บจก.สยามถนัดแฮก

NCSA CTF Boot Camp #2

Capture The Flag (CTF)

Responsible: Mr. Pichaya Morimoto
Version (Date): 1.0 (2024-09-14)
Confidentiality class: Public

whoami

Pichaya (LongCat) Morimoto
Lead Penetration Tester
Siam Thanat Hack Co., Ltd.

Peeratach (Peter) Butto
Penetration Tester
Siam Thanat Hack Co., Ltd.

Yasinthon (Not) Khemprakhon
Penetration Tester
Siam Thanat Hack Co., Ltd.

Disclaimer

- จุดประสงค์ของการบรรยาย นี้เพื่อแบ่งปันความรู้ ทางด้านความปลอดภัยระบบสารสนเทศ
- ไม่สนับสนุนการนำความรู้ทางด้านความปลอดภัยฯ ไปใช้ในทางที่ผิดกฎหมายทั้งหมด
- ตัวอย่างโค้ด และรูปใน การบรรยาย นี้ เป็นระบบจำลองของทางผู้บรรยาย ไม่ใช่ระบบลูกค้า

Agenda (Day 1)

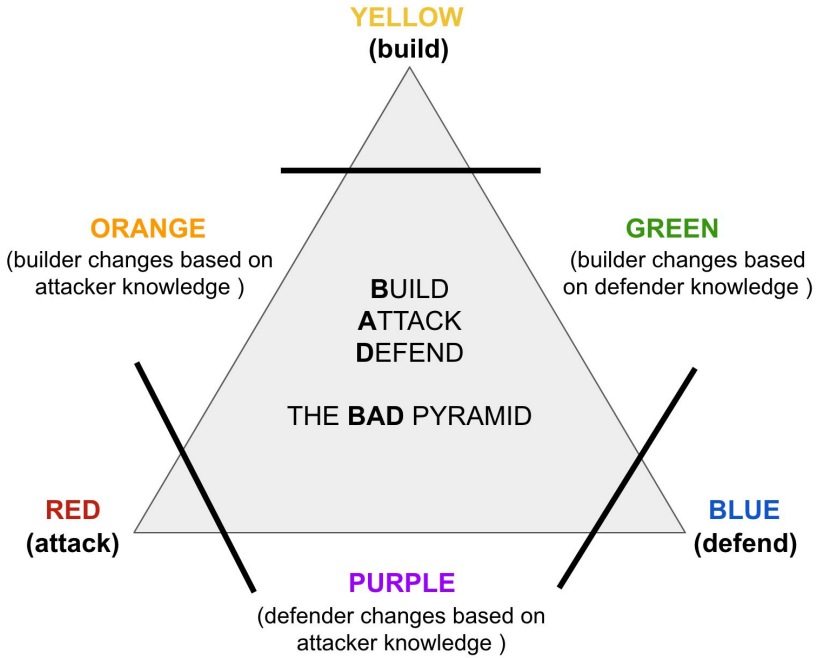
เวลา	รายละเอียด
09.15 - 09.45	ความรู้เบื้องต้นเกี่ยวกับ CTF
09.45 - 10.30	Network Security
10.30 - 10.45	พักเบรก
10.45 - 12.00	Web Application Security
12.00 - 13.00	พักรับประทาน อาหารกลางวัน
13.00 - 14.30	Digital Forensics
14.30 - 14.45	พักเบรก
14.45 - 16.00	Pwnable & Reverse Engineering
16.00 - 18.00	เข้าห้องพัก
18.00 - 19.00	รับประทานอาหารเย็น
19.00 - 21.00	เสวนาแนะแนวเส้นทางอาชีพ

Content Overview

1. **ศักยภาพของคน IT Security**
   - BAD (Build, Attack, Defend)
   - IT Security Certification
   - Learning Pyramid
2. **Online Learning Platform**
   - BlueTeamLabOnline (BTLO)
   - HackTheBox (HTB)
   - TryHackMe (THM)
3. **TryHackMe Platform**
   - Room
   - Learning Path
   - AttackBox & VPN
   - Blue Team Rooms
4. **Capture The Flag (CTF)**

บจก.สยามถนัดแฮก

BAD (Build, Attack, Defend)



Red Teams (Offensive Security)
- Penetration Tester
- Red Teamer (Adversary Simulation)

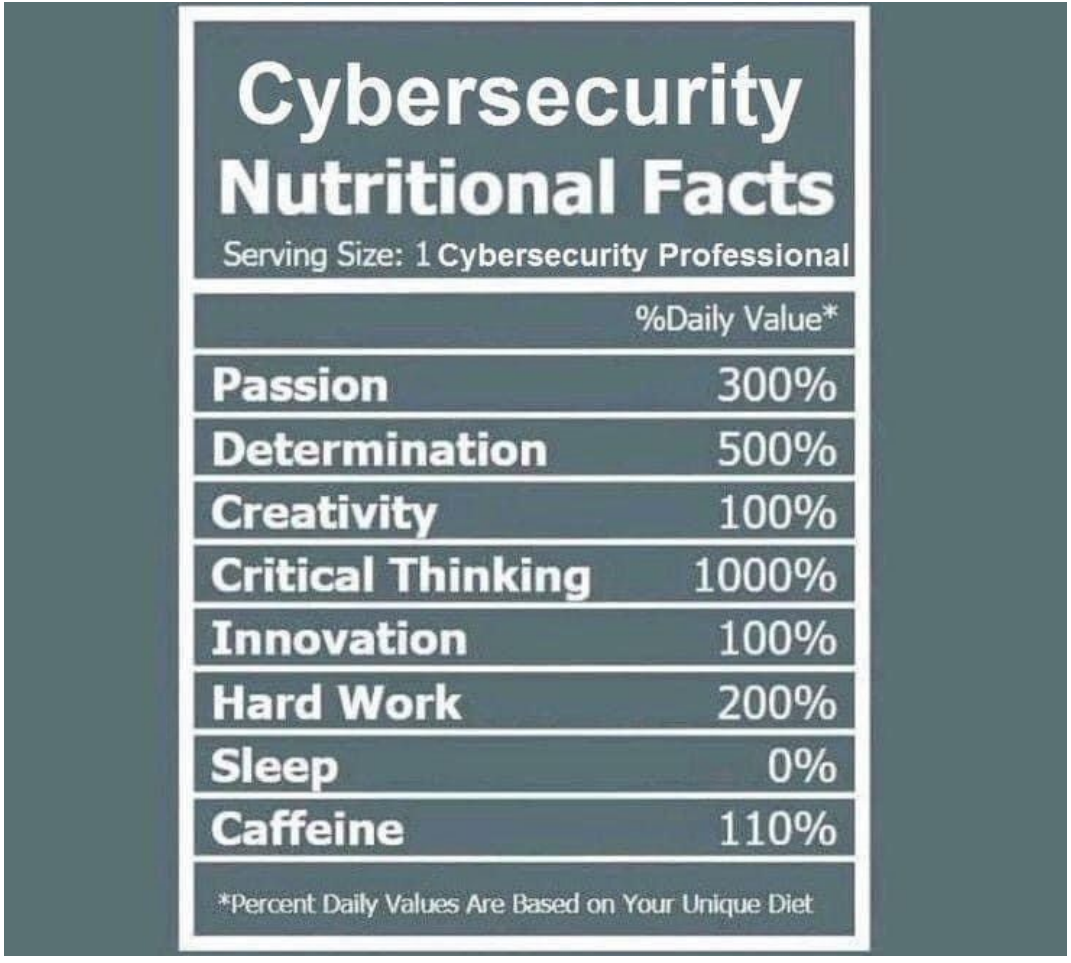
Blue Teams (Defensive Security)
- IT Security Compliance
- Internal Security Team
- IT Security Engineer (SI)
- IT Security Consultant
- Incident Responder
- Security Analyst (SOC)
- Cyber Threat Hunter
- Digital Forensics Examiner

Purple Teams
- Red + Blue

ที่มา: https://danielmiessler.com/study/red-blue-purple-teams/

Cybersecurity Nutritional Facts

- Passion (ความหลงใหล)
- Determination (ความมุ่งมั่น)
- Creativity (ความคิดสร้างสรรค์)
- Critical Thinking (การคิดวิเคราะห์)
- Innovation (สร้างนวัตกรรม)
- Hard Work (ทำงานหนัก)
- ~~*Sleep (นอน)*~~
- Caffeine (กาแฟ)



Challenges in Cybersecurity Talent Acquisition

- Everyone is looking for senior IT security staff
- Less open positions for junior IT security staff
- Hire junior IT security staff to do mid-level cybersecurity tasks

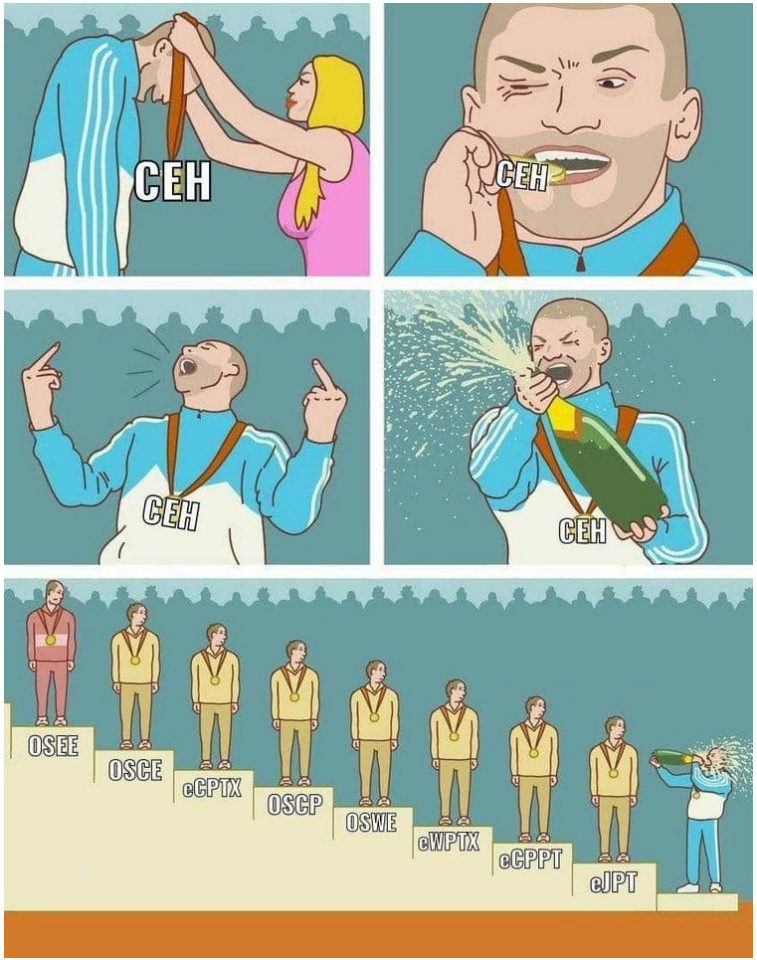
e.g.
  - 0-year experience
    - Penetration Tester
    - SOC Tier-1 Analyst
    - …

คนที่ไม่รู้ คนที่รู้

IT Security Certifications

Common Misconceptions:

- Certification equals expertise
- All certifications are equally valuable
- One-size-fits-all certification
- Certifications guarantee job security
- Certifications are only for beginners
- Recertification is not necessary

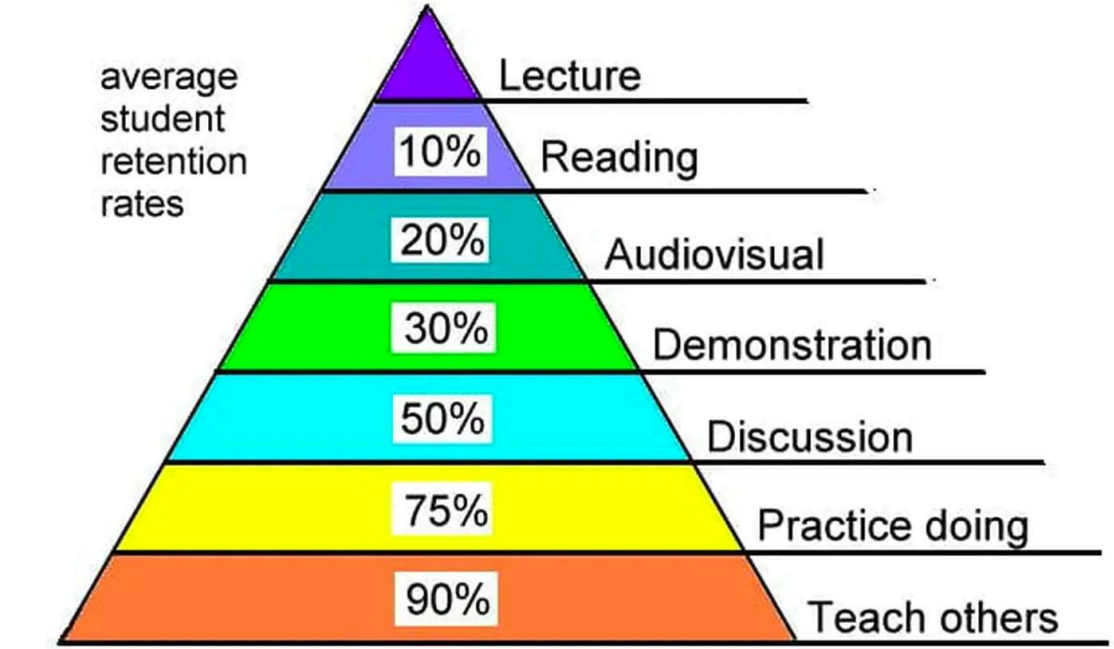


Dunning Kruger Effect

- Individuals with low ability at a task tend to overestimate their ability
- While those with high ability underestimate their own competence.

