Event Analysis: Repeated Failed Physical Logon Attempts

These analysed events were recorded when failed physical login attempts exceeded 4 within 5 minutes.

Information contained within key fields made it very clear what the nature of these events was:

- Logon Type: 2 (Interactive), which is a local/physical logon
- Network Information: Source Network Address was always 127.0.0.1, which is local host with a Source Port of 0, further indicating it was a local, non-network login attempt
- Failure Information: was always “Unknown username or bad password”, showing it failed due to incorrect login information

Figure 1: Example Repeated Failed Login Event’s Relevant Fields