

[Open in app](#)

Medium

 Search

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



TryHackMe | ItsyBitsy [Writeup]



Mohamed Ashraf · Following

3 min read · Apr 29, 2023



Listen



Share



More



Difficulty: Medium

Put your ELK knowledge together and investigate an incident

Definition

ELK is the acronym for three open source projects: **Elasticsearch**, **Logstash**, and **Kibana**. **Elasticsearch** is a search and analytics engine. **Logstash** is a server-side data processing pipeline that ingests data from multiple sources simultaneously, transforms it, and then sends it to a **stash** like Elasticsearch. **Kibana** lets users visualize data with charts and graphs in Elasticsearch

Task 1: introduction

In this challenge room, we will take a simple challenge to investigate an alert by IDS regarding a potential C2 communication.

Room Machine

Before moving forward, deploy the machine. When you deploy the machine, it will be assigned an IP **Machine IP:** `10.10.111.176`. The machine will take up to 3-5 minutes to start. Use the following credentials to log in and access the logs in the Discover tab.

Username: Admin

Password: elastic123

Task 2: Scenario — Investigate a potential C2 communication alert

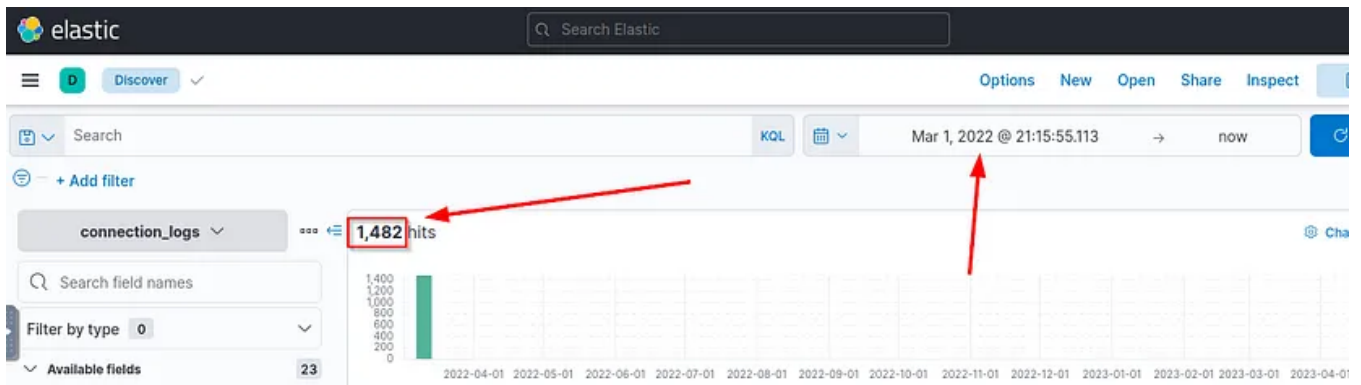
During normal SOC monitoring, Analyst John observed an alert on an IDS solution indicating a potential C2 communication from a user Browne from the HR department. A suspicious file was accessed containing a malicious pattern THM:{ _____ }

*A week-long HTTP connection logs have been pulled to investigate. Due to limited resources, only the connection logs could be pulled out and are ingested into the **connection_logs** index in Kibana.*

Our task in this room will be to examine the network connection logs of this user, find the link and the content of the file, and answer the questions.

Answer the questions below :

1-How many events were returned for the month of March 2022?

