

Question # 1:

(a) Brute Force login Attempts

Applying log filter for Audit Failures.

Filter

Apply filter to:

☒ Active event log view (File: C:\Users\Fatima Azfar\Downloads\loginAttempts.evtx)

☐ Event log view(s) on your choice

Event types

- ☐ Verbose
- ☐ Information
- ☐ Warning
- ☐ Error
- ☐ Critical
- ☐ Audit Success
- ☒ Audit Failure

Source: ... ☐ Exclude

Category: ... ☐ Exclude

User: ... ☐ Exclude

Computer: ... ☐ Exclude

Event ID(s): ☐ Exclude

Enter ID numbers and/or ID ranges, separated by commas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description: ☐ RegExp ☐ Exclude

☐ Date ☐ Time ☐ Separately

From: 12/ 8/2023 12:00:00 AM To: 12/ 8/2023 12:00:00 AM ☐ Exclude

Display event for the last 0 days 0 hours ☐ Exclude

Custom columns Description params

Name	Operator	Value
Custom column 1		
Custom column 2		
Custom column 3		
Custom column 4		
Custom column 5		

Clear Load... Save... OK Cancel

The resulting filter output are concurrent failed logon attempts

loginAttempts.evtx

83 11 1

UTC+5:00

Type	Date	Time	Event	Source	Category	User	Computer
Audit Failure	10/28/2020	1:05:00 PM	4625	Microsoft-Windows-Logon	N/A	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	1:05:00 PM	4625	Microsoft-Windows-Logon	N/A	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	3:43:51 PM	4625	Microsoft-Windows-Logon	N/A	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	3:43:51 PM	4625	Microsoft-Windows-Logon	N/A	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	4:39:28 PM	4625	Microsoft-Windows-Logon	N/A	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	4:39:28 PM	4625	Microsoft-Windows-Logon	N/A	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	4:39:28 PM	4625	Microsoft-Windows-Logon	N/A	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	4:39:28 PM	4625	Microsoft-Windows-Logon	N/A	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	4:39:28 PM	4625	Microsoft-Windows-Logon	N/A	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	4:39:28 PM	4625	Microsoft-Windows-Logon	N/A	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	4:39:28 PM	4625	Microsoft-Windows-Logon	N/A	N/A	WIN-5PVST6NBUR3
Audit Failure	10/28/2020	4:39:28 PM	4625	Microsoft-Windows-Logon	N/A	N/A	WIN-5PVST6NBUR3

Description

An account failed to log on.

Subject:

Security ID: S-1-5-18

Account Name: WIN-5PVST6NBUR3\$

Account Domain: WORKGROUP

Logon ID: 0x3e7

Logon Type: 5

Account For Which Logon Failed:

Security ID: S-1-0-0

Account Name: -

Account Domain: -

Failure Information:

Failure Reason: An Error occurred during Logon.

Description Data

(b) Account targeted by attacker

This is the account that is constantly being attacked:

Description

An account failed to log on.

Subject:

Security ID:	S-1-5-18
Account Name:	WIN-5PVST6NBUR3\$
Account Domain:	WORKGROUP
Login ID:	0x3e7

(c) Time of attack





This is the time range of the attacks i.e from 1:05:00 PM till 4:39:28 PM in the same day