Source: BrandThink
https://www.facebook.com/brandthink.me/posts/2471666556492215/

Learning Pyramid



Source: National Training Laboratories, Bethel, Maine

ความรู้พื้นฐาน IT Security สำคัญกว่า “เครื่องมือ”

เขียนโปรแกรม

ระบบปฏิบัติการ
(Linux/Windows Server)

ระบบเครือข่าย
คอมพิวเตอร์

IT Security

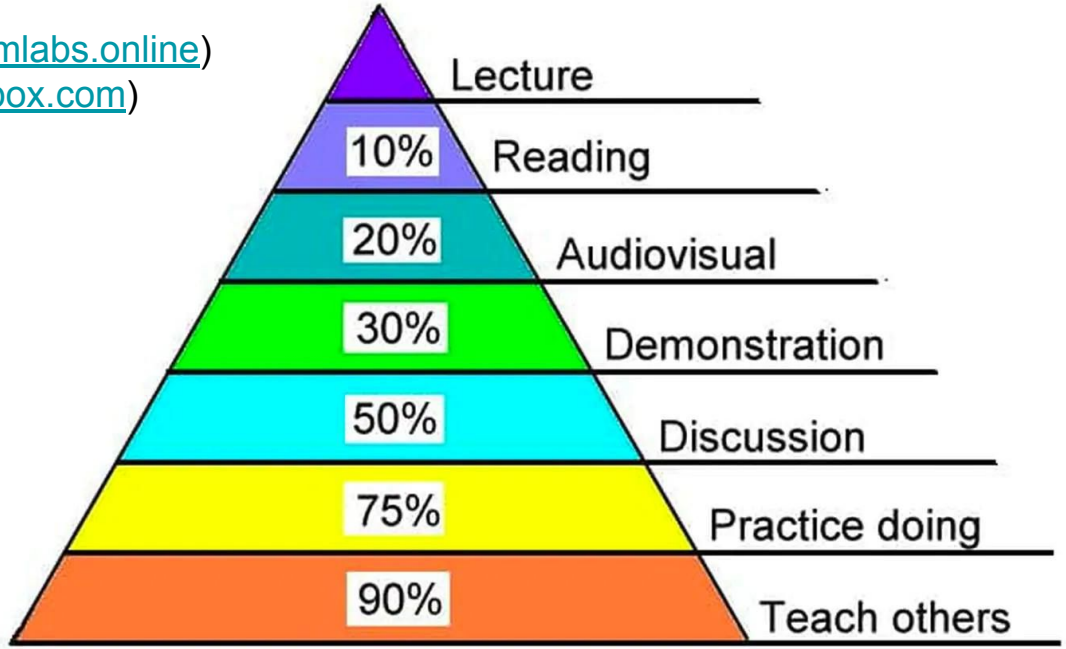
Platform แนะนำสำหรับการพัฒนาบุคลากร

ตัวอย่าง Online Learning Platform:

1. BlueTeamLabOnline (https://blueteamlabs.online)
2. Hack The Box (https://www.hackthebox.com)
3. TryHackMe (https://tryhackme.com)

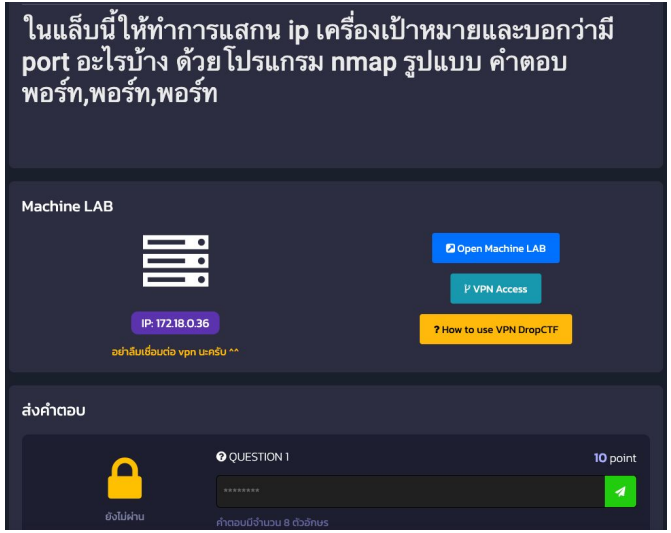
รูปแบบการเรียนรู้ :

- Lecture (มีคนพูดให้ฟัง)
- Reading (อ่านเอง)
- Demonstration (มีคนทำให้ดู)
- Practice by Doing (ลองทำเอง)

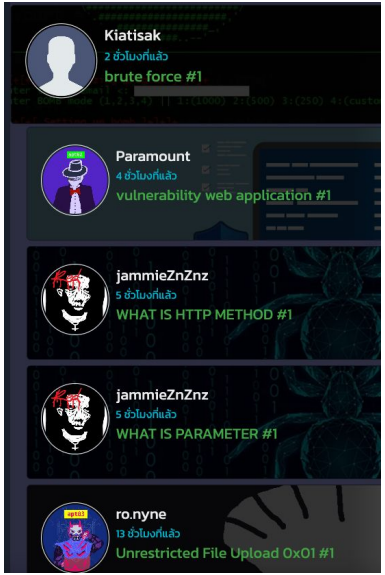


Source: National Training Laboratories, Bethel, Maine

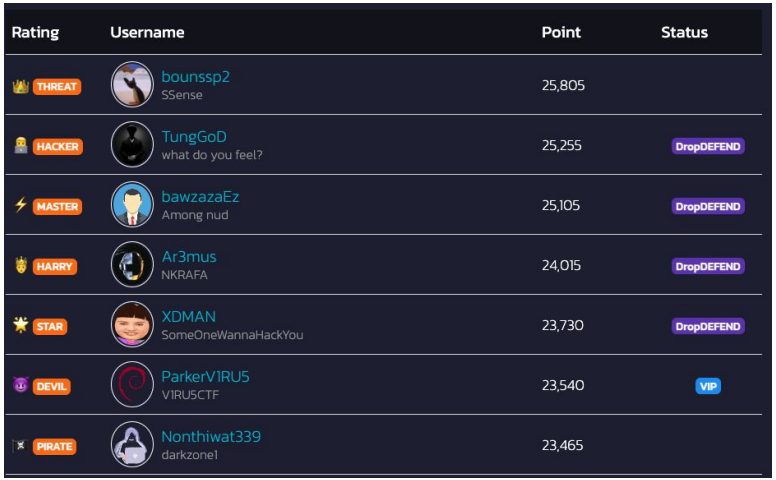
Gamification



Scenario + Point



Live Feed



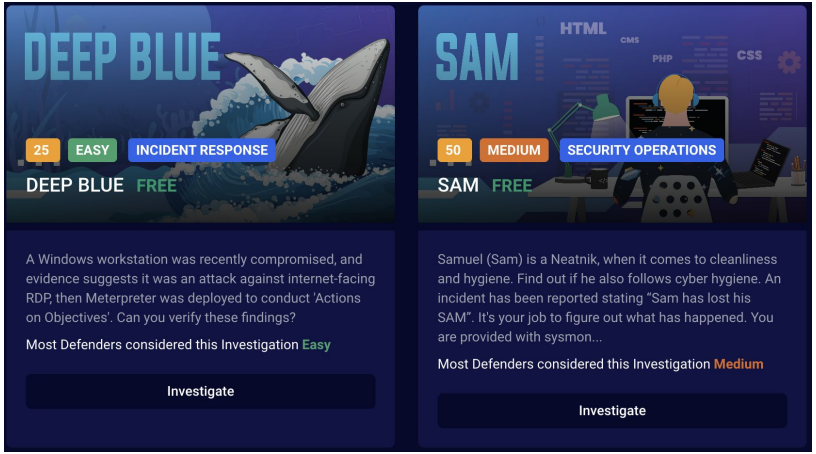
User Ranking

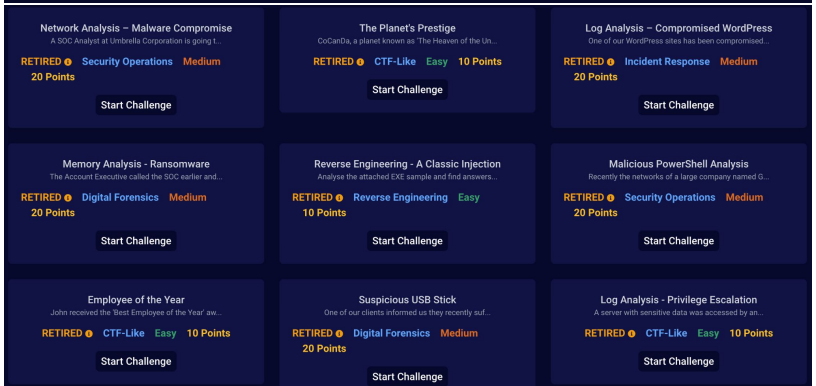
Badge

1 - Blue Team Lab Online (BTLO)

URL: https://blueteamlabs.online

- Interactive lab
- เน้น Blue Team
  - Threat Hunting
  - Digital Forensics
- รองรับ ภาษาอังกฤษ
- น่าเชื่อถือ เป็นที่รู้จักระดับสากล
- โจทย์แบบ
  - Investigation Lab
  - Challenge
- มีโจทย์ฟรี และ เสียเงิน

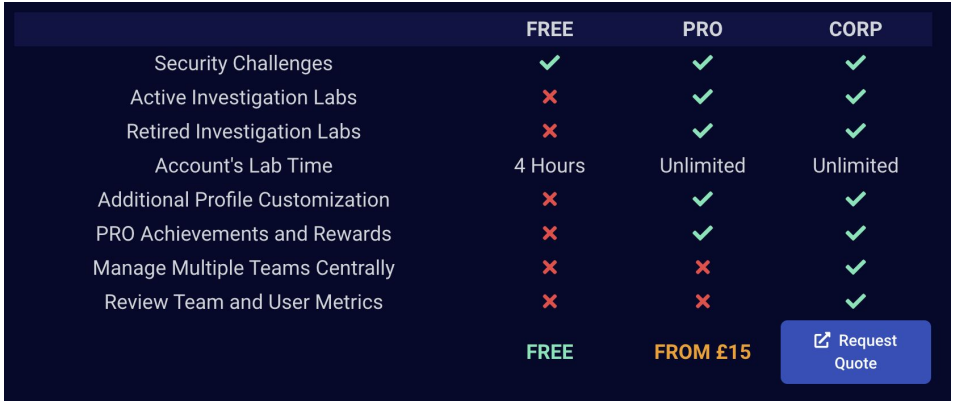




1 - Blue Team Lab Online (BTLO)

ฟรี:
- เล่นได้แต่ Challenge
- Investigation มีฟรี 2 Lab (ลองเล่นได้ 4 ชั่วโมง)

Pro:
- Investigation Lab ทั้งหมด
- 1 เดือน / 600 บาท
- 1 ปี / 5500 บาท



	FREE	PRO	CORP
Security Challenges	✓	✓	✓
Active Investigation Labs	✗	✓	✓
Retired Investigation Labs	✗	✓	✓
Account's Lab Time	4 Hours	Unlimited	Unlimited
Additional Profile Customization	✗	✓	✓
PRO Achievements and Rewards	✗	✓	✓
Manage Multiple Teams Centrally	✗	✗	✓
Review Team and User Metrics	✗	✗	✓
	FREE	FROM £15	Request Quote

1 - Blue Team Lab Online (BTLO)

โจทย์แบบ Challenge

หมวด :

- Incident Response
- Digital Forensics
- Security Operations
- Reverse Engineering
- OSINT
- Threat Hunting
- Threat Intelligence

1 - Blue Team Lab Online (BTLO)

โจทย์แบบ Challenge

The Report

You are working in a newly established SOC where still there is lot of work to do to make it a fully functional one. As part of gathering intel you were assigned a task to study a threat report released in 2022 and suggest some useful outcomes for your SOC.

PDF Reader

Points	Difficulty	Solves	OS
10	Easy	3064	Windows/Linux

Report.zip
10.4MB

Password
BTLO

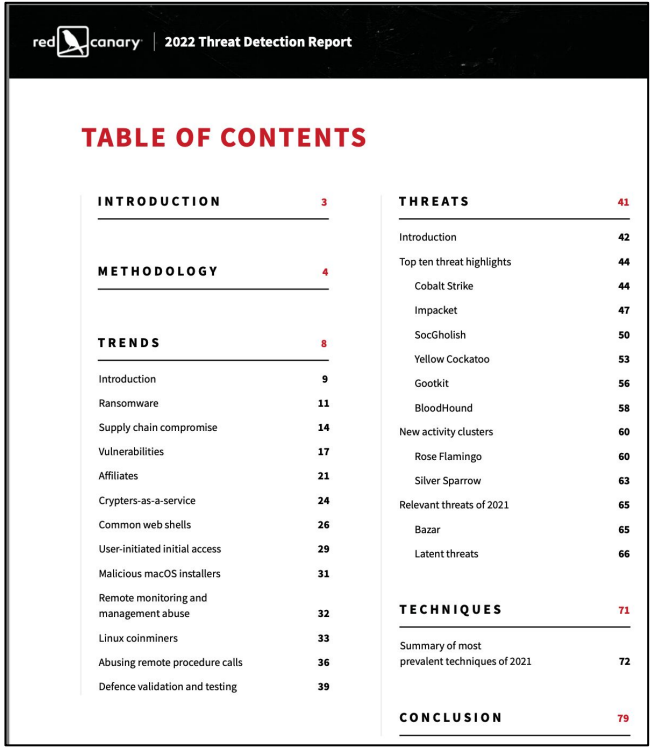
Download File

red canary | 2022 Threat Detection Report

TABLE OF CONTENTS

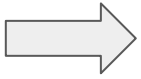
1 - Blue Team Lab Online (BTLO)

โจทย์แบบ Challenge



red canary | 2022 Threat Detection Report

TABLE OF CONTENTS



Challenge Submission

Question 1) Name the supply chain attack related to Java logging library in the end of 2021 (Format: AttackNickname) *(1 points)*

Format: AttackNickname Submit

Question 2) Mention the MITRE Technique ID which effected more than 50% of the customers (Format: TXXXX) *(1 points)*

Format: TXXXX Submit

Question 3) Submit the names of 2 vulnerabilities belonging to Exchange Servers (Format: VulnNickname, VulnNickname) *(1 points)*

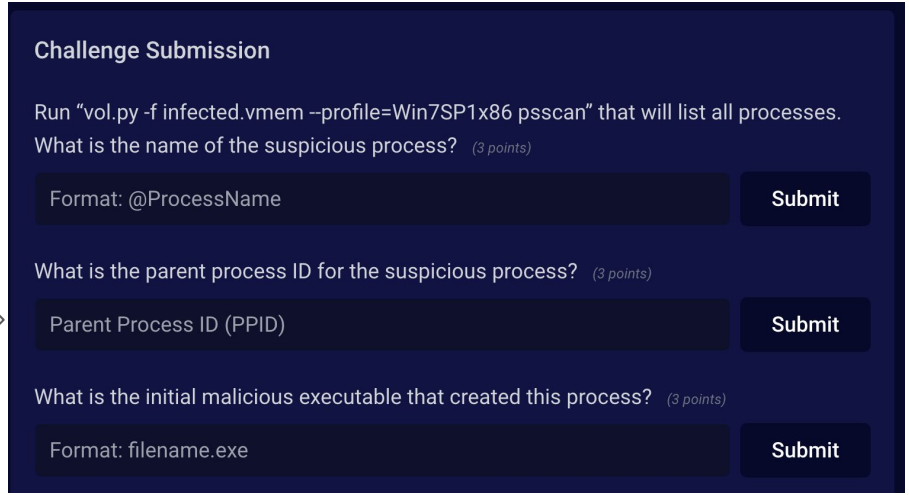
Format: Vuln Nickname, Vuln Nickname Submit

Question 4) Submit the CVE of the zero day vulnerability of a driver which led to RCE and gain SYSTEM privileges (Format: CVE-XXXX-XXXXX) *(1 points)*

Format: CVE-XXXX-XXXXX Submit

1 - Blue Team Lab Online (BTLO)