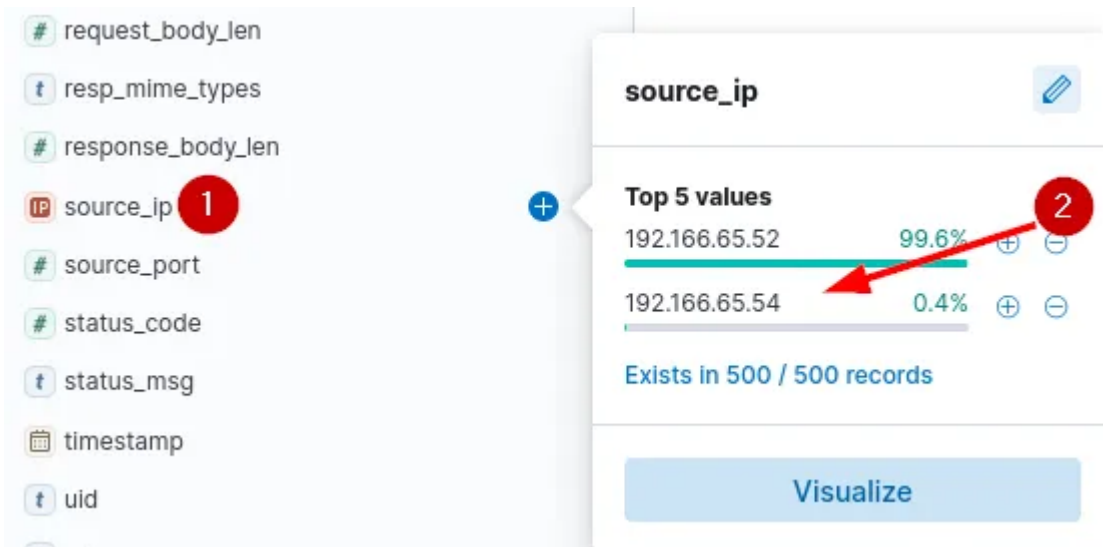


Answer:1482

2-What is the IP associated with the suspected user in the logs?

It asking us what the IP for Browne

Since there is 0.4% traffic, I think this is the abnormal IP address.



Answer:192.166.65.54

3-The user's machine used a legit windows binary to download a file from the C2 server. What is the name of the binary?

# response_body_len	5
IP source_ip	192.166.65.54
# source_port	53,249
# status_code	200
t status_msg	OK
📅 timestamp	Mar 10, 2022 @ 11:23:11.924911000
t uid	C8D20I2ggQSCXNNZn7
t uri	/yTg0Ah6a
t user_agent	bitsadmin
# version	3.2

Answer:bitsadmin

Bitsadmin is a command-line tool used to create, download or upload jobs, and to monitor their progress.

4-The infected machine connected with a famous filesharing site in this period, which also acts as a C2 server used by the malware authors to communicate. What is the name of the filesharing site?

Hint:We can find the domain address by inspecting the 'host' parameter.

# _score	-
t _type	_doc
📅 @timestamp	Mar 10, 2022 @ 11:23:11.924911000
IP destination_ip	104.23.99.190
# destination_port	80
t host	pastebin.com
t index	http_traffic

Answer:pastebin.com

5-What is the full URL of the C2 to which the infected host is connected?

Hint: Combine “ host + uri ”

timestamp	Mar 10, 2022 @ 11:23:11.924911000
uid	C8D20I2ggQSCXNNZn7
uri	/yTg0Ah6a

uri

host : pastebin.com

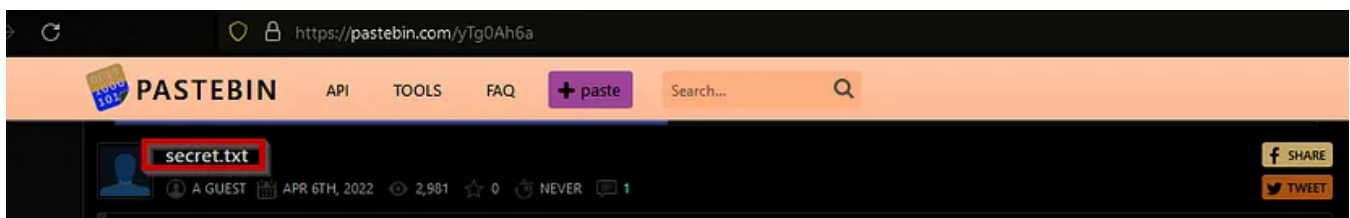
uri = /yTg0Ah6a

—Answer : **pastebin.com/yTg0Ah6a**

6-A file was accessed on the filesharing site. What is the name of the file accessed?

