Jesus Garcia

Wk-4 Assignment

September 17, 2023

Power shell report

I ran three commands that gave me the last 5 items in the output of the command.

The three commands are as follows:

Get-EventLog -LogName System -newest 5 | Format-List > C:\system.txt

Index : 47672

EntryType : Information

InstanceId : 2147489661

Message : The system uptime is 879437 seconds.

Category : (0)

CategoryNumber : 0

ReplacementStrings : {, , , ...}

Source : EventLog

TimeGenerated : 9/15/2023 12:00:01 PM

TimeWritten : 9/15/2023 12:00:01 PM

UserName :

Index : 47671

EntryType : Information

InstanceId : 1073748864

Message : The start type of the Background Intelligent Transfer Service service was changed from auto start

to demand start.

Category : (0)

CategoryNumber : 0

ReplacementStrings : {Background Intelligent Transfer Service, auto start, demand start, BITS}

Source : Service Control Manager

TimeGenerated : 9/15/2023 11:57:58 AM

TimeWritten : 9/15/2023 11:57:58 AM

UserName : NT AUTHORITY\SYSTEM

Index : 47670

EntryType : Information

InstanceId : 1073748864

Message : The start type of the Background Intelligent Transfer Service service was changed from demand

start to auto start.

Category : (0)

CategoryNumber : 0

ReplacementStrings : {Background Intelligent Transfer Service, demand start, auto start, BITS}

Source : Service Control Manager

TimeGenerated : 9/15/2023 11:55:53 AM

TimeWritten : 9/15/2023 11:55:53 AM

UserName : NT AUTHORITY\SYSTEM

Index : 47669

EntryType : Information

InstanceId : 1073748864

Message : The start type of the Background Intelligent Transfer Service service was changed from auto start

to demand start.

Category : (0)

CategoryNumber : 0

ReplacementStrings : {Background Intelligent Transfer Service, auto start, demand start, BITS}

Source : Service Control Manager

TimeGenerated : 9/15/2023 11:40:24 AM

TimeWritten : 9/15/2023 11:40:24 AM

UserName : NT AUTHORITY\SYSTEM

Index : 47668

EntryType : Information

InstanceId : 1073748864

Message : The start type of the Background Intelligent Transfer Service service was changed from demand

start to auto start.

Category : (0)

CategoryNumber : 0

ReplacementStrings : {Background Intelligent Transfer Service, demand start, auto start, BITS}

Source : Service Control Manager

TimeGenerated : 9/15/2023 11:38:20 AM

TimeWritten : 9/15/2023 11:38:20 AM

UserName : NT AUTHORITY\SYSTEM

**Get-EventLog -LogName Security -newest 5 | Format-List > C:\security.txt**

Index : 172711

EntryType : SuccessAudit

InstanceId : 4616

Message : The system time was changed.

Subject:

Security ID: S-1-5-19

Account Name: LOCAL SERVICE

Account Domain: NT AUTHORITY

Logon ID: 0x3e5

Process Information:

Process ID: 0x684

Name: C:\Windows\System32\svchost.exe

Previous Time: 2023-09-15T05:21:34.2986863Z

New Time: 2023-09-15T05:21:34.2986796Z

This event is generated when the system time is changed. It is normal for the Windows Time

Service, which runs with System privilege, to change the system time on a regular basis. Other

system time changes may be indicative of attempts to tamper with the computer.

Category : (12288)

CategoryNumber : 12288

ReplacementStrings : {S-1-5-19, LOCAL SERVICE, NT AUTHORITY, 0x3e5...}

Source : Microsoft-Windows-Security-Auditing

TimeGenerated : 9/14/2023 10:21:34 PM

TimeWritten : 9/14/2023 10:21:34 PM

UserName :

Index : 172710

EntryType : SuccessAudit

InstanceId : 4719

Message : System audit policy was changed.

Subject:

Security ID: S-1-5-18

Account Name: SEC-TS-NSA01$

Account Domain: WUNET

Logon ID: 0x3e7

Audit Policy Change:

Category: %%8278

Subcategory: %%13829

Subcategory GUID: {0cce923a-69ae-11d9-bed3-505054503030}

Changes: %%8448, %%8450

Category : (13568)

CategoryNumber : 13568

ReplacementStrings : {S-1-5-18, SEC-TS-NSA01$, WUNET, 0x3e7...}

Source : Microsoft-Windows-Security-Auditing

TimeGenerated : 9/12/2023 1:20:20 AM

TimeWritten : 9/12/2023 1:20:20 AM

UserName :

Index : 172709

EntryType : SuccessAudit

InstanceId : 4719

Message : System audit policy was changed.

Subject:

Security ID: S-1-5-18

Account Name: SEC-TS-NSA01$

Account Domain: WUNET

Logon ID: 0x3e7

Audit Policy Change:

Category: %%8278

Subcategory: %%13826

Subcategory GUID: {0cce9237-69ae-11d9-bed3-505054503030}

Changes: %%8448, %%8450

Category : (13568)

CategoryNumber : 13568

ReplacementStrings : {S-1-5-18, SEC-TS-NSA01$, WUNET, 0x3e7...}

Source : Microsoft-Windows-Security-Auditing

TimeGenerated : 9/12/2023 1:20:20 AM

TimeWritten : 9/12/2023 1:20:20 AM

UserName :

Index : 172708

EntryType : SuccessAudit

InstanceId : 4719

Message : System audit policy was changed.

