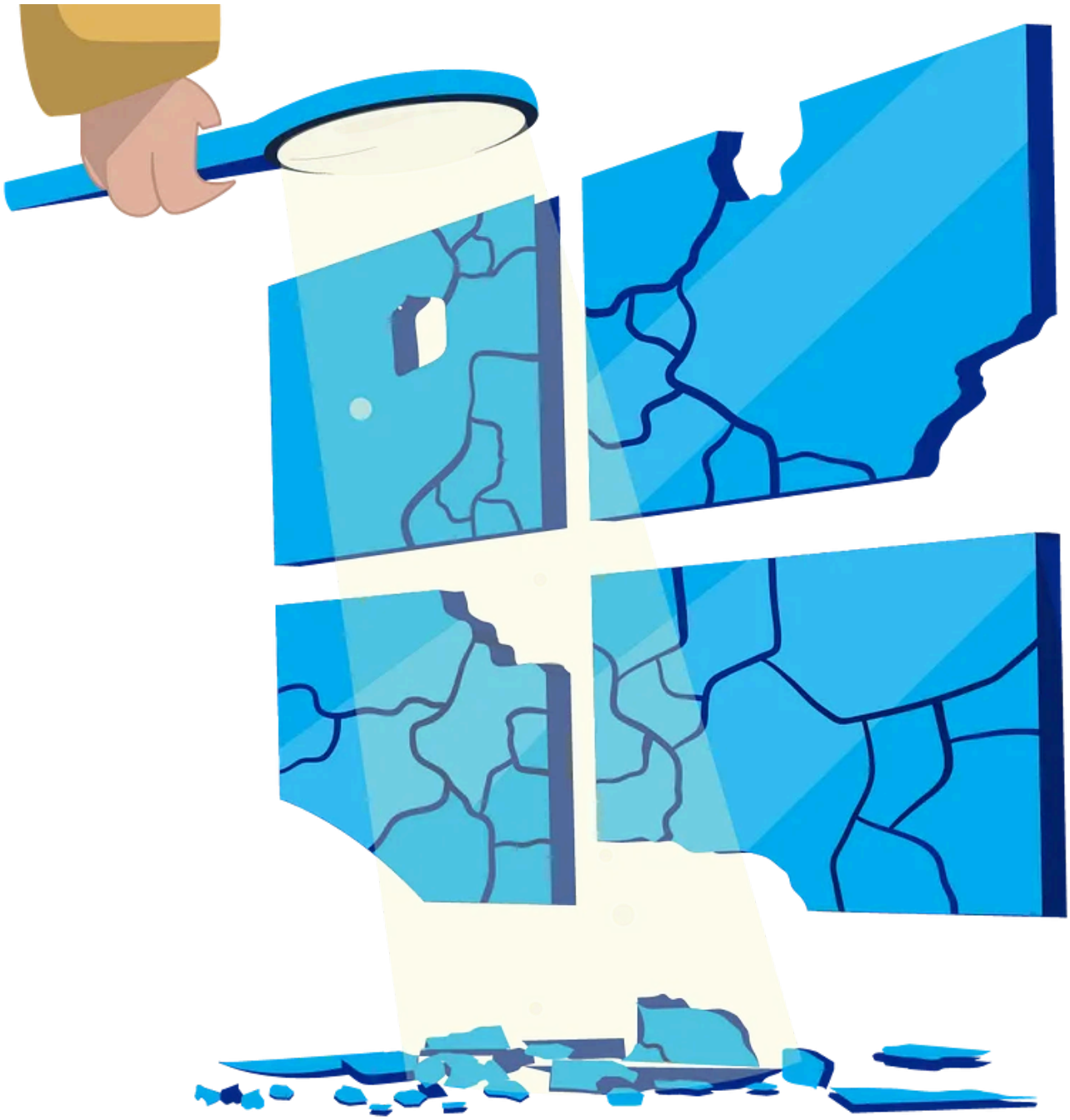
Monday Monitor — TryHackMe WriteUp

Fritzadriano · Follow
5 min read · Sep 3, 2024

Ready to test Swiftspend's *endpoint monitoring*? In today's write-up, we will learn and solve one of TryHackMe's challenges in the Endpoint Security Monitoring Module to master the Security Operations Center (SOC) role.

So, let's dive in. The first thing to do is understand the given scenarios.



Source: TryHackMe

Scenario

Swiftspend Finance, the coolest fintech company in town, is on a mission to level up its cyber security game to keep those digital adversaries at bay and ensure their customers stay safe and sound.

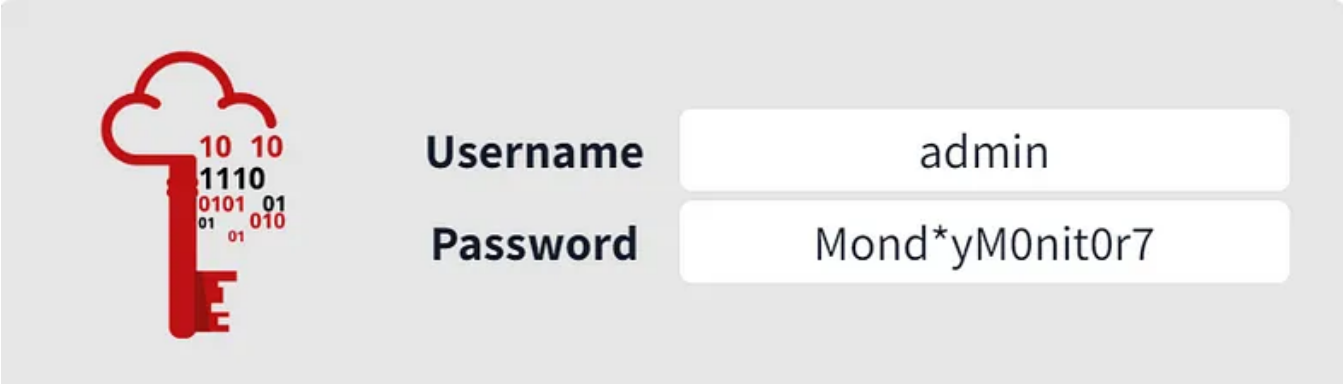
Led by the tech-savvy Senior Security Engineer John Sterling, Swiftspend's latest project is about beefing up their endpoint monitoring using Wazuh and Sysmon. They've been running some tests to see how well their cyber guardians can sniff out trouble. And guess what? You're the cyber sleuth they've called in to crack the code!

> *The tests were run on* ***Apr 29, 2024,*** between 12:00:00 and 20:00:00.

As you dive into the logs, you'll look for any suspicious process shenanigans or weird network connections, you name it! Your mission? Unravel the mysteries within the logs and dish out some epic insights to fine-tune Swiftspend's defences.

