**CIT 485 ADVANCED CYBERSECURITY-**

**Lab5: Security Operation and Monitoring**

The purpose of this lab is:

**Lab5-1: Data and Application Controls**

After completing this lab, you will be able to:

* Access the Event Viewer Logs
* Review Windows Defender Firewall Logs
* Complete Logging in Linux
* Review SIEM Logs
* Review Syslog Logs

**Lab5-2: Security Information and Event Management (SIEM)**

After completing this lab, you will be able to:

* Write Rules using SIEM
* Understand the SIEM Dashboard

**Lab5-3: Scripting**

After completing this lab, you will be able to:

* Use the Find Command
* Find Files and Commands on a Linux System
* Search for a Specific Text in a File
* Search for Specific Criteria Through a File Content or a Filesystem
* Write a Simple Bash Script
* Use Commenting
* Use Parameters
* Capture User Inputs in Scripts
* Pipe the Output of one Command to the Input of Another Command
* Use the Output of one Command as Argument to Another Command
* Send Output to Both Stdout and a File

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) Lab5-1: Log Mentoring and Review (35-points)**

Lab **Submission**

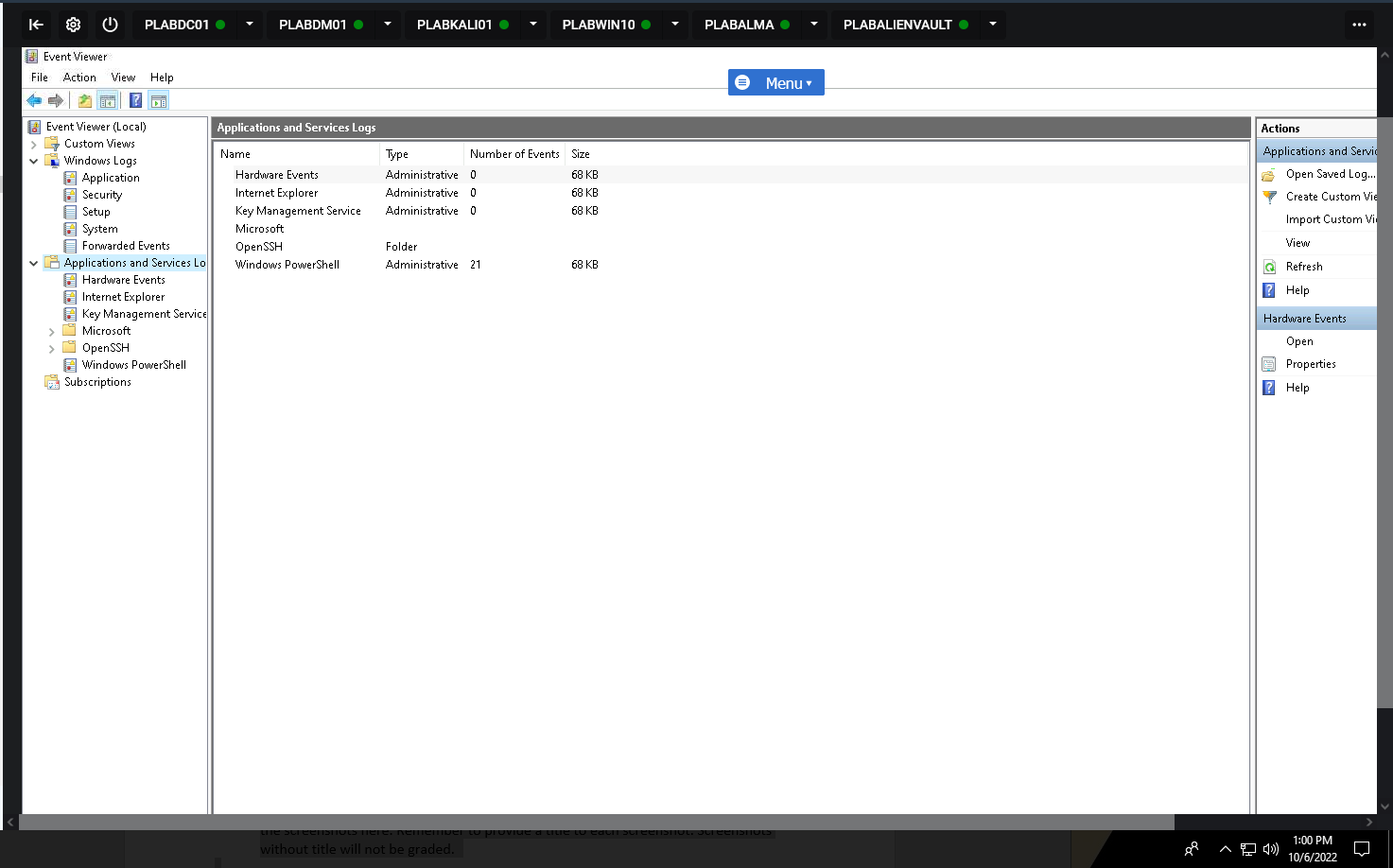
Please make sure to do all the exercises.