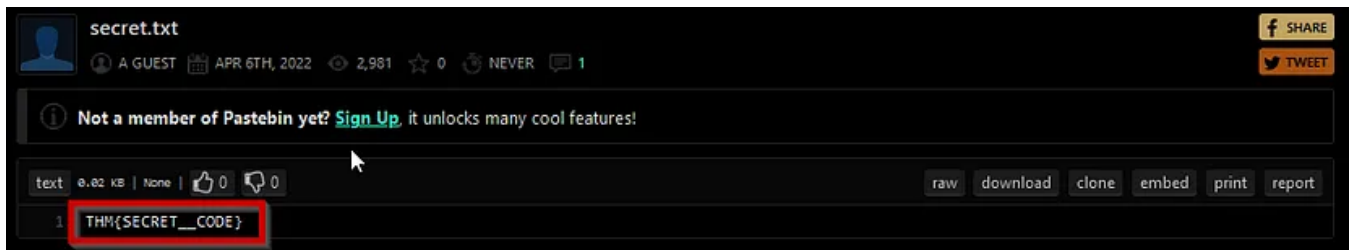
Hint:

- This connect to previous question:
- Go to the link and you will find the name



Answer: **secret.txt**

7-The file contains a secret code with the format THM{_____}.



Answer: THM{SECRET__CODE}

Thank you for your time and Happy Hacking ♥♥

Cybersecurity

Hacking

Security Analytics

Elk

Defensive Security



Following

Written by Mohamed Ashraf

92 Followers · 6 Following

Penetration tester && Jr Security Analyst | SOC L 1 | studied {OSCP|CCRTA|CRTO|CAP} | Top 1% on TryHackMe