Machine Access

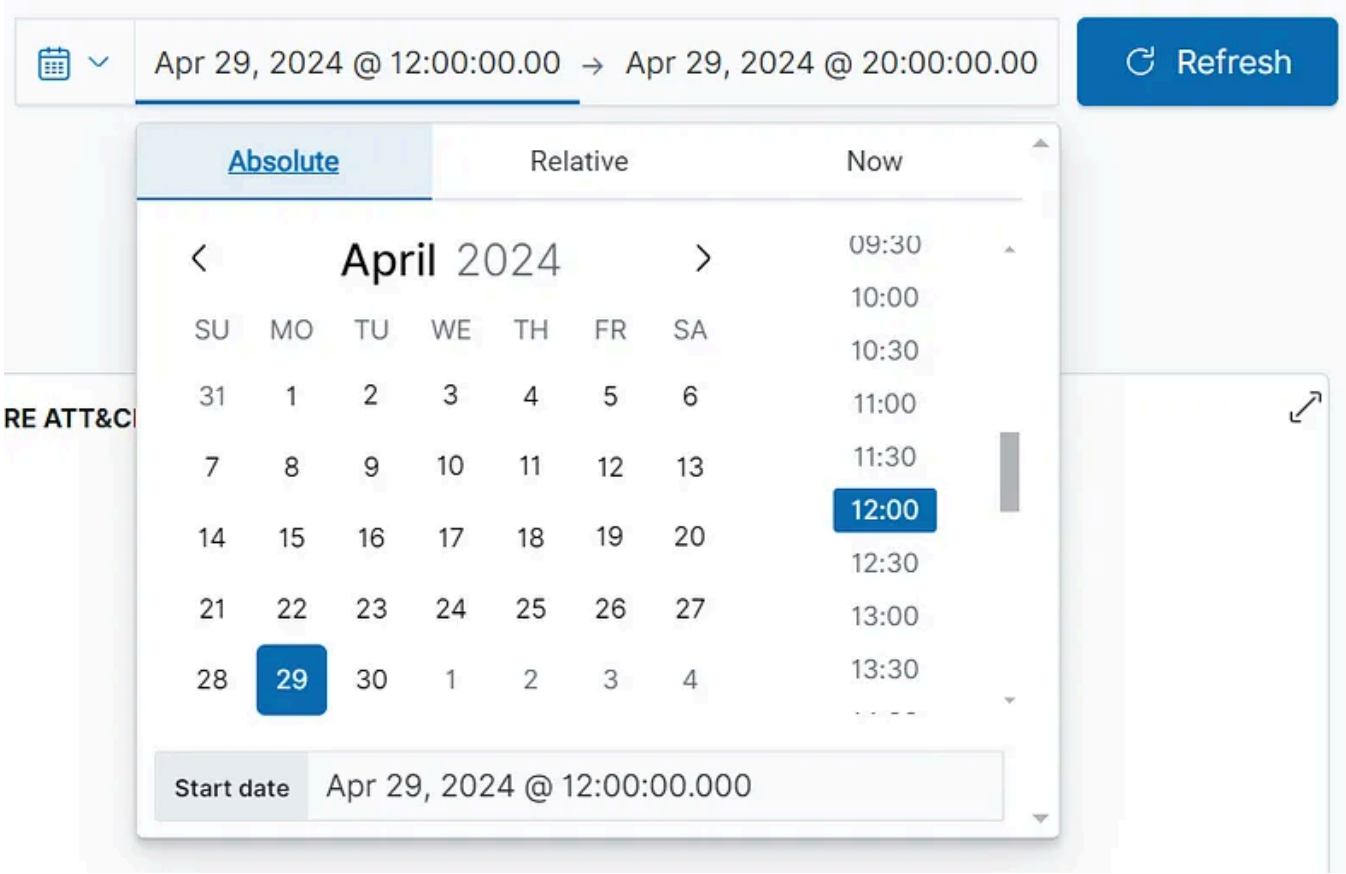
Click the **Start Machine** button attached to this task to start the VM. Give the machine about **5 minutes** to fully set up the environment. Access the Wazuh Dashboard using your browser at https://10-10-166-179.p.thmlabs.com and use the credentials listed below:



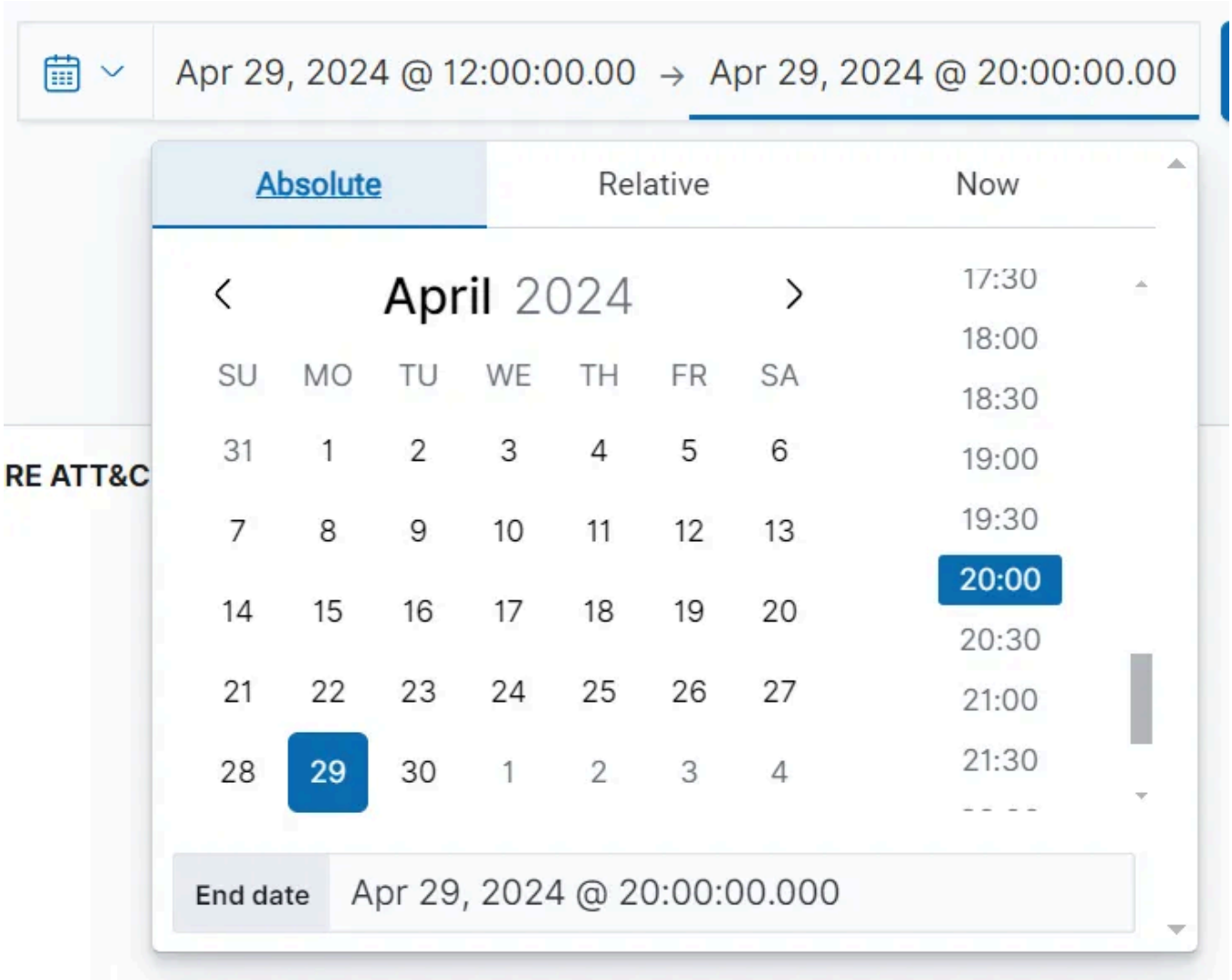
Source: TryHackMe

Once logged in, navigate to the **Security** events module and use the saved query `Monday_Monitor` to access the logs.

Okay, so we understand that we need to use the Wazuh software to complete this task. First, as stated in the scenario, we need to monitor events between ***12:00 and 20:00 on April 29, 2024***. Therefore, we must configure the settings to reflect this specific date and time

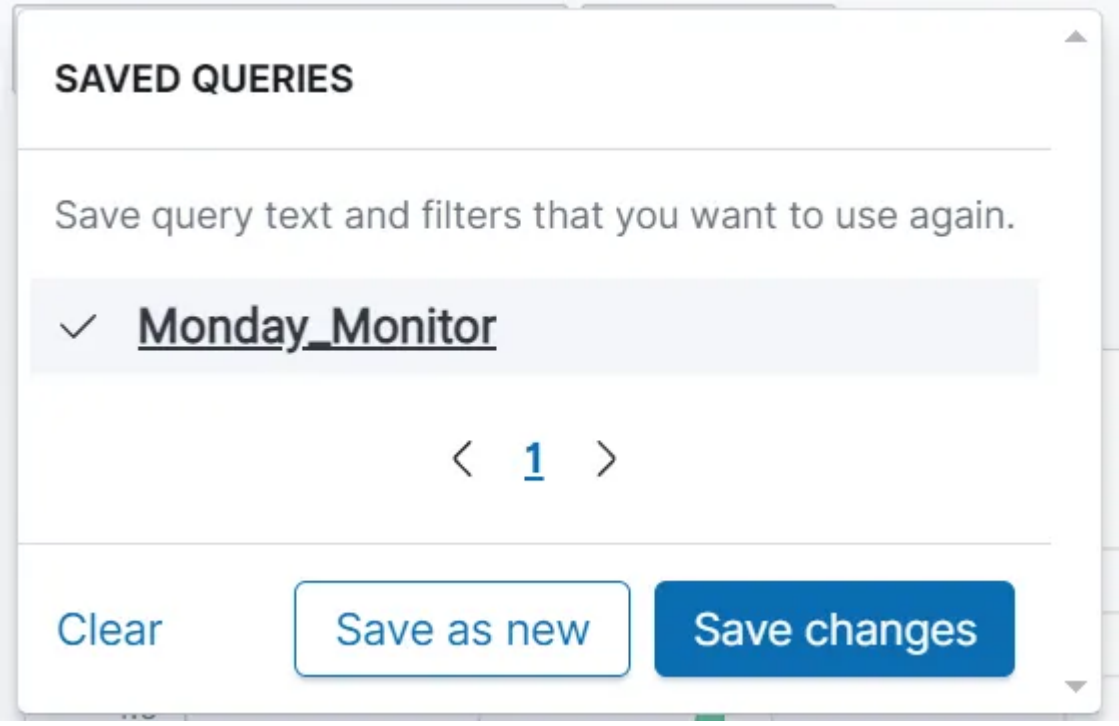


Setting the start date and time



Setting the end date and time

Lastly, please don't forget to access the *Monday_monitor* queries that have been saved by the system.



Saved queries

Let's dive into the question, shall we?

Question 1

Initial access was established using a downloaded file. What is the file name saved on the host?

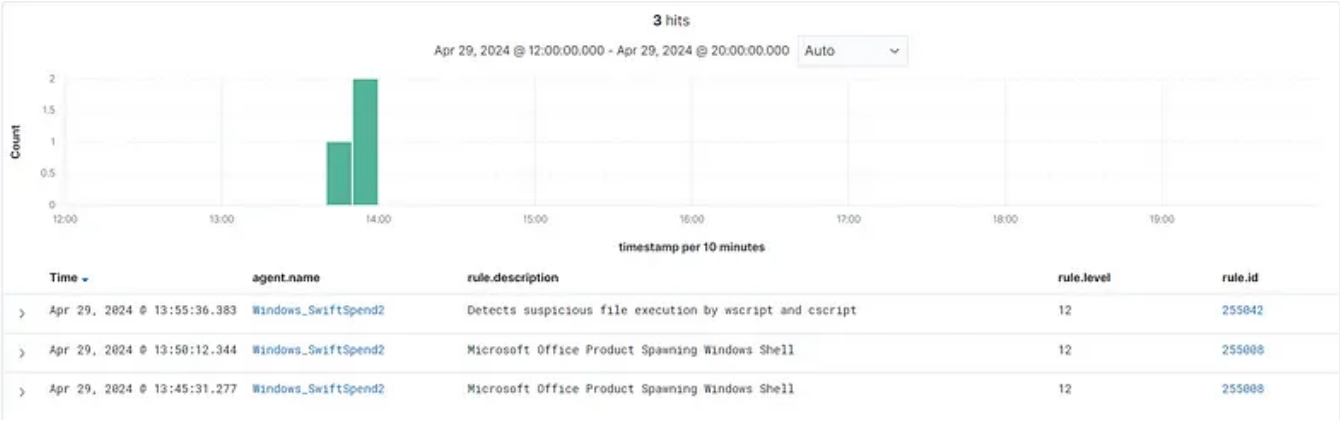
A: SwiftSpend_Financial_Expenses.xlsm

I understand that the first question might be a bit confusing at first glance. But don't worry, we'll figure it out together.

Firstly, the question asks for the file name saved on the host. To find this, you should navigate to: Events → search bar (localhost).