**Exercise 1 –Logging**

**Task 1 - Access the Event Viewer Logs**

#### **Perform the Step 1 - Step 7 Access the Event Viewer Logs and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.**

**Access the event viewer logs**



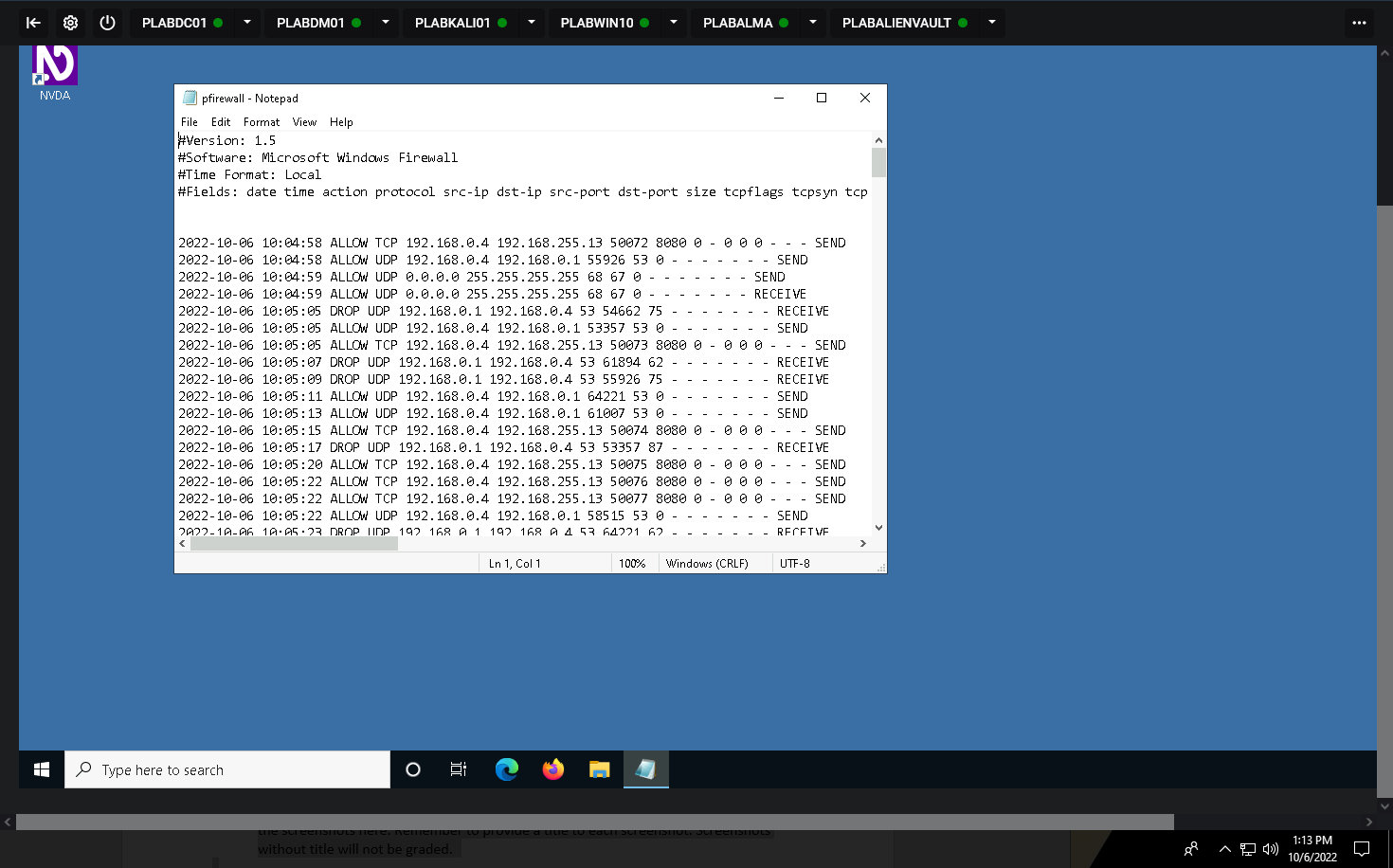
## 

## 

**Task 2 - Windows Defender Firewall Logs**

Perform the Step 1 - Step *19* Windows Defender Firewall Logs and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

