[**USING LOGS TO HELP YOU TRACK DOWN AN ISSUE IN WINDOWS**](https://github.com/Abiatchu-infinite/Module-2)

**PROCEDURE:**

**ACCESSING THE VIRTUAL MACHINE:**

* **First, we need to set the external connection**

For this, Open the **Remote Desktop Connection** in our desktop and then paste the given External **IP address** and Password.

* **Now it will connect to our virtual desktop.**

**VIEWING LOGS ON WINDOWS:**

* We have to open the **Event Viewer**, to view the logs on the window

**TASK:**

1. **LOW DISK SPACE** :
   * Go to the **Local Disk (C :)** and Search for **Size** in that Select **Gigantic** size**.**
   * In that Gigantic files , Delete **ultra\_mega\_large file** of 9.38 GB
   * Now, click on the **Run Step** in the lab.

Hence, the task to delete the large file is accomplished.

1. **CORRUPTED FILES**:
   * Go to the **Users** folder in the **Local Disk (C :)**
   * In that ,we are able to find a file called **corrupted\_file**
   * We have to **delete** that particular file
   * And then, we have to click on the **Run Step** in the lab.

Hence, the task to delete the corrupted file is accomplished.

1. **UPDATE VLC:**
   * Go to **Google** **chrome** and search for **VLC for windows**.

**(Link: https://www.videolan.org/vlc/download-windows.html)**

* + **Download** the **VLC player for 32 bit** and **install** in the computer
  + Now, again **download** the **VLC player for 64 bit** and **install** it in the computer.
  + It will **update the VLC player** from **32 bit** to **64 bit**.
  + And then, we have to click on the **Run Step** in the lab.

Hence, the task to updating the VLC player is done.

1. **END MALICIOUS PROCESSES:**
   * Open **Task Manager.**
   * Click on **More details in** Task manager.
   * In that, you are able to find the **"totaly\_not\_malicious"** task is running.
   * We have to **end the Task.**
   * And then, we have to click on the **Run Step** in the lab.

Hence, the task to end the malicious process is accomplished.

1. **FIX PERMISSIONS**:
   * Open the **Users** folder in the **Local Disk (C :)**
   * In that, open the **Temp folder**
   * There you are able to find the file called **super\_secret\_file**
   * Open the **properties** of the **super\_secret\_file**
   * Go to the **Security** in that **allows the permission for the write box** using **Edit** option.
   * And then, we have to click on the **Run Step** in the lab.

Hence, the task to fix the permission is accomplished.

|  |
| --- |
|  |