CIT 485 ADVANCED CYBERSECURITY-

Lab4: Infrastructure Security and Controls

The purpose of this lab is:

Lab4-1: Data and Application Controls

After completing this lab, you will be able to:

• Implement Access Control Lists

• Create Software Restriction Policies for blacklisting and Whitelisting Applications

• Configure a Basic Firewall Rule

• Block ICMPv4 Traffic

• Configure Logging of Firewall Traffic

• Work with Windows Sandbox

Lab4-2: Improving Network Security

After completing this lab, you will be able to:

• Update Windows Defender

• Install Snort

• Download Snort Rules

• Running Snort Tool

• Create a Folder and the Rules File in the Snort Folder

• Modify the Snort Configuration File

• Re-run Snort IDS Tool

Lab4-3: Infrastructure Security

After completing this lab, you will be able to:

• Download and Install Pentbox

• Modify Proxy Server Exceptions in PLABWIN10

• Test Honeypot Functionality

**LAB INSTRUCTIONS:**

We assume you have completed lab0 and have created and activated your practice labs account. If you have not done that yet, please refer to lab0 instructions in Canvas, Week1, Lab0 section.

**1) Lab4-1: Data and Application Controls (35-points)**

LAB SUBMISSION

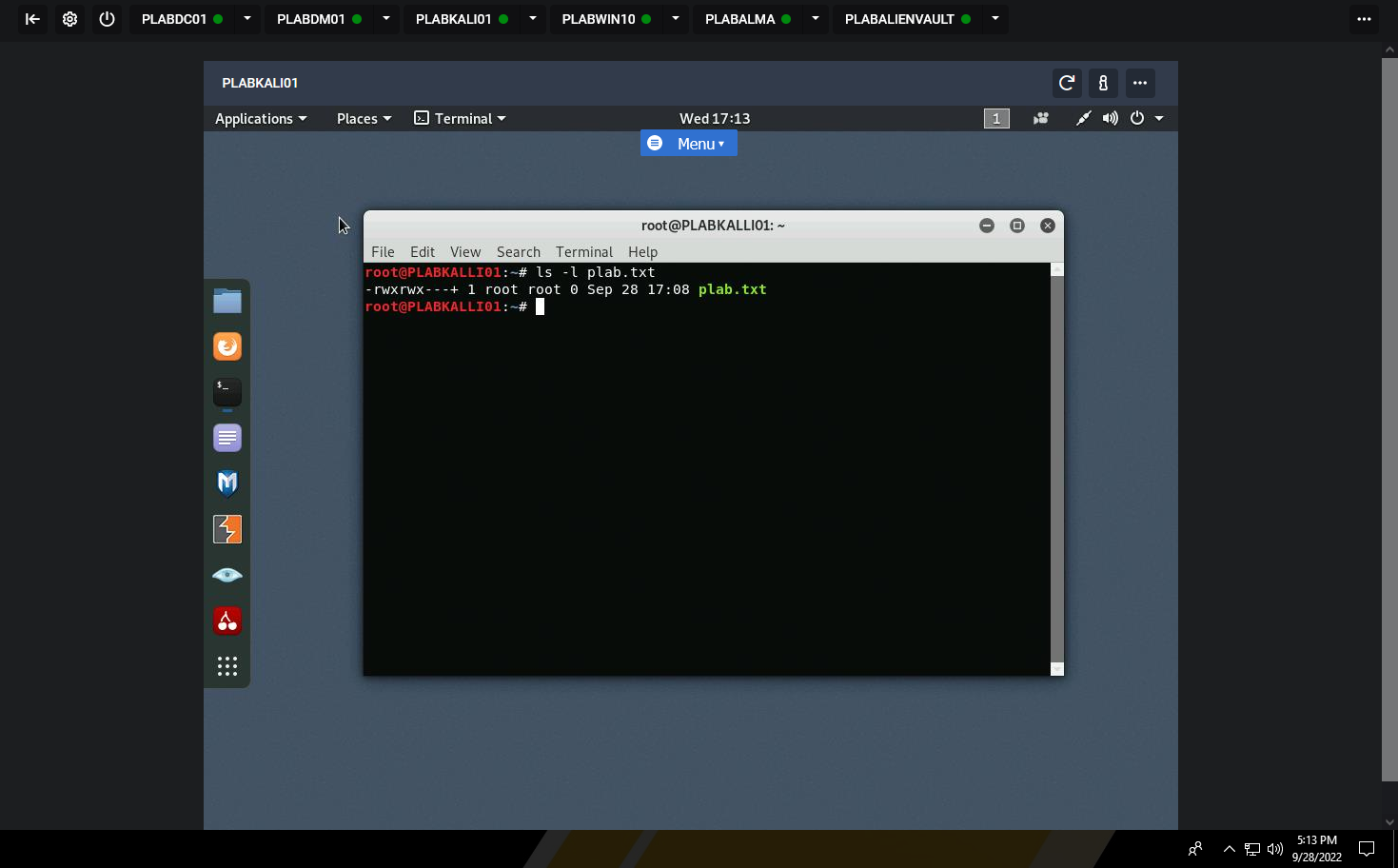
Please make sure to do all the exercises.