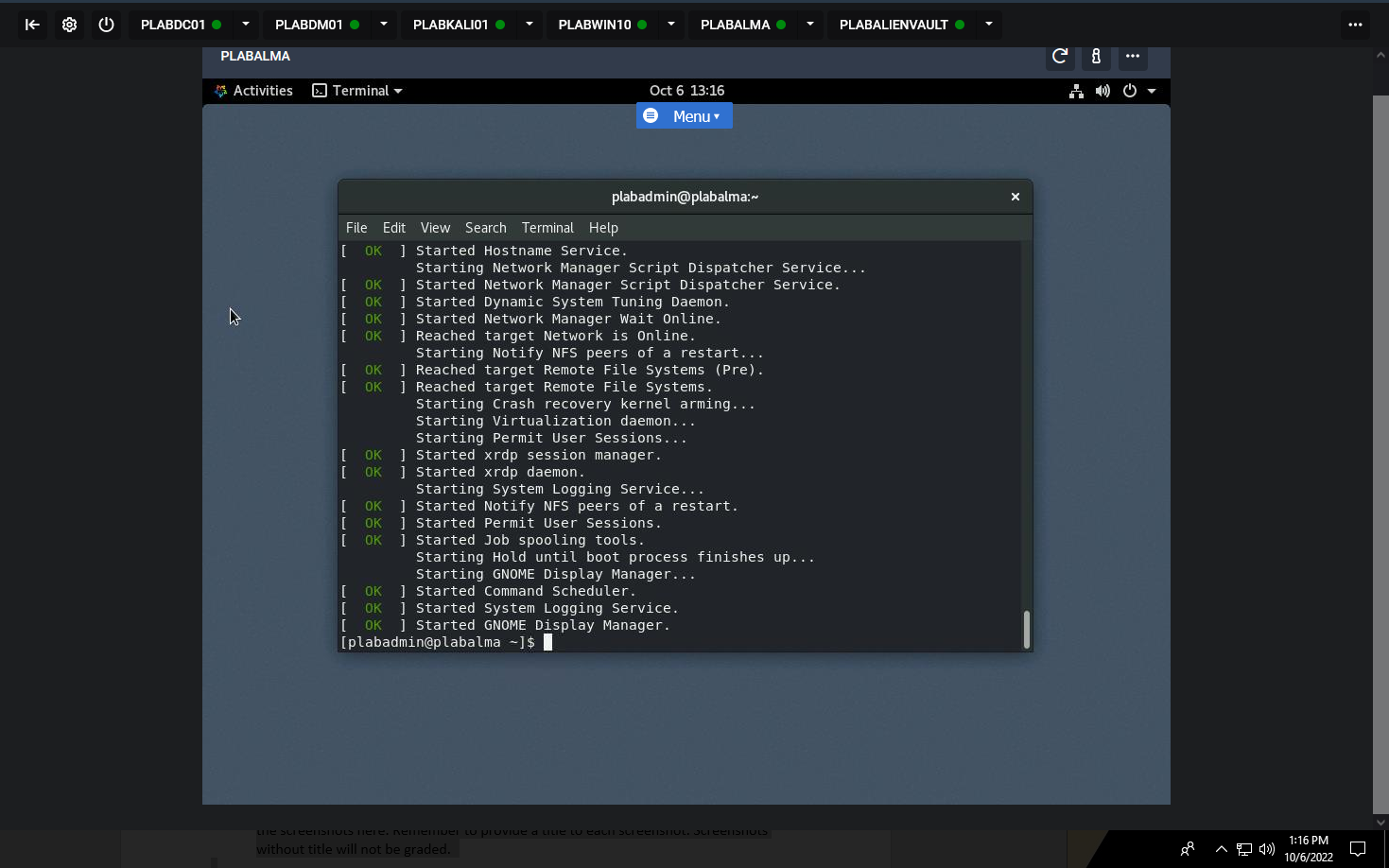
**Windows Defender Firewall Logs**

****

**Task 3 - Logging in Linux**

Perform the Step 1 - Step *7* Logging in Linux and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

