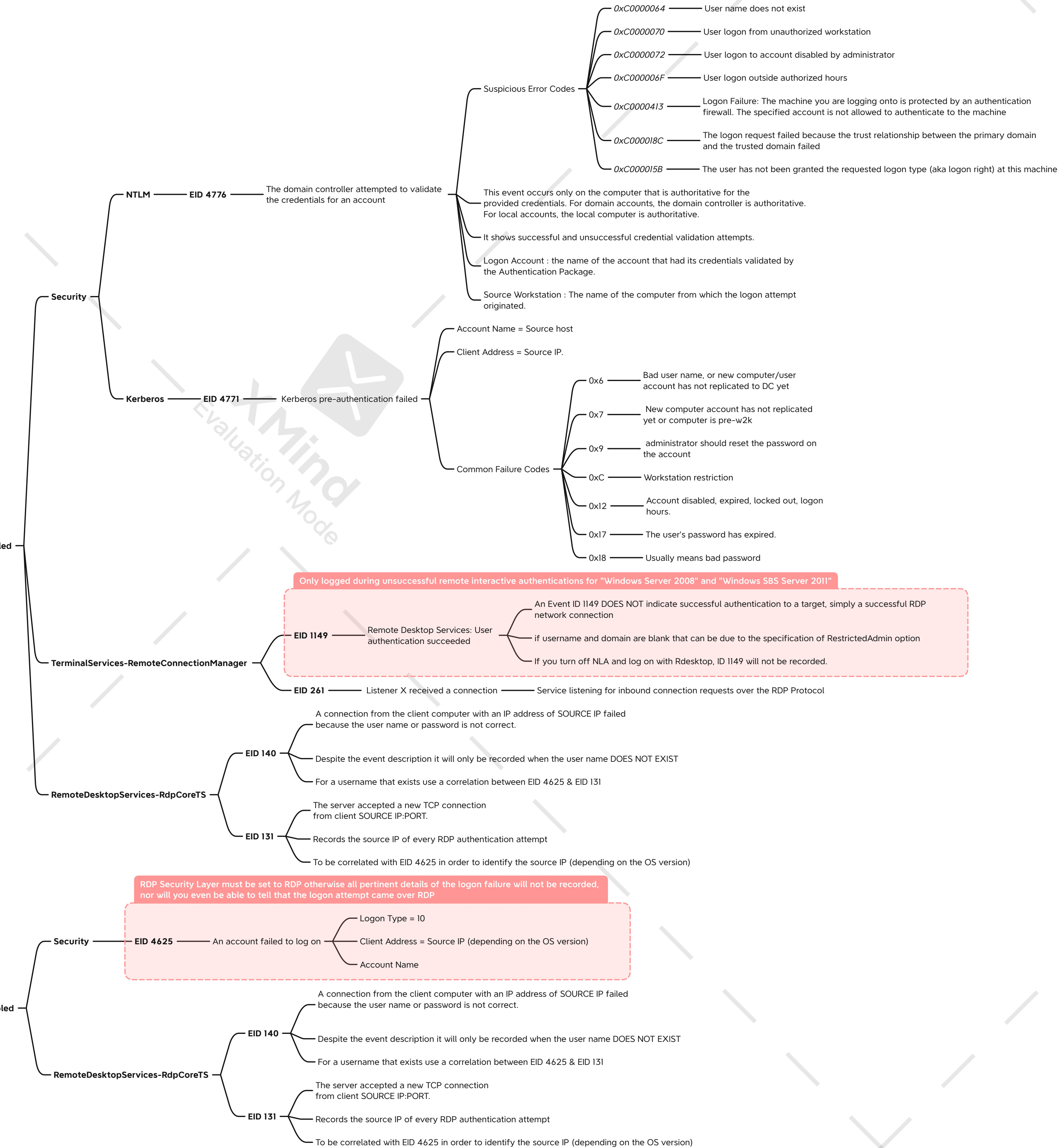


RDP DFIR

Successful Remote Interactive Logon



Unsuccessful Remote Interactive Logon



In both cases will be followed by EID 4625 with Logon Type 3 due to NLA enablement

References

- <https://purdrd.org/remote-desktop-security/auditing-remote-desktop-services-logon-failures-1/>
- <https://port139.hatenablog.com/entry/2019/03/23/091740>
- <https://ponderthebits.com/2018/02/windows-rdp-related-event-logs-identification-tracking-and-investigation/>
- https://www.13cubed.com/downloads/rdp_flowchart.pdf
- <https://dfironthemountain.wordpress.com/2019/02/15/rdp-event-log-dfir/>