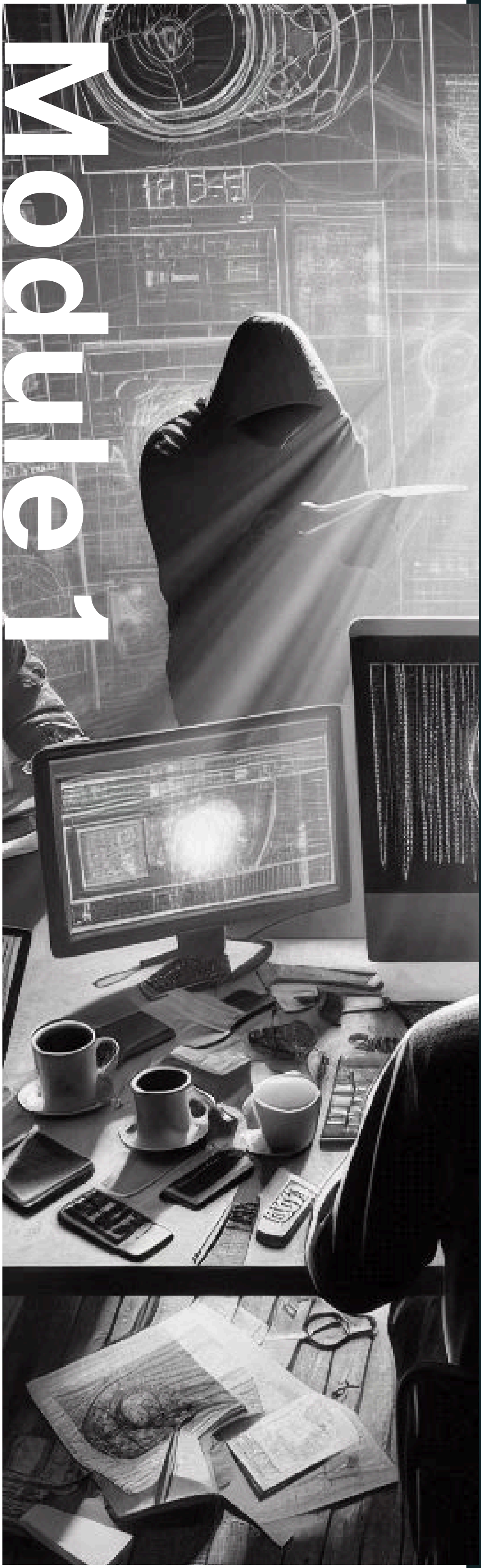


HACKER ACADEMY

External USB Alert System Report

Report By :

Keerthi TR

Approved By :

Ayush Singh

INDEX

Introduction

The objective of this lab is to create a process in a Windowsbased operating system to detect and respond to the connection of an external device, such as a USB drive, to the system. This aims to develop practical skills in incident detection, evidence collection, documentation, and notification processes, which are crucial for effective cyber security incident handling and response and will be helpful in real-world problems and daily work activities in an organization.

Technical Analysis

Affected Systems and Data

- Windows 11 in Base System
- No specific data loss was detected

Evidence Source and Analysis

- Windows Event Viewer
- Windows System Settings
- Screenshots captured during Incident analysis
- Analysis includes the problem because the notifications were not turned ON.