Source: TryHackMe's Wazuh

You will see three hits displayed above the table. Please direct your attention to the top document



Source: TryHackMe's Wazuh

Then, you will find the answer in the `data.win.event.data.commandLine` section

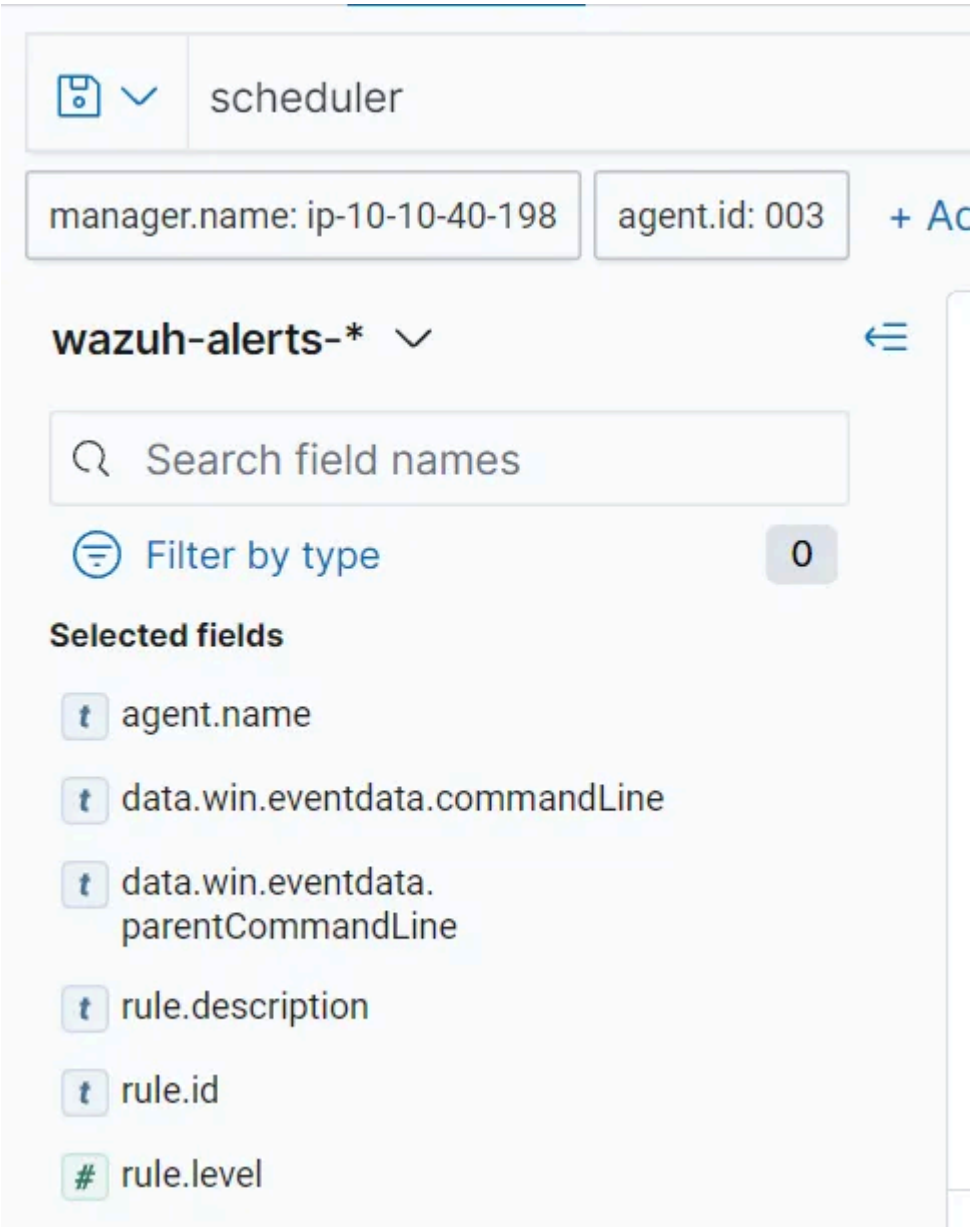
Source: TryHackMe's Wazuh

Question 2

What is the full command run to create a scheduled task?

A: *\"cmd.exe\" /c \"reg add HKCU\\SOFTWARE\\ATOMIC-T1053.005 /v test /t REG_SZ /d cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0= /f & schtasks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX([System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /sc daily /st 12:34\"*

As we learned in the Wazuh module, you can search for *'scheduler'* in the search bar. To find the full command used to create the scheduled task, add the filter `data.win.eventdata.parentCommandLine`, which will display the complete command



Source: TryhackMe's Wazuh

Then, you'll find that one of the documents contains a lengthy command

Source: TryhackMe's Wazuh

So, there they are!

Source: TryhackMe's Wazuh

Question 3

What time is the scheduled task meant to run?

A: 12:34

This one is quite simple. Scroll up a bit, and you'll find the answer in the original `data.win.eventdata.CommandLine` fields.

```
t  data.win.eventdata.commandLine        schtasks.exe  /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX([System.Text.Encodi
ng]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /
sc daily /st 12:34
```

Source: TryHackMe's Wazuh

Question 4

What was encoded?