**Exercise 1 - Permissions**

**Task 1 - Implement the Access Control List**

Perform the Step 1 - Step 23 Implement the Access Control List and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

**Implementation of the Access Control List**

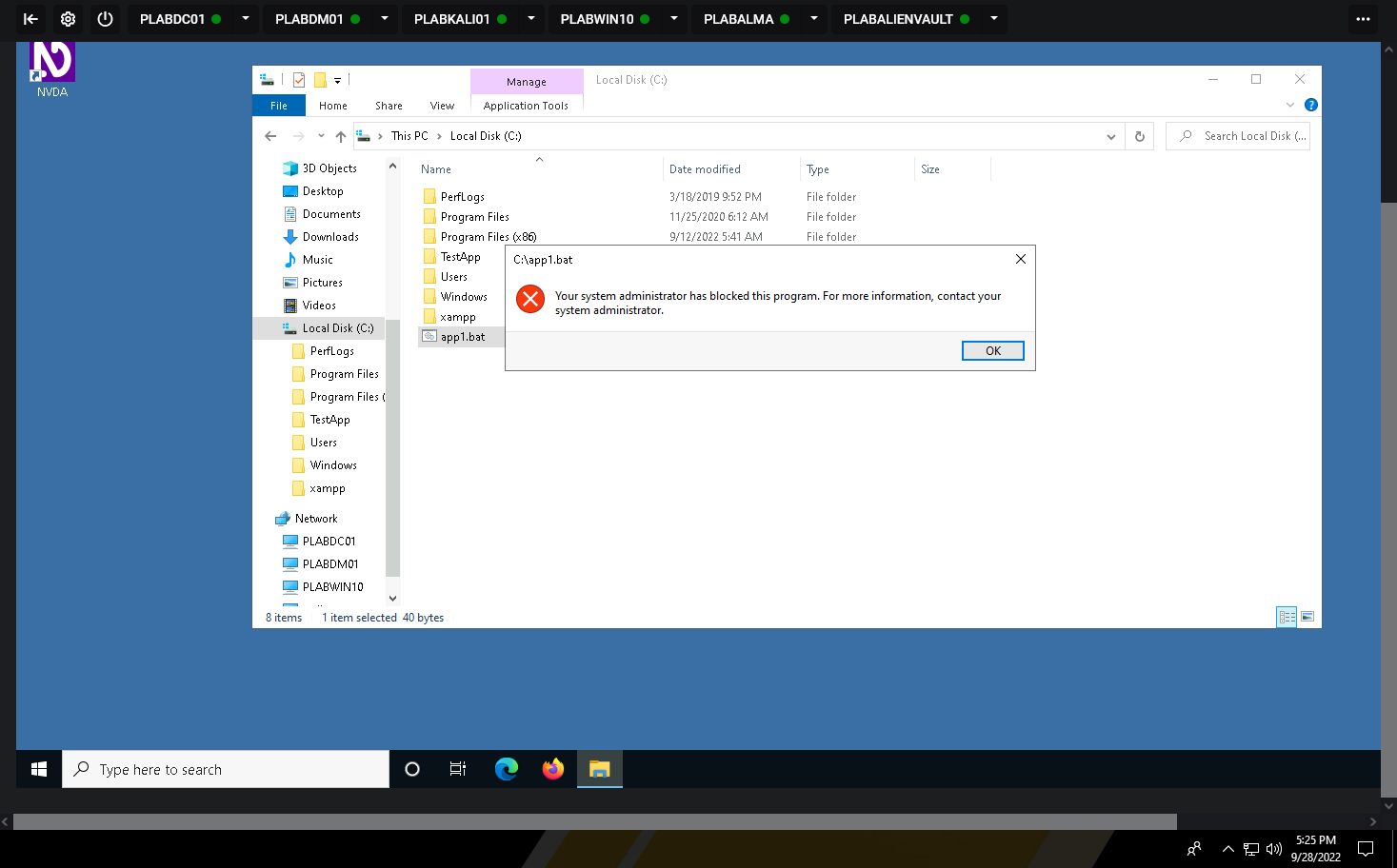
****

**Exercise 2 - Software Restriction Policies**

Task 1 - Create Software Restriction Policies for Blacklisting and Whitelisting Applications