Analysis

1 USB is inserted into the system but no alert is generated for the same

2 In system settings the Auto Play options are checked and the notifications are turned OFF.

3 For additional cross checking use Windows Event Viewer to get the log details when USB is connected.

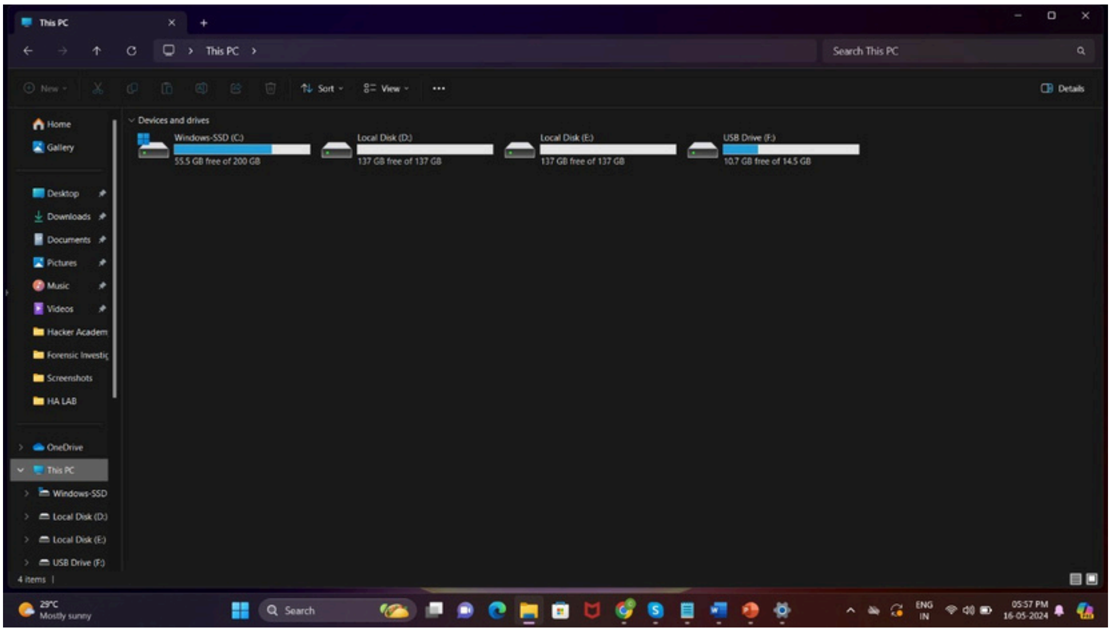
Technical Timeline

• 16-05-2024/05:57 PM – Initial connection made from an external device (USB)
• 16-05-2024/06:05 PM - Investigation started as to understand why no alert is enabled.
•16-05-2024/06:40 PM- Cross checking in Windows logs
•16-05-2024/06:48 PM - Windows settings is opened to check whether notifications are enabled
•16-05-2024/06:52 PM- Incident handling completed and alert is enabled.

Tools Used

- **Windows 11 as base Operating System**
- **Windows Event Viewer**

Identification



Devices and drives

Windows-SSD (C:)
55.5 GB free of 200 GB

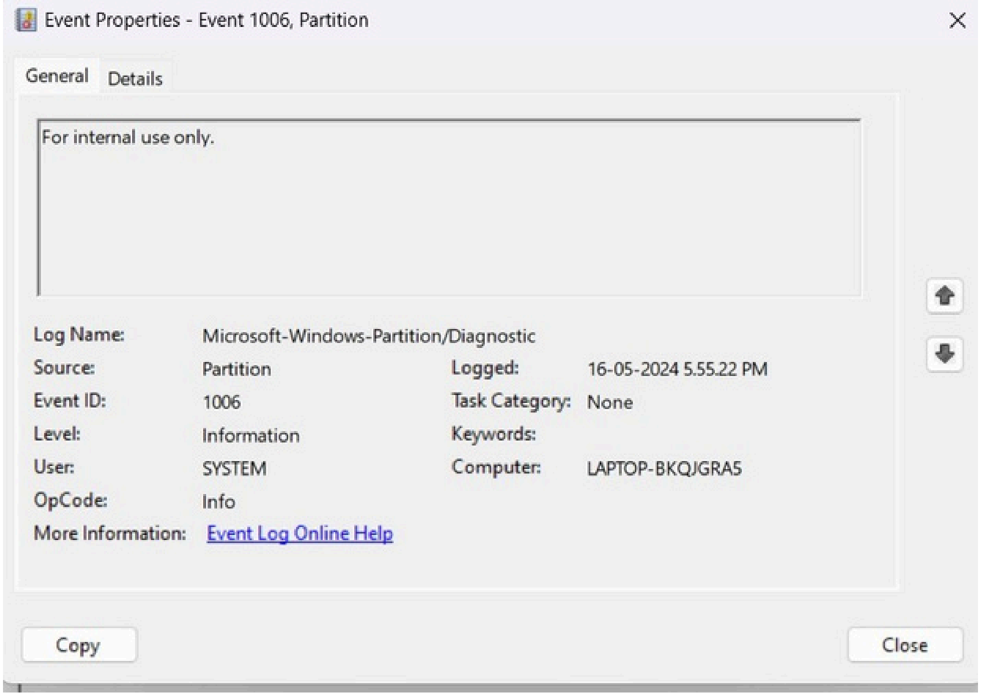
Local Disk (D:)
137 GB free of 137 GB

Local Disk (E:)
137 GB free of 137 GB

USB Drive (F:)
10.7 GB free of 14.5 GB

Fig: External USB is connected but no notification is detected

In this image we can see that when external device USB is connected there was no alert generated but if we go to the THIS PC, we can see that USB Drive (F:) is displayed there.