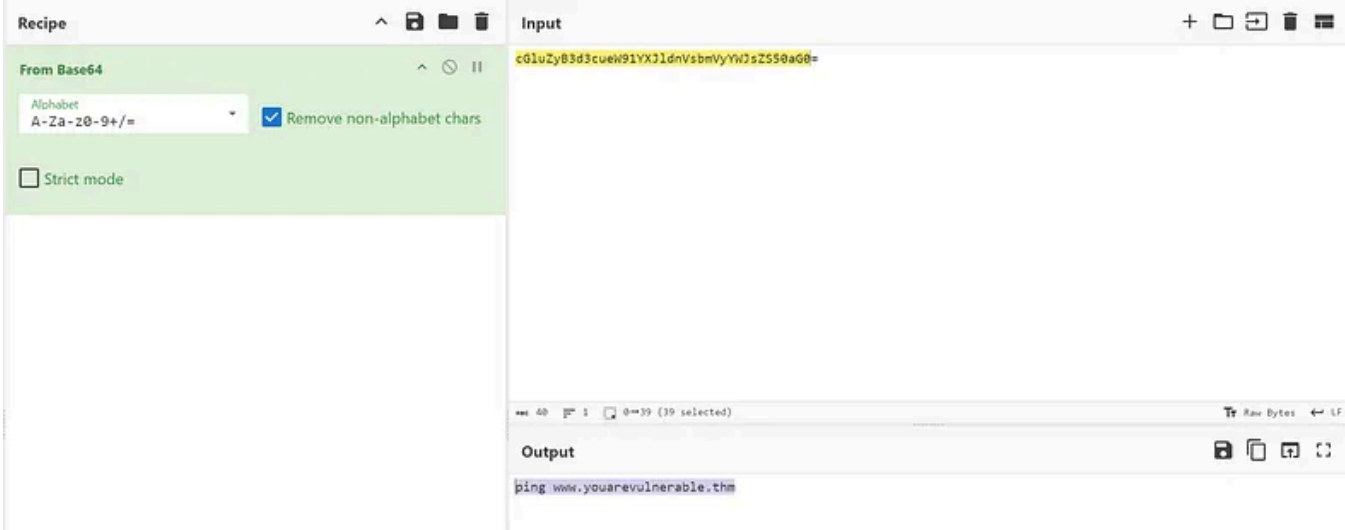
A: ping www.youarevulnerable.thm

This one might seem a bit confusing, but it's actually quite straightforward. Notice that the `data.win.eventdata.parentCommandLine` field contains a long string with seemingly random code. We need to address this, as it includes an encoded string: `cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0=`.

```
t  data.win.eventdata.parentCommandLine  >
\"cmd.exe\" /c \"reg add HKCU\\SOFTWARE\\ATOMIC-T1053.005 /v test /t REG_SZ /d cGluZyB3d3cueW91YXJldnVsbmVyYWJsZS50aG0= /f &amp; s
chtasks.exe /Create /F /TN \"ATOMIC-T1053.005\" /TR \"cmd /c start /min \\\"\\\" powershell.exe -Command IEX([System.Text.Encodin
g]::ASCII.GetString([System.Convert]::FromBase64String((Get-ItemProperty -Path HKCU:\\\\SOFTWARE\\\\ATOMIC-T1053.005).test)))\" /s
c daily /st 12:34\"
```

Source: TryHackMe's Wazuh

We use the powerful tool CyberChef to decode this string easily. And there you have it — our answer!



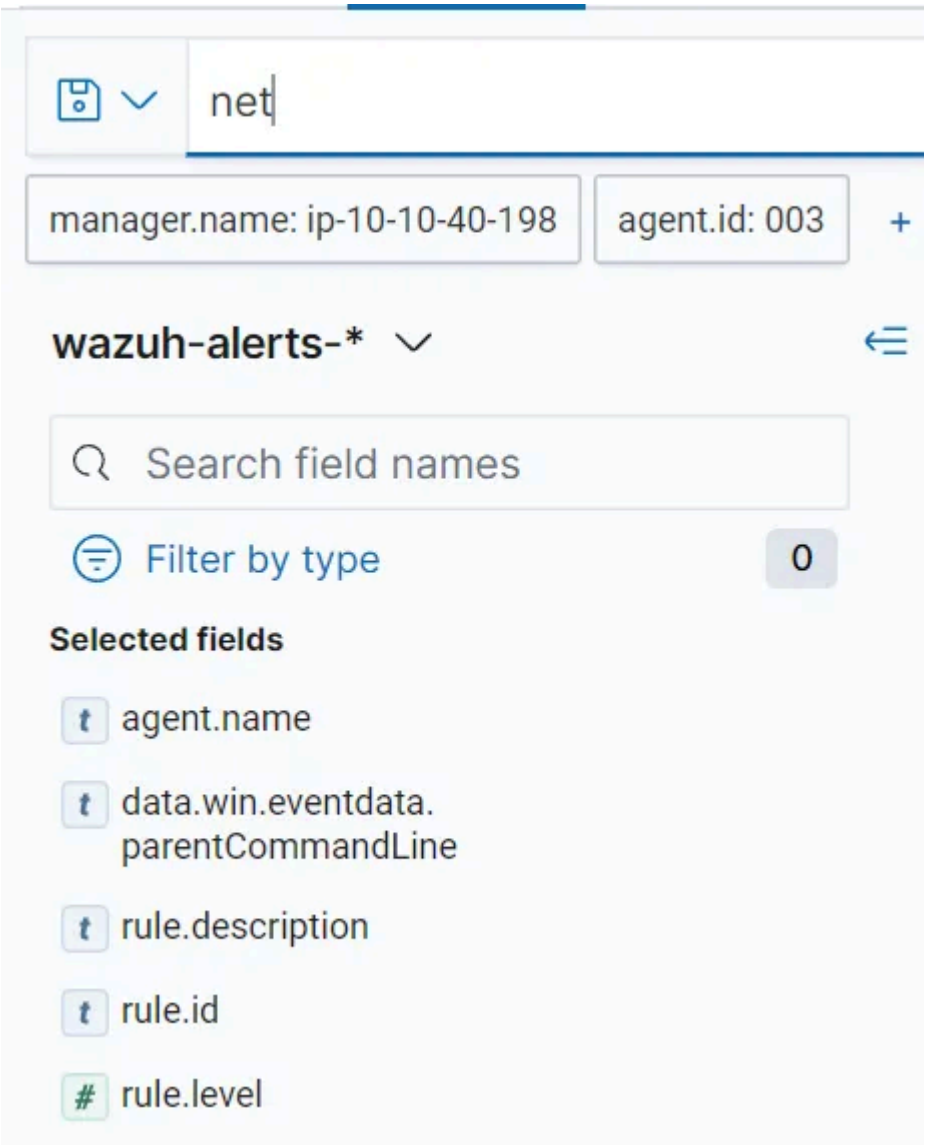
Source: TryHackMe's Wazuh

Question 5

What password was set for the new user account?

A: I_AM_M0NIT0R1NG

To answer this question, search for 'net' in the search bar. Then, look for the answer in the `data.win.eventdata.parentCommandLine` fields.



Source: TryHackMe's Wazuh

Finally, we find it among the other documents!

