


National University of Computer and Emerging Sciences, Lahore Campus

	Course Name:	Information Security	Course Code:	CS3002
	Program:	BS-CS, BS-DS	Semester:	Fall 2023
	Section	CS-D, CS-E, DS-A	Total Marks:	20
	Due Date:	10-12-2023	Weight	~3.3%
	Exam Type:	Assignment 3	Page(s):	3

Forensic Log Analysis

Background

Windows event logs contain useful information related to a system, its security, the applications on it, etc. Detailed examination of these logs helps investigators discover potential artifacts and construct a timeline for the analysis of events based on the logging information.

Suppose the attacker infiltrated the security of computer system at an office. The attackers made certain changes to the hardware configurations of the system, services running on the system, operating system, and some other critical programs running on that system to steal sensitive information. As a forensic investigator, you would examine all the event logs pertaining to the affected system, which include security logs, system logs, and application logs, to understand and analyze how this case of cyber-crime was perpetrated.

Requirements

A windows computer (or virtual machine).

Part 1: Look for login events

Download and install the 3rd party program [Event Log Explorer](#). Tasks below can be completed using the 30 days trial version.

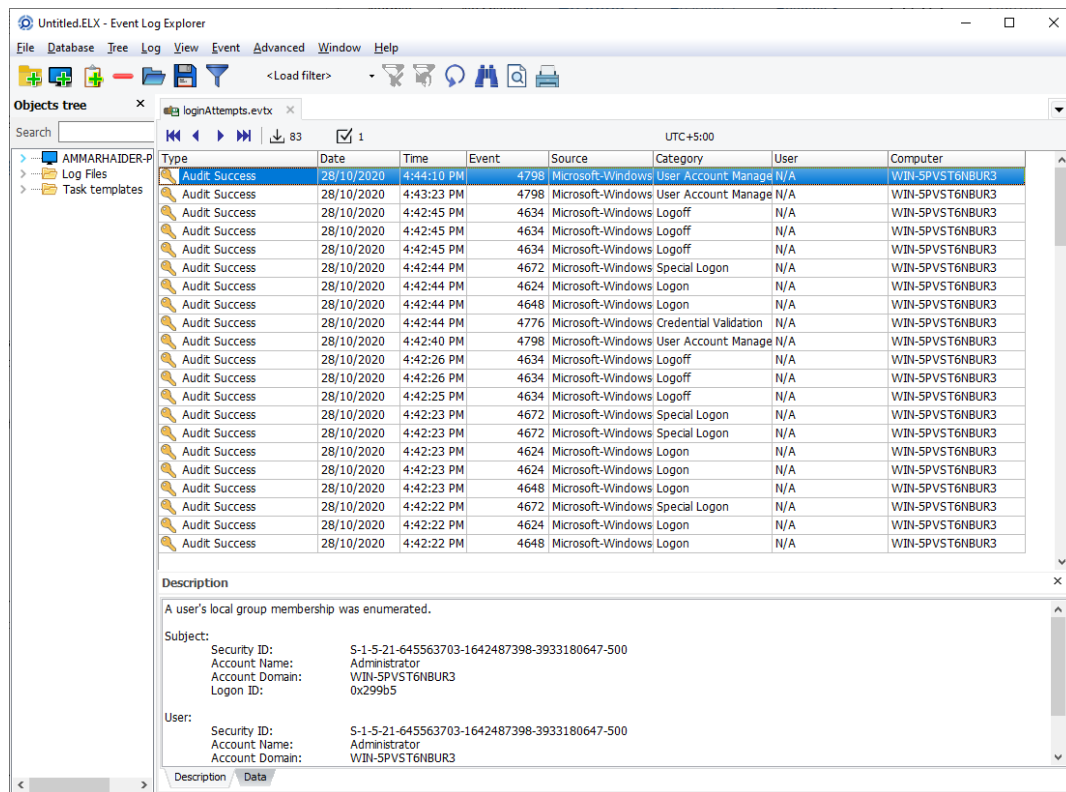
Next, download the [sample log file](#). Open it in the Event Log Explorer (File -> Open Log File...). Note that by default, the logs will be sorted by time, newest first.