Perform the Step 1 - Step 36 Create Software Restriction Policies for Blacklisting and Whitelisting Applications and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

**Software Restriction Policies for Blacklisting and Whitelisting Applications**

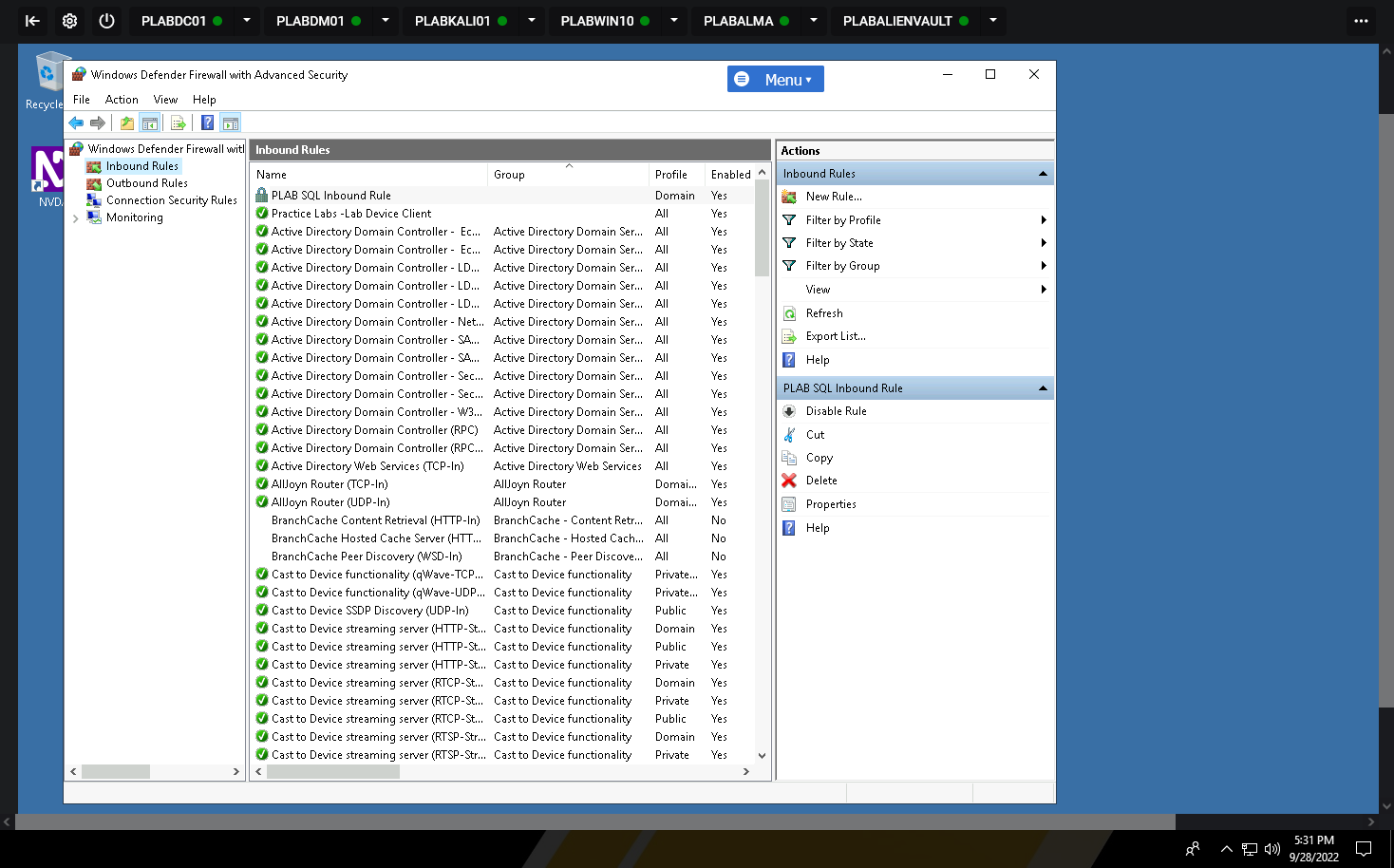
****

**Exercise 3 - Firewall**

Task 1 - Configure a Basic Firewall Rule

Perform the Step 1 - Step 21 Configure a Basic Firewall Rule and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

