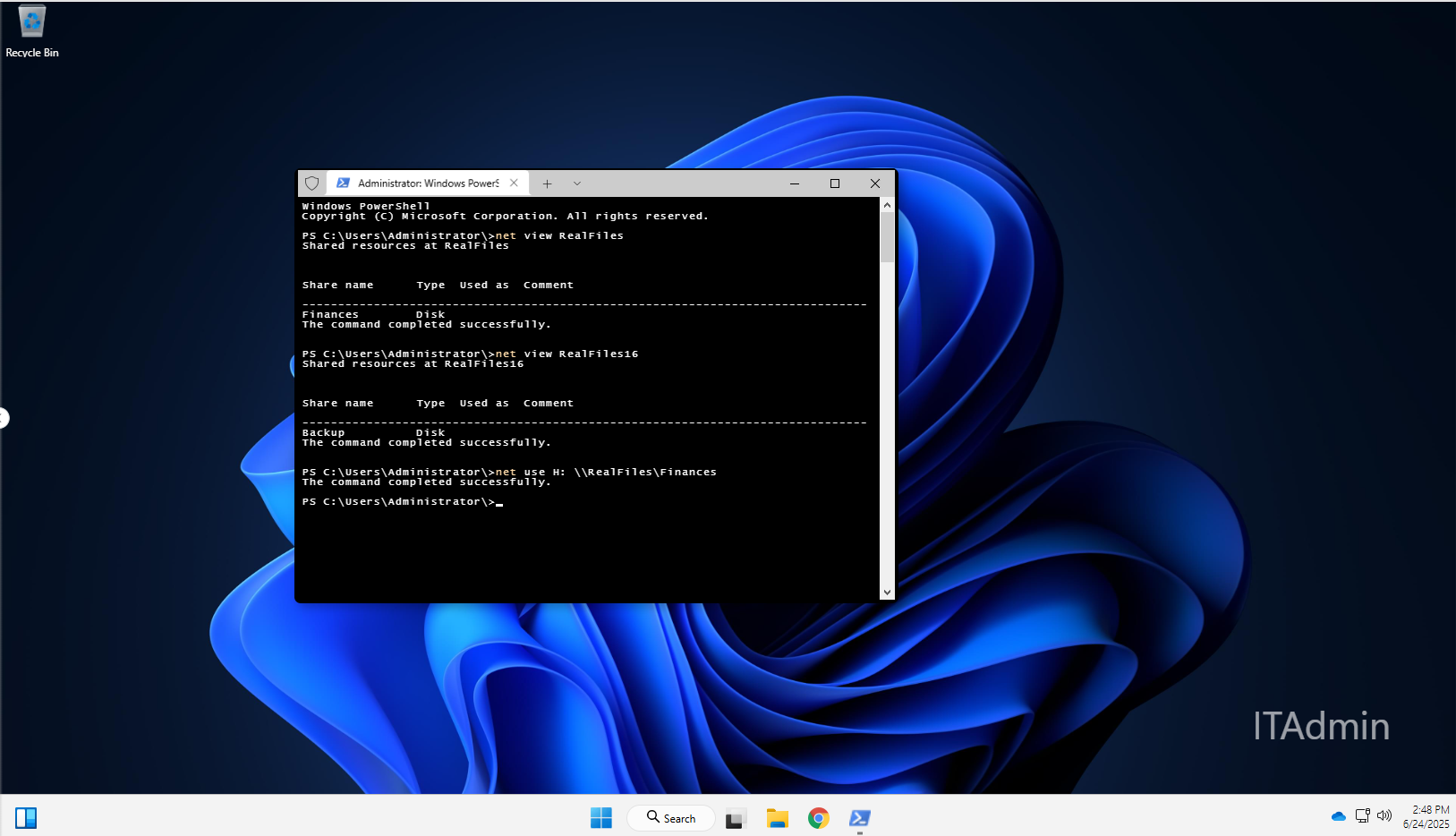
1. Results:
   * RealFiles shared folder: **Finances**
   * RealFiles16 shared folder: **Backup**