Subject:

Security ID: S-1-5-18

Account Name: SEC-TS-NSA01$

Account Domain: WUNET

Logon ID: 0x3e7

Audit Policy Change:

Category: %%8278

Subcategory: %%13824

Subcategory GUID: {0cce9235-69ae-11d9-bed3-505054503030}

Changes: %%8448, %%8450

Category : (13568)

CategoryNumber : 13568

ReplacementStrings : {S-1-5-18, SEC-TS-NSA01$, WUNET, 0x3e7...}

Source : Microsoft-Windows-Security-Auditing

TimeGenerated : 9/12/2023 1:20:20 AM

TimeWritten : 9/12/2023 1:20:20 AM

UserName :

Index : 172707

EntryType : SuccessAudit

InstanceId : 4719

Message : System audit policy was changed.

Subject:

Security ID: S-1-5-18

Account Name: SEC-TS-NSA01$

Account Domain: WUNET

Logon ID: 0x3e7

Audit Policy Change:

Category: %%8277

Subcategory: %%13571

Subcategory GUID: {0cce9232-69ae-11d9-bed3-505054503030}

Changes: %%8448, %%8450

Category : (13568)

CategoryNumber : 13568

ReplacementStrings : {S-1-5-18, SEC-TS-NSA01$, WUNET, 0x3e7...}

Source : Microsoft-Windows-Security-Auditing

TimeGenerated : 9/12/2023 1:20:20 AM

TimeWritten : 9/12/2023 1:20:20 AM

UserName :

**Get-EventLog -LogName Application -newest 5 | Format-List > C:\application.txt**

Index : 75928

EntryType : Information

InstanceId : 1073758208

Message : Successfully scheduled Software Protection service for re-start at 2023-09-15T20:38:00Z. Reason:

RulesEngine.

Category : (0)

CategoryNumber : 0

ReplacementStrings : {2023-09-15T20:38:00Z, RulesEngine}

Source : Software Protection Platform Service

TimeGenerated : 9/15/2023 11:38:00 AM

TimeWritten : 9/15/2023 11:38:00 AM

UserName :

Index : 75927

EntryType : Information

InstanceId : 3221241866

Message : Offline downlevel migration succeeded.

Category : (0)

CategoryNumber : 0

ReplacementStrings : {}

Source : Software Protection Platform Service

TimeGenerated : 9/15/2023 11:37:09 AM

TimeWritten : 9/15/2023 11:37:09 AM

UserName :

Index : 75926

EntryType : Information

InstanceId : 1073758208

Message : Successfully scheduled Software Protection service for re-start at 2023-09-15T20:38:02Z. Reason:

RulesEngine.

Category : (0)

CategoryNumber : 0

ReplacementStrings : {2023-09-15T20:38:02Z, RulesEngine}

Source : Software Protection Platform Service

TimeGenerated : 9/15/2023 11:11:02 AM

TimeWritten : 9/15/2023 11:11:02 AM

UserName :

Index : 75925

EntryType : Information

InstanceId : 3221241866

Message : Offline downlevel migration succeeded.

Category : (0)

CategoryNumber : 0

ReplacementStrings : {}

Source : Software Protection Platform Service

TimeGenerated : 9/15/2023 11:10:30 AM

TimeWritten : 9/15/2023 11:10:30 AM

UserName :

Index : 75924

EntryType : Information

InstanceId : 1073758208

Message : Successfully scheduled Software Protection service for re-start at 2023-09-15T20:37:52Z.

Reason: RulesEngine.

Category : (0)

CategoryNumber : 0

ReplacementStrings : {2023-09-15T20:37:52Z, RulesEngine}

Source : Software Protection Platform Service

TimeGenerated : 9/15/2023 10:45:52 AM

TimeWritten : 9/15/2023 10:45:52 AM

UserName :

All of these outputs can tell us multiple things about the computer. The log files in the Security incidents can help show us abnormal activities. If someone is trying to repeatedly log in, it would show up in the Security logs. In the event of a breach, we can use these logs in the assistance of the start of the attack.

I have used the **Get-Eventlog Application | Get-Member, Get-Eventlog System | Get-Member, Get-Eventlog Security | Get-Member** commands to tell me the property/method offered by the Get-Eventlog command, and the definition of each. This can help us to narrow down what exactly we are getting when we run the command.

|  |  |
| --- | --- |
| Property | Value |
| MachineName | Machine name can be useful to allow us to track machines that are affected or we are investigating. |
| EntryType | Software Protection Platform Service |
| Message | The message is valuable because it will tell us what exactly the log is saying. |
| Reason | Reason of the message is always good as it can tell us whether it was invoked by someone or just a process |
| ToString(method) | This method would be good to extract string versions of logs info, so that the datatype is all ubiquitous |
| UserName | Name of the user logged into the machine when the event happened that the log is reporting |
| Source | This would report the source of the process that ran the event the log reported. |