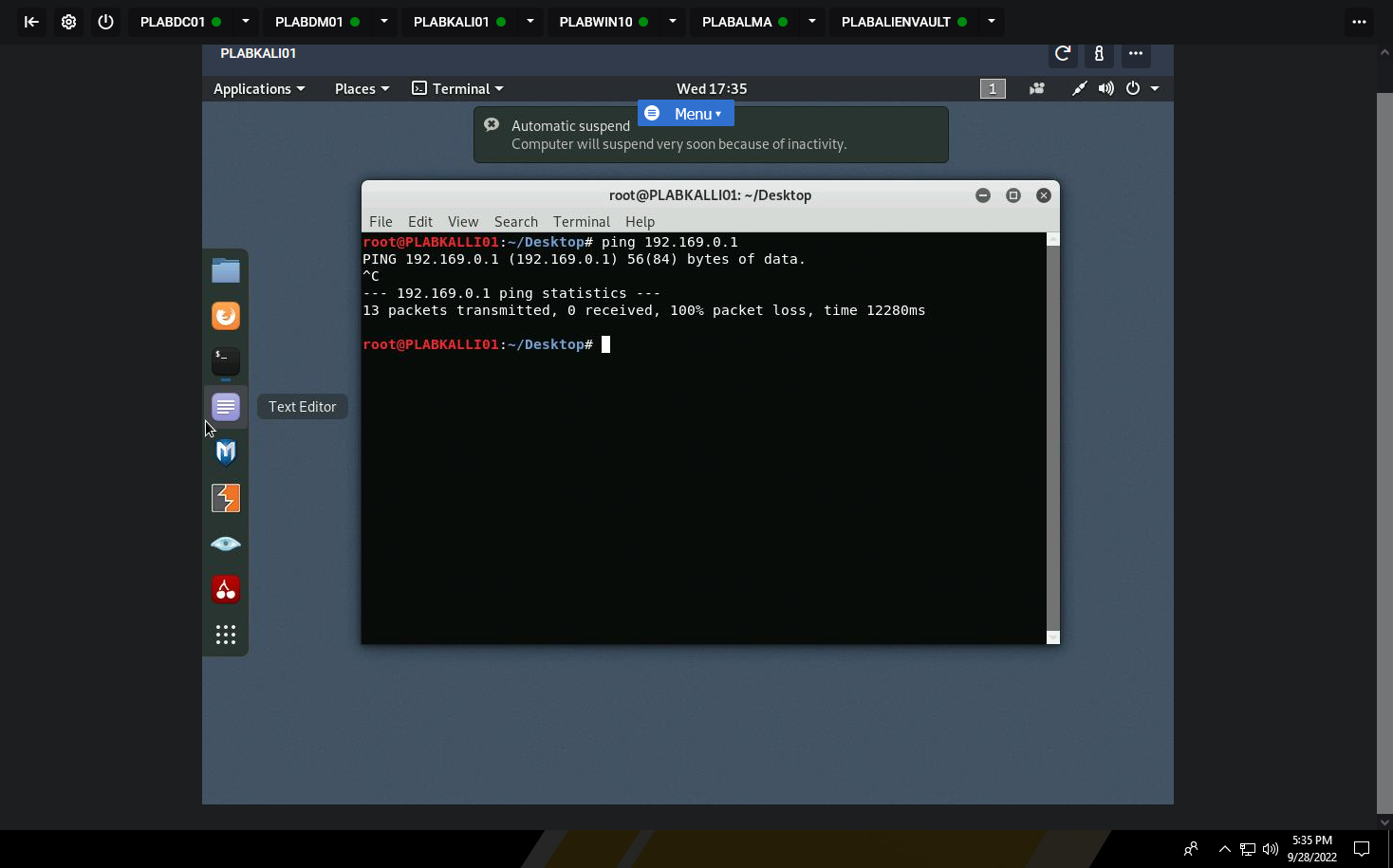
**Basic Firewall Rules**

****

**Task 2 - Block ICMPv4 Traffic**

Perform the Step 1 - Step 8 Block ICMPv4 Traffic and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