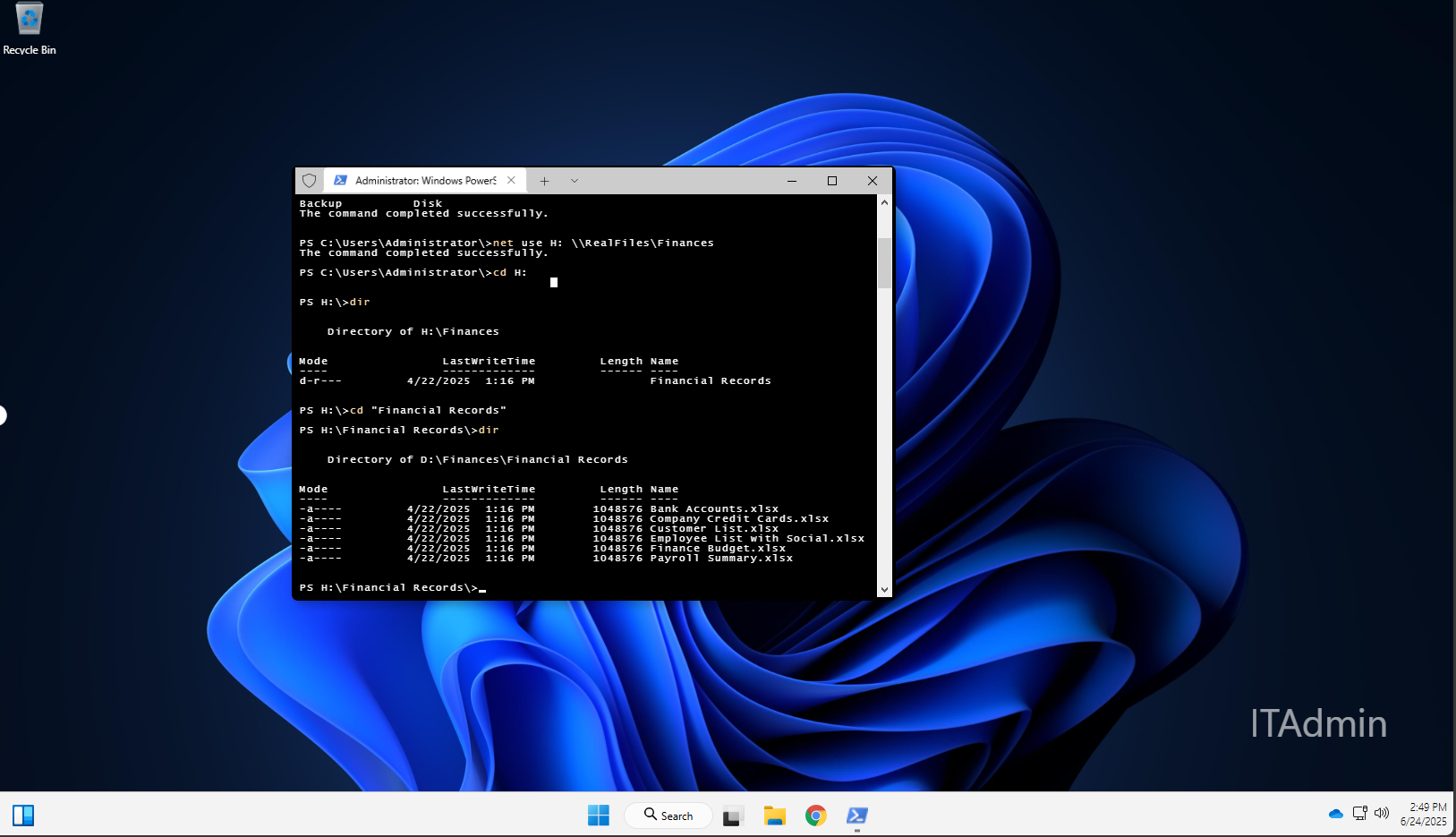
**🔗 Part 3 – Map the Network Drive**

1. Used the following command to map the shared **Finances** folder:

net use H: \\RealFiles\Finances

1. Navigated to **This PC > H: drive** in **File Explorer**.
2. Opened the **Financial Records** folder and viewed the contents.
3. Identified one of the files (example: BankAccounts.xlsx).





**📝 Conclusion:**

In this lab, I used Zenmap to identify operating systems on the network and PowerShell to enumerate shared folders. Mapping network drives and reviewing folder contents reinforced how attackers might locate sensitive data on exposed shares. This emphasizes the importance of regularly auditing network shares and OS visibility.