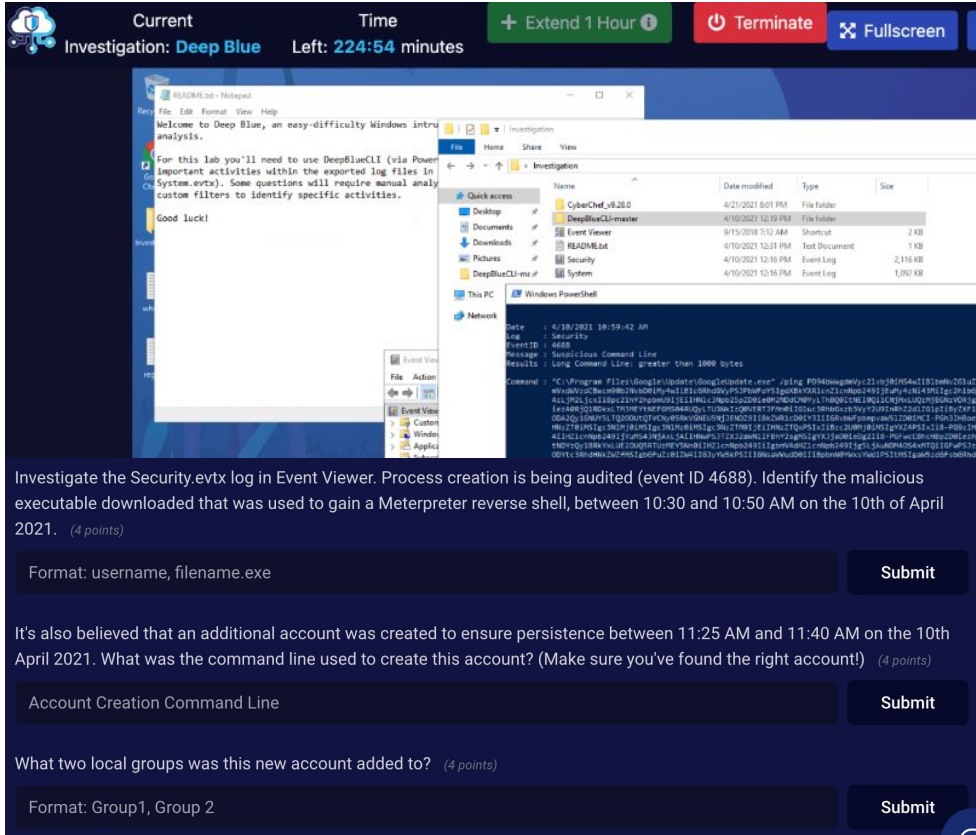
โจทย์แบบ Challenge



1 - Blue Team Lab Online (BTLO)

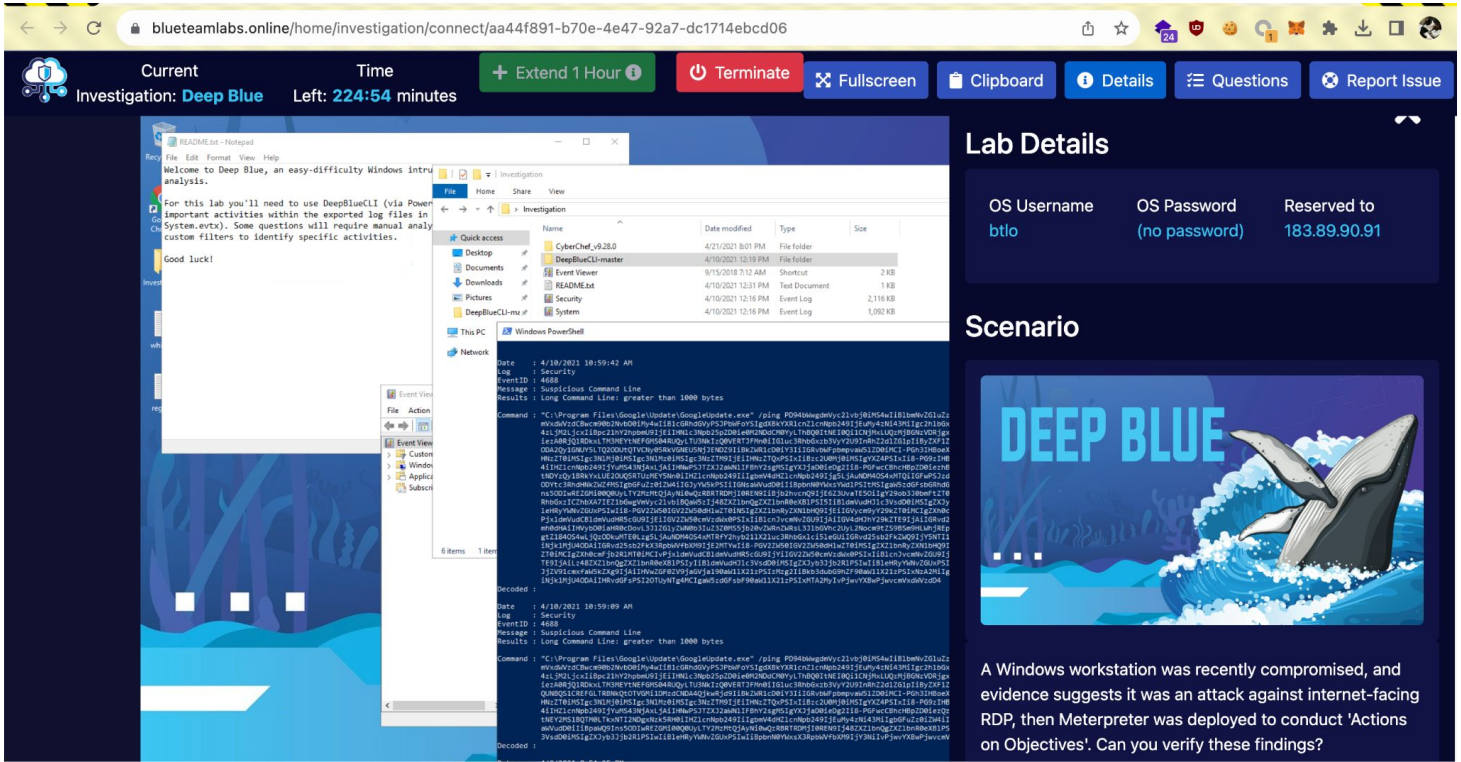
URL: https://blueteamlabs.online

โจทย์แบบ Investigation



1 - Blue Team Lab Online (BTLO)

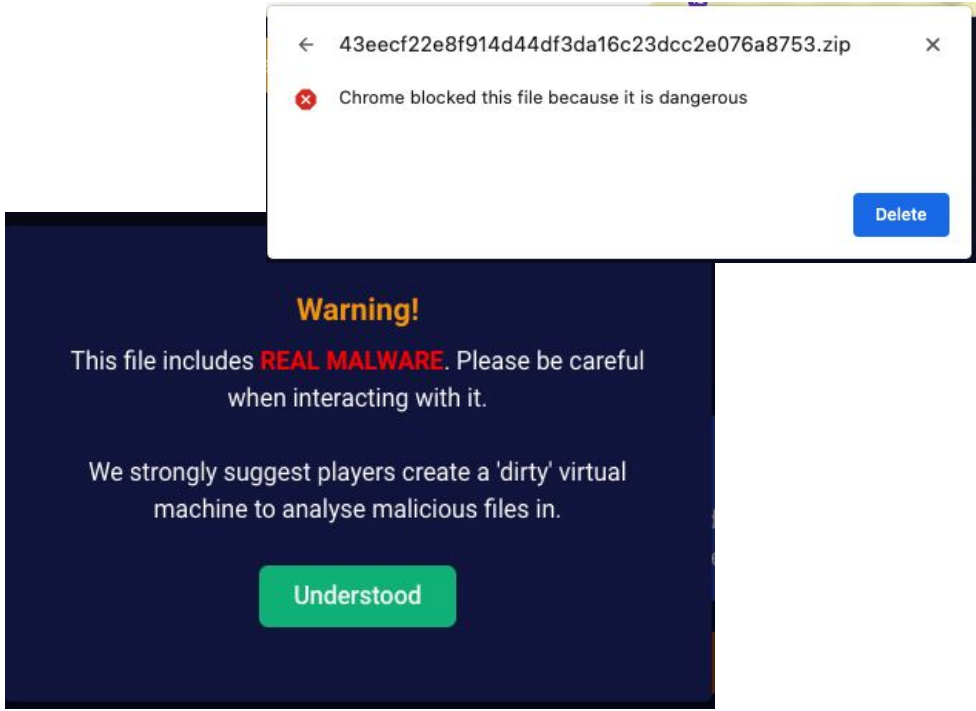
โจทย์แบบ Investigation



ข้อควรระวัง 1: วิเคราะห์ไฟล์มัลแวร์

ข้อสังเกต :
- ต้องระวัง การวิเคราะห์มัลแวร์ ในเครื่อง VM
- โปรแกรม Forensics ส่วนมากออกแบบมาใช้บน Windows x86, x64 Apple Silicon อาจทำไม่ได้

ไฟล์ติดรหัสผ่าน (infected)

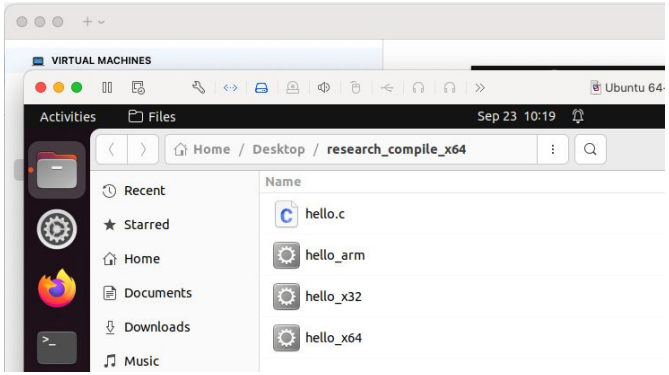


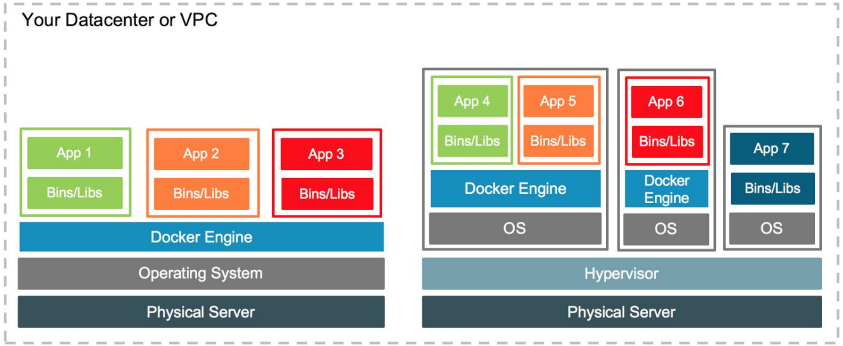
มีคำเตือนให้วิเคราะห์ใน VM ที่สร้างมาเพื่อวิเคราะห์เท่านั้น

Offline Malware Sandbox

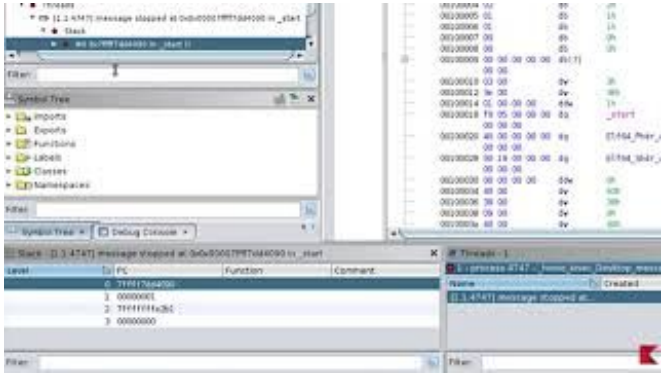
Virtual Machine:

- VirtualBox (Free)
- VMWare (Free, Commercial)

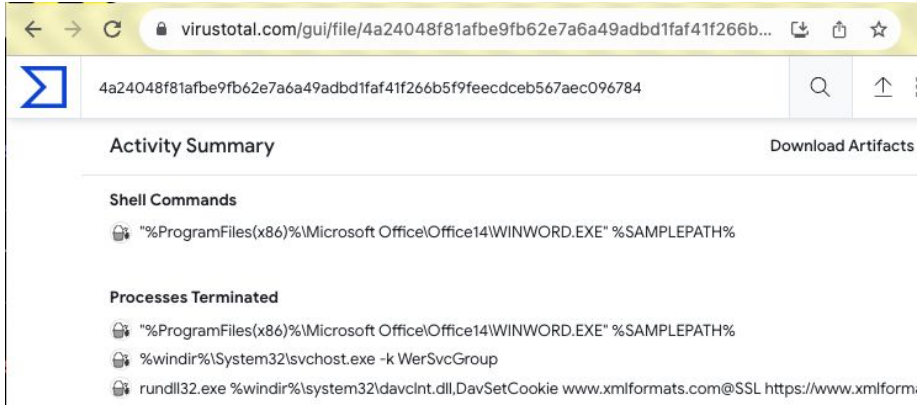




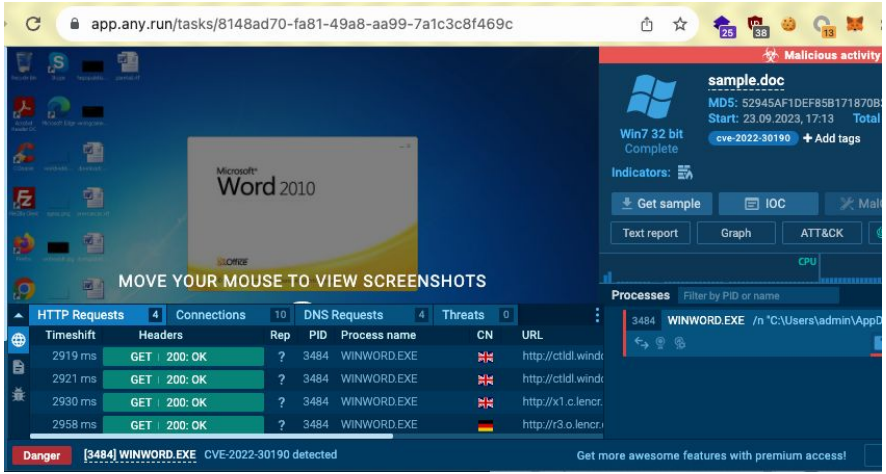
ที่มา: https://www.docker.com/blog/containers-and-vms-together/