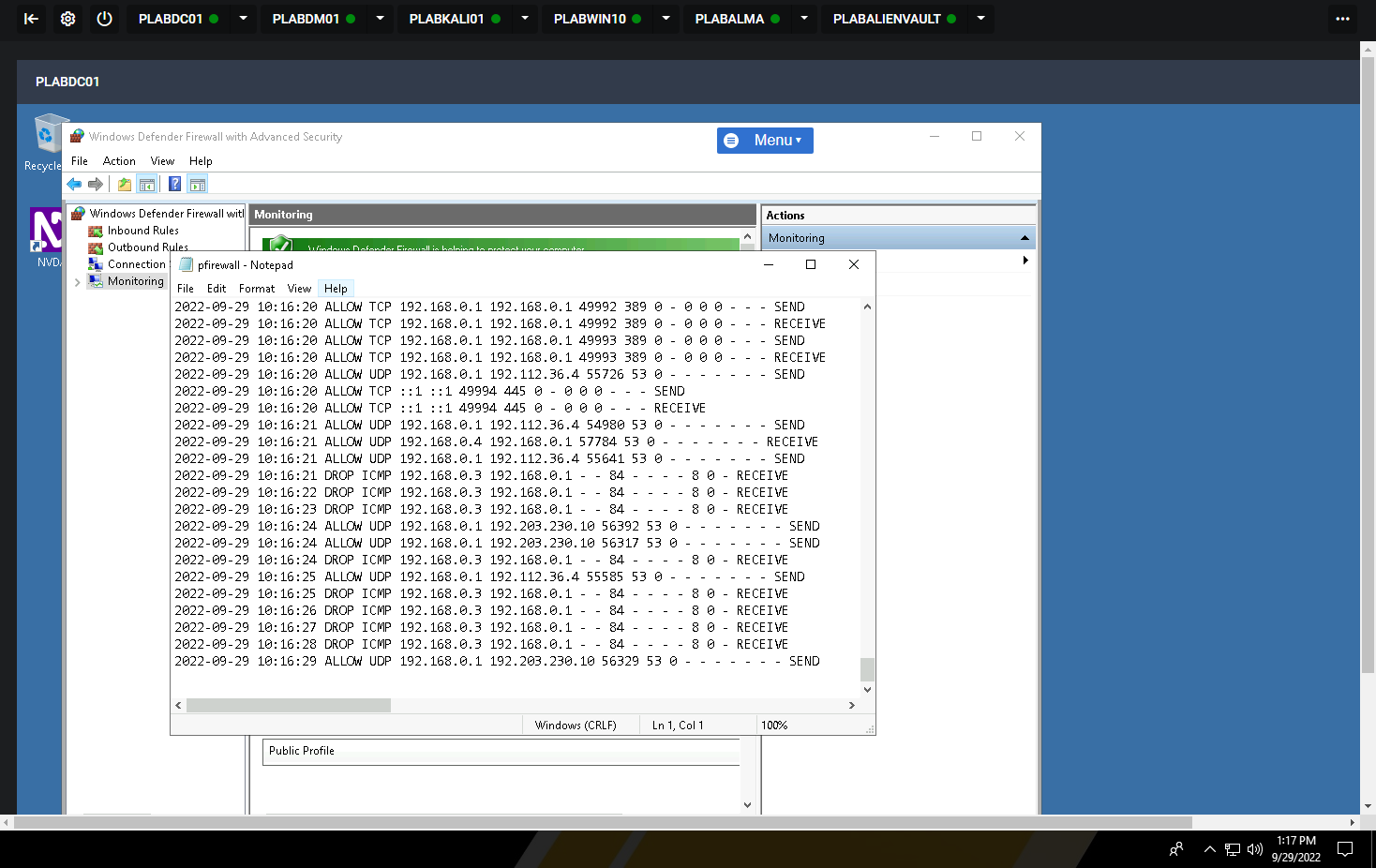
**Blocking ICMPv4 Traffic**

****

**Task 3 - Configure Logging of Firewall Traffic**

Perform the Step 1 - Step 20 Configure Logging of Firewall Traffic and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

