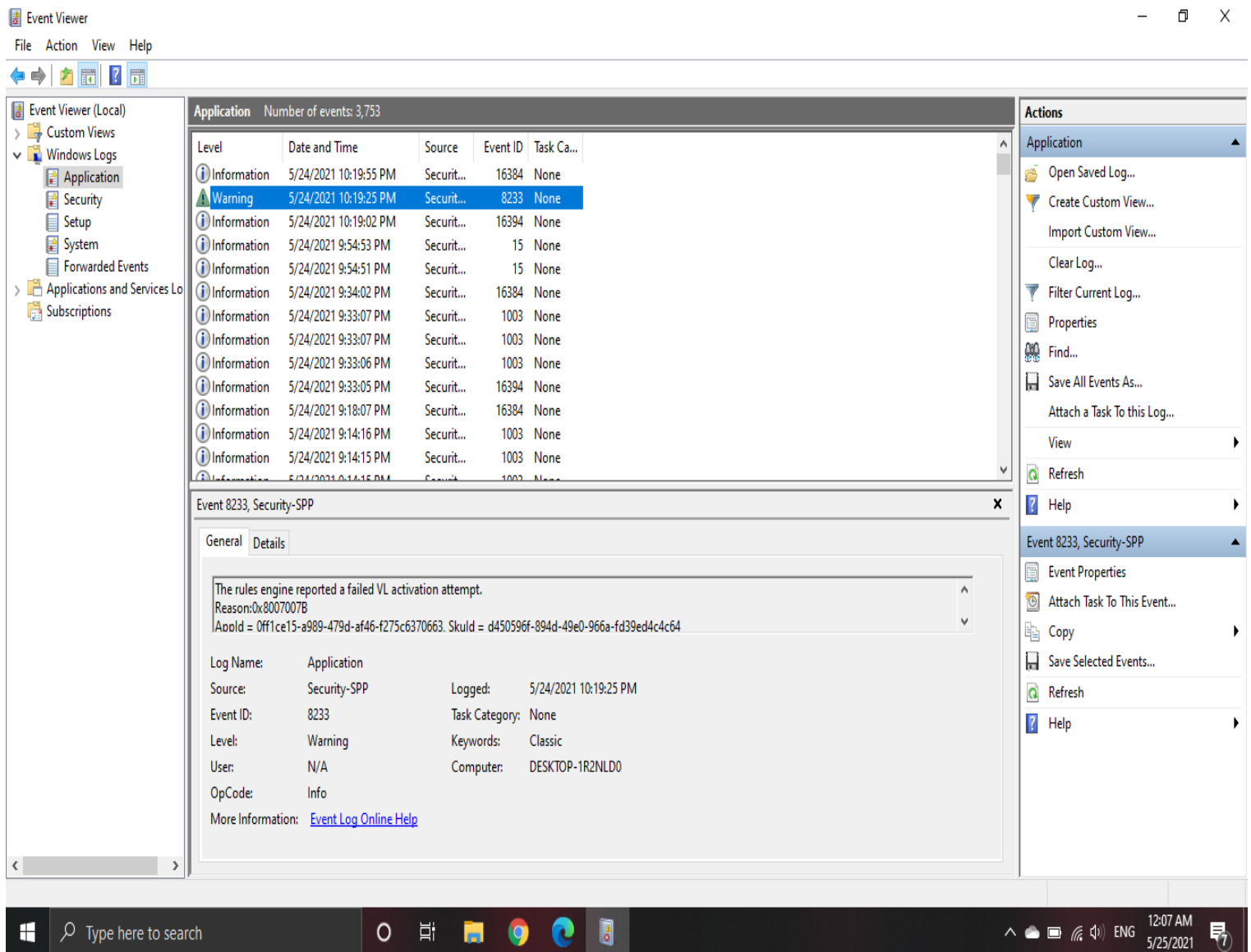


Module 2

Assignment 2

Using Logs to Help You Track Down an Issue in Windows



The logs don't have any issues pertaining to the required topics.
It only has security warnings.

