**Name**

**Lab # 9:**

**Exercise one:**

**Sandbox Installed**

**Graphical user interface, text, application

Description automatically generated**

**Sandbox Activated**

**A picture containing graphical user interface

Description automatically generated**

**Sandboxed browser**

**Graphical user interface, website

Description automatically generated**

**Browser Slowed down**

**Graphical user interface, application

Description automatically generated**

**Running notepad**

**Graphical user interface, application

Description automatically generated**

**Sandboxed notepad**

**Graphical user interface, application, Word

Description automatically generated**

**Q1:**

Sandbox is actually a lightweight virtual machine. It is often used by developers and researchers for testing a new software within controlled environments. It creates virtual hard drive, computer storage and memory. Sandboxie is slower because of its popularity and number of projects running on single server.

**Exercise 2:**

Q2:

We have explored how events are generated in windows and which type of event occurs.

First we open administrative tools

Graphical user interface, text, application

Description automatically generated

It shows event types and their typing plus their logs .

Application and services it contains default generated logs as shown.

Graphical user interface, text, application

Description automatically generated

It shows warning event types of warning events that occur on a certain time.

Graphical user interface, text, application

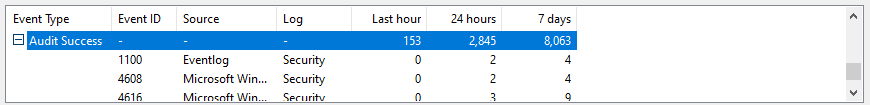
Description automatically generated

It shows error events

Graphical user interface

Description automatically generated

It shows audit success events and their time



This shows information events about application logs.

Graphical user interface, text, application

Description automatically generated

Here we show windows generated default logs. We have expanded security events that occur as shown 27,153 events occured

Graphical user interface, text, application, email

Description automatically generated

**Q3 part b of exercise3**

Exercise 3:

In this we will demonstrate how to create custom views

Graphical user interface, text, application, email

Description automatically generated

We have done settings to show our event such as logged at any time means system will capture event every time we log in. also event level and other settings now we click ok and our event gets created.

Graphical user interface, application, email

Description automatically generated

We can view our events file name as All events created here it shows 12,739 events created.

Graphical user interface, text

Description automatically generated

After that we restart our system to see if there are new events available. As you can see below 50 new events are available.

Graphical user interface, application

Description automatically generated

As you can see first is error event and second is information event and so on.

Graphical user interface, application

Description automatically generated with medium confidence