Source: TryHackMe's Wazuh

Question 6

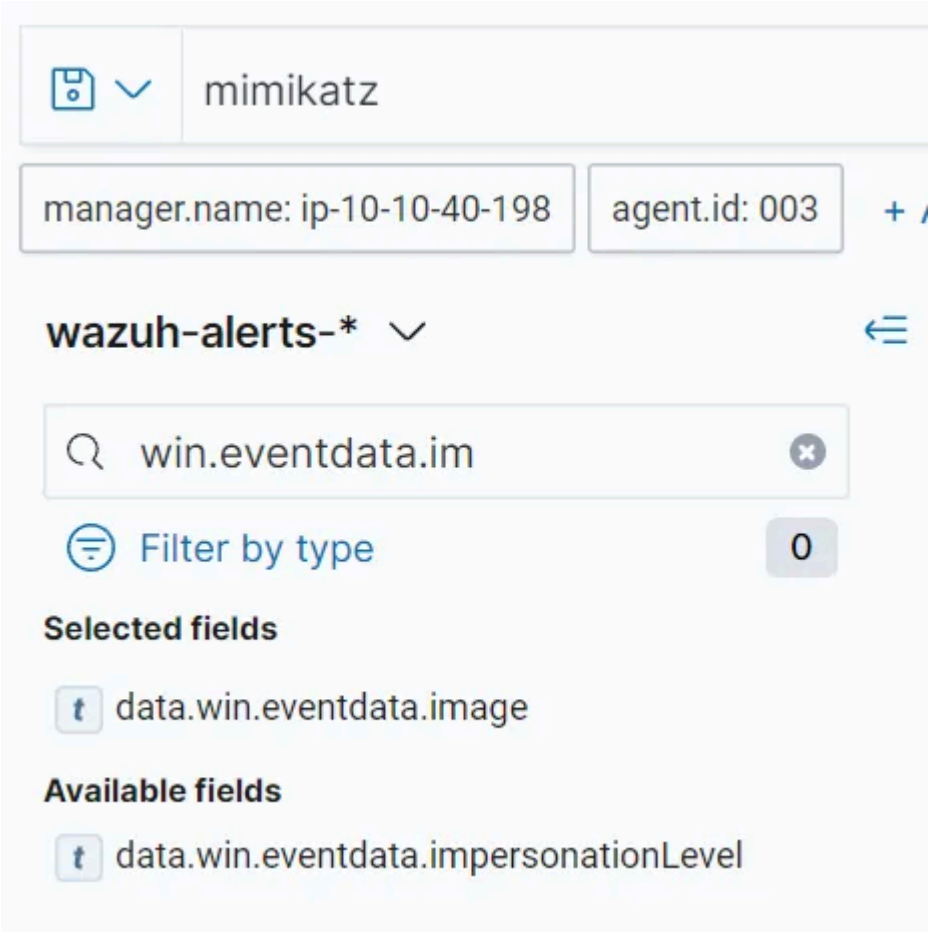
What is the name of the .exe that was used to dump credentials?

A: memotech.exe

To answer this question, search for 'mimikatz' since the question emphasizes dumping credentials.

Mimikatz is a post-exploitation tool used by attackers to extract sensitive credentials, such as passwords and hashes, from a Windows operating system. 13 Mei 2024

After that, filter by `data.win.eventdata.Image`.



Source: www.wallarm.com

And you'll get the answer right away.

Time	agent.name	rule.description	rule.level	rule.id	data.win.eventdata.parentCommandLine	data.win.eventdata.image
Apr 29, 2024 @ 14:21:41.365	Windows_SwiftSpend2	Microsoft Office Product Spawning Windows Shell	12	255008	\"cmd.exe\" /c \"C:\\Tools\\AtomicRedTeam\\atomics\\T1003.001\\bin\\x64\\memotech.exe \"sekurlsa::pth /user:john.sterling /domain:%userdnsdomain% /ntlm:6963989ca61ef2541bd614609964eabc\"\"	C:\\Tools\\AtomicRedTeam\\atomics\\T1003.001\\bin\\x64\\memotech.exe

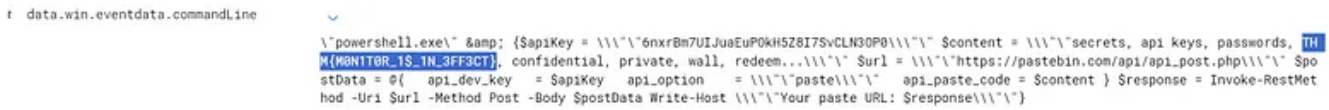
Source: TryHackMe's Wazuh

Question 7

Data was exfiltrated from the host. What was the flag that was part of the data?

A: THM{M0N1T0R_1$_1N_3FF3CT}

This one is straightforward. To find the THM flag, simply search for ‘THM’ in the search bar to avoid missing it. Additionally, focus on `data.win.eventdata.CommandLine` to locate the flag.



That concludes today’s write-up. I hope you followed the step-by-step guide and didn’t just seek the answer.

By understanding how to use Wazuh, a Security Information and Event Management tool, you can gain valuable knowledge for your career or enhance your understanding of cybersecurity tools. :)

Tryhackme Walkthrough | Endpoint Security | Cybersecurity | Blue Team | Cyber Security Awareness