Online Malware Sandbox

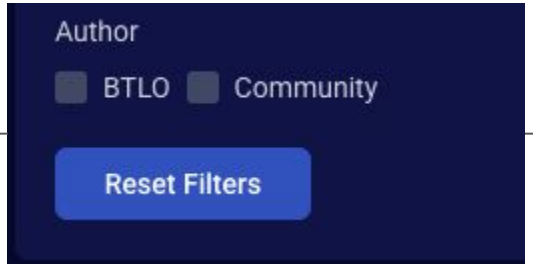


https://www.virustotal.com

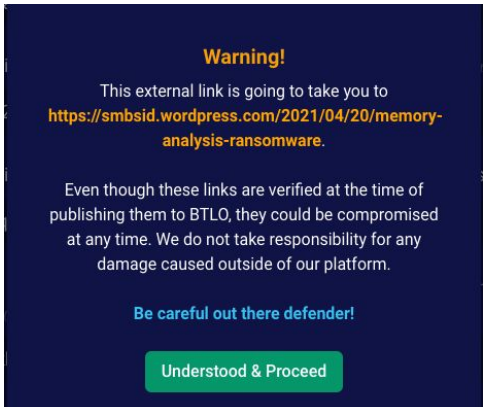


https://app.any.run

ข้อควรระวัง 2: User-Generated Content



เจ้าของ Platform สร้างโจทย์เอง (Official)



Unofficial Writeup

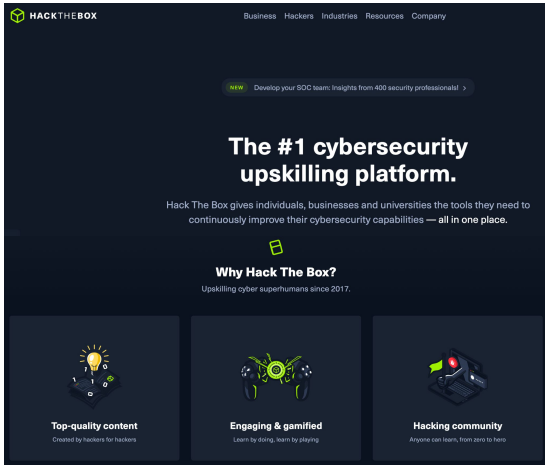
ผู้ใช้งาน (Community) ช่วยกันสร้างโจทย์

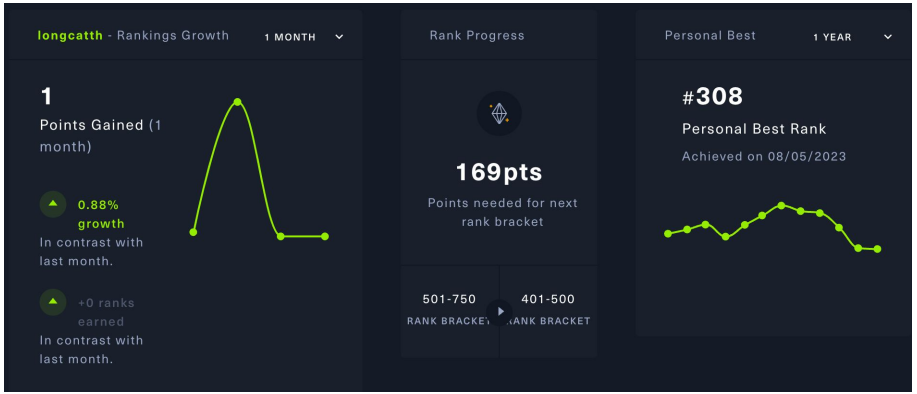
2 - Hack The Box

- จำลองการโจมตีระบบที่มีช่องโหว่ เรียกว่า Box
- เน้นสำหรับ Red Team
- รองรับ ภาษาอังกฤษ
- เริ่มตั้งแต่การหาช่องโหว่ไปจนถึงการลงมือโจมตี

แยกย่อยออกเป็น:

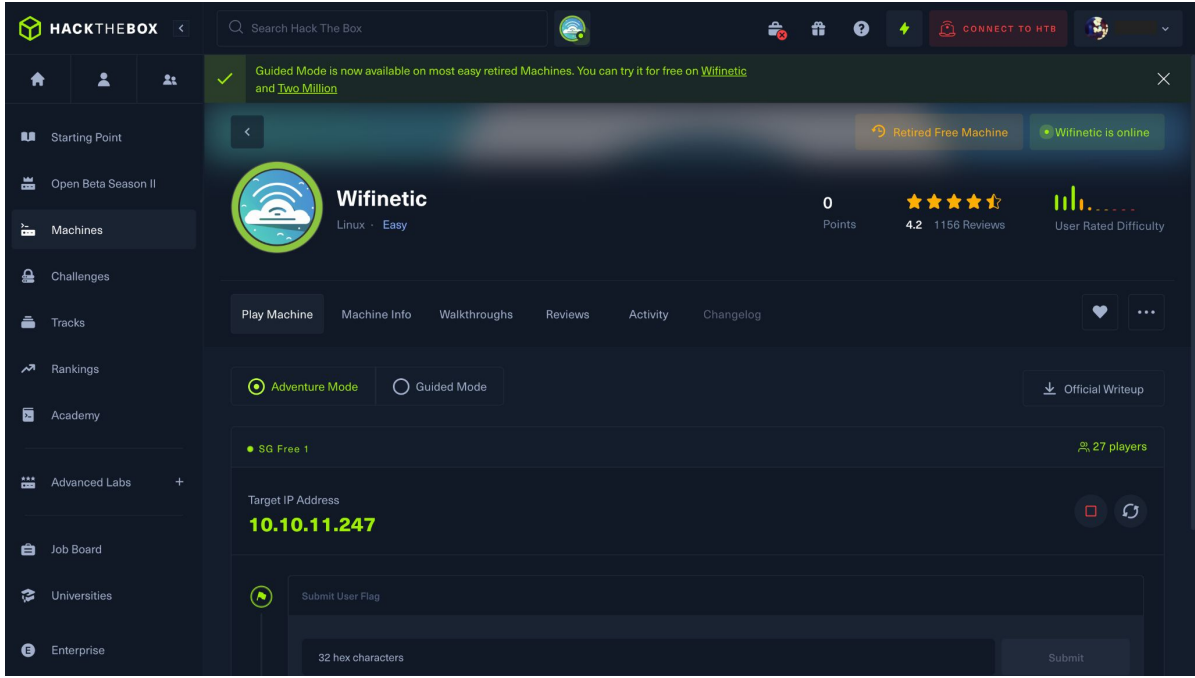
- HTB Machine
- HTB Pro Labs
- HTB Challenges
- HTB Academy
- HTB PwnBox



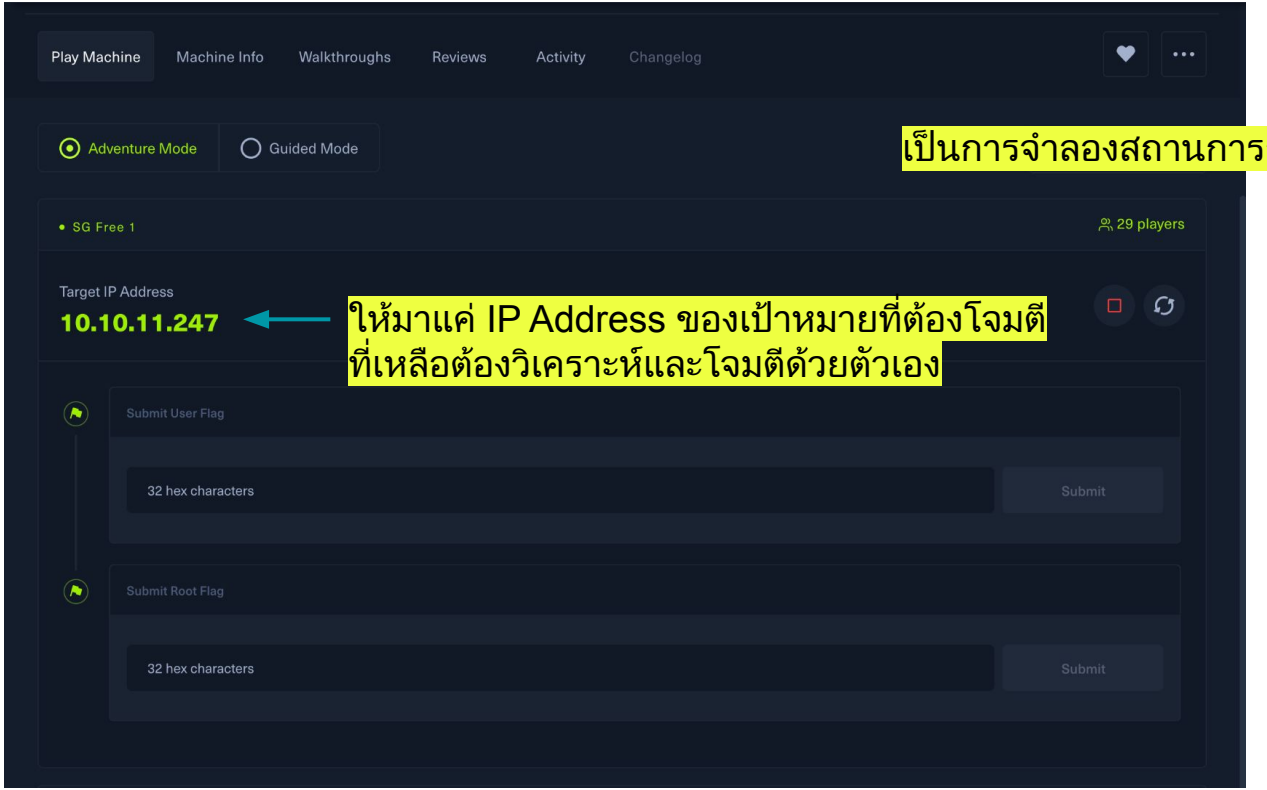


2 - Hack The Box

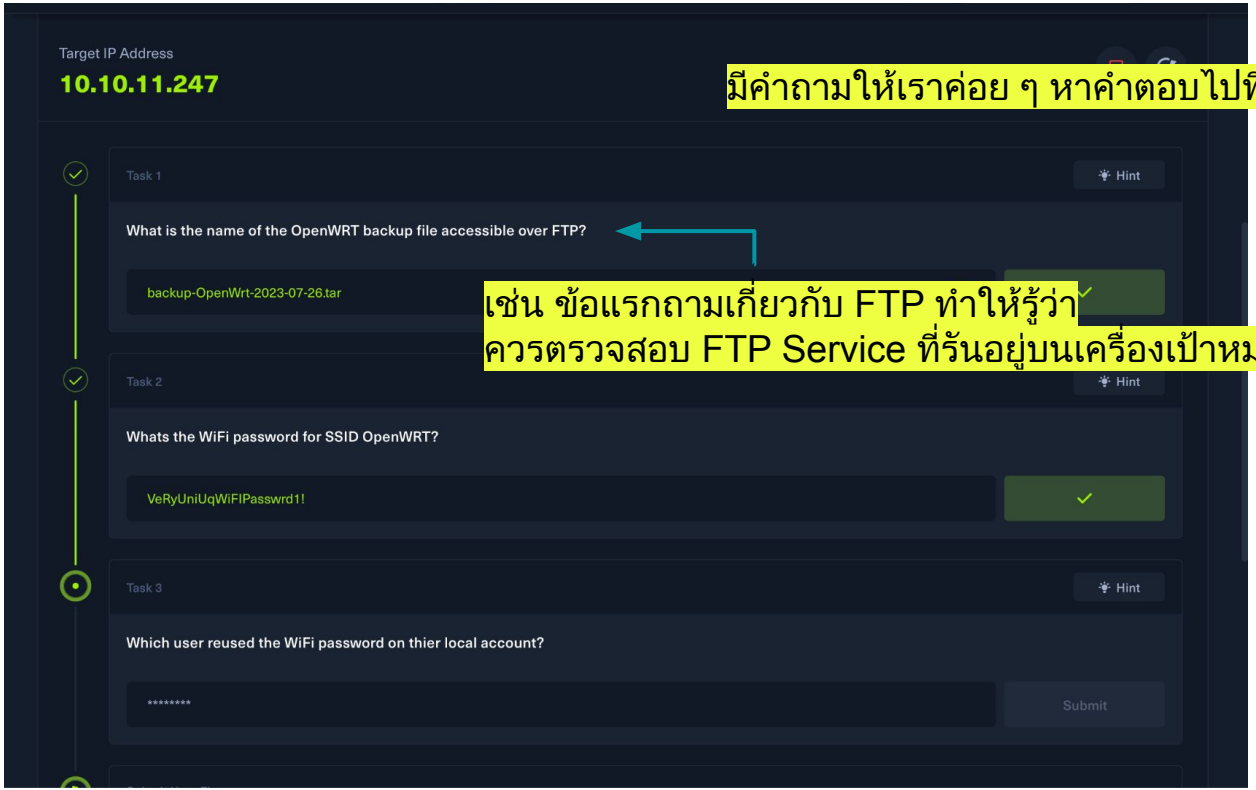
HTB Machine
- ไม่มีเนื้อหาให้เรียน
- มีแต่แลปให้ลองแฮก
  - เป็นระบบที่มีช่องโหว่
  - ให้ลองแฮกเข้าไป
    - สิทธิ์ต่ำ (user.txt)
    - สิทธิ์สูง (root.txt)
- สามารถเลือกได้ระหว่าง
  - Adventure mode
  - Guided mode