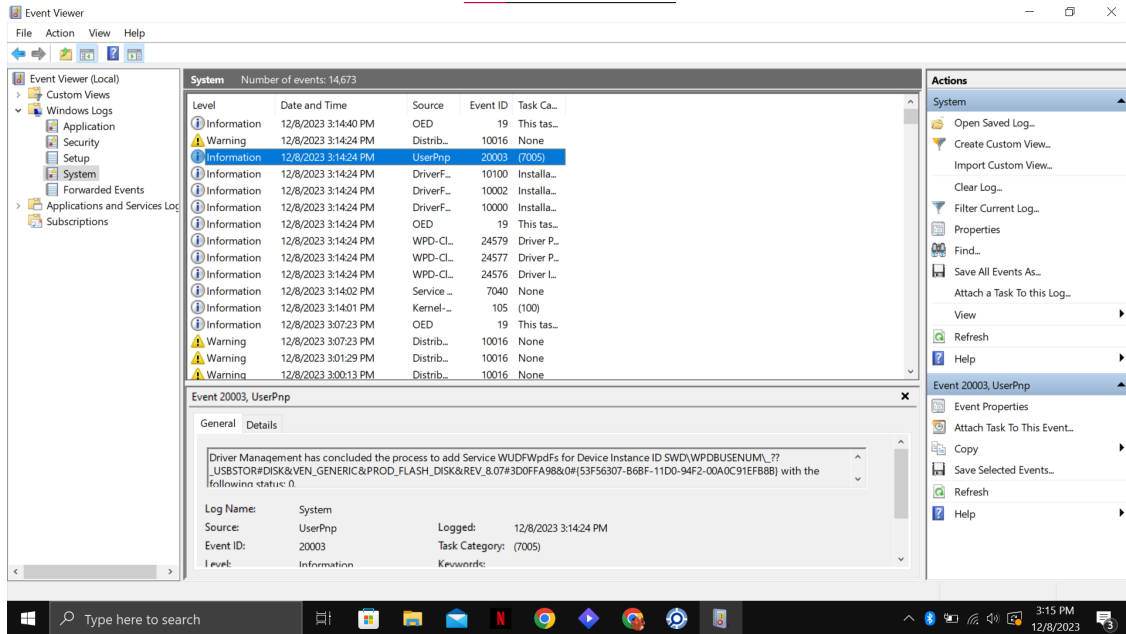
Date	Time
10/28/2020	4:39:28 PM
10/28/2020	4:39:28 PM
10/28/2020	4:39:28 PM
10/28/2020	4:39:28 PM
10/28/2020	4:39:28 PM
10/28/2020	4:39:28 PM
10/28/2020	4:39:28 PM
10/28/2020	3:43:51 PM
10/28/2020	3:43:51 PM
10/28/2020	1:05:00 PM
10/28/2020	1:05:00 PM

Question # 2:

(a) Plug in and remove a USB device

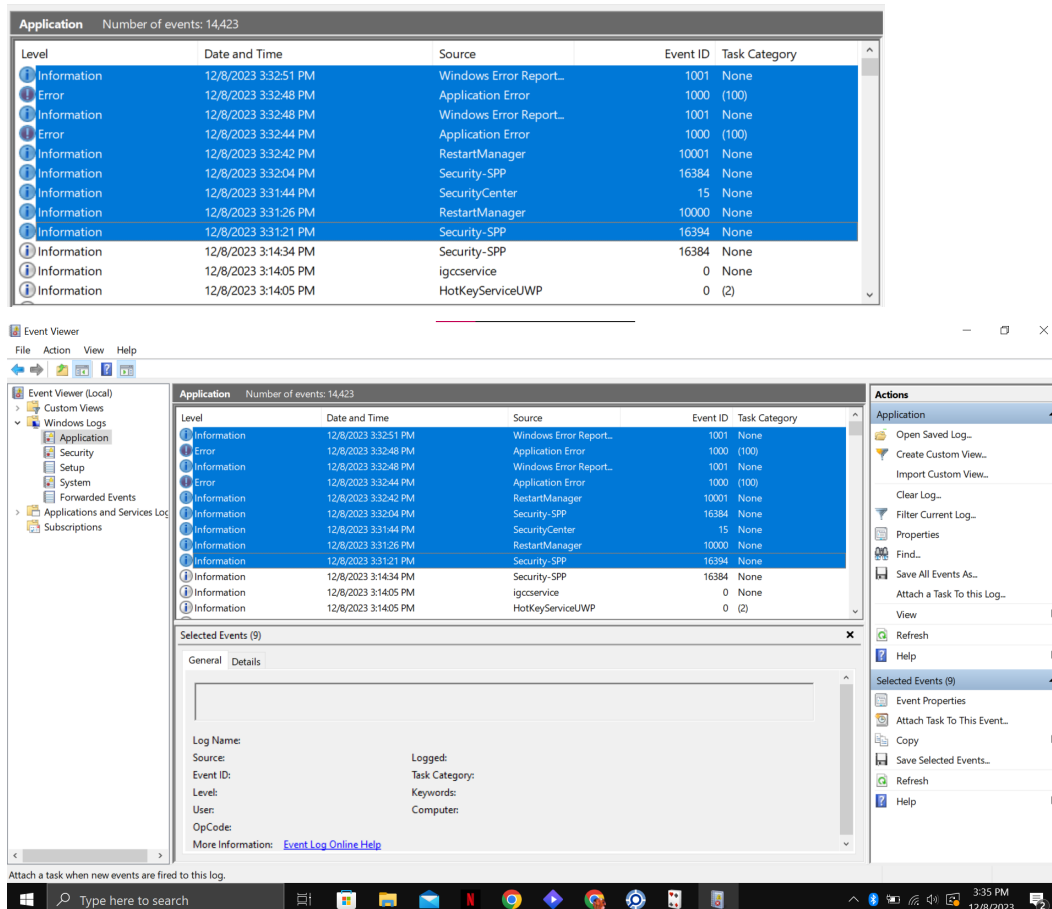
The log I have highlighted with the Event ID: 20003 and the Source: UserPnp is the one that indicates the USB activity.