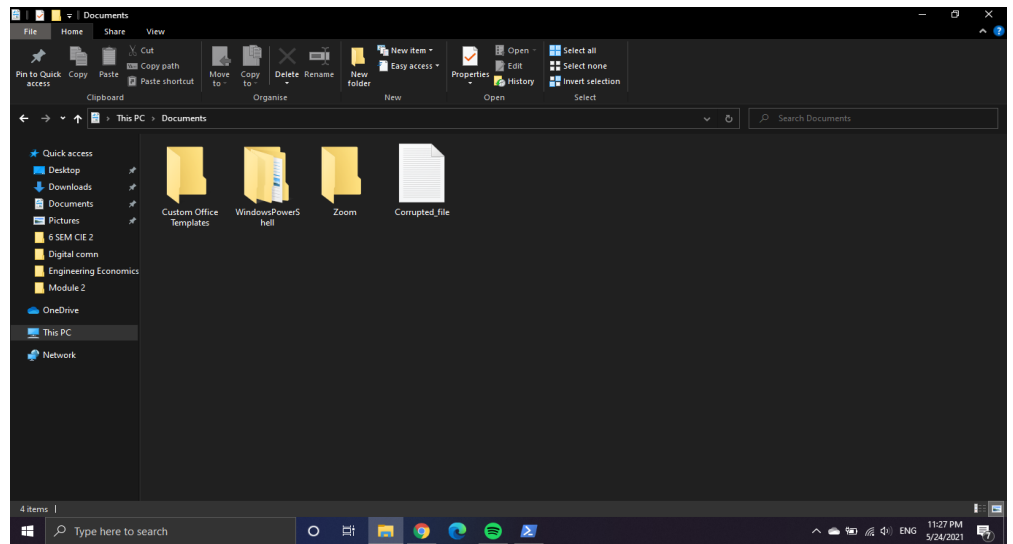
- **Low Disk Space**

If there was an event log warning about a large file that's taking up disk space. Then it can be searched from the file explorer by configuring our search. When found it can be deleted.

- **Corrupted File**

If there was a log warning about a corrupted file in the system. It can be removed by first locating it and then its deletion.

Consider a corrupted file is located in Documents. It can be removed either by using PowerShell or the direct deletion using GUI.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\user> cd C:\Users\user\Documents\
PS C:\Users\user\Documents> ls

    Directory: C:\Users\user\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          5/24/2021   9:32 PM          Custom Office Templates
d-----          5/21/2021   4:46 PM          WindowsPowerShell
d-----          4/23/2021   4:48 PM          Zoom
-a-----          5/24/2021  11:23 PM              0 Corrupted_file.txt

PS C:\Users\user\Documents> rm .\Corrupted_file.txt
PS C:\Users\user\Documents> ls

    Directory: C:\Users\user\Documents

Mode                LastWriteTime         Length Name
----                -
d-----          5/24/2021   9:32 PM          Custom Office Templates
d-----          5/21/2021   4:46 PM          WindowsPowerShell
d-----          4/23/2021   4:48 PM          Zoom