**Configure Logging of Firewall Traffic**

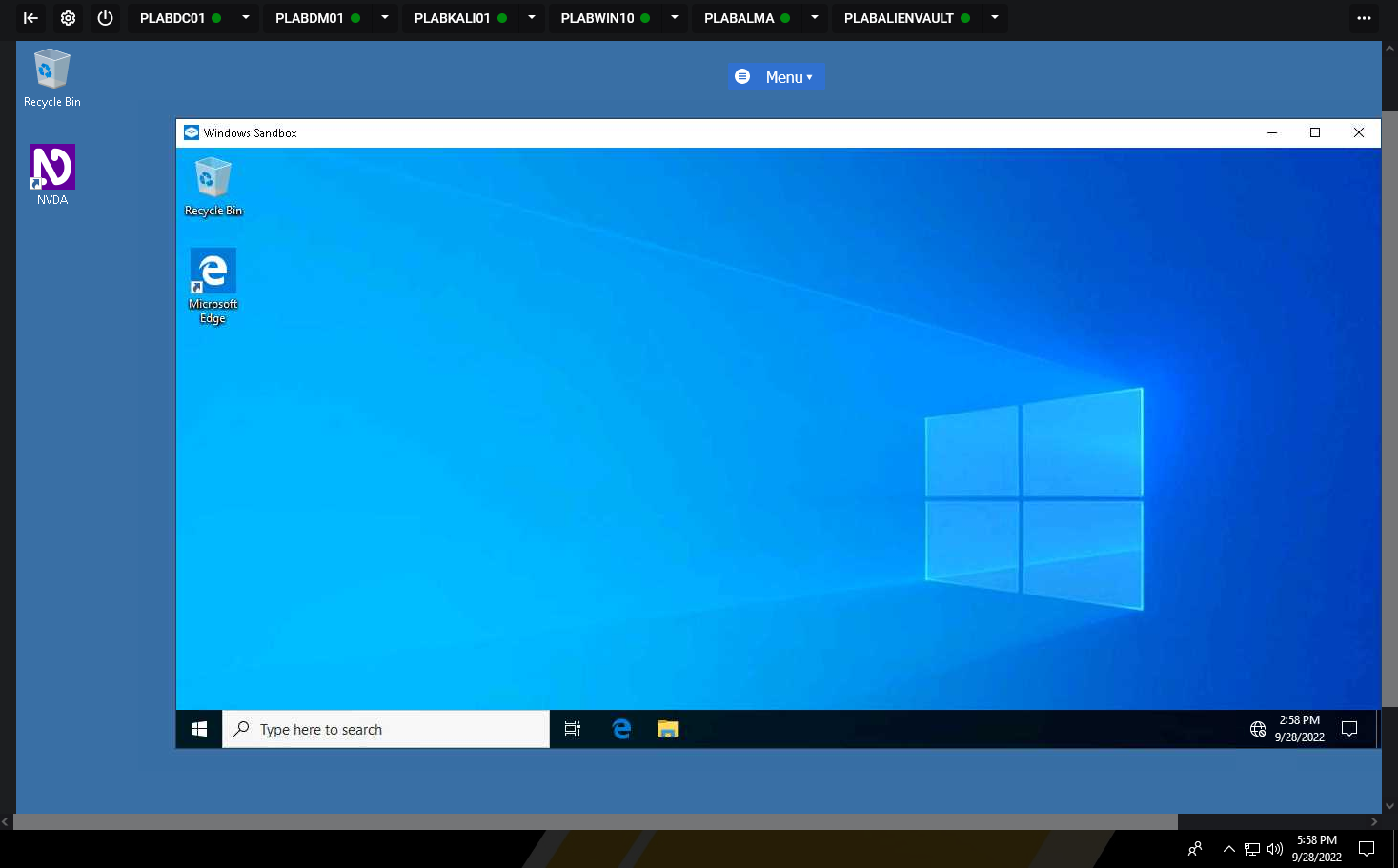


**Exercise 4 - Sandboxing**

**Task 3 - Windows Sandbox**

Perform the Step 1 - Step 14 Windows Sandbox and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded

**Sandbox**

****

• Save the report as a docx file (first name and last name: ex. Awad\_Mussa1.docx)

• Keep this file as you will upload it when you take the lab4’s quiz.