Follow

Written by Fritzadriano

3 Followers · 1 Following

No responses yet

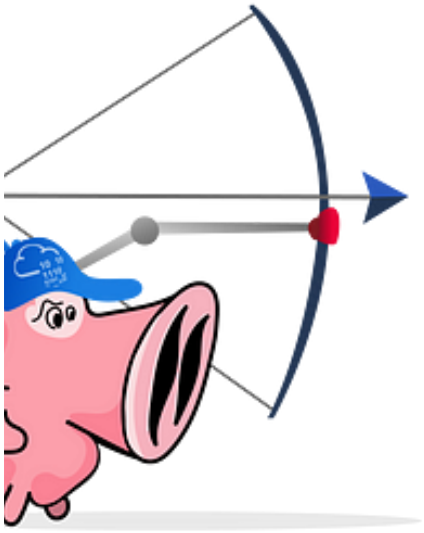
More from Fritzadriano

Fritzadriano

Retracted — TryHackMe WriteUp

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

Sep 4, 2024 50

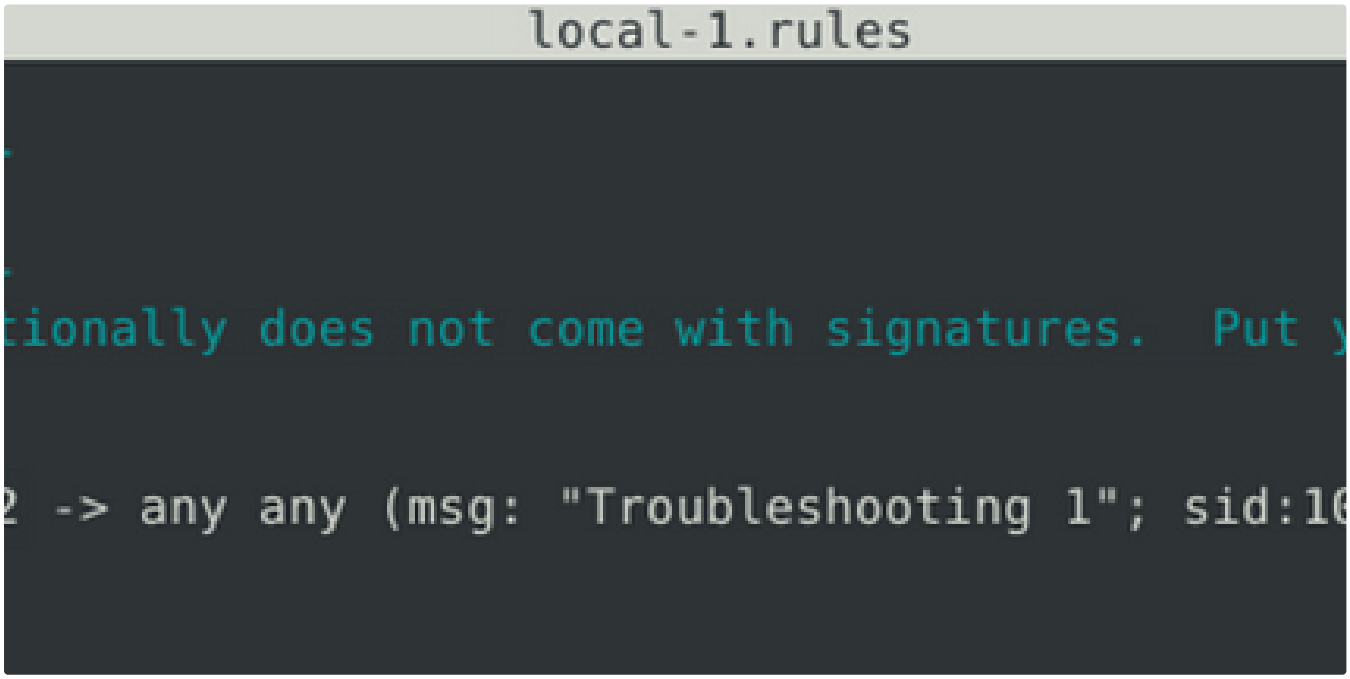


Fritzadriano

Snort Challenge—The Basics WriteUp (Part 1)

Today's writeup aims to investigate a series of traffic data and stop malicious activity under two different scenarios. Let's start...

Aug 6, 2024

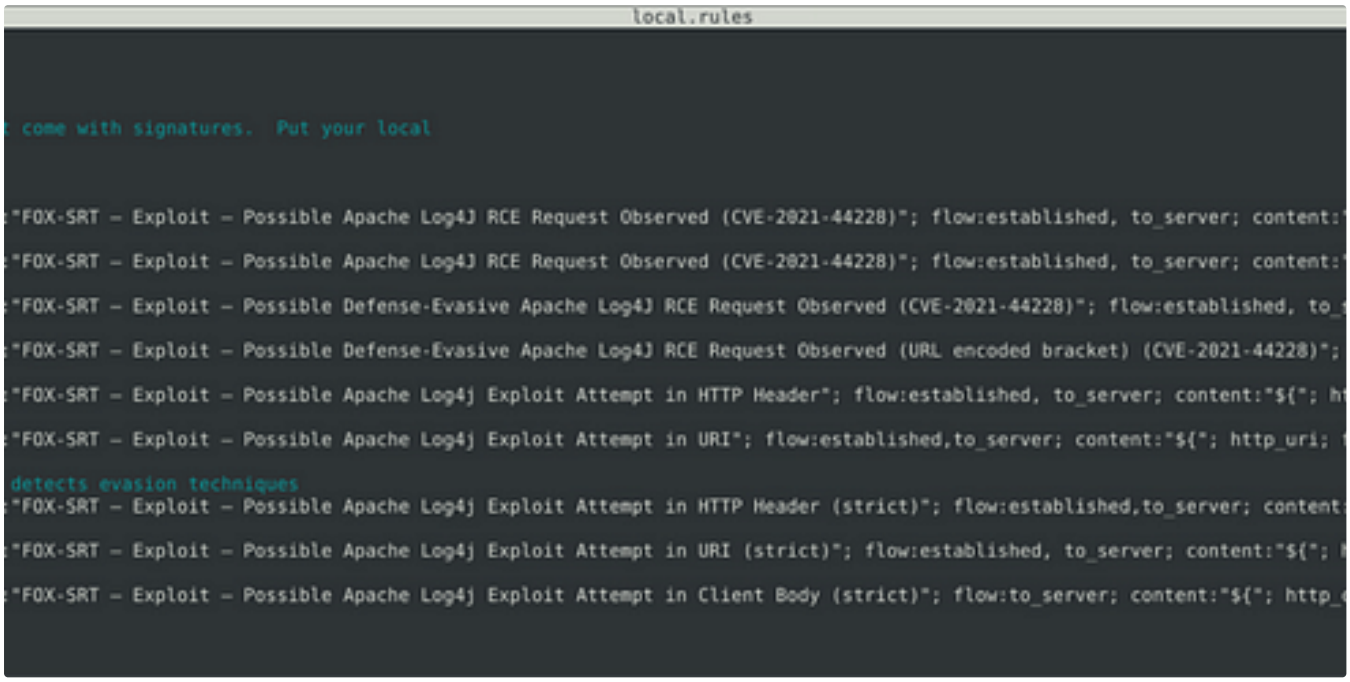


Fritzadriano

Snort Challenge—The Basics WriteUp (Part 2)

In this continuation, we will further explore sophisticated methods for analyzing traffic data and enhancing security measures.

Aug 6, 2024



Fritzadriano

Snort Challenge—The Basics WriteUp (Part 3)

In In this final part, we'll complete our journey in understanding how Snort works, review the insights gained, and discuss final steps to...

Aug 7, 2024

See all from Fritzadriano

Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

High (CVSS: 10.0)
NVT: OpenVAS / Greenbone Vulnerability Manager Default Credentials (OID: 1.3.6.1.4.1.25623.1.0.108554)

Product detection result: cpe:/a:openvas:openvas_manager:7.0 by OpenVAS / Greenbone Vulnerability Manager Detection (OID: 1.3.6.1.4.1.25623.1.0.103825)

Summary

The remote OpenVAS / Greenbone Vulnerability Manager is installed/configured in a way that it has account(s) with default passwords enabled.

Vulnerability Detection Result

```
It was possible to login using the following credentials (username:password:role):

admin:admin:Admin
```

Impact

This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.

Solution

Solution type: Workaround

Change the password of the mentioned account(s).

Vulnerability Insight

It was possible to login with default credentials: admin/admin, sadmin/changeme, observer/observer or admin/openvas.

