NTLM Brute Force

https://www.varonis.com/blog/investigate-ntlm-brute-force

> More specifically, you will need to use Event ID 8004 in Event Viewer to identify the actual device that is on the receiving end of these NTLM brute force attack attempts. Locating the victim device will be the first step in the remediation process.

> 8004 events are typically not enabled by default and may require configuration changes in specific Domain Controller group policies to enable logging.

Revision #1
Created 2022-05-10 18:25:29 UTC by Clinton
Updated 2022-05-10 18:26:25 UTC by Clinton