**Event Log Exercise**

Please type your answers in **red** and submit this Word Document.

------------------

1. List all of the event logs on your system. How many entries are currently in each of the logs?

Get-eventlog -list

System: 40,343

Security: 0

Application: 33,448

Windows PowerShell: 14,251

2. Look up Windows Event Logs online. What is recorded in:

a. The System Log? Information about device changes, device drivers, system changes, events, operations, and more

b. The Security Log? Records of login/logout activity along with other events specified by the system audit policy

c. The Application Log? Contains information about events that have occurred within a software application. The log includes errors and warnings as well as informational events.

For items 3-5, I am only looking for an abbreviated descriptions of the types of events.

3. Retrieve the 25 most recent events from the System Log for each entry type.

What types of events were generated for:

get-eventlog system -newest 25 -entrytype type

Error events: SQL Server PolyBase, AMDRyzenMaster, A fatal hardware error, shadow copies of

Information events: description for E…, driver management… driver package, UMDF service, system uptime, port, start type, NIC information, Miniport Nic

FailureAudit events: no matches found

SuccessAudit events: no matches found

Warning events: description for E…, command sent, disk 5 has been, bluetooth HID device, command sent, name resolution for…

4. Retrieve the 25 most recent events from the Security Log for each entry type.

What types of events were generated for:

get-eventlog security -newest 25 -entrytype type

Error events: no matches found

Information events: no matches found

FailureAudit events: an account failed to… (only 5 all together)

SuccessAudit events: Special privilages, account was success, user’s local group, credential manager, cryptographic operati...

Warning events: no matches found

5. Retrieve the 25 most recent events from the Application Log for each entry type.

What types of events were generated for:

get-eventlog application -newest 25 -entrytype

Error events: description for e…, Faulting application, storage optimizer

Information events: Successfully schedule…, offline downlever, svchost, updated windows defender, harware has changed, winlogon notification

FailureAudit events: no matches found

SuccessAudit events: no matches found

Warning events: description for E… from autoenrollment and ovrservicelauncher