Adventure Mode ของ Hack The Box



Guided Mode ของ Hack The Box



Guided Mode ของ Hack The Box

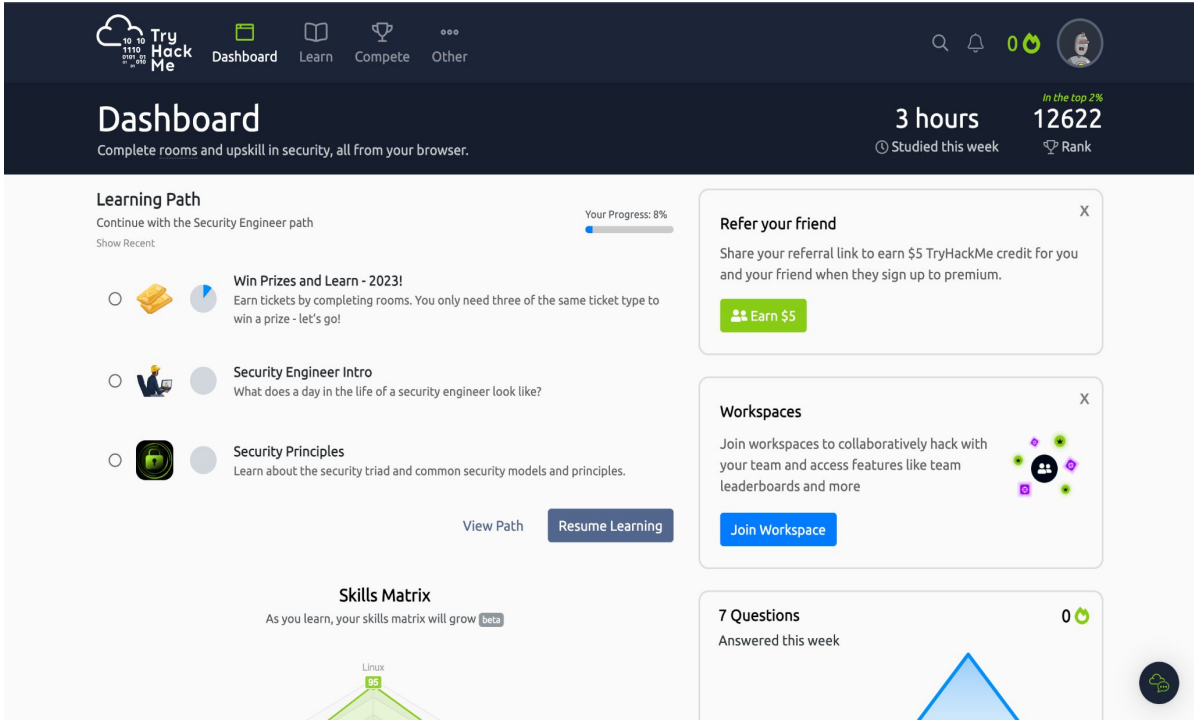
```
└─# ftp
ftp> open 10.10.11.247
Connected to 10.10.11.247.
220 (vsFTPd 3.0.3)
Name (10.10.11.247:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||45433|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp          4434 Jul 31 11:03 MigrateOpenWrt.txt
-rw-r--r--    1 ftp      ftp       2501210 Jul 31 11:03 ProjectGreatMigration.pdf
-rw-r--r--    1 ftp      ftp         60857 Jul 31 11:03 ProjectOpenWRT.pdf
-rw-r--r--    1 ftp      ftp         40960 Sep 11 15:25 backup-OpenWrt-2023-07-26.tar
-rw-r--r--    1 ftp      ftp         52946 Jul 31 11:03 employees_wellness.pdf
226 Directory send OK.
ftp> get backup*
local: backup* remote: backup*
229 Entering Extended Passive Mode (|||43784|)
550 Failed to open file.
ftp> get backup-OpenWrt-2023-07-26.tar
local: backup-OpenWrt-2023-07-26.tar remote: backup-OpenWrt-2023-07-26.tar
229 Entering Extended Passive Mode (|||41332|)
150 Opening BINARY mode data connection for backup-OpenWrt-2023-07-26.tar (40960 bytes).
100% |*****************************************************************************************************************************************| 40960        1.17 MiB/s    00:00 ETA
226 Transfer complete.
40960 bytes received in 00:00 (603.79 KiB/s)
ftp> close
221 Goodbye.
ftp> exit
```

เมื่อตรวจสอบ FTP Service จึงพบว่ามีช่องโหว่อยู่

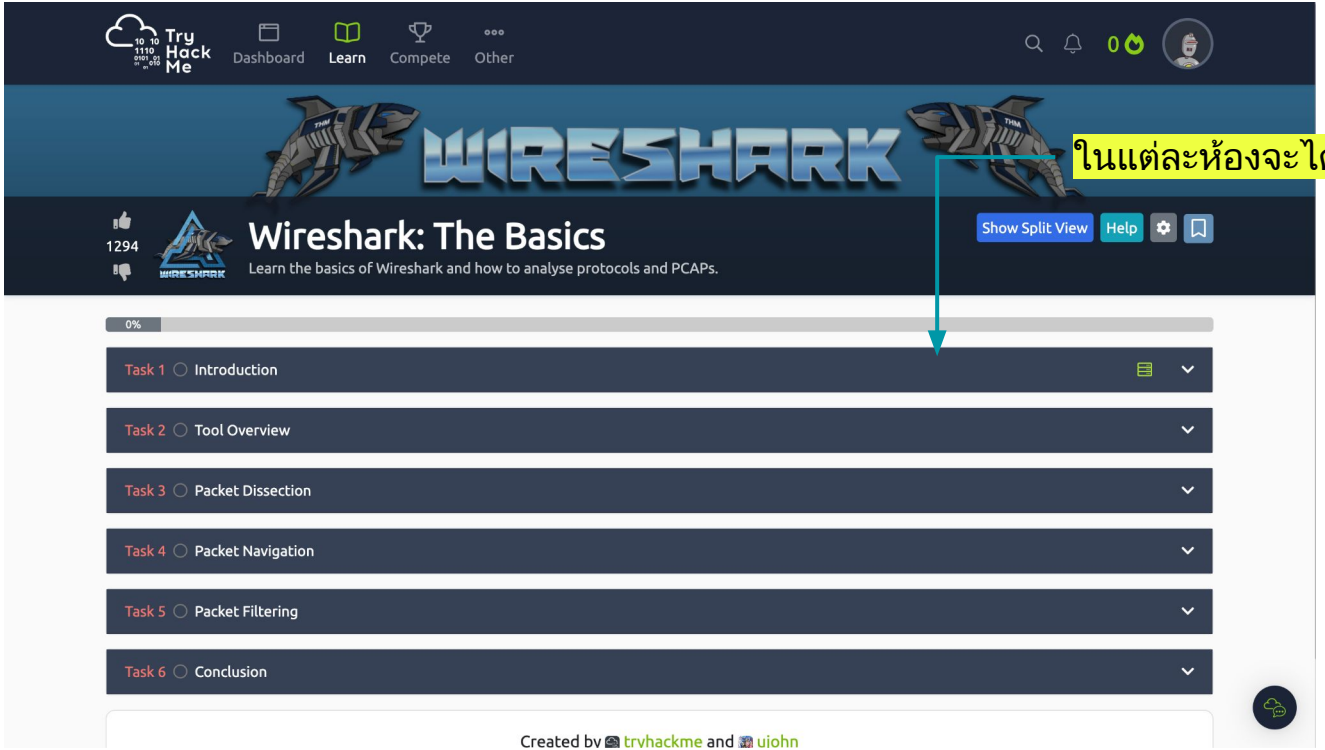
ทำให้ใน Guided Mode เราสามารถเรียนรู้การโจมตีในแต่ละขั้นได้

3 - TryHackMe

- คอร์สเรียนพร้อม Lab
- อธิบายแบบ Step-by-step เหมาะกับการเรียนรู้
- มีทั้งคอร์สฝั่ง Red Team และ Blue Team
- เลือกเรียนตาม Path ที่สนใจ หรือเลือกเรียนทีละหัวข้อได้
- มีทั้งแบบฟรีและแบบที่ต้องสมัคร Premium
- คอร์สเรียนหลากหลาย



ตัวอย่างห้องใน TryHackMe



ในแต่ละห้องจะได้เรียนทีละ Task

ตัวอย่างห้องใน TryHackMe

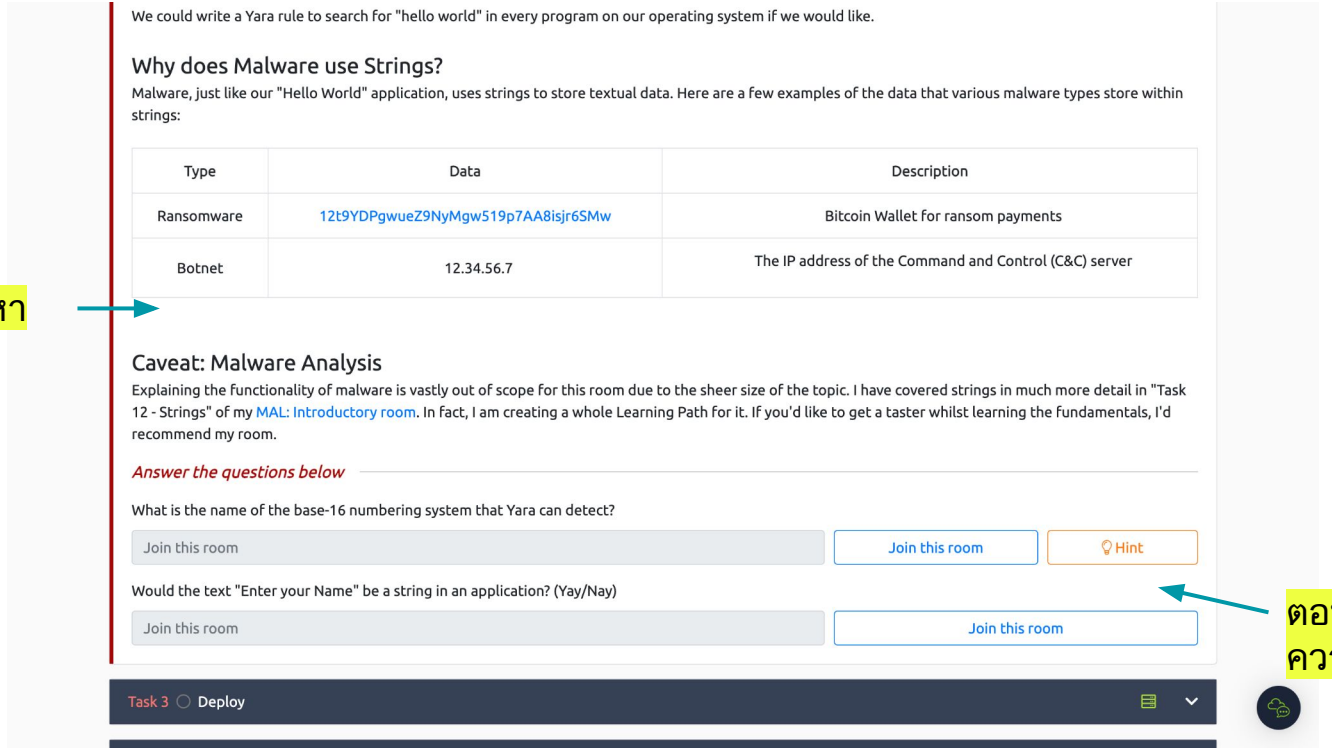
คำถามในแต่ละ Step มีหลายรูปแบบ ได้แก่

- ทำความเข้าใจเนื้อหา แล้วตอบคำถาม
- ทำความเข้าใจเนื้อหา แล้วหาคำตอบจากไฟล์ที่กำหนดให้
- ทำความเข้าใจเนื้อหา แล้วหาคำตอบจากระบบ Interactive ผ่านหน้าเว็บ
- ทำความเข้าใจเนื้อหา แล้วหาคำตอบจากการทำ Lab ผ่าน VPN หรือ AttackBox

ตัวอย่างห้องใน TryHackMe - (1) ตอบคำถาม

ทำความเข้าใจเนื้อหาแล้วตอบคำถาม

เรียนเนื้อหา



We could write a Yara rule to search for "hello world" in every program on our operating system if we would like.

Why does Malware use Strings?

Malware, just like our "Hello World" application, uses strings to store textual data. Here are a few examples of the data that various malware types store within strings:

Type	Data	Description
Ransomware	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw	Bitcoin Wallet for ransom payments
Botnet	12.34.56.7	The IP address of the Command and Control (C&C) server

Caveat: Malware Analysis

Explaining the functionality of malware is vastly out of scope for this room due to the sheer size of the topic. I have covered strings in much more detail in "Task 12 - Strings" of my MAL: Introductory room. In fact, I am creating a whole Learning Path for it. If you'd like to get a taster whilst learning the fundamentals, I'd recommend my room.

Answer the questions below

What is the name of the base-16 numbering system that Yara can detect?

Join this room | Join this room | Hint

Would the text "Enter your Name" be a string in an application? (Yay/Nay)