System Number of events: 14,673 (!) New events available				
Level	Date and Time	Source	Event ID	Task Category
 Information	12/8/2023 3:14:40 PM	OED	19	This task logs error c...
 Warning	12/8/2023 3:14:24 PM	Distrib...	10016	None
 Information	12/8/2023 3:14:24 PM	UserPnp	20003	(7005)
 Information	12/8/2023 3:14:24 PM	DriverF...	10100	Installation or updat...



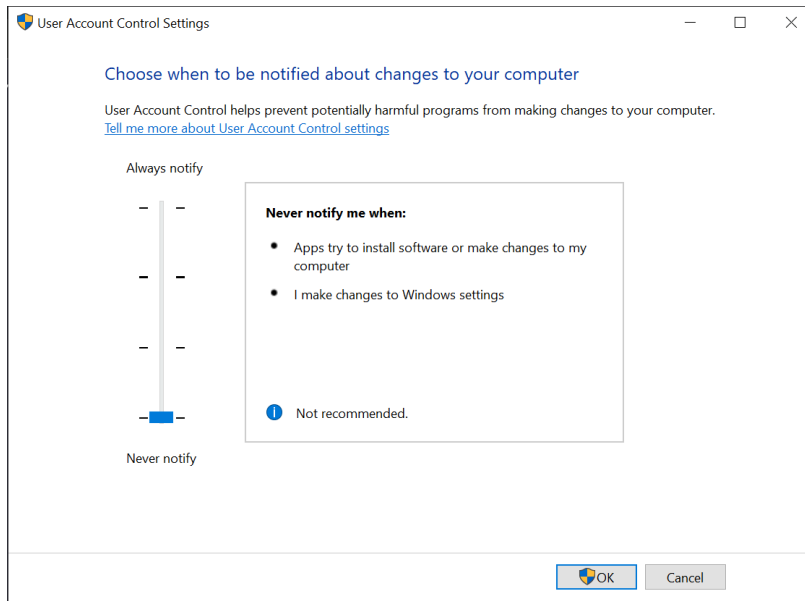
(b) Install a program

The events that I have highlighted are the ones that took place when I installed the 123 Free Solitaire game on my system.