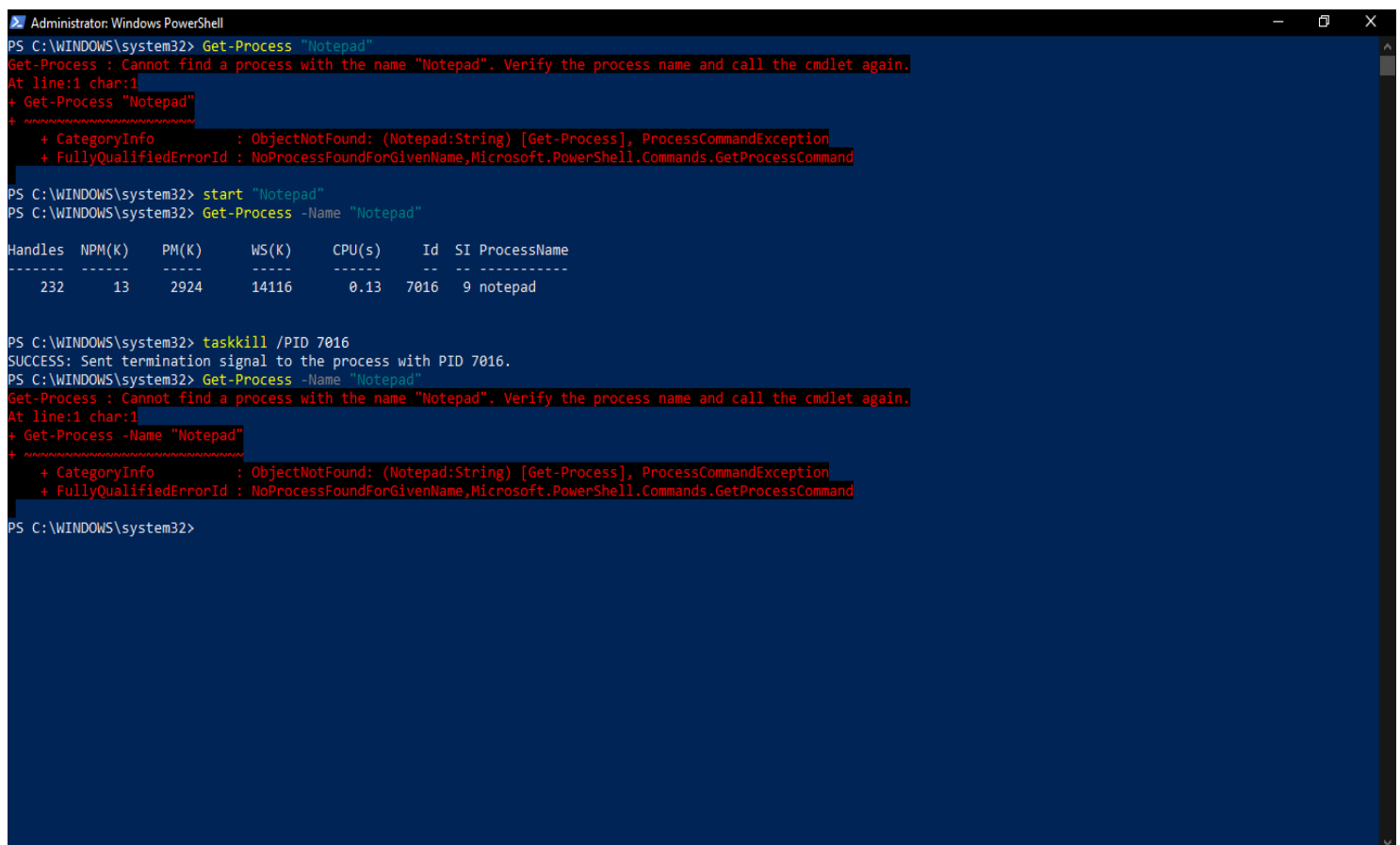
PS C:\Users\user\Documents>
```

- **Updating a Software**

If a software is outdated and there is a warning log in the event viewer. It can be updated by installing its latest version. The issue will be solved.

- **End Malicious processes**

If there is a malicious process running and causing problems to the system. It can be terminated by using the task-kill command in PowerShell.



```
PS C:\WINDOWS\system32> Get-Process "Notepad"
Get-Process : Cannot find a process with the name "Notepad". Verify the process name and call the cmdlet again.
At line:1 char:1
+ Get-Process "Notepad"
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Notepad:String) [Get-Process], ProcessCommandException
+ FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand

PS C:\WINDOWS\system32> start "Notepad"
PS C:\WINDOWS\system32> Get-Process -Name "Notepad"

Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName
-----
232 13 2924 14116 0.13 7016 9 notepad

PS C:\WINDOWS\system32> taskkill /PID 7016
SUCCESS: Sent termination signal to the process with PID 7016.
PS C:\WINDOWS\system32> Get-Process -Name "Notepad"
Get-Process : Cannot find a process with the name "Notepad". Verify the process name and call the cmdlet again.
At line:1 char:1
+ Get-Process -Name "Notepad"
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Notepad:String) [Get-Process], ProcessCommandException
+ FullyQualifiedErrorId : NoProcessFoundForGivenName,Microsoft.PowerShell.Commands.GetProcessCommand

