Disable Windows Event Logging | Red Team Notes 2.0

Published: 2021-01-23 · Archived: 2026-04-05 20:43:07 UTC

⌘Ctrlk

1. Red Team Techniques
2. Defense Evasion
3. T1562: Impair Defenses

Disable Windows Event Logging

Adversaries may disable Windows event logging to limit data that can be leveraged for detections and audits. Windows event logs record user and system activity such as login attempts, process creating, and much more. This data is used by security tools and analysis to generate detections.

Adversaries may target system-wide logging or just that of a particular application. By disabling Windows event logging, adversaries can operate while leaving less evidence of a compromise behind.

Example:

We can also disable the eventlog service from the workstation this can be done with PowerShell but we will need to apply the **-Force** flag since this service has other services dependent from it.

We can confirm it with CMD as well and we see that it is unable to start since the service is also disabled, besides being stopped as well.

Set it back how it was is simple.

And a restart then all back to normal. As we can see this is a great method to hide our tracks and a progression done in an environment APT have a use for these techniques to evade Defenses

Last updated 5 years ago
