HTB Meetup #4

Welcome to HTB Meetup #4

Organizer intro

- Cybersecurity community in IIUM
- Proudly full of skill issue people
- Clap for organizer lesgoo!

Whoami?

- My name is Syamil Yusof
- Student at IIUM
- ICE Community Founder
- MCC2025 Agent
- HTB Meetup Kuala Lumpur Host
- Connect me at LinkedIn:)

& Supporters Sponsors





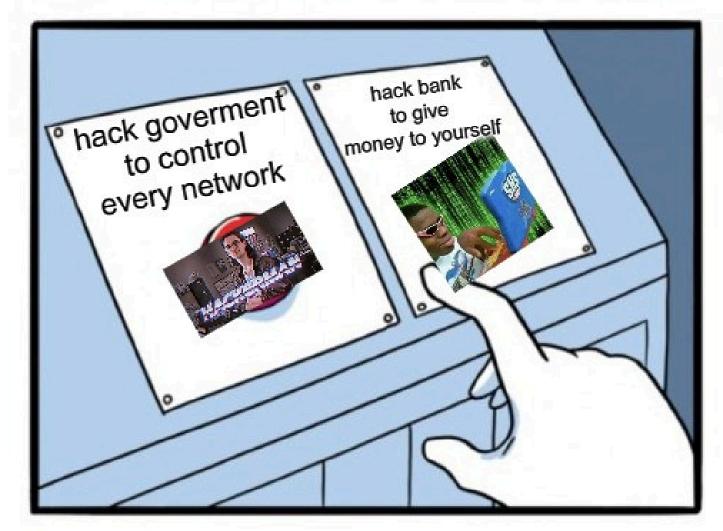






HTB in Nutshell

- Online platform to learn cybersecurity hands-on
- Realistics labs, machines and challenges
- Have labs, academy, enterprise
- Its legal





Why do HTB Meetup and some disclaimer

HTB Sherlock

- Labs to upgrade our defensive skills
- SOC, TI, ICS, Malware Analysis and many more
- Difficulties from Very Easy to Insane
- Disclaimer again: I also not yet good in this

Whats for today?

We play 2 sherlocks
We eat
We do SpeedHack : DFIR Edition

Things Not Allowed in This Meetup

To say "This is hard"

Say "Not yet easy" instead:)

Quiz Time!

HTB Enterprise

After this slides is for second sherlock

Sherlock #2 - Dream Job 1

Challenge Description

You are a junior threat intelligence analyst at a Cybersecurity firm. You have been tasked with investigating a Cyber espionage campaign known as Operation Dream Job. The goal is to gather crucial information about this operation.

Understanding the Challenges

- 1. Espionage campaign Operation Dream Job
- 2. To gather crucial information about this operation

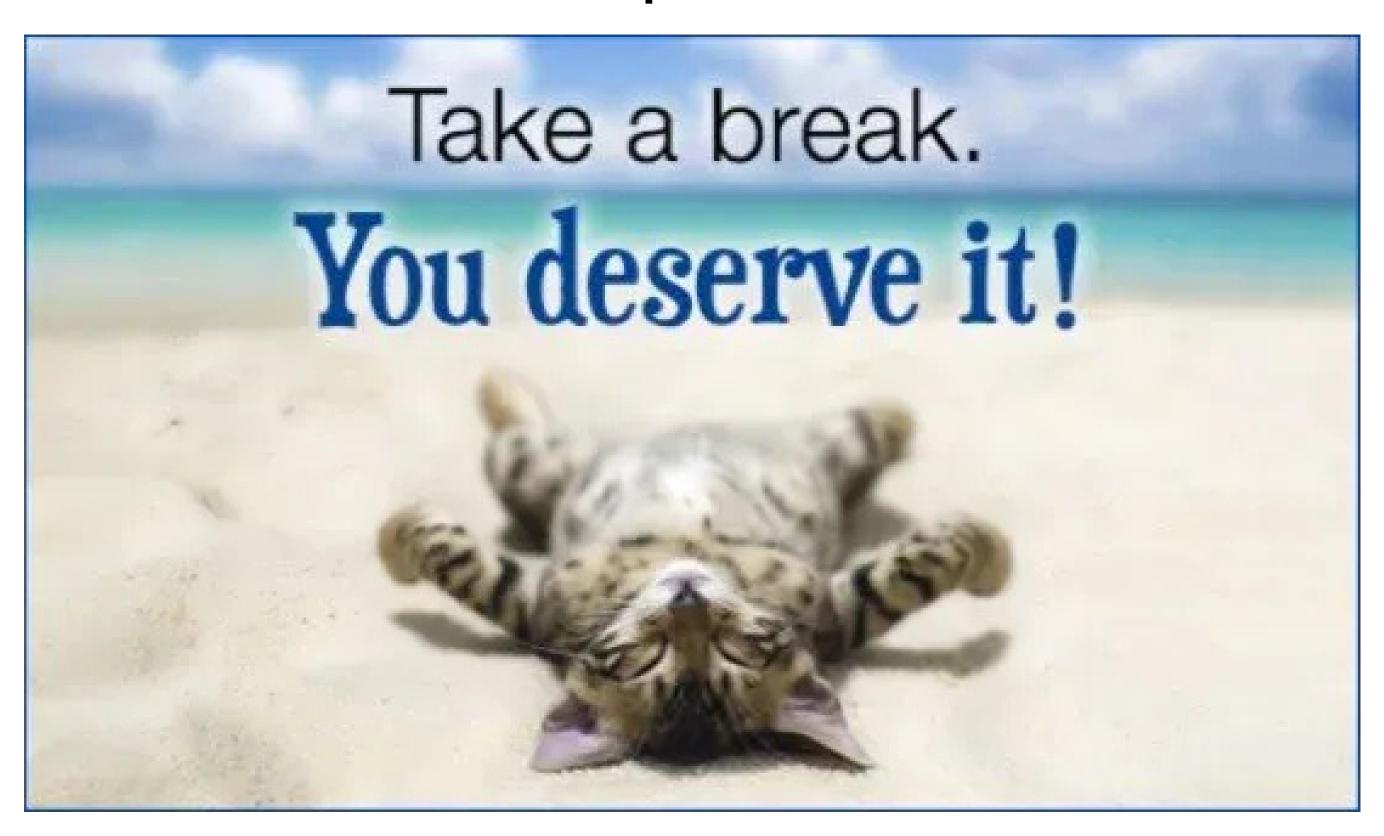
Step #1

Understand how do we gather information of cyber attack

MITRE ATT&CK Framework

- Stands for Adversarial Tactics, Techniques and Common Knowledge
- Framework created by MITRE
- Catalog of how real-world cyber attackers behave
- https://attack.mitre.org/

Step #1.5



Step #2

No more slides, lets go through the web

Step #3

Yeay we are now a CTI, lesgo! (daydreaming)



Quiz Time!

Lets Take A Break

Lets Eat We gonna resume at 10:xx

SpeedHack: DFIR Edition!

After this is closing timee!

Lucky Draw!

Feedback



Feedback Form

- 1. Don't forget to give feedback in Meetup.com
- 2. Tag Us At Linkedln!
 a. SIG Cybersecurity IIUM
 b. ICE

Our LinkedIn





Thats all for today guys :~) Thank you for joining us!