**🧪 Cybersecurity Portfolio**

**Hide Data Using Alternate Data Streams**

**🔍 Objective:**

To simulate a data-hiding technique used in real-world attacks by creating and managing **Alternate Data Streams (ADS)** in the Windows NTFS file system using the Command Prompt.

**🛠️ Tools & Files Used:**

* **Command Prompt**
* **Main file:** C:\HR\TERMS.docx
* **Hidden streams created:**
  + TERMS.docx:hidden.txt (manual message)
  + TERMS.docx:details.txt (copied from EMPLOYEES.csv)
* **Source file for copy:** C:\HR\EMPLOYEES.csv

**🧾 Steps Performed:**

**1. Opened Command Prompt**

* Logged into the MS10 VM as an administrator (jaime user).
* Launched Command Prompt.

**2. Created the First ADS Stream**

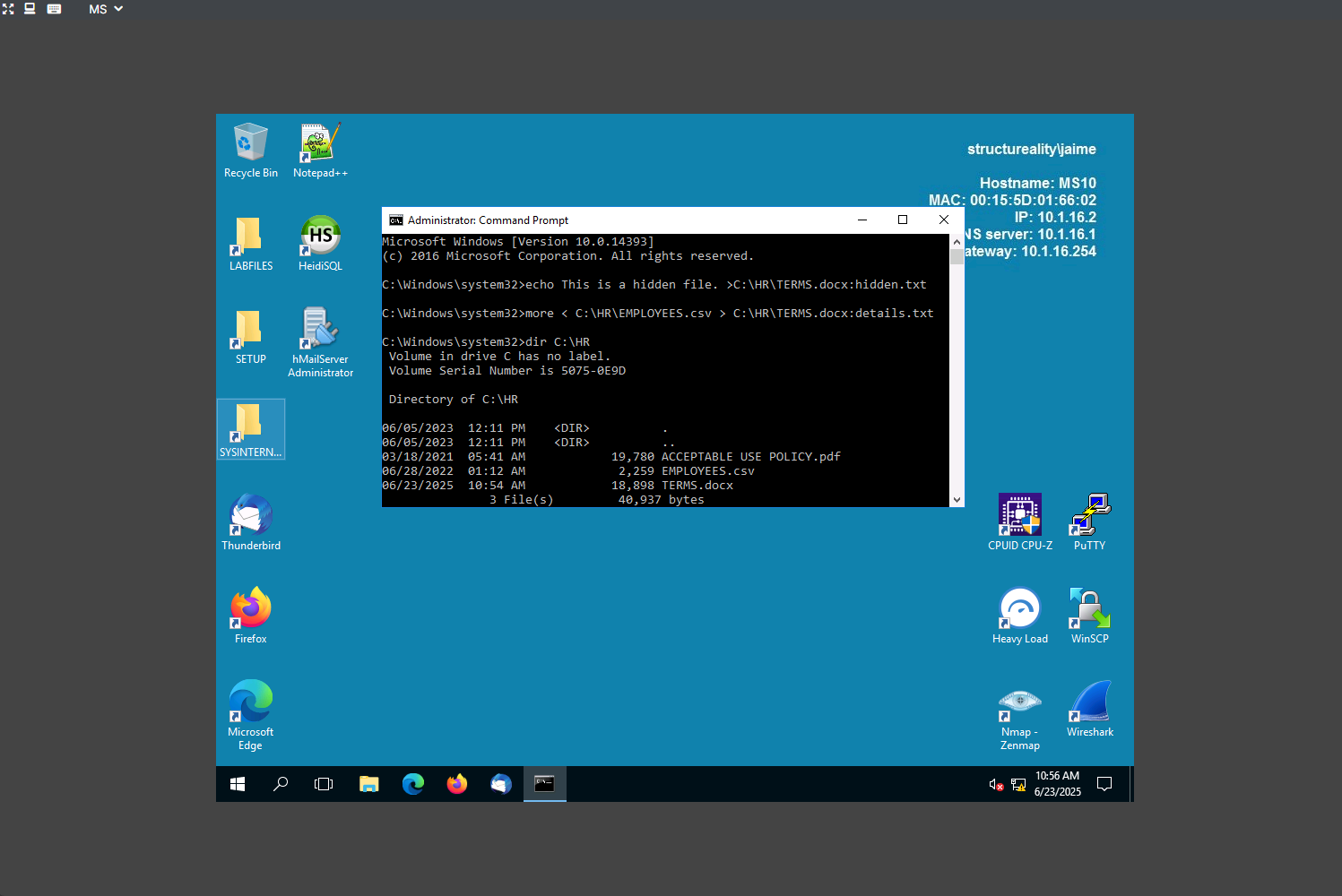
echo This is a hidden file. > C:\HR\TERMS.docx:hidden.txt

* This created an ADS named hidden.txt attached to the file TERMS.docx.

**3. Created Second ADS by Copying a File**

more < C:\HR\EMPLOYEES.csv > C:\HR\TERMS.docx:details.txt

* This hid the full contents of EMPLOYEES.csv as a stream named details.txt.



**4. Viewed Directory Listing**

dir C:\HR

* Confirmed that TERMS.docx was present but **ADS streams were not visible**, which is normal for NTFS ADS.

**5. Opened and Verified ADS Contents**

notepad C:\HR\TERMS.docx:hidden.txt

✅ Displayed: *"This is a hidden file."*

notepad C:\HR\TERMS.docx:details.txt

✅ Displayed contents identical to EMPLOYEES.csv.

**✅ Results:**

* Both alternate data streams (hidden.txt and details.txt) were successfully created and verified.
* ADS files were **not visible** in dir output, confirming their stealth nature.
* Contents were retrievable and intact using Notepad.

**🧠 Key Concepts Learned:**

* **ADS (Alternate Data Streams)** are a powerful feature of NTFS that can be used to hide data inside normal files without visibly changing them.
* ADS are invisible to basic directory listings, making them useful in both **forensics** and **threat detection** scenarios.
* Detection of ADS requires special tools or commands (e.g., dir /r, Streams.exe from Sysinternals).