Collin Williams

Reading Assignment 1

Incident Response and Handling (ITSY-2442-007)

Brian Stuhl

What are the different types of Windows logon events? Explain how to examine Windows event logs.

Windows keeps track of how users log on, which is important for security. According to the CHFI v11 textbook, “Windows OS stores detailed log information related to the system, security, and installed applications, which are referred to as Windows event logs. Event logs can serve as a repository of evidence during forensic investigations and can help investigators to build a timeline analysis of events related to a cybercrime” (EC-Council, 2016). These records, called logon events, show who is getting onto the system and how. There are different types of logons, identified by a Logon Type number. For example, Type 2: Interactive means someone is sitting right at the computer. Type 3: Network happens when a user accesses a shared folder over the network. If someone uses Remote Desktop, that’s usually Type 10: RemoteInteractive. The two main event IDs to look for are 4624 (Successful Logon) and 4625 (Failed Logon). Knowing these types helps security people figure out the kind of access that occurred: local, remote, or just checking a network share.

To check these records, you use a tool called Event Viewer. You open it and go to Windows Logs, and then select the Security log. This log has all the logon and security-related events. Since there are usually too many events to look through, you need to use the filter. Click Filter Current Log… and put in the Event IDs you care about, mainly 4624 and 4625. You can also filter by the specific Logon Type (like Type 10 for RDP) or a certain time. Filtering makes it much faster to find the specific events you are looking for instead of scrolling through everything. Security best practices emphasize this focused approach; for instance, the Open Text Corporation recommends that for optimal analysis, systems should “collect only the relevant Event IDs that pertain to the critical security concerns of the organization” (Open Text Corporation, 2023).

After you filter the log, you double-click an event to see the details. The details will tell you the User Name, the specific Logon Type that was used, and the Source Network Address (the IP address if it was a remote logon). Successful logons also get a Logon ID to track what happened in that session. Essentially, Windows Logon Types show the method of access, and the Event Viewer’s filtering is the key tool for security professionals to quickly find and check these access methods to maintain system security.

Bibliography

EC-Council. (2016). *Computer forensics: Investigation procedures and response (CHFI)* (11th ed., p. 658). Cengage Learning.

Open Text Corporation. (2023). *Recommendations for Windows Event Log Collection* (ArcSight SmartConnectors 8.4.3). https://www.microfocus.com/documentation/arcsight/arcsight-smartconnectors-8.4/pdfdoc/sc-recommendations-for-windows-event-log-collection/sc-recommendations-for-windows-event-log-collection.pdf