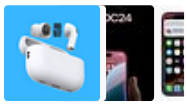
embossdotar

TryHackMe—Vulnerability Scanner Overview—Writeup

Key points: Vulnerability scanners | Vulnerability scanning | CVE | CVSS | OpenVAS.
Vulnerability Scanner Overview by awesome TryHackMe! 🎉

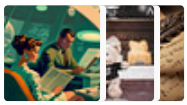
Oct 22, 2024 65 1

Lists



Tech & Tools

22 stories · 380 saves



Medium's Huge List of Publications Accepting Submissions

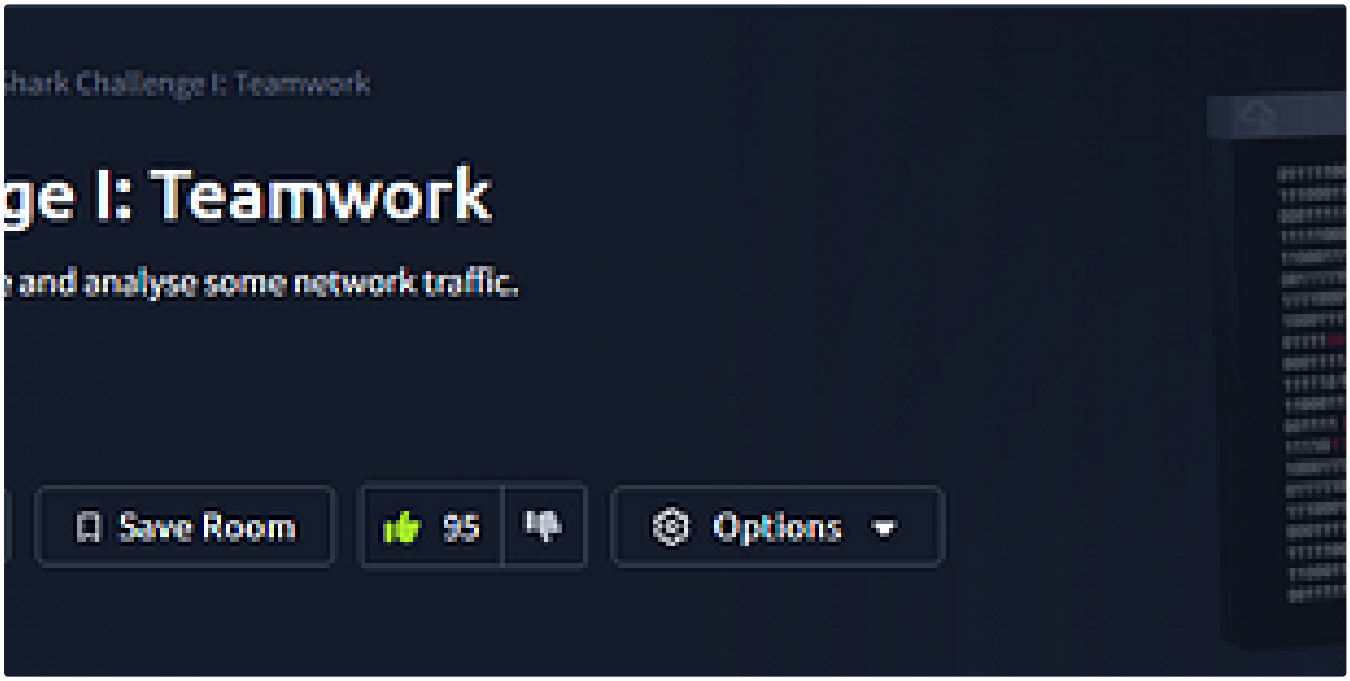
377 stories · 4341 saves

Staff picks

796 stories · 1559 saves

Natural Language Processing

1884 stories · 1529 saves

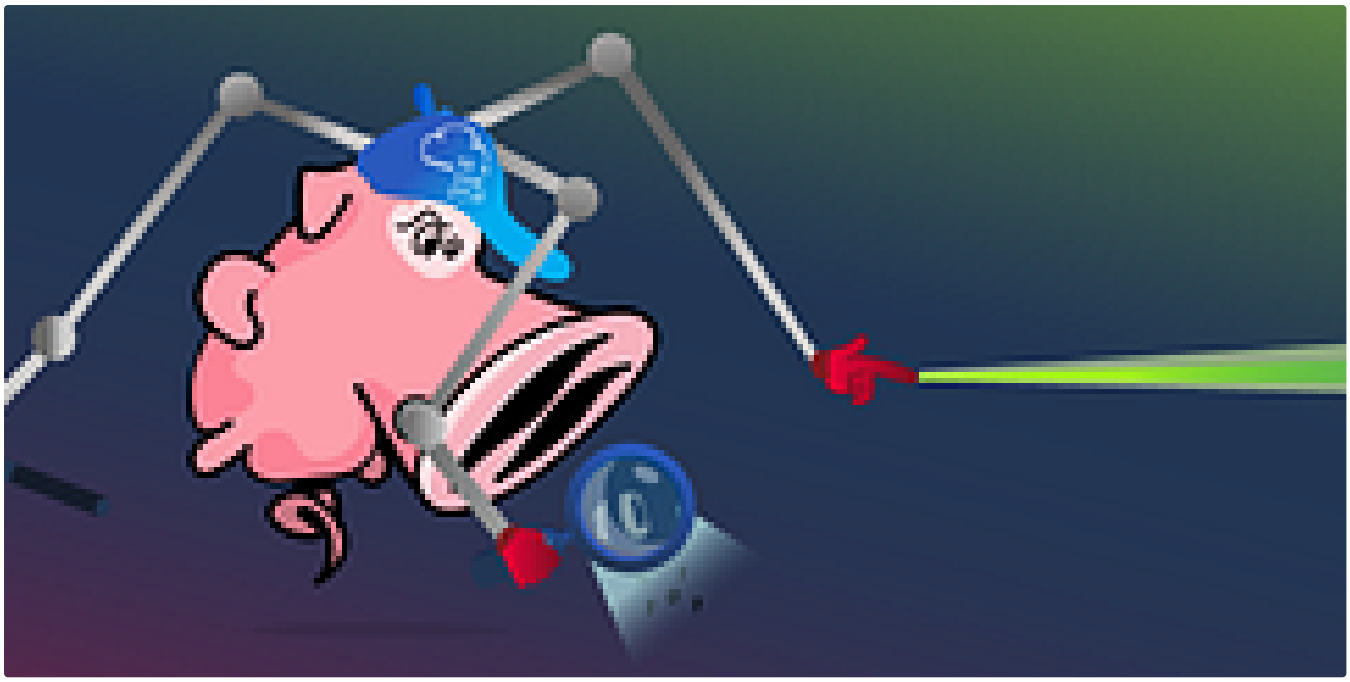


Abhijeet Singh

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

Task 1 - Introduction

Nov 11, 2024



In T3CH by Axoloth

TryHackMe | Snort Challenge—The Basics | WriteUp

Put your snort skills into practice and write snort rules to analyse live capture network traffic

Nov 9, 2024 100

Fritzadriano

Retracted—TryHackMe WriteUp

IInvestigate 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

See more recommendations