LEMUEL OKECHUKWU

VEPH/20B/CY082

TASK 20B

**SPLUNK**

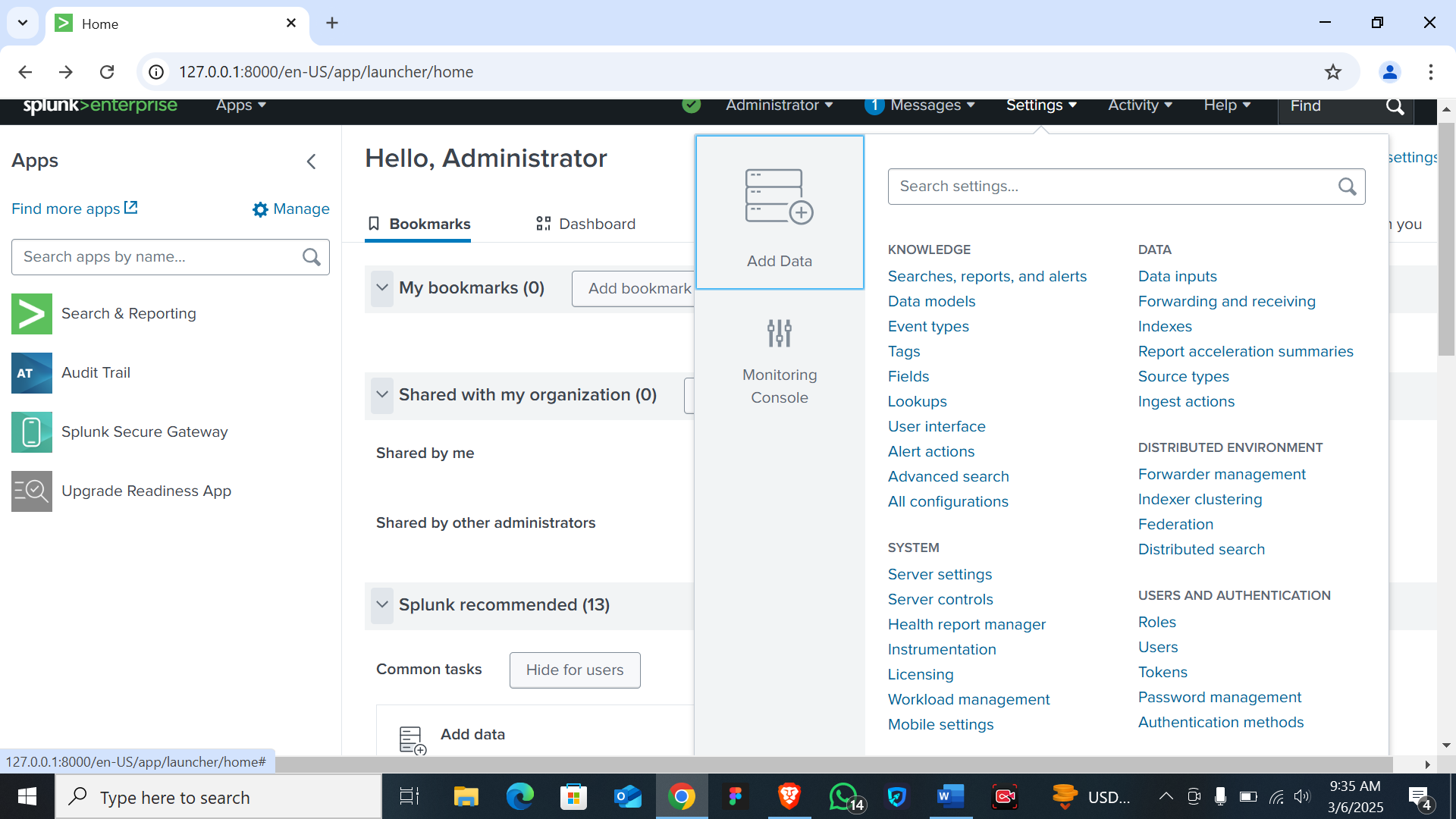
**Task 20B**: **Follow-Up Report Based on Provided Template**

Using the attached template [here](https://docs.google.com/document/d/1F-so7BUInVWznscj4ZPzk-D-_51DSSvIA4wfhzajnSc/edit?usp=sharing) , rewrite the technical report for Task 18B(**Could you provide a detailed, step-by-step guide on downloading and installing Splunk, including clearing event viewer security logs and creating a dashboard on splunk.**, ensuring all required sections are included:

* **Introduction:** Overview of the objective and methodology.
* **Procedure:** Step-by-step execution.
* **Findings:** Summary of scan results.
* **Conclusion:** Insights and security implications.