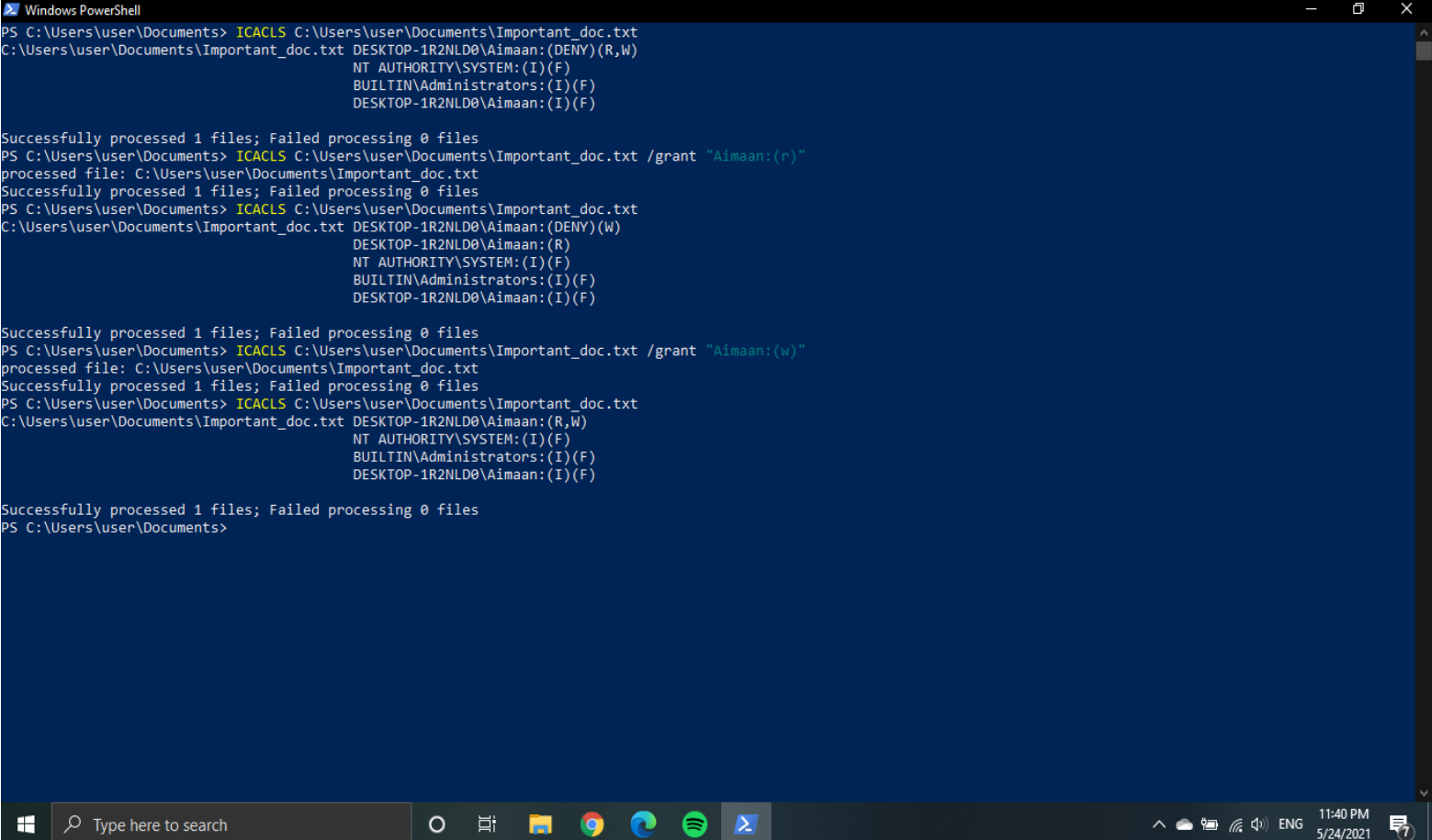
PS C:\WINDOWS\system32>
```

Since there was no error log in my laptop let's consider Notepad as our malicious process.

We first get the Process ID(PID) using the Get-Process command. The process can be terminated using its PID along with the taskkill command. The process is then terminated. Similar steps can be followed to end any such process.

- **Fix Permissions**

Consider an important document being denied crucial permissions. It can be fixed in the following way.



```
Windows PowerShell
PS C:\Users\user\Documents> ICACLS C:\Users\user\Documents\Important_doc.txt
C:\Users\user\Documents\Important_doc.txt DESKTOP-1R2NLD0\Aimaan:(DENY)(R,W)
NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administrators:(I)(F)
DESKTOP-1R2NLD0\Aimaan:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\Users\user\Documents> ICACLS C:\Users\user\Documents\Important_doc.txt /grant "Aimaan:(r)"
processed file: C:\Users\user\Documents\Important_doc.txt
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\user\Documents> ICACLS C:\Users\user\Documents\Important_doc.txt
C:\Users\user\Documents\Important_doc.txt DESKTOP-1R2NLD0\Aimaan:(DENY)(W)
DESKTOP-1R2NLD0\Aimaan:(R)
NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administrators:(I)(F)
DESKTOP-1R2NLD0\Aimaan:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\Users\user\Documents> ICACLS C:\Users\user\Documents\Important_doc.txt /grant "Aimaan:(w)"
processed file: C:\Users\user\Documents\Important_doc.txt
Successfully processed 1 files; Failed processing 0 files
PS C:\Users\user\Documents> ICACLS C:\Users\user\Documents\Important_doc.txt
C:\Users\user\Documents\Important_doc.txt DESKTOP-1R2NLD0\Aimaan:(R,W)
NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administrators:(I)(F)
DESKTOP-1R2NLD0\Aimaan:(I)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\Users\user\Documents>
```

Initially the user was denied Read & Write permissions to the document.

It was fixed by granting the permissions.

The ICACLS command along with the path gives information about the permissions.