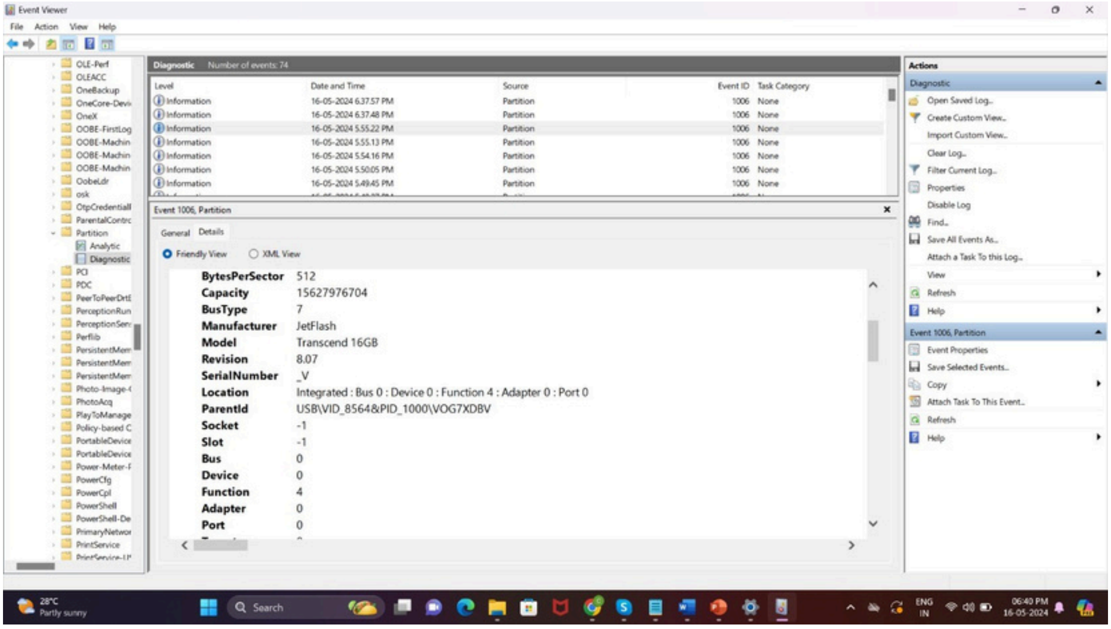


Event Properties - Event 1006, Partition

For internal use only.

Log Name: Microsoft-Windows-Partition/Diagnostic
Source: Partition
Logged: 16-05-2024 5.55.22 PM
Event ID: 1006
Task Category: None
Level: Information
Keywords:
User: SYSTEM
Computer: LAPTOP-BKQJGRA5
OpCode: Info
More Information: Event Log Online Help

Fig: When USB is connected a log with event ID 1006 is created
Troubleshooting steps include disconnecting the USB and trying to connect it once again to check whether it is a onetime error or not.



Diagnostic Number of events: 74

Level	Date and Time	Source	Event ID	Task Category
Information	16-05-2024 6.37.57 PM	Partition	1006	None
Information	16-05-2024 6.37.48 PM	Partition	1006	None
Information	16-05-2024 5.55.22 PM	Partition	1006	None
Information	16-05-2024 5.55.13 PM	Partition	1006	None
Information	16-05-2024 5.54.16 PM	Partition	1006	None
Information	16-05-2024 5.50.05 PM	Partition	1006	None
Information	16-05-2024 5.49.45 PM	Partition	1006	None