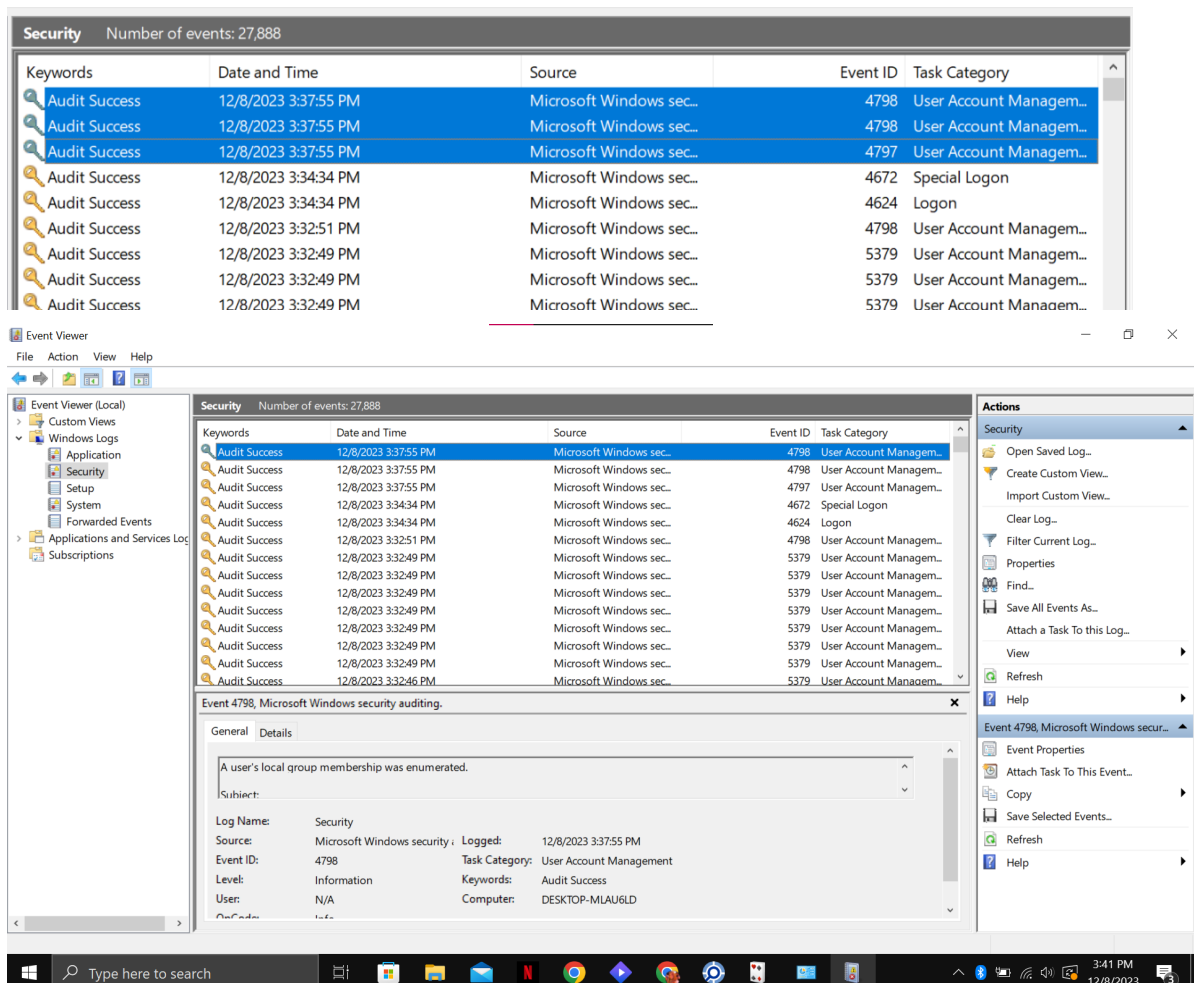


(c) Disable User Account Control (UAC) notifications in the Control Panel.

I changed the user account control settings to never notify.

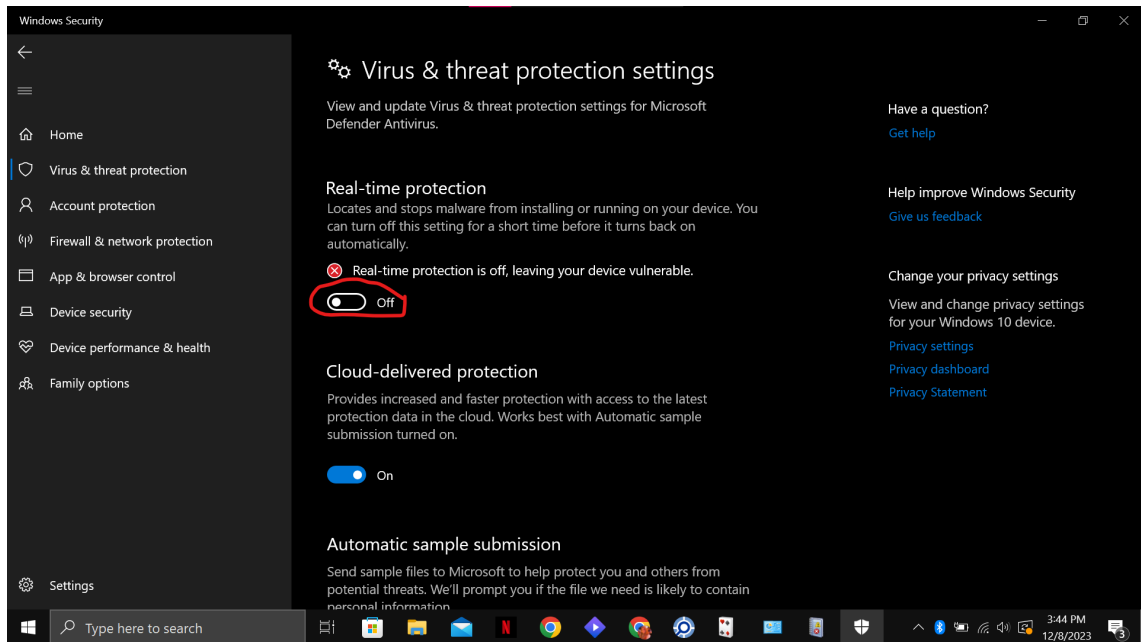


These events took place on changing the UAC:



(d) Turn off real time virus protection in Windows Security settings.

I turned off the real-time protection from windows security settings.



Then I checked the Event viewer and these are the events that took place on my actions

