

Log Tampering Simulation (T1562.002)

Time	Event
2025-05-29T14:00:09+0530	<p>05/29/2025 02:00:09 PM LogName=Security EventCode=1102 EventType=4 ComputerName=DESKTOP-F049LOK SourceName=Microsoft-Windows-Eventlog Type=Information RecordNumber=810893 Keywords=Audit Success TaskCategory=Log clear OpCode=Info Message=The audit log was cleared. Subject: Security ID:S-1-5-21-743153983-3650556082-3479164291-1002 Account Name:testuser Domain Name:DESKTOP-F049LOK Logon ID:0x4FC301</p>
2025-05-29T14:00:09+0530	<p>05/29/2025 02:00:09 PM LogName=Microsoft-Windows-PowerShell/Operational EventCode=4104 EventType=5 ComputerName=DESKTOP-F049LOK User=NOT_TRANSLATED Sid=S-1-5-21-743153983-3650556082-3479164291-1002 SidType=0 SourceName=Microsoft-Windows-PowerShell Type=Verbose RecordNumber=185356 Keywords=None TaskCategory=Execute a Remote Command OpCode=On create calls Message=Creating Scriptblock text (1 of 1): Clear-EventLog -LogName Security ScriptBlock ID: 116faeba-44f7-42d0-b347-b1c293860bb4 Path:</p>
2025-05-29T13:44:38+0530	<p>05/29/2025 01:44:38 PM LogName=Security EventCode=1102 EventType=4 ComputerName=DESKTOP-F049LOK SourceName=Microsoft-Windows-Eventlog Type=Information RecordNumber=808791 Keywords=Audit Success TaskCategory=Log clear OpCode=Info Message=The audit log was cleared. Subject: Security ID:S-1-5-21-743153983-3650556082-3479164291-1002 Account Name:testuser Domain Name:DESKTOP-F049LOK Logon ID:0x4FC301</p>

Time	Event
2025-05-29T13:44:38+0530	<p>05/29/2025 01:44:38 PM</p> <p>LogName=Microsoft-Windows-Sysmon/Operational</p> <p>EventCode=1</p> <p>EventType=4</p> <p>ComputerName=DESKTOP-F049LOK</p> <p>User=NOT_TRANSLATED</p> <p>Sid=S-1-5-18</p> <p>SidType=0</p> <p>SourceName=Microsoft-Windows-Sysmon</p> <p>Type=Information</p> <p>RecordNumber=93084</p> <p>Keywords=None</p> <p>TaskCategory=Process Create (rule: ProcessCreate)</p> <p>OpCode=Info</p> <p>Message=Process Create:</p> <p>RuleName: -</p> <p>UtcTime: 2025-05-29 08:14:38.112</p> <p>ProcessGuid: {a9155468-176e-6838-9203-000000002a00}</p> <p>ProcessId: 7412</p> <p>Image: C:\Windows\System32\wevtutil.exe</p> <p>FileVersion: 10.0.19041.5794 (WinBuild.160101.0800)</p> <p>Description: Eventing Command Line Utility</p> <p>Product: Microsoft® Windows® Operating System</p> <p>Company: Microsoft Corporation</p> <p>OriginalFileName: wevtutil.exe</p> <p>CommandLine: wevtutil cl Security</p> <p>CurrentDirectory: C:\Windows\system32\</p> <p>User: DESKTOP-F049LOK\testuser</p> <p>LogonGuid: {a9155468-16a8-6838-01c3-4f0000000000}</p> <p>LogonId: 0x4FC301</p> <p>TerminalSessionId: 2</p> <p>IntegrityLevel: High</p> <p>Hashes: MD5=D4C99E01B0061D2EEA2A3EB422CDBC8,SHA256=0B732D9AD576D1400DB44EDF3E750849AC481E9BBAA628A3914E5EEF9B7181B0,IMPHASH=1864B7EA6A87A2BBB43783BD42E11204</p> <p>ParentProcessGuid: {a9155468-1725-6838-7d03-000000002a00}</p> <p>ParentProcessId: 6420</p> <p>ParentImage: C:\Windows\System32\cmd.exe</p> <p>ParentCommandLine: "C:\Windows\system32\cmd.exe"</p> <p>ParentUser: DESKTOP-F049LOK\testuser</p>