IT System Security & Physical Security Lab

Exercise -1

Name: Divyam Kumar

SAPID: 500083141

Batch: B2

Question 1. Experiment- To make a list of 10 critical events that you came across in the Windows log.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S.No | Windows Log | Source | Event ID | General Info | Mitigation Steps |
| 1 | System Log | Kernel-Power | 41 | The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly | The preferred way to shut down Windows is to select Start, and then select an option to turn off or shut down the computer. |
|
|
|
|
| 2 | System Log | Service Control Manager | 7000 | The Service KMSELDI service failed to start due to the following error:  The system cannot find the file specified. | Restore system to a previous state. OR Restart the Service OR Adjust the Service Login Settings. |
|
|
|
|
| 3 | System Log | VBoxNetLwf | 12 | The driver detected an internal driver error on \Device\VBoxNetLwf | Run SFC scan. OR Update Virtual Box OR Delete .VirtualBox Folder OR Disable hardware virtalization |
|
|
|
|
|
| 4 | System Log | Event Log | 6008 | The previous system shutdown at a specific time and date was unexpected. | Check for Windows update and update to the latest one. |
|
|
| 5 | System Log | Windows Update Client | 20 | Installation Failure: Windows failed to install the following update with error 0x8024200B: Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.343.25.0). | Check your Anti-Virus as it may interfere with the system. OR Try performing an in place upgrade. OR Make sure registry is configured |
|
|
|
|
|
| 6 | Application Log | ESENT | 455 | svchost (5856,R,98) TILEREPOSITORYS-1-5-18: Error -1023 (0xfffffc01) occurred while opening logfile C:\WINDOWS\system32\config\systemprofile\AppData\Local\TileDataLayer\Database\EDB.log. | Open a CMD shell as Administrator.  c:\Windows\system32. cd config\systemprofile\AppData\Local mkdir TileDataLayer cd TileDataLayer mkdir Database |
|
|
|
|
|
| 7 | Application Log | Application Error | 1000 | It occurs when an application crashes, and we cannot launch the required program as it may unexpectedly close | Reinstall Software OR Run System File Checker scan OR Clean Boot Windows OR Scan the Registry |
|
|
|
|
|
| 8 | Application Log | .NET Runtime | 1026 | Event 1026 indicates that the problem lies with the application itself and Runtime error 1026 associated with .NET Framework mainly occurs when the framework fails or crashes while running as it was not programmed to handle properly (an “exception”) | Disable and re-enable the .NET framework OR Re-install Runtime Libraries OR Troubleshoot in Clean Boot State |
|
|
|
|
|
| 9 | Application Log | PerfNet | 2004 | Unable to open the Server service performance object. The first four bytes (DWORD) of the Data section contains the status code. | Restart Server service OR Change Server service startup type |
|
|
|
| 10 | Application Log | Firefox Default Browser Agent | 12007 | Either the component that raises this event is not installed on your local computer or the installation is corrupted | Install or repair the component on the local computer. |
|
|
|