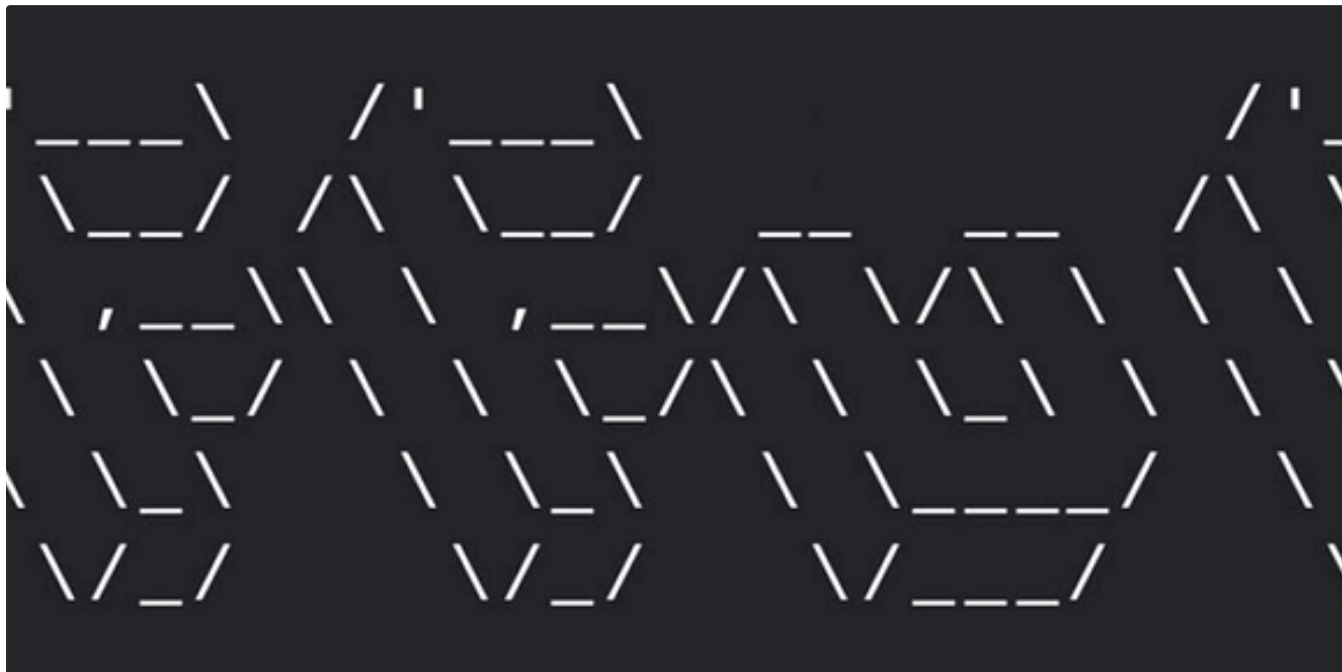
No responses yet



What are your thoughts?

Respond

More from Mohamed Ashraf



 Mohamed Ashraf

Attacking Web Applications with Ffuf | Skills Assessment — Walkthrough

Hello friend, how are you? I hope you are well.