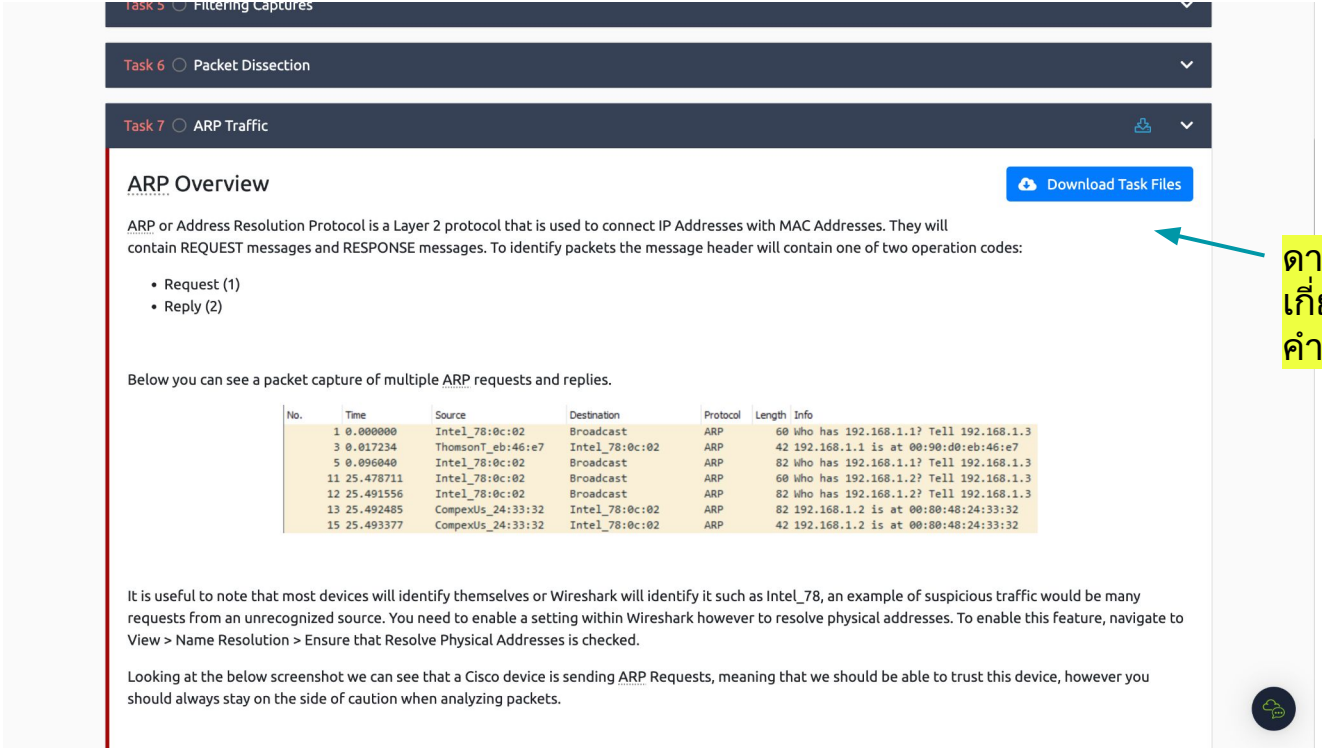
Join this room | Join this room

Task 3 Deploy

ตอบคำถามตามความเข้าใจ

ตัวอย่างห้องใน TryHackMe - (2) ดาวน์โหลดไฟล์

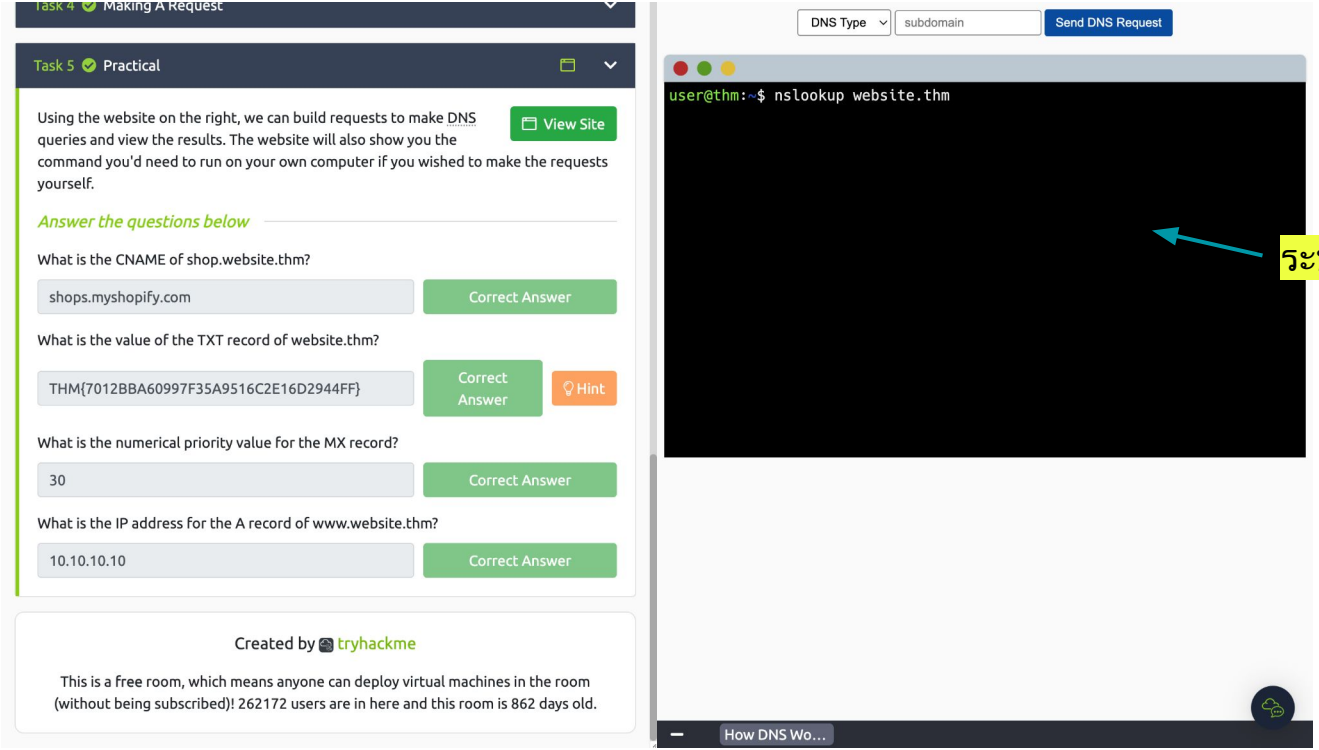
ทำความเข้าใจเนื้อหาแล้วหาคำตอบจากไฟล์ที่กำหนดให้



ดาวน์โหลดไฟล์ที่เกี่ยวข้องเพื่อหาคำตอบ

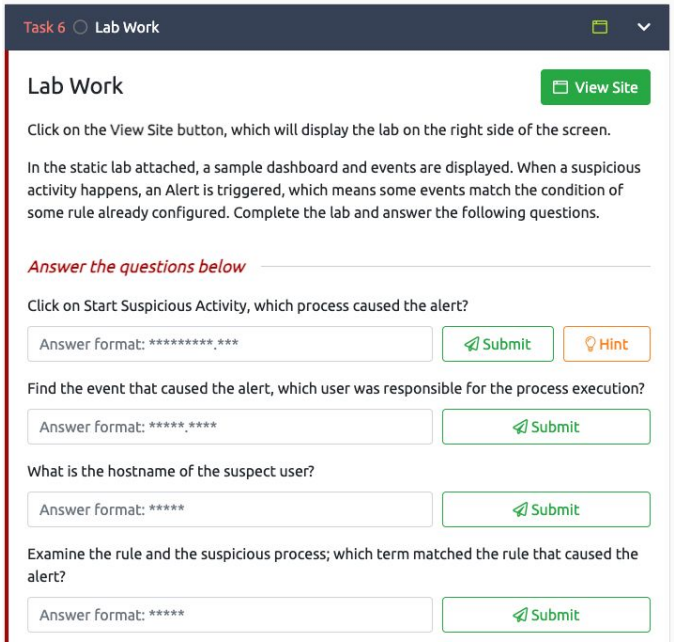
ตัวอย่างห้องใน TryHackMe - (3) Interactive

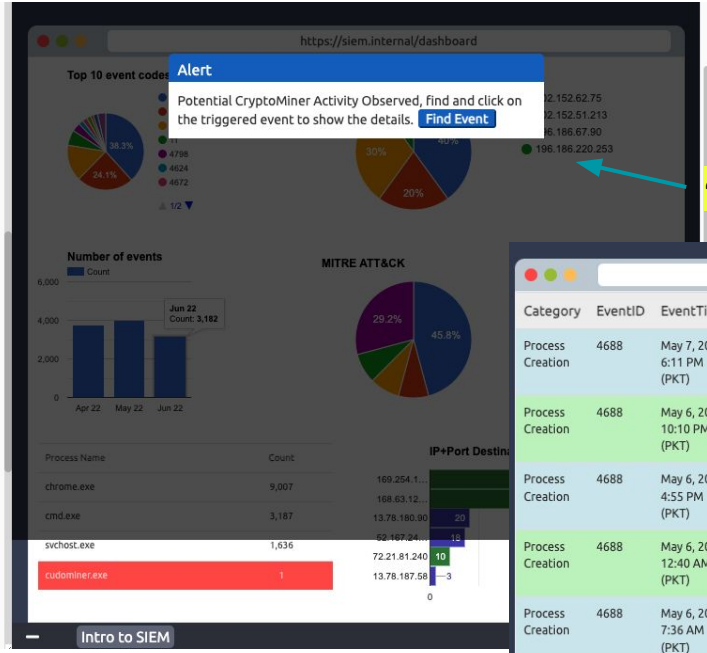
ทำความเข้าใจเนื้อหาแล้วหาคำตอบจากระบบ Interactive บนหน้าเว็บ



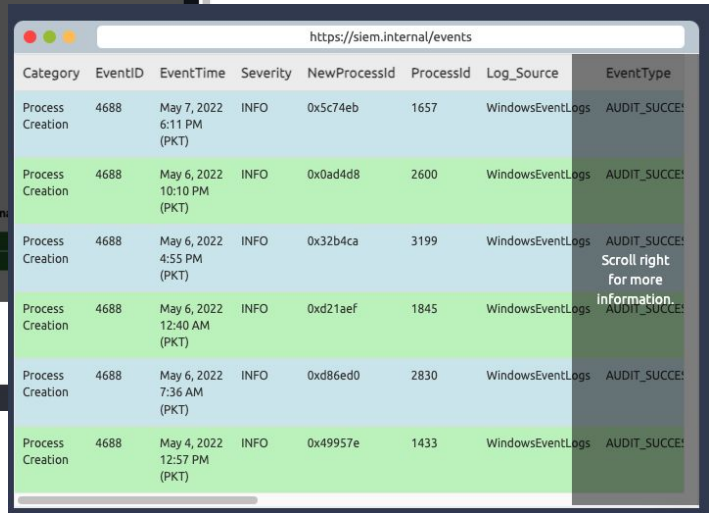
ตัวอย่างห้องใน TryHackMe - (3) Interactive

ทำความเข้าใจเนื้อหาแล้วหาคำตอบจากระบบ Interactive บนหน้าเว็บ





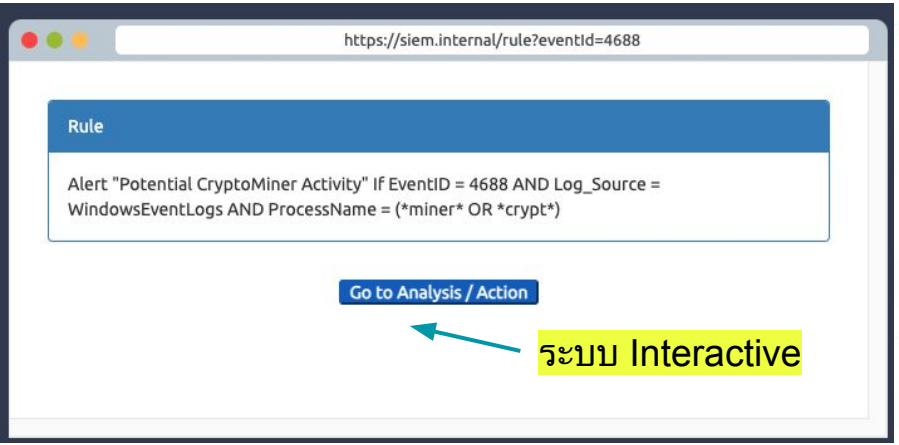
ระบบ Interactive



ที่มา: https://tryhackme.com/room/introtosiem (ฟรี)

ตัวอย่างห้องใน TryHackMe - (3) Interactive

ทำความเข้าใจเนื้อหาแล้วหาคำตอบจากระบบ Interactive บนหน้าเว็บ



Answer the questions below

Click on Start Suspicious Activity, which process caused the alert?

cudominer.exe — Correct Answer — Hint

Find the event that caused the alert, which user was responsible for the process execution?

Chris.fort — Correct Answer

What is the hostname of the suspect user?

HR_02 — Correct Answer

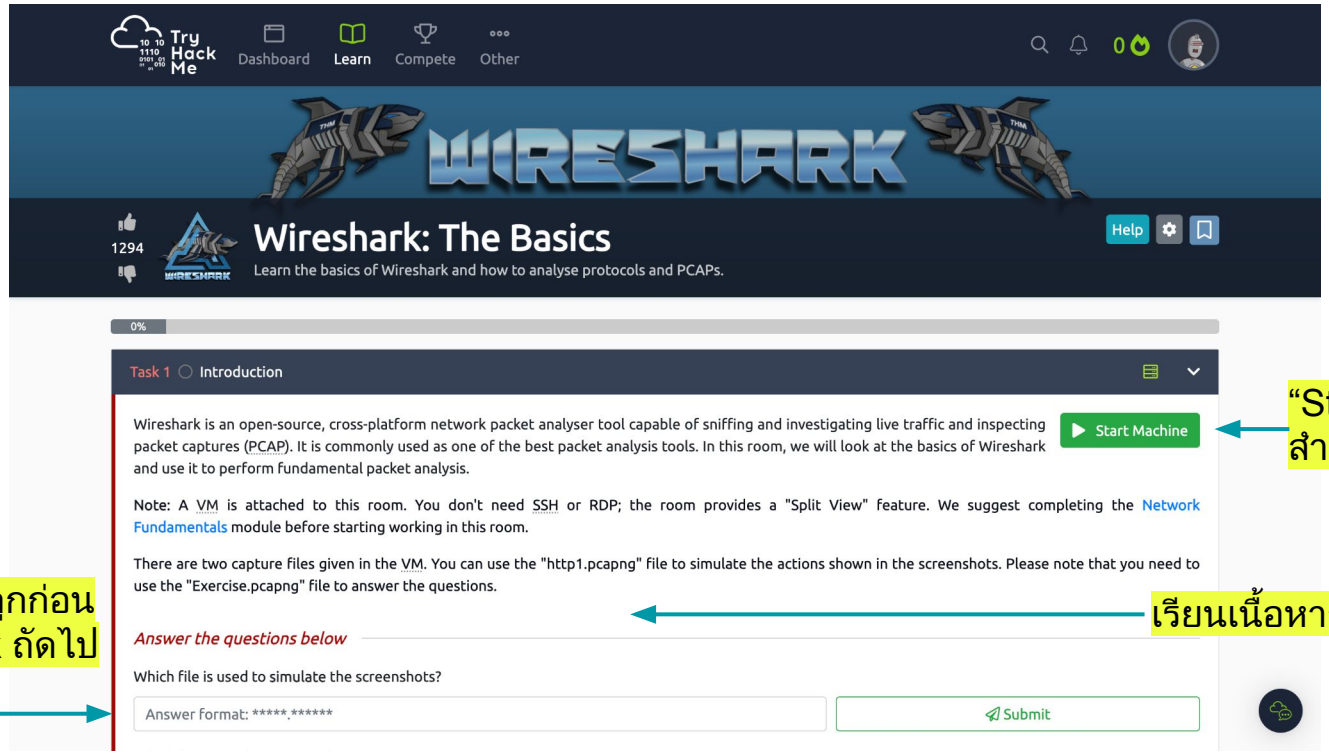
Examine the rule and the suspicious process; which term matched the rule that caused the alert?

miner — Correct Answer

ที่มา: https://tryhackme.com/room/introtosiem (ฟรี)

ตัวอย่างห้องใน TryHackMe - (4) Lab

ทำความเข้าใจเนื้อหาแล้วหาคำตอบจากการทำ Lab



"Start Machine" สำหรับทำ Lab

เรียนเนื้อหาก่อนเริ่มทำ Lab

ตอบคำถามให้ถูกก่อน จะผ่านไป Task ถัดไป

ตัวอย่าง Learning Path ใน TryHackMe

Learning Paths

Work your way through a structured learning path

Red Teaming

Learn the skills needed to become a Red Team Operator

- Use diverse techniques for initial access
- Enumerate and persist on targets`
- Evade security solutions
- Exploit Active Directory

Intermediate 48 hours

Introduction to Cyber Security

Learn the core skills required to start a career in cyber security

- Learn about different careers in cyber
- Hack your first application
- Defend against a live cyber attack
- Explore security topics in the industry

Easy 24 hours

Jr Penetration Tester

Learn the necessary skills to start a career as a penetration tester

- Pentesting methodologies and tactics
- Enumeration, exploitation and reporting
- Realistic hands-on hacking exercises
- Learn security tools used in the industry

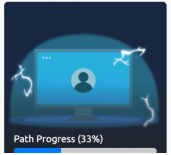
Intermediate 64 hours

Pre Security

Before hacking something, you first need to understand the basics

- Cyber security basics
- Networking basics and weaknesses
- The web and common attacks
- Learn to use the Linux operating system

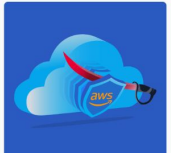
Easy 40 hours



Cyber Defense

Learn how to analyse and defend against real-world cyber threats/attacks

- Detect threats
- Gather threat actor intelligence
- Understand and emulate adversary TTPs
- Identify and respond to incidents



Attacking and Defending AWS

Learn how attackers compromise AWS environments

- Compromise EC2 instances
- Reduce the privileges of policies
- Abuse Lambda Authorizers
- Enumerate IAM users

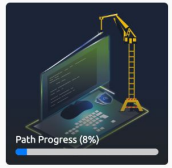
Intermediate 48 hours

SOC Level 1

Learn the skills needed to work as a Junior Security Analyst in a Security Operations Centre

- Detect and analyse traffic anomalies
- Monitor endpoints for threats
- Utilise SIEM tools to handle incidents
- Investigate forensic artefacts

Easy 56 hours



Security Engineer

Learn the skills required to jumpstart your career in security engineering.