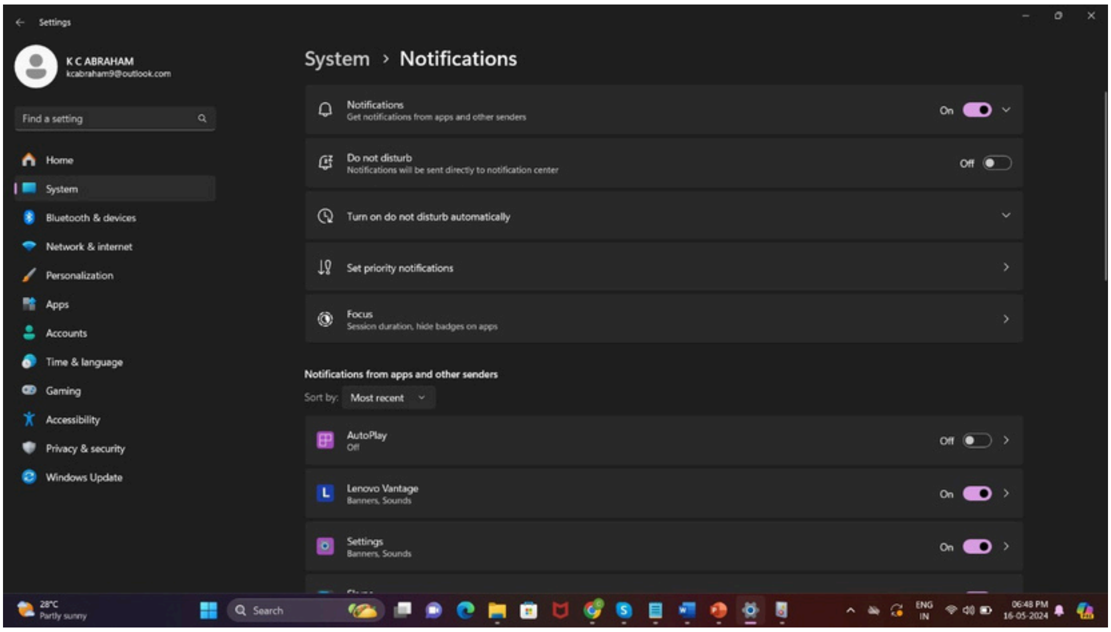
Event 1006, Partition

General Details

● Friendly View ○ XML View

```
BytesPerSector  512
Capacity        15627976704
BusType         7
Manufacturer    JetFlash
Model           Transcend 16GB
Revision        8.07
SerialNumber    _V
Location        Integrated : Bus 0 : Device 0 : Function 4 : Adapter 0 : Port 0
ParentId        USB\VID_8564&PID_1000\VOG7XDBV
Socket          -1
Slot            -1
Bus             0
Device          0
Function        4
Adapter         0
Port            0
```

Fig: Detailed Log analysis shows that USB is connected
From the above two images we can find that when USB is connected to the system an event log with Event ID 1006 is generated in Applications and Services Logs\Microsoft\Windows\Partition. We can see the details of the USB that is connected that is it is a 16GB pen drive from Jet Flash manufacturer with model name as Transcend 16GB.



System › Notifications

Notifications
Get notifications from apps and other senders
On

Do not disturb
Notifications will be sent directly to notification center
Off

Turn on do not disturb automatically

Set priority notifications

Focus
Session duration, hide badges on apps

Notifications from apps and other senders

Sort by: Most recent

AutoPlay
Off
Off

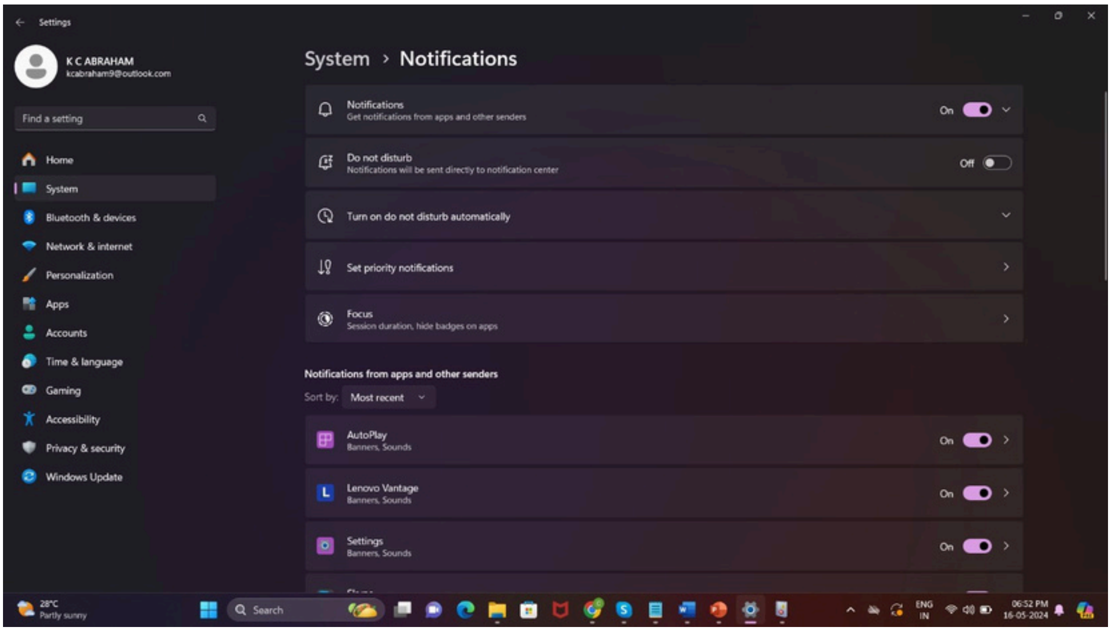
Lenovo Vantage
Banners, Sounds
On

Settings
Banners, Sounds
On

Fig: System notifications settings shows that the AutoPlay option is turned OFF

From this image we can see that for external device to show alert the AUTO PLAY settings should be turned on to see the alert when an external device is connected to the system. With AutoPlay, you don't have to open the same app or reselect preferences every time you plug in a certain device. You will only see an AutoPlay notification when you have AutoPlay turned on and connect a device, media, or content that you chose Choose a default (default) or Ask me every time as its AutoPlay default.