May 31, 2024  9

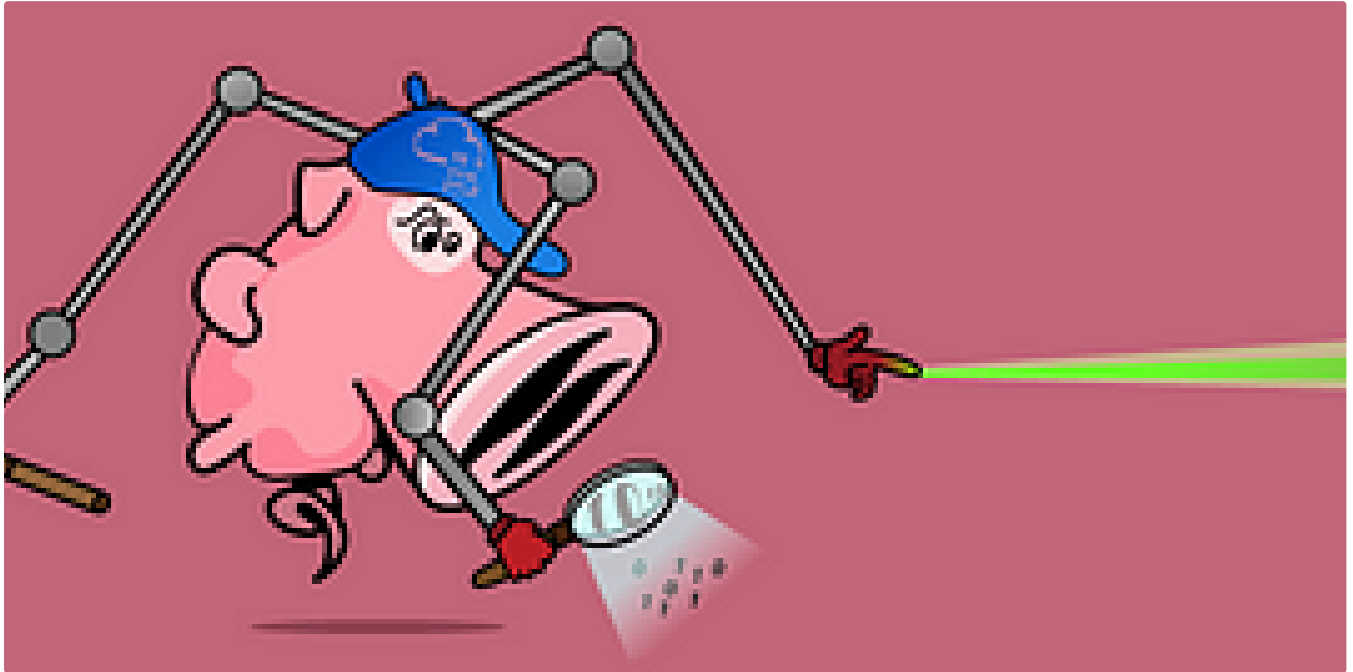





socat | Cheat Sheet

By Mx0o14

May 25, 2023 🖱 2



 In System Weakness by Mohamed Ashraf

TryHackMe | Snort Challenge—The Basics

Task 1: introduction

Apr 17, 2023 🖱 8





Mohamed Ashraf

TryHackMe|AV Evasion: Shellcode

by Mx0o14

Nov 2, 2024



24



See all from Mohamed Ashraf

Recommended from Medium

nts

	▼	User Name	▼	Name	▼	Surname	▼	Email
3		student1		Student1				studi
4		student2		Student2				studi
5		student3		Student3				studi
9		anatacker		Ana Tacker				
10		THM{Got.the.User}		X				
11		qweqwe		qweqwe				

« ‹ 1 › »



embossdotar

TryHackMe—Session Management—Writeup

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



Aug 7, 2024



27



In Offensive Black Hat Hacking & Security by Harshad Shah

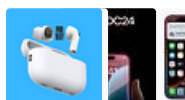
Cybersecurity Roadmap 2025

How to start cybersecurity in 2025?