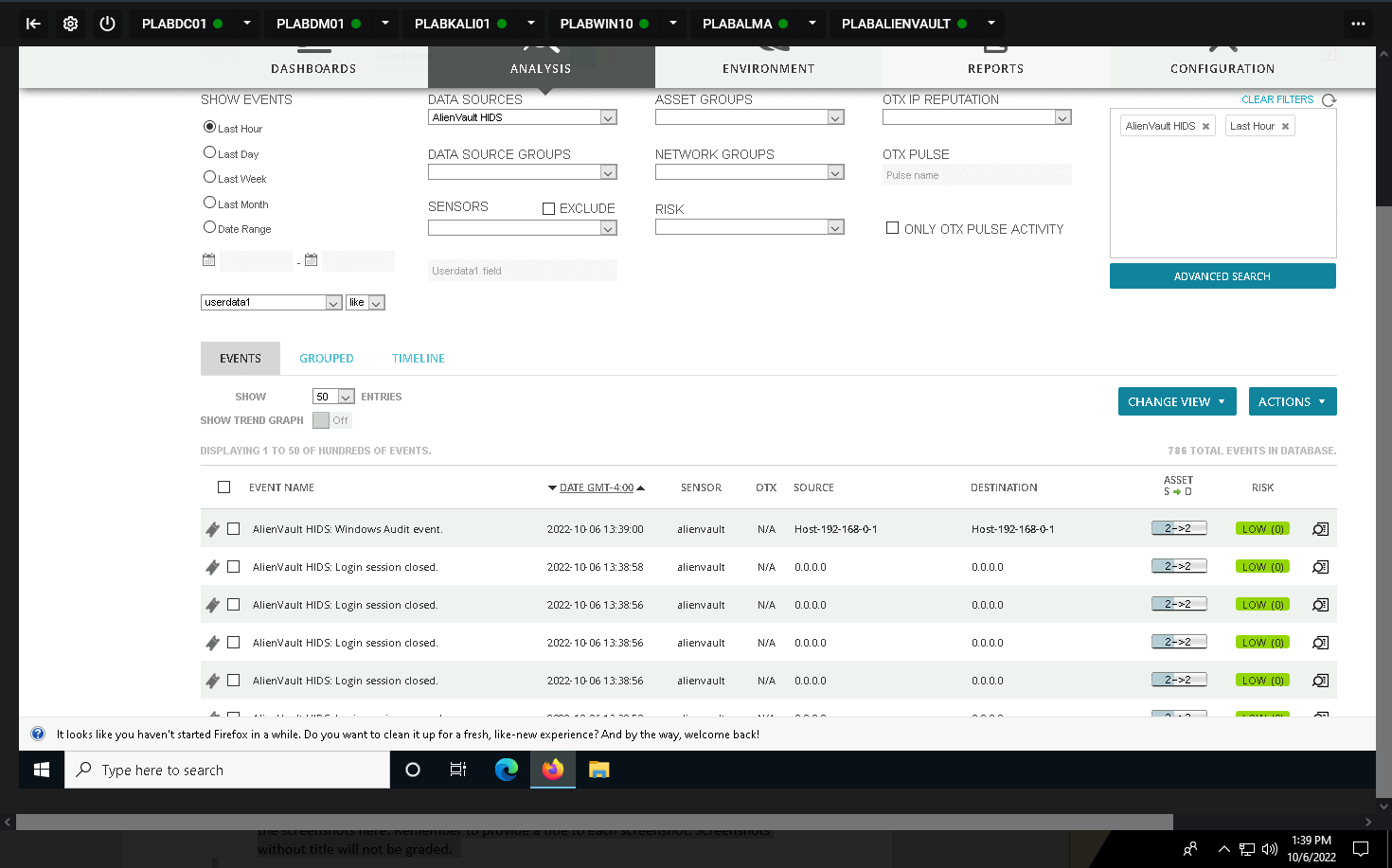
**Logging in Linux**

****

**Task 4 – SIEM Logs**

Perform the Step 1 - Step 20 SIEM Logs and copy and paste the screenshots here. Remember to provide a title to each screenshot. Screenshots without title will not be graded.

**SIEM Logs**

****

· 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 lab5’s quiz.