Mitigation



System › Notifications

Notifications
Get notifications from apps and other senders — On

Do not disturb
Notifications will be sent directly to notification center — Off

Turn on do not disturb automatically

Set priority notifications

Focus
Session duration, hide badges on apps

Notifications from apps and other senders

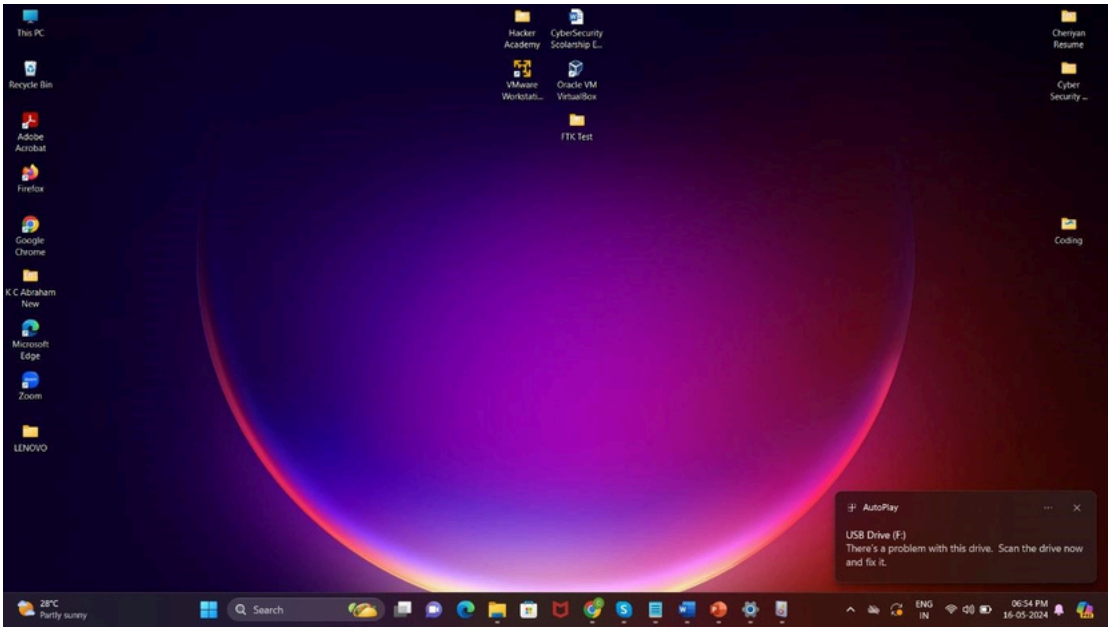
Sort by: Most recent

AutoPlay
Banners, Sounds — On

Lenovo Vantage
Banners, Sounds — On

Settings
Banners, Sounds — On

Fig: AutoPlay notification is turned ON



AutoPlay

USB Drive (F:)
There's a problem with this drive. Scan the drive now and fix it.

Fig: Notification when Pen Drive is connected

From the above images we can find that when Auto Play notification is turned ON whenever an external device is connected then an alert is generated and the user will get to know about it.

Lesson Learnt

- The lab demonstrated that system settings, such as AutoPlay notifications for external devices, need to be properly configured to ensure effective incident detection and alerting. Failure to enable relevant settings can lead to incidents going unnoticed, increasing the potential for data breaches or other security risks.
- The lab exercise highlighted the significance of monitoring system logs and events for detecting potential security incidents. In this case, the Windows Event Viewer played a crucial role in identifying the USB device connection event (Event ID 1006), which was essential for troubleshooting and incident analysis.
- The lab report emphasized the importance of conducting a thorough analysis of the incident, including collecting relevant screenshots and logs as evidence. This documentation provides a comprehensive understanding of the incident and supports further investigation or legal proceedings if necessary.

Conclusion

This lab successfully established a process for detecting and responding to the connection of an external USB drive on a Windows 11 system. The investigation revealed that disabled AutoPlay notifications were the root cause for the lack of initial alerts. By enabling these notifications, the system can now effectively alert users upon USB connection, promoting improved security awareness and mitigating potential risks.