★ Dec 14, 2024 🖱 107 💬 1



Lists



Tech & Tools

22 stories · 387 saves



Medium's Huge List of Publications Accepting Submissions

414 stories · 4387 saves



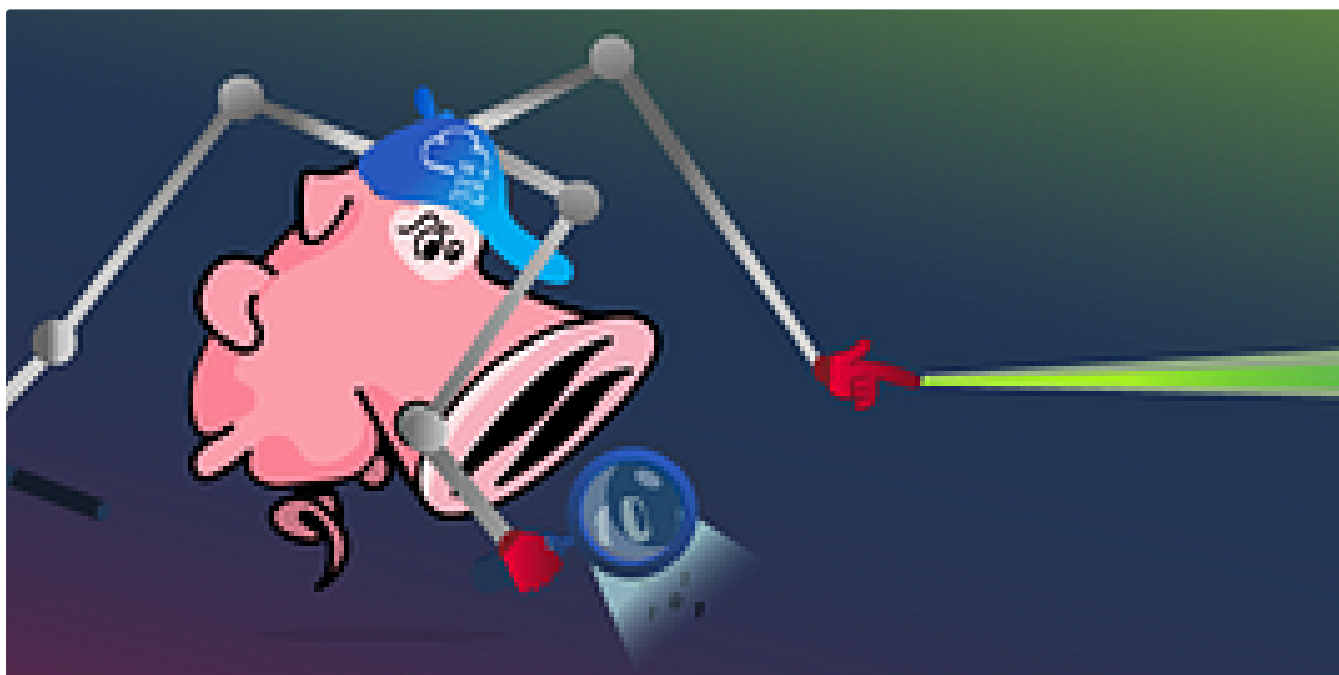
Staff picks

800 stories · 1569 saves



Natural Language Processing

1889 stories · 1546 saves



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



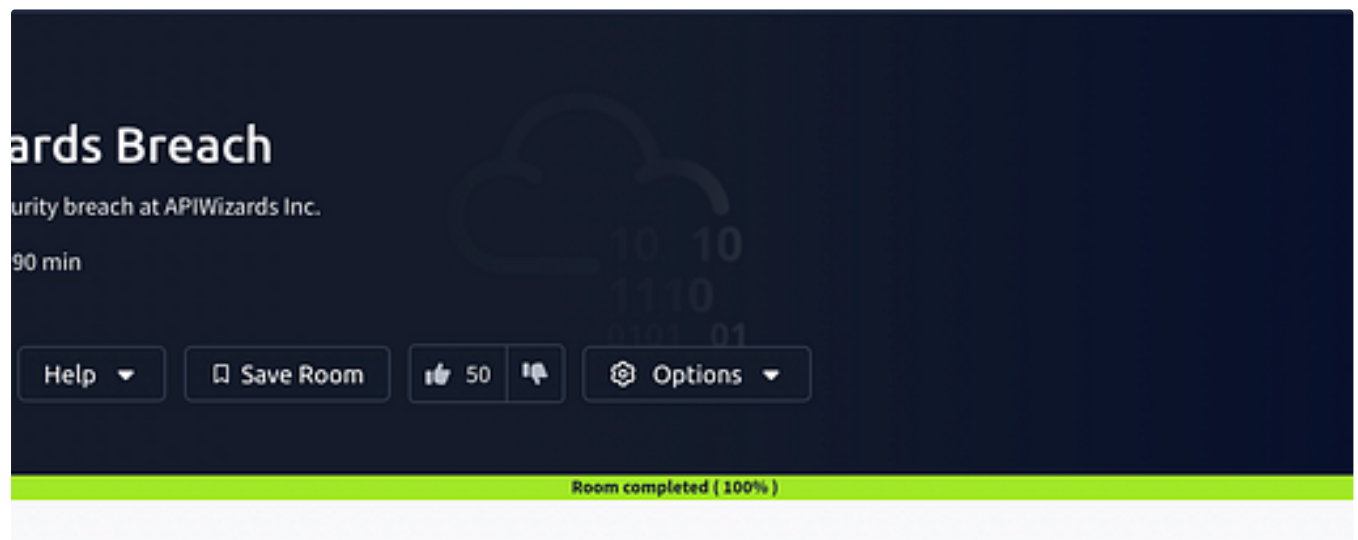


 Sunny Singh Verma [SuNnY]

IR Playbooks TryHackMe Walkthrough Writeup THM |—SuNnY

Kudos to The Creators of this Room :

Sep 13, 2024  100  1



board  Write-ups

 Aakash Raman

TryHackMe APIWizards Breach Walkthrough

This is an interesting room for all the DFIR Enthusiasts on Linux Forensics & Linux Persistence Techniques! Let's get started!

Aug 5, 2024 🖱 58



Visir

THM | Microservices Architectures| Write-Up

As microservices architectures continue to rise in popularity, Kubernetes has become a key platform for managing containerized...

Sep 24, 2024 🖱 153

[See more recommendations](#)