- Network security engineering
- System security engineering
- Software security engineering
- Risk management & responding to…

Easy 40 hours

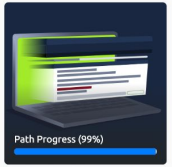
CompTIA Pentest+

Learn the practical skills and prepare to ace the Pentest+ exam.

- Hands-on exercises aligning to PenTest+ exam objectives
- Practical exam preparation to help you with the Performance Based Questions

Easy 32 hours

Intermediate 40 hours



Complete Beginner

Learn the core skills required to start a career in cyber security

- Web application security
- Network security
- Basic Linux
- Scripting

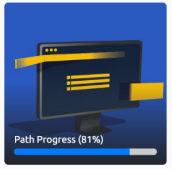
Easy 64 hours

Offensive Pentesting

Prepare yourself for real world penetration testing

- Utilise industry standard tools
- Learn realistic attack scenarios
- Train in offensive security
- Supporting exercises & resources

Intermediate 47 hours



Web Fundamentals

A pathway to web application security

- Understand web fundamentals
- Major vulnerabilities explained
- Learn industry-used tools
- Web application assessments

Easy 32 hours

เปรียบเทียบ TryHackMe แบบฟรีและ Premium

	Free	Premium	Businesses
Personal hackable instances	✓	✓	✓
Hacking challenges	✓	✓	✓
Learning content	Free rooms	Premium rooms	Premium & Business rooms
Full access to learning paths	⊗	✓	✓
Web-based AttackBox & Kali	1 hour a day	Unlimited	Unlimited
Access to Networks	⊗	✓	✓
Faster Machines	⊗	✓	✓
Private OpenVPN Servers	⊗	✓	✓
Private King of the Hill Games	⊗	✓	✓
Custom Learning Paths	⊗	⊗	✓
Advanced Reporting	⊗	⊗	✓
Transferable Licensing	⊗	⊗	✓
Dedicated Customer Success Manager	⊗	⊗	✓

ฟรี 4xx ห้อง
Premium 2xx ห้อง

แต่ห้อง Premium จะมีเนื้อหาที่ละเอียดและครบถ้วนกว่า

ที่มา: https://tryhackme.com/why-subscribe

แนะนำห้อง TryHackMe ที่น่าสนใจ

Red Team

- Red Team Fundamentals (ฟรี)
- Red Team Recon (ฟรี)
- Bypassing UAC (ฟรี)
- Lateral Movement and Pivoting (Premium)
- Active Directory Basics (ฟรี)
- Credentials Harvesting (Premium)

Blue Team

- Incident handling with Splunk (Premium)
- Linux System Hardening (Premium)
- Sigma (Premium)
- Yara (Premium)
- Intro to Endpoint Security (ฟรี)
- Phishing Prevention (Premium)

Key Takeaway (1/2)

- Learning Platform มีเยอะ แต่ละที่โจทย์ เยอะ-น้อย แตกต่างกัน, ราคา ฟรี-ถูก-แพง แตกต่างกัน
  - BTLO
  - HackTheBox
  - TryHackMe
- แต่เวลา เรียนรู้เรามีจำกัด
- ควรทดลองหลาย ๆ Platform แล้วหาอันที่มองว่าเหมาะกับตนเอง และคุ้มค่าที่จะใช้เวลากับมัน
- ระวังความเสี่ยงจากการดาวน์โหลดไฟล์ที่อาจอันตรายจาก Learning Platform ต่าง ๆ

CTF คืออะไร ?

ย่อมาจาก Capture The Flag

ในฝั่ง Computer Security

★ แข่ง**แฮก** เพื่อชิงธง
★ ธง คือข้อความลับ (flag)

ที่จะได้มาเมื่อแก้ไขปัญหาได้
FLAG{YOU_WON_1337}

★ ตัวอย่างงานแข่ง เช่น
- DEFCON CTF
- Google CTF
- SECCON CTF

From CTF to Cybersecurity Career Path

แข่งยังไงแข่งแฮกใน CTF

เหมือนเล่นเกม เล่นเดี่ยว/เป็นทีม เก็บคะแนนให้ได้มากที่สุด ก่อนหมดเวลาแข่ง
ส่วนมากจัดเป็นออนไลน์เล่นที่ไหนก็ได้ แต่บางงานต้องไปสถานที่จริงก็มี

CTF แบ่งตามวิธีเล่นมี 3 รูปแบบหลัก ๆ

1. **Jeopardy**

   แบบถาม - ตอบ มีโจทย์ปัญหาให้แก้เมื่อแก้ได้แล้วจะได้คำตอบ
   เป็นข้อความลับ (flag หรือธงนั่นเอง) เอาไว้ยืนยันเพื่อเก็บคะแนน

2. **Attack-Defence**

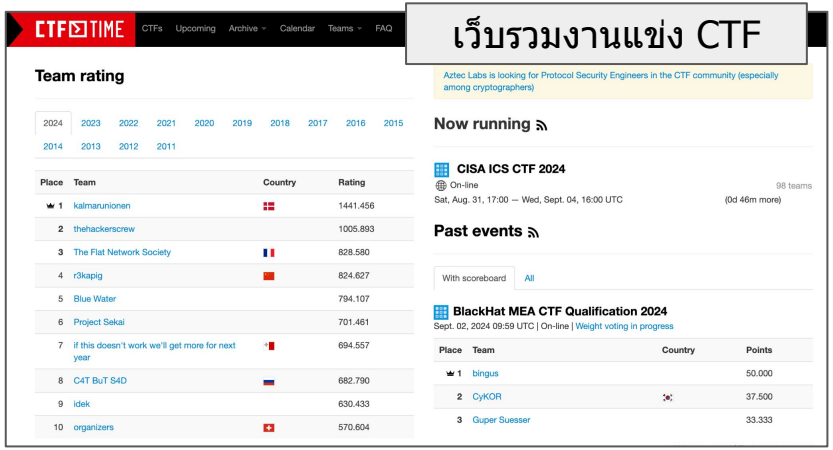
   แต่ละทีมมีคอมพิวเตอร์เป็นฐานของตัวเอง ให้แฮกไปที่เครื่องทีมอื่น โดยหาช่องโหว่
   เขียนโค้ดขึ้นมาโจมตี เพื่อชิงธงมา ธงอาจอยู่ในไฟล์ เช่น C:\flag.txt
   และอาจจะสามารถป้องกันเครื่องของตัวเอง ได้ด้วยโดยจะมี
   กฎกติกาว่าให้ทำการแก้ไขอะไรได้บ้าง

3. **Mixed หรือแบบอื่น ๆ**

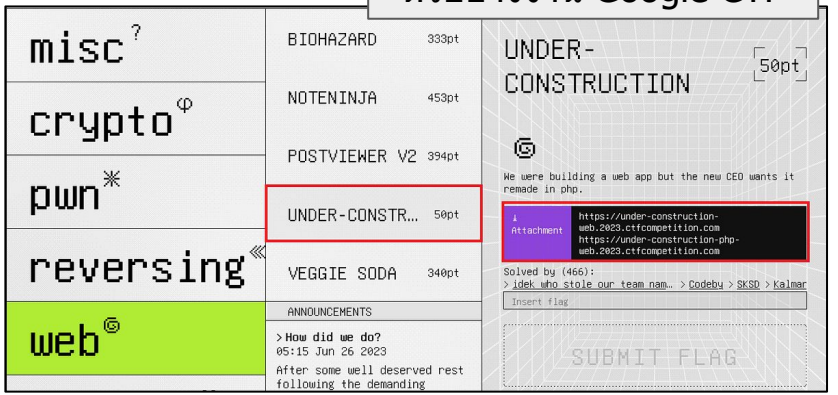
   ตามแต่จะเอาไปดัดแปลงใช้ได้ เช่น wargame ที่เล่นเมื่อไรก็ได้

https://ctftime.org

เว็บรวมงานแข่ง CTF



ตัวอย่างงาน Google CTF



Badge ของผู้ชนะ DEFCON CTF
(เข้างานสัมมนาฟรีตลอดชีพ)

ทำไมถึงควรเล่น CTF

- ★ สนุก มันส์ เหมือนถามว่าทำไมถึง เล่นเกม อ่านการ์ตูน
- ★ งานใหญ่ ๆ จะมีรางวัลให้คนชนะ เป็นเงินบ้าง แรร์ไอเท็มบ้าง
- ★ ได้เรียนรู้ Computer Security แบบลงมือทำจริง ได้ลองแฮก ลองแก้ไขโจทย์ปัญหายาก ๆ ที่ต้องไปหาอ่านสิ่งใหม่ ๆ อัปเดตความรู้อยู่ตลอดเวลา เทคนิคนี้ วิธีนี้ โปรแกรมนี้เคยปลอดภัยวันนี้ พรุ่งนี้อาจไม่ปลอดภัย เราอ่านข่าว อ่านบทความช่องโหว่งั้นงี้เหมือนเข้าใจ ลองทำจริง ๆ จากโจทย์ CTF ช่วยยืนยันได้ว่าเข้าใจจริง ๆ
- ★ IT Security Expert ทั่วโลกนิยมเล่นกันอย่างแพร่หลาย คนเล่น CTF ส่วนมากทำงานเกี่ยวกับ IT Security เช่น นักทดสอบเจาะระบบ (Penetration Tester) เพราะฉะนั้นถ้าอยากฝึกหรือวัดความเก่งด้าน IT Security ในระดับโลกการเล่น CTF ก็เป็นอีกตัวเลือกที่ดีเพราะมี Scoreboard ให้ดูด้วยว่าเราอยู่ตรงไหน คนอื่น ๆ เค้าอยู่ตรงไหน และช่วยเพิ่มแรงจูงใจในการพัฒนาตนเอง

หมวด: แข่งแฮกโจทย์มันเป็นยังไง

โจทย์ใน CTF มีหลากหลาย เราอาจไม่ต้องรู้ทุกด้าน ถ้าในทีมมีหลายคน เช่น

★	Cryptanalysis	ถอดรหัส การเข้ารหัสที่ไม่ปลอดภัย / ไม่ถูกวิธี
★	Reverse Engineering	วิเคราะห์และแก้ไข binary aka. crack โปรแกรม
★	Web Application Security	แฮกเว็บ เช่น SQL injection
★	Binary Exploitation	แฮกโปรแกรม เช่นทำ buffer overflow
★	Digital Forensics	ตรวจสอบหาร่องรอยข้อมูลอิเล็กทรอนิกส์
★	Trivia / Misc	อื่น ๆ ที่ไม่เข้าพวกเช่นอ่าน QR โค้ดครึ่งอัน

โจทย์ใน CTF ทุกข้อ จะต้องมีวิธีแก้ไขได้อย่างน้อย 1 วิธีแน่นอน แต่อาจแก้ได้หลายวิธีเช่นกัน ทำไงก็ได้ให้ได้ flag คนตั้งโจทย์ CTF จะต้องไม่สร้างโจทย์ที่วิธีทำไม่ Practical ในการแก้ไข เช่นการ bruteforce เป็นเดือน ๆ จะไม่มีทางเป็น solution ของโจทย์ CTF โดยปกติ

ตัวอย่างการแข่งขันแนว CTF ในประเทศไทย

★ Thailand Cyber Top Talent

จัดโดย กสมช.

★ STDiO CTF

จัดโดย กลุ่ม 2600 Thailand

https://mgronline.com/cyberbiz/detail/9660000099861

ใช้ในคอร์ส สอนแฮกราคา 2 แสน

[redacted] Authorized Training

Network Penetration Testing and Ethical Hacking - [redacted]	
Schedule :	25-30 May 2015 (6 days)
Taught by :	[redacted] Certified Instructor (English language)
Usual price :	198,625 Baht (Excl. Vat 7%)
Promo price :	N/A
Outline :	Download

Special offer : Join VIP Membership to enjo

560.6 HANDS ON: Penetration Testing Workshop and Capture the Flag Event

This lively session represents the culmination of the network penetration testing and ethical hacking course, where you'll apply all of the skills mastered in the course so far in a full-day, hands-on workshop. You'll conduct an actual penetration test of a sample target environment. We'll provide the scope and rules of engagement, and you'll work with a team to achieve your goal of finding out whether the target organization's Personally Identifiable Information (PII) is at risk. And, as a final step in preparing you for conducting penetration tests, you'll make recommendations about remediating the risks you identify.

Topics: Applying Penetration Testing and Ethical Hacking Practices End-to-end; Scanning; Exploitation; Post-Exploitation; Pivoting; Analyzing Results

[redacted] For schedules, cour
or lap

ตัวอย่าง CTF ในต่างประเทศ (1)

งานสัมมนาด้าน Hacking ที่ใหญ่ที่สุดในโลก DEFCON จัด CTF ทุกปี

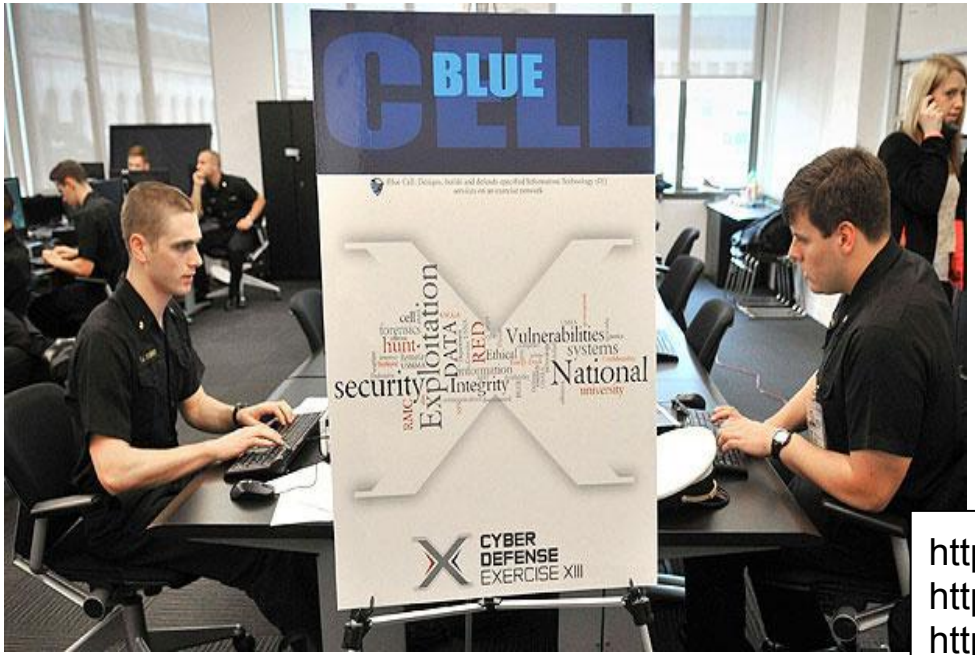
DefCon CTF Final
Las Vegas, NV, USA

CodeGate CTF Final
Seoul, Republic of Korea

SECCON CTF Final
Tokyo, Japan

ตัวอย่าง CTF ในต่างประเทศ (2)

NSA หน่วยงานความมั่นคงอเมริกาใช้การแข่งขันแบบ CTF ช่วยสอนทางการทหารไซเบอร์ ด้วย Cyber Defence Exercise (CDX), NATO ก็มี



https://www.youtube.com/watch?v=HnnvVnsDCGw
https://www.youtube.com/watch?v=aoG1XzUk7sU
https://www.youtube.com/watch?v=DCLL9f4onvY

ตัวอย่าง CTF ในต่างประเทศ (3)

หลักสูตรปริญญาเอกที่ มหาวิทยาลัย Carnegie Mellon เปิดวิชา “Special Topics in Security I” ให้นักศึกษาเล่น CTF เพื่อเก็บคะแนนเอาไปคิดเกรดได้

CTF contests

- Boston Key Party: Feb 27 - March 1, 2015. Note this is not a regular class time! Participation means working at least 10 hours total. Required.
- Ghost in the shell: Jan 16-18, 2015. Optional. Extra Credit.
- Codegate (when announced). Required.