It is a security information and event management platform that collects data, analyzes and monitors their logs. It is used for threat hunting and forensic investigation. It can serve in both defensive and offensive cybersecurity. Splunk is a technology used for application management, security, and compliance, as well as business and web analytics. It is a digitized platform that assists in accessing machine-generated data, which will be useful and worthwhile for everyone.

It makes use of a forwarder, indexer and search head.



**Splunk Enterprise Installation for Windows**

1. To get started with Splunk, follow these steps:
2. First, visit the official page, <https://www.splunk.com/>, and sign up for free.
3. For the installation, run the Splunk wizard and follow the further instructions.
4. Run the installer package (.msi file) for Windows installation.
5. Enter the Splunk platform and start exploring the features.
6. After completing the installation, launch Splunk and set up your instance.
7. Follow the wizard to configure basic settings like your admin password and license agreement for premium features.
8. Now that you are in the Splunk dashboard with multiple impeccable data resource handling capabilities, use it as it suits your needs.

**Clearing Windows Event Viewer Logs**

1. **Open Event Viewer**:
   * Press Win + R, type eventvwr.msc, and press Enter to open the Event Viewer.
2. **Clear Specific Logs**:
   * Navigate to the log you want to clear (e.g., Windows Logs > Application).
   * Right-click on the log and select Clear Log.
   * Choose whether to save the log before clearing and click OK.
3. **Clear All Logs**:
   * To clear all logs, you can use a PowerShell script:

Get-EventLog -List | ForEach-Object { Clear-EventLog $\_.Log }

**Applying Advanced Search Filters in Splunk**

1. **Install the Splunk Add-On for Microsoft Windows**:
   * Download and install the Splunk Add-On for Microsoft Windows from the Splunkbase.
   * This add-on helps in collecting and parsing Windows event logs.
2. **Configure Inputs**:
   * Navigate to Settings > Data inputs in the Splunk web interface.
   * Select Windows Event Logs and click New to add a new input.
   * Configure the input to specify the event logs you want to monitor (e.g., Security, System, Application).
3. **Create Advanced Filters**:
   * To create advanced filters, edit the inputs.conf file in the local directory of the Splunk Add-On for Microsoft Windows.
   * Example of an advanced filter to whitelist specific Event IDs:
   * **[WinEventLog://Security]**
   * disabled = false
   * current\_only = true
   * start\_from = oldest
   * checkpointInterval = 5

whitelist = EventCode=4740|EventCode=4771|EventCode=4625

1. **Apply Ingest Actions**:
   * Ingest actions allow you to filter, mask, and route data at the point of ingestion.
   * Navigate to Settings > Ingest Actions in the Splunk web interface.
   * Create a new ingest action rule to filter out unnecessary verbosity from Windows event logs.
   * Example rule to filter out specific Event IDs:
   * **[ingest\_actions:windows\_event\_logs]**
   * filter = EventCode=1101 OR EventCode=1104 OR EventCode=4616

action = drop

1. **Refine Search Queries**:
   * Use Splunk's search language (SPL) to refine your event analysis.
   * Example search query to find logon failures:

index=windows sourcetype=WinEventLog:Security EventCode=4625

By following these steps, you can effectively install Splunk, clear Windows Event Viewer logs, and apply advanced search filters to refine your event analysis. This setup will help you manage and analyze your Windows event logs more efficiently.

As no scan was carried out, it could not be ascertained if there was any flaw(S), but the process was seamless.

[*"How Splunk Is Riding IT Search Toward an IPO — Tech News and Analysis"*](https://web.archive.org/web/20110820192249/http:/gigaom.com/cloud/how-splunk-is-riding-it-search-toward-an-ipo/)*. Giga OM. December 17, 2010. Archived from*[*the original*](http://gigaom.com/cloud/how-splunk-is-riding-it-search-toward-an-ipo/)*on August 20, 2011. Retrieved April 22, 2013.*