Go through the logs, identify the following.

- (a) Brute force login attempt(s).
- (b) Account targeted by attacker.
- (c) Time of attack.

You may find it helpful to use the filtering options in the toolbar.

Your findings should be backed up with screenshots.

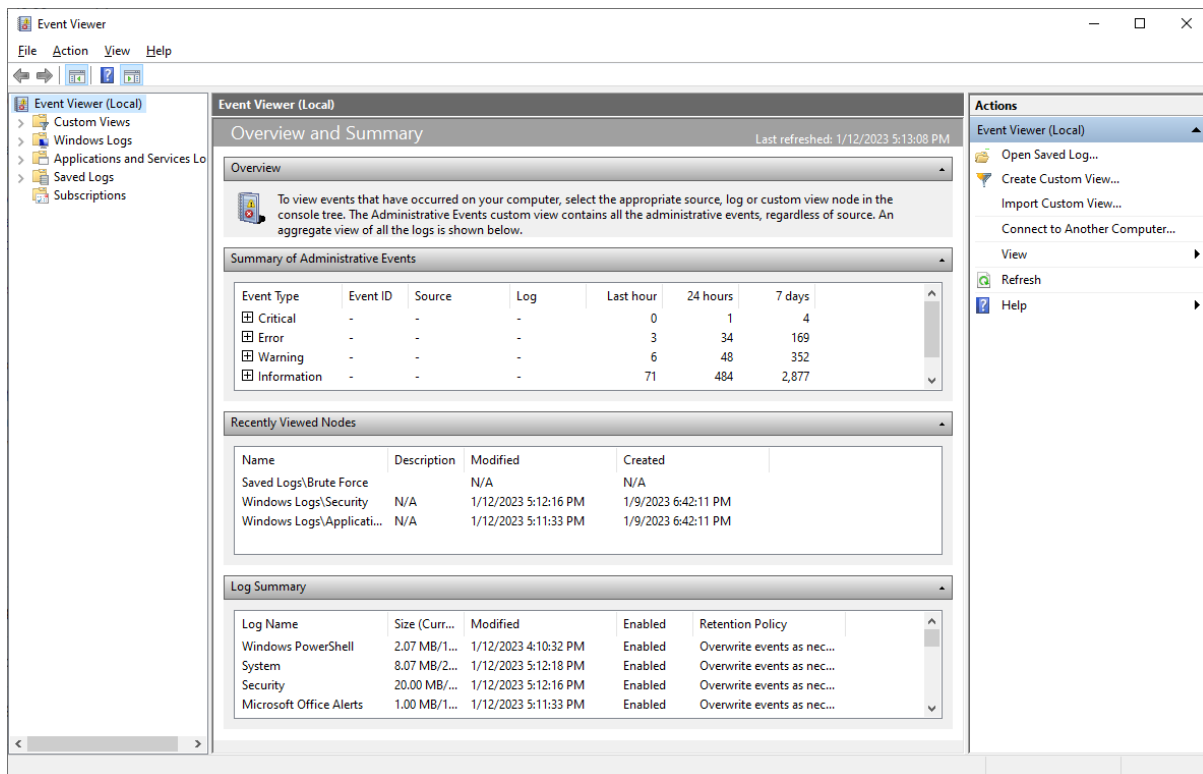


Part 2: Simulate attacker's actions

Now use your computer (somewhat) like an attacker, and perform following actions

- Plug in and remove a USB device.
- Install a program.
- Disable User Account Control (UAC) notifications in Control Panel.
- Turn off real time virus protection in Windows Security settings.

Having performed these actions, open the windows 'Event Viewer' app. This is a log viewer built into Windows. Use it to look for log entries that match the above actions. You will likely need lot of googling to identify the relevant log entries.



Deliverables

Prepare a PDF document containing response and screenshots of above activities. **All screenshots must include the system tray so that current date and time is visible.**

For assignment evaluation, you will be asked to demonstrate some of these activities and explain your written answers.