Students should register using a name that is prefixed with CMU (assuming you are not competing as PPP). We will use github to map which students (by andrew ID) are on each team. Students must submit a screen shot at the end of the contest with their score.

https://ece.cmu.edu/courses/items/18739L.html
https://github.com/CMU-18739L-S15/18763 9L-s15-coursedocs

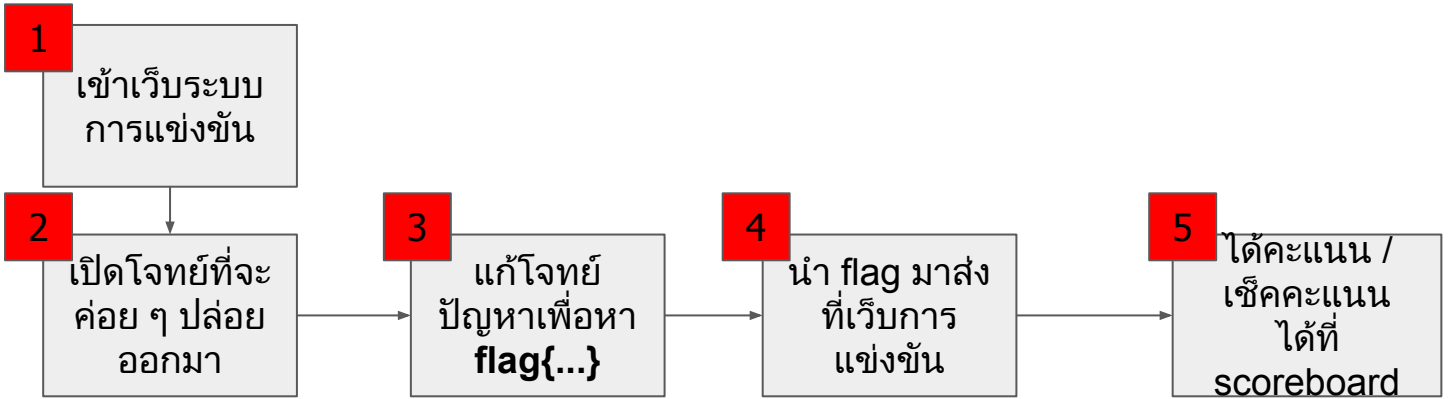
Wargames

- picoCTF. Grading: 3500 and up: A, 3000 - 3500: B, 2500-3000: C, 2000-2500: D, Fail below, and I will ask you to drop the class.
- Microcorruption. 16 and up: A, 14-16: B, 12-14: C, 11: D, below that: F.
- IO: Level 8 and up: A, Level 7: B, Level 6: C, Level 5: D, Level 4: F. If you have already done some of the levels in the x86 version, please try doing levels in the ARM version.
- ~~Web hacking: TBD.~~

ในไทยก็มี

https://ctf.in.th/news/1982/

ตัวอย่างขั้นตอนการแข่งขัน CTF

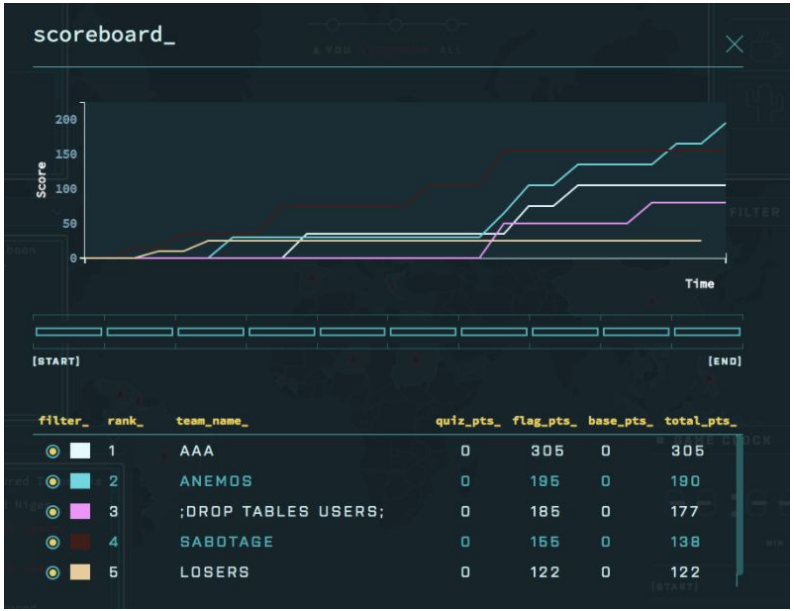


ตัวอย่างเงื่อนไขอื่น ๆ

- ทีมที่แก้โจทย์แต่ละข้อได้เป็นทีมแรกจะได้คะแนน bonus + 10% ของข้อนั้น (first blood)
- กรรมการจัดการแข่งขันจะปล่อยคำใบ้ ถ้าไม่มีทีมใดแก้โจทย์ได้ (hint)
- โจทย์จะทยอยปล่อยออกมาเรื่อย ๆ จนครบทุกข้อ
- โจทย์จะมีข้อง่ายให้ทุกทีมร่วมสนุกกับการแข่งขันได้, ข้อยากปานกลางให้ไปศึกษาเพิ่มเติมก่อนมาทำโจทย์ได้ และข้อยากปราบเซียนที่ต้องใช้ความรู้ระดับสูง

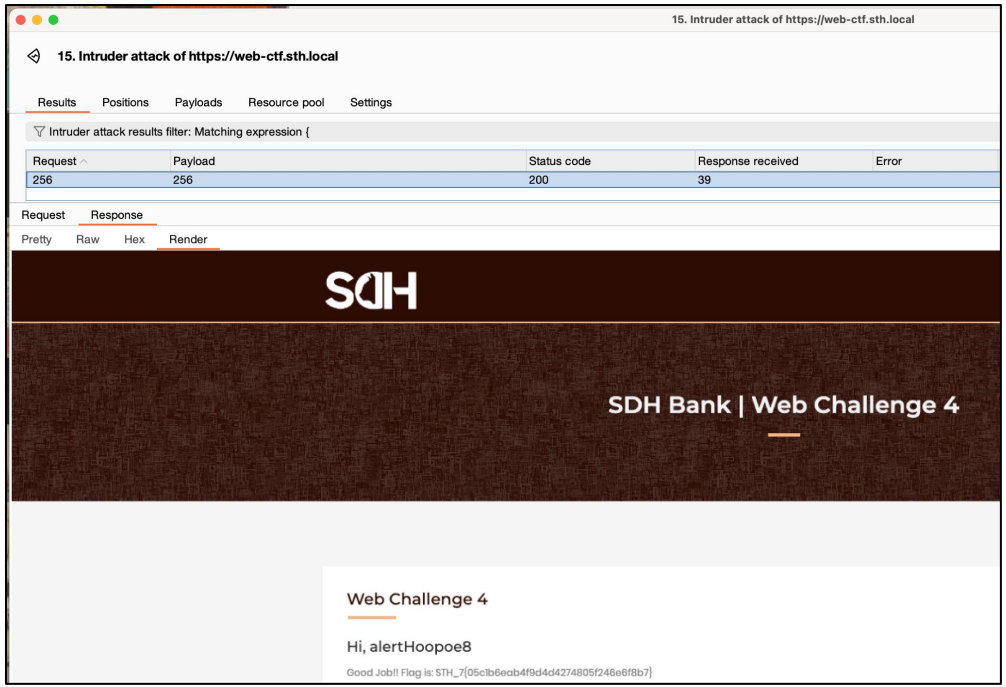
ตัวอย่างระบบส่งคำตอบ CTF และ Scoreboard

โจทย์, คะแนน, ทีมที่ทำได้, ตอบ flag



แสดงและจัดอันดับคะแนน

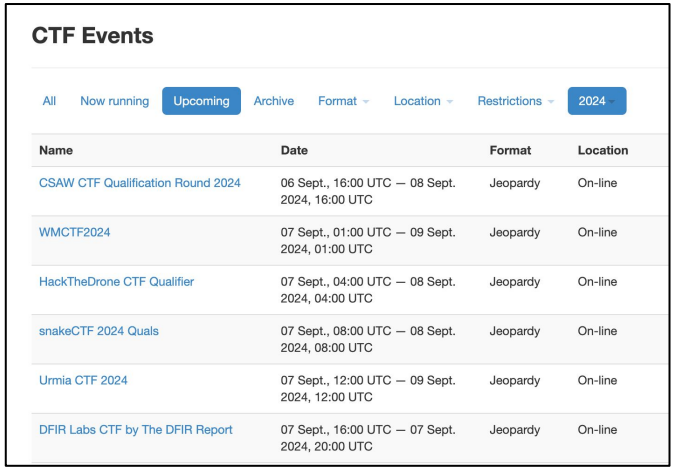
ตัวอย่างการแก้ไขโจทย์ CTF และได้ Flag



ช่องโหว่ IDOR

Key Takeaway (2/2)

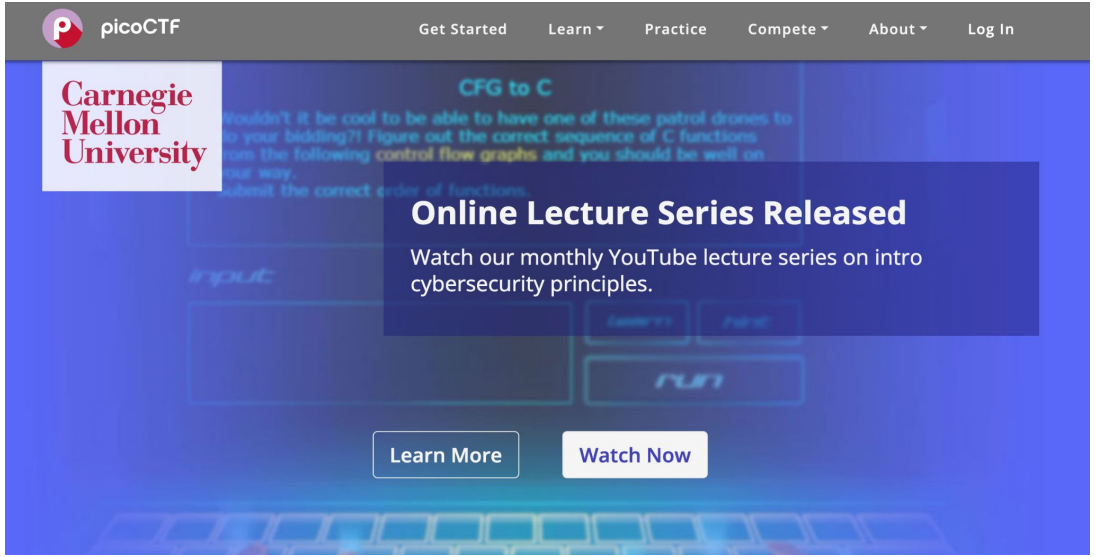
- Learning Platform เช่น TryHackMe หรือ HackTheBox
  ใช้เรียนรู้ ได้ไม่จำกัดเวลา การแก้ไขปัญหาโจทย์ต่าง ๆ
- CTF (Capture The Flag) เป็นงานแข่งขัน มีการกำหนดเวลาแข่งชัดเจน
  (มีเวลาแข่งจบ) และมักจัดเป็นประจำทุกปีหรือตามรอบ ของงานสัมมนา
- ทั้ง Learning Platform และ CTF ช่วยส่งเสริมการเรียนรู้ทางด้าน
  Cybersecurity ได้เป็นอย่างดี
- เริ่มตามหางาน CTF ที่กำลังจะเกิดขึ้น ได้ที่:
  https://ctftime.org/event/list/upcoming



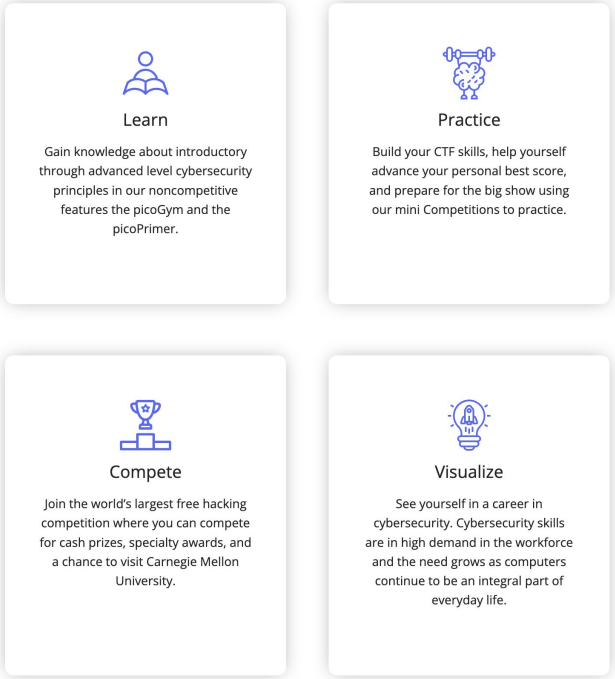
Agenda (Day 1)

เวลา	รายละเอียด
09.15 - 09.45	ความรู้เบื้องต้นเกี่ยวกับ CTF
09.45 - 10.30	Network Security
10.30 - 10.45	พักเบรก
10.45 - 12.00	Web Application Security
12.00 - 13.00	พักรับประทาน อาหารกลางวัน
13.00 - 14.30	Digital Forensics
14.30 - 14.45	พักเบรก
14.45 - 16.00	Pwnable & Reverse Engineering
16.00 - 18.00	เข้าห้องพัก
18.00 - 19.00	รับประทานอาหารเย็น
19.00 - 21.00	เสวนาแนะแนวเส้นทางอาชีพ

Credit for Challenges from PicoCTF



https://picoctf.org



Thank you !!